Kantor Management Consultants

ibf INTERNATIONAL CONSULTING

ICMPD 20YEARS

eptisa

European Commission

DIRECTORATE GENERAL FOR NEIGHBOURHOOD AND ENLARGEMENT NEGOTIATIONS – DG NEAR

Short term high quality studies to support activities under the Eastern Partnership

HiQSTEP PROJECT

HARMONISATION OF THE DIGITAL MARKETS IN THE EASTERN PARTNERSHIP

STUDY REPORT

First draft submitted:	20.4.2015
Final draft submitted:	8.6.2015
Final version submitted:	19.10.2015 (v1.0.4)

PREFACE

This cross-country report on the Harmonisation of the Digital Markets in the Eastern Partnership is part of the project 'Short term high quality studies to support activities under the Eastern Partnership – HiQSTEP, EuropeAid/132574/C/SER/Multi', carried out by an international consortium under the leadership of Kantor Management Consultants.

In this study report, a team of international and national experts examines the level of digital market infrastructures, regulation and services development in the six Eastern Partnership (EaP) countries. The study focuses on six priority areas in digital market and namely: Network and Information Security and Cyber-security; Electronic Identification and Trust Services; eCustoms; eCommerce for SMEs; Digital Skills, and Telecom Rules.

The present study has been implemented by a study team under the leadership of **Vladimir Abramytchev** (Study Team Leader, eCustoms, eCommerce), and composed of senior international experts **Yuri Misnikov** (Network and Information Security and Cyber-security, Electronic Identification and Trust services) and **Peter Lundy** (Digital skills, Telecom Rules) together with national experts: **Gohar Malumyan** (Armenia), **Vusal Abbasov** (Azerbaijan), **Anna Pobol** (Belarus), **Ana Nakashidze** (Georgia), **Olga Demian** (Moldova) and **Sofia Belenkova** (Ukraine)[1].

Overall supervision has been carried out by Przemysław Musiałkowski, Team Leader of the HiQSTEP Project. Methodological assistance was assured by Vassilis Kopanas (DG CONNECT), Simone Rave (DG NEAR), Isabelle Pellier (DG NEAR), and Valery Virkovski (HDM Working Group). The definition of the EU baseline has been conducted in consultation with Alessandra Falcinelli (DG CONNECT), Alessandra Sbordoni (DG CONNECT), Zahouani Saadaoui (DG TAXUD), Tamas Kenessey (DG CONNECT), Marietta Grammenou (DG CONNECT) and Vassilis Kopanas (DG CONNECT).

Sincere gratitude is expressed by the entire team to all the contacted stakeholders in the six countries who provided information during interviews and using responses to questionnaires. Sincere gratitude is also given to the participants of HDM Workshop and the members of the HDM Working Group for their highly valuable feedback and information, and to Dimitra Malandraki (Kantor) for efficient administrative and back-up support.

[1] For any request about the study, please contact Vassilis Kopanas (Vassilis.Kopanas@ec.europa.eu) and Vladimir Abramytchev (vladimir@archev.net)

Finally yet importantly, appreciation goes to all staff members of the European Commission and specialists in the Eastern Partnership countries who directly or indirectly helped to complete this study.

June 2015

CONTENTS

LIST OF EXHIBITS

LIST OF TABLES

EXECUTIVE SUMMARY

The purpose of the study is to assess the readiness of digital markets in the Eastern Partnership countries for harmonisation with the EU's Digital Single Market. The Geographical scope of this study covers the six EaP countries: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

The study evaluates the level of digital market infrastructures, regulation and services development focusing on six priority HDM areas: Network and Information Security and Cyber-security, Electronic Identification and Trust Services, eCustoms, eCommerce for SMEs, Digital Skills, and Telecom Rules.

The specific objectives of the study are the following:

a) To lay the foundation for the development of Digital Market Agendas for the Eastern Partnership countries;

b) To analyse the benefits that would result from an HDM between the Partner Countries and the EU, and

c) To identify follow-up actions in the form of a roadmap for the priority areas under the HDM and for each Partner Country.

The study analyses the Digital Markets using as a baseline the EU legal framework, best practices, standards and Information and Communication Technology (ICT) platforms. For each of the six HDM areas, the study identifies the EU baseline (that comprises relevant EU legislation, best practices, standards and ICT platforms), conducts stock taking in the six Partner Countries, analyses gaps in the state of play of the digital market, analyses benefits and readiness for harmonisation, and identifies follow-up actions needed in the short to medium term for the Region and each Partner Country.

The Eastern Partnership is based on a commitment to the principles of international law and fundamental values, including democracy, rule of law and respect for human rights and fundamental freedoms, as well as to a market economy, sustainable development and good governance. Digital technologies have significant impact on all areas of economic and political cooperation in the Eastern Partnership. The issues of multilateral cooperation on economic integration, rule of law and contacts between people could be facilitated through the single digital market.

Network, information and cyber security (NIS) refers to the security of the Internet and

the private networks and information systems underpinning the functioning of our societies and economies.

All Partner Countries demonstrate strong political will to address the constantly evolving NIS-related challenges, including the willingness to cooperate with the EU and internationally. Whereas there is a minimally sufficient legal certainty about Cyber Security – supported in some cases by the availability of strategic national plans and programmes – the Region substantially lags behind the EU. Only Georgia and Moldova have full-fledged national Cyber security strategies, although the other countries have plans to develop ones. On the other hand, the Region is technologically well advanced, using latest software of high international standards.

Overall, the NIS area in the Region is still regulated by fragmented and disparate (and sometimes outdated) legal and regulatory acts, especially by secondary regulations rather than consolidated laws. Internet openness and confidentiality of personal data and online privacy is protected by law in all Partner Countries. However, the legal base of such protection is not sufficiently streamlined and consists of different legal and regulatory frameworks that do not adequately address challenges posed to internet safety, as technology is advancing and societies are becoming more concerned about such challenges.

The Partner Countries share common problems and challenges that need to be addressed in a coordinated manner in order to harmonise with the EU. The Association Agreement countries have more harmonised legislation with the EU. The largest gaps are those caused by the absence of dedicated national cyber-security strategies; lack of services provided to National Regulatory Authority (NRA); inadequate technical, human and financial resources available for managing security threats; insufficient transparency and openness in reporting on security breaches; and existing vulnerabilities of private sector (critical) infrastructures. Most countries do not practise cyber-attack simulations on a regular basis. Action is required for ensuring well-functioning alert platforms and hotlines for both experts and the general public.

Priority steps and common projects include:

- Reforming current legal and regulatory frameworks by consolidating the regulatory environment to:

  (a) specify requirements needed for establishing minimal security levels in the field of critical information infrastructure, including in the private sector, and

  (b) guarantee internet safety while maintaining its openness.

- Formulating national Cyber Security Strategies and other country-specific and inter-country projects linked with national development priorities.
- Empowering national Computer Emergency Response Teams (CERTs) by building their capacities through cooperation with CERT-EU and the European Network and Information Security Agency (ENISA).
- Establishing effective cooperation mechanisms and channels of information exchange.
- Aligning HDM priorities with the Digital Single Market (DSM) pillars.

Electronic identification (eID) and electronic trust services (eTS) encompass electronic signatures, seals, time stamp, electronic delivery service and website authentication. These are key enablers for secure cross-border electronic transactions and are central building blocks of the Digital Single Market.

Partner Countries demonstrate rather close results in the field of eID/eTS. In general, eGovernment development (including eProcurement as well as eCommerce) has been the main driving force of building national certification infrastructure and related services. The best progress has been achieved in the field of creating the eID/eTS infrastructure and implementing eSignatures. Legal certainty about eID is largely sufficient and leadership is fairly strong. Achieving the EU baseline lies in the national interest of each country in the Region, given new commercial opportunities that may emerge as a result of making digital signature operational across borders. Some Partner Countries have already significantly aligned their national legislation and real-life practices with those of the EU (Georgia and Moldova). Moreover, Moldova and Azerbaijan have created mobile identification infrastructure and services.

However, European experience and best practices are not sufficiently known in the Region except the Estonian x-Road secure interoperability solution that is currently being applied in Georgia, Moldova, Azerbaijan and Ukraine. The access to European knowledge in eID/eTS is still rather restricted. At the moment, the Region’s digital markets are still closed markets. Yet, all Partner Countries express readiness to change legislation in order to enable cross-border electronic signatures and related certification services, although solutions for the EU Association Agreement Countries, Belarus and Armenia may differ. Also, all Partner Countries, especially the Association Agreement Partners, are advised to align with the provisions on electronic identification and trust services for electronic transactions in the EU

internal market (eIDAS regulation); in addition, an opportunity of joining the large-scale project STORK[2] on a pilot basis might be considered as well.

Legally and technically, each Partner Country has a sufficiently well-developed eID/eTS infrastructure. However, its actual usage is inadequate as yet. Digital signature as a main tool of electronic identification is not used widely and is not interoperable across borders. Interoperability of state and private sector information systems (technical, organisational and, legal) and inter-agency coordination are still weak areas, as is manifested by the overall lack of well-integrated and secure eGovernment architecture realised on the whole-of-government principle. There is a clear lack of e-services requiring secure electronic identification.

Until now, electronic signatures have served the business community better than citizens. Public procurement is steadily moving online (this has already been done in Armenia). However digital signatures are not fully integrated into eProcurement processes and platforms. This undermines security and also puts limits on the full automation of award and post-award stages where strong identification is needed.

Priority steps and common projects include:

- Reforming the legal basis as a first step to establishing an enabling regulatory environment (compatible with eIDAS Regulation) which would make digital signature interoperable across borders and facilitate access to services in other countries, both in the Region and the EU.
- Aligning HDM priorities with the Digital Single Market (DSM) pillars.
- Establishing a common link with the EU knowledge management mechanism to facilitate exchange of information and replicate good practices.
- Establishing fast-track initiatives to enable Partner Countries benefit quickly, for example, from such successful EU large-scale pilots as STORK 2.0.
- Clarifying cooperation modalities for cross-border eIDs

[2] Secure idenTity acrOss boRders linKed http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-5action_en.htm

This would enable a better understanding of the conditions to be met by both public service and trust service providers to guarantee the required security assurance levels for accessing services of other countries and granting access to local services.

eCustoms initiatives aim to replace paper format customs and trade procedures with electronic ones, thus creating a more efficient and modern customs environment.

The legal framework related to eCustoms in the Partner Countries is the most advanced towards harmonisation with the EU. The overall legal framework and several major regulatory provisions related to the eCustoms area (paperless environment for customs and trade, risk management framework, status of authorised economic operator) are in line with the EU baseline. The main processes of customs procedures have been automated. In contrast, few Partner Countries have established the national single window systems and the overall automation of the trade procedures is low.

For harmonisation of eCustoms, the main challenge is the creation of interoperability of electronic customs and single window systems (at legal, infrastructures and services levels) with the systems of EU and third countries that obstruct the creation of a paperless trade environment at the EaP level.

The biggest common gaps of the Partner Countries are in the implementation and use of information services such as a system for registration and identification of authorised economic operators. Several key information services have not yet been developed and implemented in the Region. Automated data exchange with the EU or even with other neighbouring countries is very limited.

At the level of infrastructures, little has been done to implement electronic interfaces for economic operators so as to enable them to conduct all customs-related business, if other countries are involved, with the customs authorities of the country where they are established. With the exception of Ukraine, there is no possibility for traders of the Region to submit electronic documents to the customs authorities of other countries.

The requested follow-up actions for the HDM are in two categories:

- Priority actions in infrastructure and services with the biggest common gaps for harmonisation: to set up an Economic Operators Registration and Identification system; to set up a centralised Anti-Counterfeiting and Anti-Piracy System for the Partner Countries and connect it with the EU central Anti-Counterfeiting and Anti-Piracy System (COPIS) system; to automate exchange of export/import/transit data

and data about Authorised Economic Operators with EU and to create national segments for the Registered Exporters System.

- Harmonisation of the legal frameworks within the Region in the following aspects: Single Window – paperless environment for customs and trade; regulatory basis for lodging summary declarations; harmonised legal basis for Anti-Fraud and Anti-Piracy requests.

The study has identified some suitable pilot projects for the Region:

- Electronic exchange of summary electronic declaration for pre-arrival and pre-departure information (export, import, transit), exchange of national data on Authorised Economic Operators, interconnection of national system for management of electronic trade certificates, uniform user management and the digital signatures framework.
- Setting up a common Anti-Fraud Information System (which is the easiest project to start).

eCommerce is trading in products or services using computer networks, such as the Internet.

The Region has achieved on average about a half of full compliance towards the harmonisation of practices with the EU in eCommerce for SMEs. The Partner Countries have defined their legal frameworks and deployed basic infrastructures and services, mainly for eCommerce operating inside their own country. The legal provisions and information services toward international integration are lacking.

The weakest aspect is electronic payments for eCommerce transactions where a number of factors obstruct the implementation of a seamless approach to cross border payments. The average levels for three other indicators - internet security and privacy, consumer rights and eLogistics - display a similar degree of achievements. Only basic aspects of the national legal frameworks have been introduced in relation to eCommerce. The required national components for the implementation of information systems of an eCommerce platform have been initiated.

The aspect of competition in eCommerce for SMEs in the Partner Countries is the most advanced from the point of view of harmonisation with the EU. Partner Countries are open for competition on the eCommerce market and have no generalised obstacles for market access by SMEs from other Eastern Partnership countries. The regulatory framework in

eCommerce is business friendly for international harmonisation and open to free movement of information society services.

The biggest common gaps of the Partner Countries are related to the legal provisions and frameworks assuring consumer rights (international cooperation mechanisms for consumer protection – which is an important gap per se, out-of-court dispute settlement mechanisms and transparency of commercial communications information to be provided by eCommerce traders). None of the Partner Countries has established an on-line dispute resolution system for customers of eCommerce transactions. There are no national schemes of online trustmarks for eCommerce retail websites in the Region. In most of the Partner Countries, the national legislation does not define specific liability regimes for three categories of essential services assuring the provision of eCommerce online services - transmission conduit operators, caching providers and hosting services providers.

Only Armenia and Belarus have introduced in their national legislations the provisions specifying terms and conditions related to the risk of loss of or damage[3] to the goods purchased through eCommerce and responsibilities of the parties involved in case of loss or damage of goods.. The same applies to the definition of the rights on delivery of goods.

The study has identified the following priority follow-up action for the Region:

- Enhance international cooperation mechanisms on consumer protection,
- Define a specific liability regime for intermediary service providers,
- Limit fees for the use of eCommerce means of payment,
- Define - in the legislation - the conditions for the risk of loss of or damage to goods
- Define rights on delivery of goods
- Harmonise the legal frameworks in the following aspects: definition of common minimum general information to be provided by eCommerce service providers in the Region, common transparency requirements for commercial communications, rules on the conditions for risk of loss or damage to goods, harmonisation of rights on delivery of goods

In eCommerce for SMEs, the main projects would be:

- Development of a pilot eCommerce platform that assists SMEs in their digital activities across the Eastern Partnership.

[3] Referred to as “conditions for the risk of loss or damage of goods” in the text that follows.

- Creation of a common online trustmark scheme for retail websites in the Region
- From the perspective of cross-border consumer rights protection, an important project is the setting up of an online dispute resolution system for customers of eCommerce.

Digital Skills are broadly defined as ICT-related skills for the labour force, including ICT professionals, digital learners and citizens)[4]. The role of ICT in raising productivity and living standards is critical. The largest obstacle to harnessing the power of ICT is the shortage of digital skills. By 2020, Europe might face a shortage of almost 825,000 ICT professionals. This is what is termed the "*digital skills gap"*.

The Region faces the same critical skills shortages, but unlike in the EU, the digital skills gap has not yet been systematically measured and monitored. Although some good progress has been made across the Region in bringing better ICT into education, there is still a lack of awareness at policy level and a lack of coordination of initiatives at regional, national and local levels.

The development of Digital Skills requires a co-ordinated policy approach, within the context of national policies for uptake of ICT for competitiveness, growth, employment, education, lifelong training and social inclusion. Digital Skills must be elevated to have an important place in long-term national policy. Harmonisation efforts should play a central role in developing these national policies and actions, within which a long-term Regional Digital Skills agenda is launched, to improve cooperation and mobilisation of all stakeholders and to adopt best strategies and practices in order to better face global competitive challenges.

Policy makers across the Region generally recognise the importance of ICT in economic and social development, but focus on Digital Skills is insufficient, especially in the context of creating growth and jobs. Moldova has already made good progress in creating a policy context for Digital Skills under its "Digital Moldova 2020" initiative. All countries of the Region are already implementing projects to bring ICT learning into schools and universities.

Working with companies in national and local coalitions, using the same model as the Europe's Grand Coalition for Digital Jobs, should focus particularly on the young workforce. This can be done by training individuals and seeking to reduce youth unemployment, helping

[4] See also http://eskills-monitor2013.eu/fileadmin/monitor2013/documents/MONITOR_Final_Report.pdfwww

business “start-ups” grow by giving them bigger markets to sell to from Day 1 and supporting labour force changes in companies which have not adapted to new digital, data-driven business models.

Digital Skills development is a long-term project. It is proposed the following initiatives should be adopted across the Region in the short term.

- Measuring the skills gap. The earliest need is the systematic measurement and monitoring of the digital skills gap. Without this measurement, awareness of the need to match demand and supply is missing.
- Co-ordination of Digital Skills initiatives. Policy development and implementation of initiatives would be greatly leveraged by welcoming the Region into Europe’s Grand Coalition for Digital Jobs. Initiatives could then follow to form national and local coalitions that would coordinate active participation, awareness raising and resources facilitation.

Telecom Rules consist of the policy, legal, regulatory and implementation frameworks which are necessary for effective electronic communications markets to operate. Harmonisation of Telecoms Rules has benefits to all market participants. There can be positive impacts across digital markets by improving broadband investment and access for market participants, particularly through greater connectivity. Benefits in broadband penetration occur at the macro-economic level[5,6] as well as providing the access platform for digital single market growth, for example through cloud computing, enhanced cross-border payments and increased physical delivery services[7]. Harmonisation of telecoms rules has already progressed well within the EU and will continue in 2016 through the Digital Single Market strategy[8].

[5] Based on Katz 2010; Analysys Mason 2010; McKinsey 2010; Qiang & Rossotto 2009; and Czernich et al. 2009. See also ITU publication “The Impact of Broadband on the Economy: Research to Date and Policy Issues April 2012” https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf

[6] From EC 2010 report “The socio-economic impact of bandwidth” http://ec.europa.eu/digital-agenda/en/news/study-socio-economic-impact-bandwidth-smart-20100033

[7] From European Parliament report: http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510981/EPRS_STU%282014%29510981_REV1_EN.pdf

[8] http://ec.europa.eu/digital-agenda/en/digital-single-market

There are significant gaps in telecoms rules both within the Region and between the six Partner Countries and the EU. There is no unified policy in the Region that encapsulates the EU's "Digital Agenda" target for universal access to high speed (>30Mbps) broadband by 2020. The average broadband penetration in the Region currently lags well behind the EU for both fixed and mobile broadband services. Fixed broadband penetration per capita in the Region stands at 13% compared with 30% in the EU. For mobile broadband, the gap is even wider at 21% for the Region compared with 61% for the EU. The gap is still wider outside urban areas, with rural broadband penetration typically only one tenth of urban penetration across the Region. The closing of this "broadband connectivity gap" is of vital importance, not just in the potential to boost GDP growth (estimated in the report at between 2.9Bn and 4.3Bn in the Region for fixed broadband alone) but also by providing the essential connectivity platform for other areas of digital market progress including the priority topics studied in this report.

The legal and regulatory frameworks in the six Partner Countries are all different. Gaps are particularly evident in the Region's Telecoms Rules that impact broadband connectivity, including the regulatory enablers to market entry, the necessary competitive market safeguards for private investors and in the state-aid rules applied to public investments.

For the Region, the most important initiatives to harmonise digital markets should be:

- Harmonisation of policy for broadband access. There is a pressing need for the creation of a common policy across the Region to close the "broadband connectivity gap". This should mirror the ambitious targets for universal high-speed broadband access across the EU. Azerbaijan and Belarus have already committed significant state funding to broadband infrastructure. In harmonising policy with the EU, better competitive conditions in these countries will lead to more efficient markets with greater consumer choice and improved private sector confidence. In the other four countries, existing broadband service provision has been left almost entirely to the private sector. Although this has already given good broadband coverage in urban areas, rural areas are left relatively unserved due to less attractive investment returns. The alignment of policy with the EU should focus on more effective enablers to all investments, especially into rural areas. Alignment of Telecoms Rules policy, legal and regulatory frameworks would give a significant boost to investor confidence in the Region, because investors could expect the same conditions that are already in place in the EU.

- Better conditions for investment in broadband infrastructure. Closing the broadband connectivity gap will require significant further investments, particularly in the outreach of infrastructure to rural areas. The legal and regulatory frameworks across the Region need to be adjusted to ensure that the investment-enabling provisions for high-speed broadband infrastructure already contained in the EU are adopted by the six Partner Countries. This process has already begun in Georgia, Moldova and Ukraine. The alignment embraces not only key enablers to fixed infrastructure investment, but also requires harmonisation of spectrum management procedures, particularly with respect to the “digital dividend” spectrum which is especially useful for deployment in rural areas.

The study analyses the Digital Markets in the six Partner Countries of the Region, using as a baseline the EU legal framework, best practices, standards and ICT platforms in each of the six priority areas. A number of benchmarks are established to define the EU baseline in each priority area. For each priority area, several benchmarks are grouped into four to six thematic indicators.

Assessment consists in choosing a score that is most appropriate to the status of a country for each benchmark. Scoring is done by scoring on a 0% to 100% scale of compliance with the EU baseline. 100% score means that the country is in line with the EU baseline benchmark. After collecting scores for benchmarks, scores of indicators are calculated as an average of the sum of benchmarks that are included into these indicators. The overall score of a country is an average of all indicators from a priority area.

CONTEXT

In November 2013, the Heads of State and representatives of the six Eastern Partnership countries and the EU's Member States met in Vilnius for the Eastern Partnership (EaP) Summit. In the **Vilnius Summit declaration**, they defined the jointly agreed political priorities for the future of the Eastern Partnership. Among others, they called for "*promotion of information society policies and continued capacity building in the EaP, related to the creation of interoperable cross-border services*". The Vilnius joint declaration has been preceded by a **non-paper** on 'Information and Communication technologies (ICT) development with EaP Countries', presented in July 2013 to the Council's Working Party on Eastern Europe and Central Asia (COEST) by Poland, Estonia, Finland, Lithuania, Sweden, Georgia and Moldova. With their non-paper these countries stressed the need for a

"*comprehensive approach in exploring the role of ICT for creating a common room for interoperable pan-European services*".

In May 2014, during the 11th EaP Platform 2 plenary meeting, Belarus presented a concept note for **a new draft initiative,** in line with the non-paper and the Vilnius declaration. The concept note focused on promoting Harmonisation of the Digital Markets (HDM) of the Eastern Partnership countries and with the EU. This draft initiative mirrors well ongoing EU actions for developing a Digital Single Market, as well as political priorities of the incoming 'Juncker' Commission and the Latvian presidency of the Council. The concept, received several positive reactions from both Partner Countries and EU MS representatives.

In order to reflect on the best way of transforming this political priority into a concrete Eastern Partnership initiative, the **first HDM workshop** took place in Brussels on 29 July 2014. The workshop gathered 60 delegates from nine EU Member States, all six Partner Countries and officials from EU Institutions. In this workshop, participants discussed the objectives, the scope and the level of ambition of the future initiative, feasibility, impact, implementation modalities and sources for its financing. The workshop included presentations by EU Member States of their efforts towards a Digital Single Market, as well as presentations of similar efforts by the Partner Countries. The discussion on potential topics for harmonisation led to the identification of five priority topics that could lead to pilot HDM projects in the EaP. A feasibility and cost/benefit analysis study on HDM was deemed necessary. A roadmap of activities and milestones until mid-2015 was agreed.

The **second HDM Workshop** took place in Brussels, on 21-22 October 2014 aiming to:

- Consolidate and expand EU Member States support to the draft initiative
- Confirm and validate the choices for priority HDM topics made during the first workshop
- Elaborate on priority topics for a roadmap on HDM in the priority areas identified.
- Discuss and agree on the terms of reference for the HDM study on the priority areas
- Discuss further the governance model of the proposed HDM initiative
- Update the roadmap of activities and milestones until mid-2015

HDM study was addressed at two levels during the 2nd workshop. Firstly, on Tuesday 21 Oct 2014, in a dedicated one hour session (14:30-15:30) entitled 'HDM Study', the participants received a short general presentation of the EaP Study Facility and the kind of services that could be offered for HDM. Then, discussion helped identify more concretely various

elements of the study such as the aim, scope, geo coverage, expected results, timing, sources of information etc.

Following that, on Wednesday 22 October, **three parallel sessions** allowed in-depth discussion on three groups of HDM topics:

- HDM and Digital Service Infrastructure:
  - Network and Information Security and Cyber-security and
  - Electronic identification and Trust Services
- HDM and Digital Services:
  - eCustoms,
  - eCommerce (for SMEs),
- HDM and eSkills

Each of these parallel sessions issued more specific recommendations for the HDM study, complementing the more general conclusions from the previous day.

1 ASSESSMENT METHODOLOGY

1.1 HDM priority areas

The study evaluates the level of digital market infrastructures, regulation and services development focusing on six priority HDM areas:

Network, information and cyber security (NIS) refers to the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. The EU approaches NIS from both a policy and a single market perspective. Cyber Security is an even wider and multi-dimensional issue where other perspectives come to play: home affairs, fight against cybercrime, defence, democracy, diplomacy and foreign relations. The area is governed by the European Cyber Security Strategy - an open, safe and secure cyberspace. The Strategy also includes EU policy in relation to international cyberspace. It is accompanied by a legislative proposal to strengthen the security of the EU's digital networks and information systems and thus strengthen confidence in online public services and commercial transactions, encouraging economic growth with the expansion of the digital economy.

Electronic identification (eID) and electronic trust services (eTS) encompass electronic signatures, seals, time stamp, electronic delivery service and website authentication. These are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. The area is governed by the eIDAS Regulation (No 910/2014 of 23 July 2014). It sets a comprehensive general legal and technical framework for electronic transactions by regulating the mutual recognition of notified electronic identification schemes and means, by providing electronic trust services, as well as by ensuring the non-discrimination of electronic documents vis-à-vis their paper equivalent. Such measures should ensure legal validity of electronic transactions and seamless electronic interactions between businesses, citizens and public authorities. National electronic identification schemes can be used across borders to access public services in other EU countries.

The **eCustoms** initiative aims to replace paper format customs procedures with electronic ones, thus creating a more efficient and modern customs environment. For the purposes of this study, eCustoms also comprises aspects of automation of cross border trade and interaction between different government and non-government authorities involved in the procedures of issuing permits for external trade.

eCommerce for SMEs is trading in products or services provided by SMEs using computer networks, such as the Internet. This includes the sharing of standardised unstructured or structured business information by any electronic means through the World Wide Web for at least one part of the transaction's life cycle, although other technologies such as e-mail may also be used.

Digital Skills are broadly defined as ICT-related skills for the labour force, including ICT professionals, digital learners and citizens. The largest obstacle to harnessing the power of ICT is the shortage of digital skills.

Telecom Rules consist of the policy, legal, regulatory and implementation frameworks that are necessary for effective electronic communications markets to operate. Harmonisation of Telecoms Rules has benefits for all market participants – consumers, small and medium businesses, large corporations, investors in telecommunications infrastructure, network operators and service providers. There can be positive impacts across the digital markets by improving broadband investment and access for market participants, particularly through greater connectivity.

1.2 Assessment approach

The HDM progress assessment methodology aims to assess the readiness of digital markets in the Partner Countries for harmonisation with the EU's Digital Single Market. The expected key benefits of harmonisation have been appraised in order to define broad indicators plus more detailed benchmarks for the assessment of the state of play and progress towards harmonisation in each country.

The EU baseline comprises the descriptions of the state of play in the relevant EU legislation, best practices, standards, ICT platforms (as appropriate for each HDM area) for each indicator and benchmark.

Stock-taking in the six Partner Countries and comparison with the EU baseline allows identification of the gaps in the readiness of digital markets in the Partner Countries for harmonisation with EU's Digital Single Market.

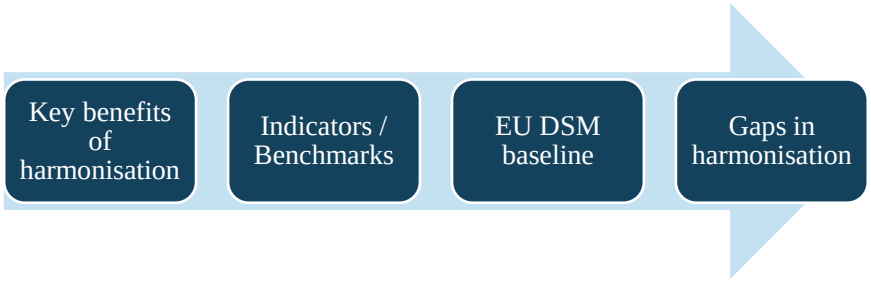

Exhibit 1 - Framework for assessing progress in the HDM process

The analysis of the gaps leads to the proposal of follow-up actions in the form of a roadmap, for each of the priority areas under the HDM and for each Partner Country.

1.3 Indicators, benchmarks and scoring

For each of the six priority digital market areas, several unique assessment indicators are defined. The indicators characterise the most important aspects - from economic, technical and political perspectives - of the harmonisation of the digital market in a particular priority area between the EU Member States and the Partner Countries. Each indicator contains two groups of benchmarks - enablers and results. A benchmark is a smallest criterion used to assess the readiness of the digital market in a Partner Country on its way towards harmonisation with EU's Digital Single Market.

Benchmarks for the enablers indicate what a Partner Country does in order to achieve the harmonisation of digital markets. Benchmarks for results reflect what a country has achieved.

Assessment of the status of the digital markets of a Partner Country against these benchmarks for enablers and results defines the overall state of play of the HDM priority areas in this country.

Benchmarks are defined and described for each of the six priority HDM areas, and then grouped into indicators.

Several indicators for a group of Enablers:

1. Indicator 1 (Leadership)
    a. Benchmark 1.1
    b. Benchmark 1.2
    c. …other benchmarks
2. Indicators 2(Policy)
    a. Benchmark 2.1
    b. Benchmark 2.2
    c. …etc.
3. Indicators 3 (Strategy)
4. Indicators 4 (Resources)
5. Indicator 5 (Implementation)

The following indicators describe Results:

6. Indicator 6 (Legal framework)
    a. Benchmark 6.1
    b. Benchmark 6.2
7. Indicator 7 (Infrastructure)
8. Indicator 8 (Services)

The study analyses the Digital Markets in the six countries of the Region, using as a baseline the EU legal framework, best practices, standards and ICT platforms. The benchmarks are used to assess the gaps in the state of play in the Partner Countries in comparison to the EU baseline.

Stock taking in the partner counties was conducted using assessment questionnaires prepared for each priority area. In the assessment questionnaires, a benchmark is presented

in the form of a title and a statement. Assessment consists in choosing a score that is most appropriate to the status of a country on a particular benchmark. The statement corresponds to the EU baseline level (objective or expected level).

Scoring	Strongly disagree 0%	Disagree 25%	Uncertain 50%	Agree 75%	Strongly agree 100%
Benchmark title	Statement (EU baseline or EU best practice)				
Benchmark notes	Benchmark description				
Evidence description	Filled in by national experts during/after conducting interview with national stakeholders. Also provides reference to documentation or records that justify the finding				

Exhibit 2 - Assessment questionnaire

The full questionnaires for the six priority topics of the study are presented in the Annex.

Scoring is done by choosing on 0% to 100% scale of compliance with the EU baseline statement from “Strongly disagree” to “Strongly agree” for each benchmark. A “strongly agree” response means that the country is in line with the EU baseline benchmark and so scores 100% for the benchmark. A “strongly disagree” response means that the country has no alignment with the EU baseline benchmark and so scores 0%.

Benchmark notes provide more detailed explanation about what each benchmark means. An evidence description field is provided for writing observations and answers during interviews.

Scores of indicators are calculated as an average of the sum of benchmarks that are included into these indicators. Scores are presented in graphical charts for indicators and benchmarks.

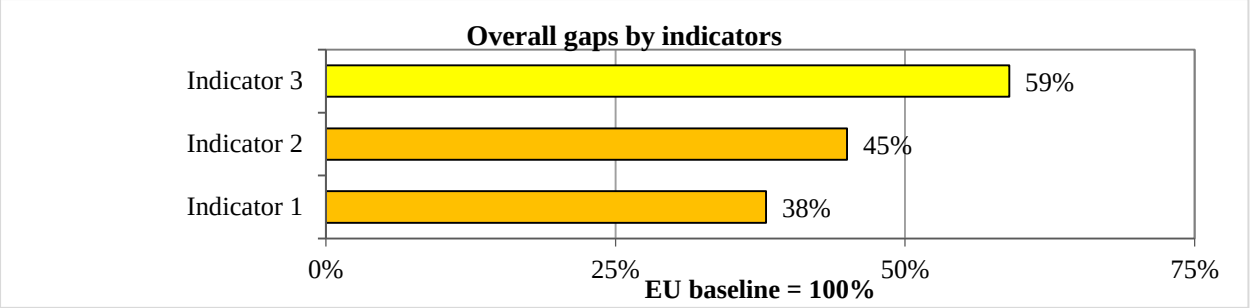

Exhibit 3 – Example of indicators

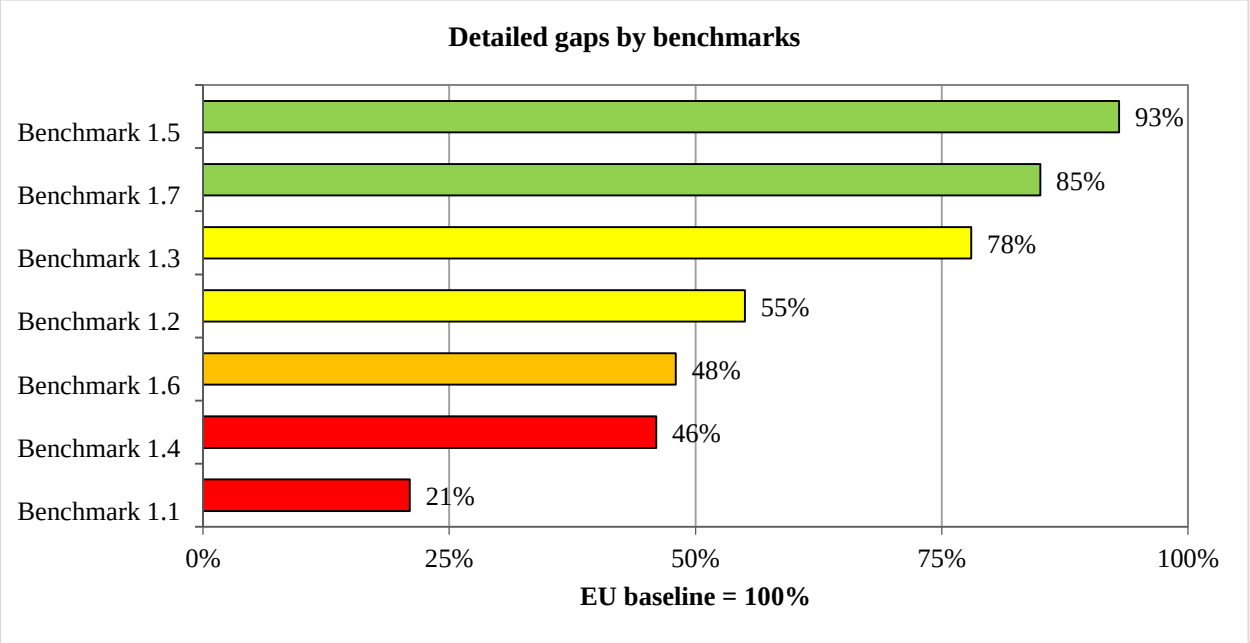

Exhibit 4 - Example of benchmarks

The overall score of a country is an average of all indicators from a priority area.

1.4 Framework for assessing progress in the HDM process

The gap analysis of the state of play of the digital market in each Partner Country with respect to the EU baseline is based on evaluation of scores received after assessment of each benchmark in comparison to the EU baseline level. Based on scores and evidence description, a detailed gap analysis per indicator and/or per benchmark is provided.

The comparison of the gaps of individual countries with the EU baseline identifies follow-up actions in the form of a roadmap, for each priority area under the HDM and for each Partner Country.

To address common gaps in most of the Partner Countries, recommendations are made with respect to the priority projects that can be initiated by the Region.

Exhibit 5.3 - Identification of follow-up actions and the roadmap

The assessment of the state of play and gap analysis can be repeated in the future in order to track the progress in the HDM process achieved by a Partner Country during over a period of time.

A supplementary way of evaluating the progress in the HDM process is comparison of the Region using the scoring tool provided by the Digital Economy and Society Index (DESI)[9]. This Index is a composite mark that summarises relevant indicators on Europe's digital performance and tracks the evolution of EU Member States in digital competitiveness.

2 RESULTS

2.0 Overview of the Region

2.0.1 State of play and gap analysis for the Region

Network, information and cyber security

Five Partner Countries, except Belarus, have signed and ratified the Council of Europe Cybercrime Convention. While the Region demonstrates strong political will to address the issue of network, information and cyber security, including willingness to cooperate internationally, it substantially lags behind the level of the European baseline.

The largest gaps are caused by the following: the absence of dedicated national cyber-security strategies; lack of services provided to National Regulatory Authority (NRA); inadequate technical, human and financial resources available for managing security threats; insufficient transparency and openness in reporting on security breaches; existing

[9] European Commission / Digital Agenda for Europe - http://ec.europa.eu/digital-agenda/en/digital-economy-and-society-index-desi

vulnerabilities of the private sector (critical) infrastructures. Most countries do not practise cyber attack simulations on a regular basis, run alert platforms and hotlines for both experts and the general public.

While, as mentioned above, the Region demonstrates strong political will to address the issue of network, information and cyber security, and there is a relatively sufficient legal certainty about Cyber Security supported by strategic national plans and programmes), only Georgia has a full-fledged national Cyber security strategy, while Moldova has a dedicated component under Digital Moldova 2020. Ukraine and Belarus have plans to formulate new stand-alone Cyber Security Strategies. In other Partner Countries, the area is insufficiently regulated by fragmented and disparate (and often outdated) legal and regulatory acts. Internet openness and confidentiality of personal data and privacy is formally protected by law, often by a number of different older laws that do not adequately address the new emerging challenges to internet safety, as technology is constantly advancing. As a result, countries are struggling to balance internet openness and freedoms with safety and security. The European Cyber Security Strategy: An Open, Safe and Secure cyberspace represents an important model for legal reform. Most of the Partner Countries are quite strong on the technical side using latest software solutions (e.g. some countries such as Ukraine and Belarus produce their own solutions on which are comparable with high international standards). The EU Association Agreement countries (Georgia, Moldova, and Ukraine) are pro-active in learning from EU experience, especially in the field of legal frameworks, capacity building to replicate good practices, for instance, via cooperation with CERT-EU. The training courses offered by ENISA represent a particularly valuable asset, although not yet utilised adequately.

There are more commonalities than differences among the Partner Countries. They share common problems and challenges that need to be addressed in order to create a level playing field with the EU to make stronger progress in NIS. The main difference is the degree of harmonisation of legislation with the EU – the Association Agreement countries (Georgia, Moldova, and Ukraine) are more advanced compared with Armenia, Azerbaijan and Belarus. Georgia has the most comprehensive legal and institutional system governing the field – it is a clear leader among the Partner Countries as its approach is the most closely aligned with the EU. Moldova and Ukraine are pro-active in aligning their legislations and practices with Europe. Although Belarus has not joined the Convention on Cybercrime, its legislative and regulatory framework on NIS is complex and diverse minimally responding to many different needs and situations complemented by a clear division of responsibilities

between government agencies. The situation in Armenia that does not have yet its national or government CERT is particularly worrying

Electronic identification and trust services

The best progress has been achieved in the field of creating the eID/eTS infrastructure and implementing eSignature. Legal certainty about eID is sufficient and leadership is relatively strong. However, digital signature as a main tool of electronic identification is not used widely and is not interoperable across borders. E-Government interoperability in general and e-services for citizens in particular are the weakest among other indicators.

The Partner Countries demonstrate rather close results in the field of Electronic identification and trust services, with most of the countries being consistently within the range. Achieving the EU baseline is in the national interest of all the Partner Countries given the new trade opportunities that may emerge as a result of making digital signature operational across borders. All countries express readiness to change legislation to eliminate this barrier, although solutions for the EU Association Agreement countries and the members of the Eurasian economic Union may differ. The availability of e-services requiring electronic identification is not sufficient at the moment. Until now, electronic signature has served better business community rather than the citizens. In general, eProcurement has been among the key drivers of building relevant infrastructure and services closely linked with eCommerce. In some countries all public procurement is implemented online (other countries plan to do it in the near future). At the moment, the Partner Countries' digital markets are still closed markets. Yet, the first signs of their opening are coming through. EU countries experiences and best practices are barely known in the Region (with the exception of Estonia's x-Road interoperability solutions which are applied in Georgia, Moldova, Azerbaijan and Ukraine). The access to the European knowledge in eID and eTS is still rather restricted. There must be much better knowledge sharing and solution adaptation mechanisms created in the region so as to expose the Partner Countries to the wealth of EU expertise.

Electronic identification and trust services are at the heart of building national digital markets and the Partner Countries' leadership is aware of this imperative. Similar performance by the Partner Countries is indicative of the commonality of not only the achieved levels, but also of the challenges they are facing in this area. Consequently, the benefits and opportunities are similar as well. Differences are not significant – all Partner Countries are weak in providing e-services to citizens and creating common e-government interoperable architecture. Armenia stands out in terms of being on par with the EU in eProcurement

(measured in both sophistication and availability terms). However, as a rule, the use of digital signature is not integrated into eProcurement platforms which undermines their security and also puts limits to the full automation of award and post-award stages where strong identification is needed. Overall, Moldova has been the best performer over the past several years. It has demonstrated impressive progress in aligning its legislation and actual practices with those of the EU. The government common technology platform M-Cloud builds on the open architecture and European principles of e-government interoperability is already at the level of the EU baseline in this regard. Moldova and Azerbaijan offer mobile identification services, while Ukraine needs to advance across the board. The newly established Agency for e-Government has started reviewing the outdated legal and regulatory framework in line with European standards.

eCustoms

The legal framework in relation to eCustoms in the Partner Countries is the most advanced towards the harmonisation with the EU Member States. The overall legal framework and several major regulatory provisions related to eCustoms a (paperless environment for customs and trade, risk management framework, status of authorised economic operator) are in line with the EU baseline.

The weakest aspect is the information services. Several key information services have not yet been developed and implemented in the Partner Countries. Information exchange with the EU or even with other neighbouring countries is very limited, with the exception of Belarus and Armenia where the automated information exchange is well organised.

The biggest common gaps of the Partner Countries are in the implementation and use of information services such as a system for registration and identification of authorised economic operators. There is a gap in defining the interoperability of electronic customs systems (at legal, infrastructures and services levels) with the customs systems of the EU and third countries which obstruct the creation of a paperless environment at the EaP level.

None of the Partner Countries has set up an anti-counterfeiting and anti-piracy system that allows right holders to submit online claims and ask the intervention of Customs in order to take measures against goods infringing certain Intellectual Property Rights (IPR)rights.

The biggest differences between the Partner Countries are observed in the following aspects: uniform user management and digital signatures (most countries use electronic signature for customs declarations, while Armenia, Azerbaijan and Moldova use it for interagency exchanges and submission of electronic documents to other government

agencies), the national single window systems for the paperless trade have been developed and operational in three Partner Countries (Armenia, Azerbaijan, Georgia) while the other three have just started by adjusting their legal frameworks, and the usage of the status of Authorised Economic Operator is fully implemented only in Azerbaijan, Moldova, and Belarus.

Belarus and Armenia have significantly more developed regulatory frameworks, infrastructure and services for cross border aspects of eCustoms harmonisation as compared to other Partner Countries.

Only the customs system of Ukraine is connected to the Single Point for Entry or Exit of Data portal, the secured network infrastructure that is provided by the European Commission to facilitate the exchange of information between the National Administrations of the Customs and Taxation area. This kind of system allows secure data exchange between the EU and other countries, which are not candidates for EU membership. Ukraine exchanges data on transit within the New Computerised Transit System (NCTS).

eCommerce for SMEs

The legal framework of the most of the Partner Countries applies the principle excluding prior authorisation to pursue the activity of eCommerce service provider. The regulatory framework in eCommerce of the Partner Countries is business friendly for international harmonisation and open to free movement of information society services. Another aspect in the state of play of the Partner Countries which complies well with the EU baseline is that eCommerce service providers shall render easily, directly and permanently accessible to the recipients of the service and competent authorities minimum general information that may be vital for customers claiming their rights. The Partner Countries do not restrict the freedom to provide information society and eCommerce services by service providers from another EaP country.

The biggest common gaps of the Partner Countries are related to the legal provisions and frameworks assuring consumer rights (international cooperation mechanisms for consumer protection, out of court dispute settlement mechanisms, transparency of commercial communications information to be provided by eCommerce traders). None of the Partner Countries has established an on-line dispute resolution system for customers of eCommerce transactions.

The Region has achieved in average about half of full compliance towards the harmonisation of practices with the EU Member States in eCommerce. The Partner Countries have defined

the legal frameworks, and deployed basic infrastructures and services mainly for eCommerce operating inside the countries. Legal provisions and information services towards international integration are missing. Harmonisation of the legal frameworks between the EaP is the indispensable stage for the successful implementation of cross border eCommmerce services.

For building trust of customers in eCommerce retail websites, the EU Member States favour the establishment of online trustmark schemes at the national and now at the EU level. In contrast, the Partner Countries rely more on measures to create good reputation of online traders through promotion and communication.

Consumer rights in the EU Member States are more strongly protected through defining the minimum pre-contractual information required for distance contracts and setting up out-of-court dispute settlement mechanisms. Partner Countries put emphasis on defining more strictly the minimum of general information to be provided by eCommerce services providers and assuring different mechanisms to check this information (restriction to selling online without having a physical shop, online registers to confirm the legal identity of eCommerce traders and products certification). Also, several Partner Countries, such as Moldova and Belarus, invest in the development of robust ePayment and eLogistics solutions rather than in the improvement of the legal protection measures preferred by the EU Member States (e.g. fines for sending unsolicited commercial communications, rules on the conditions for the risk of loss of or damage to the goods).

Digital Skills

For Digital Skills, the main finding is that there is no systematic measurement of the digital skills gap across the Region. This measurement is necessary to increase awareness and to monitor the progress of digital skills development. Some initiatives have already started, particularly in the area of ICT deployment for better education. The Region would particularly benefit from harmonising with the Grand Coalition for Digital Jobs, Europe's largest collaborative effort to address the digital skills shortage. By establishing national and local coalitions across the Region, awareness would be raised and better coordination with the EU would accelerate innovative learning and teaching, increase the number of ICT specialists, foster digital entrepreneurship, provide certification of digital skills and improved digital literacy.

Telecom Rules

For Telecom Rules, the main finding is that there are significant gaps in access and take up of broadband services between the Region and the EU, particularly in rural areas. There is no consistent policy for universal access to high speed broadband across the Region. By harmonising with a “Digital Agenda” policy for universal access to high-speed broadband (>30 Mbps), the Region could benefit from an accelerated removal of the large digital divide between the urban and rural areas. There are currently widely different approaches to infrastructure investment across the region. In countries where this investment is largely state-funded, there remain significant barriers to alternative investment and the roll-out of competitive broadband services. In other countries where investments are left entirely to the competitive market, there is insufficient high-speed broadband infrastructure in rural areas. By harmonising the policy and regulatory frameworks for telecom rules with the EU, these significant gaps could be closed faster, enabling much greater access and take-up of broadband services. Faster investment in infrastructure across the Region, giving better access to high-speed broadband, is an essential pre-requisite for the overall harmonisation of digital markets.

For Telecom Rules, the largest gap is in the lack of policies and regulatory enablers for investment in infrastructure for universal access to high-speed broadband access (both in terms of private investment and effective state aid) in harmony with the EU “Digital Agenda”. The investment gap is particularly large in rural areas, prolonging a significant digital divide. This is the single most pressing barrier to the harmonisation of digital markets.

For the Partner Countries who have signed an Association Agreements or DCFTA with the EU, the mapping of achievements, gaps and recommended actions for the related topics of the AAs or DCFTA are presented in the Annex

2.0.2 Common actions for the Region

Network, information and cyber security

Helping to reform the legal basis is a first step to establish an enabling regulatory environment that would include the minimal level of requirements in relation to NIS, especially in the field of critical information infrastructure.

The Region needs help in establishing an effective multilateral cooperation mechanisms and channels of information exchange in the field of cybercrime (e.g. knowledge sharing facility).

There is a need to develop a dedicated Cyber Security Strategy modelled on the European Cyber Security Strategy as a good European practice. More help can be provided to empower national CERTs by building their capacities through cooperation with CERT-EU and ENISA; establishing alert-platforms and hotlines for the public's feedback; ensuring greater transparency in reporting on NIS incidents/ breaches when the disclosure of such information is in the public interest; guaranteeing confidentiality of personal data and privacy by passing a dedicated law on the protection on personal data.

Electronic identification and trust services

Making digital signature and related trust services operational across borders, would require that the national legislation is brought in line with the eIDAS law. The Association Countries are already applying the EU approaches in this field, whereas Armenia and Belarus may need different cooperation mechanisms given that they have already passed two legal acts regulating the interoperability of e-signatures. eProcurement is seen as an area where, on the one hand, there are clear opportunities for mutual economic benefits through cross-border trade and even participation in public procurement. On the other hand, this is one of the most problematic areas where electronic identification and trust technologies are not used, which undermines the security of international transactions.

eCustoms

The easiest and also the most rewarding areas for harmonisation are those where the needs and interests of EaP countries are overlapping. The study has identified several areas where the Partner Countries can initiate priority actions.

Common projects between the EaP countries are: electronic exchange of summary electronic declaration for pre-arrival and pre-departure information (export, import, transit); exchange of national data on Authorised Economic Operators; interconnection of national system for management of electronic trade certificates; uniform user management and the EaP digital signatures framework. The easiest action to implement would besetting-up a common EaP Anti-Fraud Information System.

eCommerce for SMEs

The priority areas for harmonisation are those who bring bigger economical and political benefits in shorter period of time with less invested resources. These are the areas which help in the creation of more accessible markets and facilitate a rapid boost in trade for SMEs. With proper financing, the development of information services is easier for the Partner Countries compared to the long cycle of harmonisation of the legal and regulatory

frameworks. Pilot projects in information services development would show immediate benefit for SMEs and customers that use these services.

The Partner Countries would get significant benefits from establishing a new eCommerce trustmark scheme for the Region. Another option is to join the work in progress on EU-wide trustmark schemes, which aims to reassure consumers on the reliability of accredited traders. These trustmarks will facilitate the promotion of EaP-wide eCommerce platforms for SMEs. Such certified sites help consumers to make informed decisions when using online retail services. The Partner Countries can start by jointly developing specifications with regard to the implementation mechanisms, form, the presentation, composition, size and design of the trust mark for qualified trust services.

Digital Skills

For Digital Skills, the earliest need is the systematic measurement and monitoring of the skills gap. Without this measurement, awareness of the need to match demand and supply is missing and the beneficial coordination of initiatives and sharing of best practices with the EU is not in place.

In the area of Digital Skills, initiatives could be commenced immediately to measure and monitor the skills gaps, to raise awareness and to form national and local coalitions in coordination with Europe's Grand Coalition for Digital Jobs.

Telecom Rules

For Telecoms Rules, the policy and regulatory framework for the promotion of investment in high-speed broadband infrastructure using the EU baseline is already being initiated in Georgia and could be commenced elsewhere.

2.0.3 Pilot projects for the Region

Proposed pilot projects are mostly target individual Partner Countries and not necessarily have a regional scope involving all six countries. They map concrete "pilot" areas for cooperation that could be easily implemented, replicated and produce immediate benefit. Before launching big initiatives of large geographical scale, the study first identifies small scale activities conducted in order to evaluate feasibility, time, cost, adverse events, and effect size (sustainability) in an attempt to predict an appropriate sample size and improve upon the design prior to performance of a full-scale implementation. The identified concrete projects do not necessitate legislative or regulatory changes and should preferably focus on

enterprises and municipalities, where concepts can be tested locally with the aim of showcasing the benefits of the harmonisation of digital markets in the priority areas.

Network, information and cyber security

The proposed three projects aim at raising the level of Cyber Security in all Partner Countries by helping to:

1) Develop and implement Cyber Security Strategies to improve the effectiveness of the fight against cyber crime, facilitate exchange of information, increase trust in cyber space and expand trade opportunities between the EU and Partner Countries. For the AA countries, the project would help implement relevant AA provisions; Georgia and Moldova have achieved successes in harmonising their strategies with that of the EU and can share relevant experience gained. Finally the project would also facilitate a ratification of the Council of Europe (CoE) Cybercrime Convention by Belarus.
2) Consolidate legal and regulatory frameworks for ensuring confidentiality of personal data and the protection of online privacy while transmitting and processing data over electronic communication networks; the project would help share and exchange good practices available in Partner Countries.
3) Build capacities of national/government CERTs and expanding their services to a wide range of clients, improve competencies for reporting on security incidents and risks, increase transparency of such reporting, better protect critical information infrastructures, engage private sector operators, raise trust in cyber space; the project would also help share and exchange good practices available in Partner Countries.

Pilot projects for Network, information and Cyber Security are summarised below.

Pilot project name		
Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation	**Aims**	• Raise Cyber Security in both Partner Countries and EU • Harmonise with EU laws/ policies • Balance internet openness and safety
	Scope	Regional
	Rationale	• Network, information and Cyber Security is a policy priority in each partner country • Obligation to implement relevant AA provisions

		• Availability of good practices for sharing between Partner Countries • Lack of adequate progress in most partner countries
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Disparities in the current state of play and inadequate technical and organisational readiness
	Benefits/ Impact	• Will increase trust to cyber space • Will facilitate fight against cyber crime • Will facilitate trade and strengthen DSM • Will facilitate implementation of AA agreements for signatory countries
	Work required before launch	Awareness-raising, capacity and needs assessment, consultations, fact-finding missions
	Organisations involved	• EC: DG Connect, European Parliament, Council of Europe • Region: government agencies responsible for ICT, information society, public security, judiciary, law making
	Project deliverables	• National Cyber Security Strategies and respective action plans in 6 Partner Countries • Identified good practice and recommendations • Model strategies
	Total person-months (per country)	To be estimated
Policy support to confidentiality of data processing, protection of personal data and online privacy	**Aims**	• Protect basic liberties and freedoms • Consolidate mostly fragmented legal and regulatory frameworks
	Scope	Regional
	Rationale	• Lack of adequate progress in most Partner Countries • Obligation to implement relevant AA provisions • Fragmented legal and regulatory basis
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Disparities in the current state of play and inadequate technical and organisational readiness • Sensitivity of the issue

	Benefits/ Impact	• Will strengthen democracy • Will facilitate implementation of AA agreements for signatory countries
	Work required before launch	Awareness-raising, capacity and needs assessment, consultations, fact-finding missions
	Organisations involved	• EC: DG Connect, European Parliament, Council of Europe • Region: government agencies responsible for ICT, information society, public security, judiciary, law making
	Project deliverables	• Identified good practice and recommendations • Model laws • Passed and draft law bills in each partner country
	Total person-months (per country)	To be estimated
Capacity building plan for national/government CERTs, including through cooperation with ENISA	**Aims**	• Strengthen CERTs' capabilities provide value-added services • Improve reporting on security risks, incidents, breaches • Engage private business community • Increase awareness among the general public • Protect Critical Information Infrastructures
	Scope	Regional
	Rationale	• Lack of adequate progress in most partner countries, especially in reporting and cooperation with business community • Strong local expertise in cyber security
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Inadequate laws and regulations governing CERTs' operations
	Benefits/ Impact	• Will strengthen cyber security • Will increase trust to cyber space • Will facilitate trade and strengthen DSM
	Work required before launch	• Will strengthen cyber security • Will increase trust to cyber space • Will facilitate trade and strengthen DSM
	Organisations involved	Awareness-raising, capacity and needs assessment, consultations, fact-finding missions
	Project	• EC: DG Connect, ENISA

	deliverables	• Region: government agencies responsible for ICT, information society, public security, judiciary, law making, ICT industry, academia
	Total person-months (per country)	To be estimated

Table 1 - pilot projects for Network, information and cyber security

Electronic identification and trust services

The proposed four projects aim at raising the level of secure electronic transactions, expanding e-services for businesses and implementing innovative e-government interoperability solutions in all Partner Countries by helping to:

1) Improve legal and regulatory frameworks in the area of eID/TS services harmonised as much as feasible with the European eIDAS Regulation 910/2014 so as to raise the security of electronic identification/authentication and expand the use of digital signature both within and outside national borders for secure access to public services in general and electronic procurement in particular.

2) Develop and implement cross-border cooperation modalities aimed at the mutual recognition of digital signatures and related certification, identification/authentication trust services between Partner Countries and EU Member States; the project will consider various – technical, legal and organizational – options of such recognition, including the current and forthcoming legislation and practices of the Eurasian Economic Union; the project would also consider joining a STORK platform on a pilot basis for select Partner Countries ; available good practice experience will also be documented and shared, such as the mobile eSignature solutions implemented in Azerbaijan and Moldova; special attention should be paid to increasing the trust in electronic identification and transactions among entrepreneurs and ordinary citizens.

3) Apply the European e-service maturity model to the basic public services provided to citizens and business; the project would extend the method of e-service benchmarking to Partner Countries willing to participate in the benchmarking exercise; special emphasis will be put on developing and measuring eProcurement services; a sub-project aimed at building capacities of national agencies responsible for digital services and procurement both in the AA and non-AA Partner Countries would be launched; the project would facilitate good practice exchanges among

Partner Countries (e.g. eProcurement practices of Armenia).

4) Promote and share e-government interoperability solutions based on the European Interoperability Framework by creating a Demonstration and Knowledge Transfer Centre in one of the EU Member States with teams set up in each Partner Country; the Centre will deal with all key aspects of interoperability, including legal, technical, semantic, and organisational, according to best EU practices.

Pilot projects for Electronic identification and trust services are summarised below.

Pilot project name		
Policy support for mutual recognition of eID/TS	**Aims**	• Raise quality and security of electronic identification and trust services • Expand the use of digital signature • Facilitate recognition of digital signature across border • Creating an enabling legal and regulatory environment harmonised with eIDAS Regulation 910/2014 • Facilitate mutual recognition of electronic identification and trust services beyond national borders • Improve relevant legislation and regulations
	Scope	Regional
	Rationale	• Digital signature is a policy priority in each partner country • Obligation to implement relevant AA provisions • Inadequate use of digital signature by businesses and citizens • Emerging demand for using eSignature internationally • Impossibility of recognising digital signatures of other countries
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Disparities in the current state of play and inadequate technical and organisational readiness • Political and technical difficulties of cooperation with the Eurasian Economic Union
	Benefits/ Impact	• Will help expand national digital markets in line with European standards • Will facilitate trade and strengthen DSM • Will raise security of international trade • Will facilitate implementation of AA agreements for signatory countries
	Work required	Awareness-raising, capacity and needs

	before launch	assessment, consultations, fact-finding missions
	Organisations involved	EC: DG Connect and other DGs Region: government agencies responsible for ICT, economy, security, public services, information society, judiciary, law making
	Project deliverables	• Policy papers on the conditions and opportunities for mutual recognition of electronic identification and related trust services for each country and the entire region • Working paper on the conditions and opportunities for mutual recognition of electronic identification and related trust services with the Eurasian Economic Union • Passed and draft law bills in each partner country
	Total person-months (per country)	To be estimated
Piloting digital signature across borders	**Aims**	• Facilitate participation in STORK project • Finding a mechanism of cooperation with the Eurasian Economic Union Member States • Facilitate exchange of good practices in using mobile eSignature
	Scope	Regional
	Rationale	• Digital signature is a policy priority in each partner country • Emerging demand for using eSignature internationally • Impossibility of recognising digital signatures of other countries • Inadequate use of eSignature by businesses and citizens
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Disparities in the current state of play and inadequate technical, organisational and legal readiness • Political and technical difficulties of cooperation with the Eurasian Economic Union
	Benefits/ Impact	• Will help find workable solution of using eSignature across borders including with the Eurasian Economic Union • Will facilitate implementation of AA agreements for signatory countries • Will increase economic transactions with the EU • Will facilitate trade and strengthen DSM
	Work required before launch	Awareness-raising, capacity and needs assessment, consultations, fact-finding missions

	Organisations involved	EC: DG Connect and other DGs Region: government agencies responsible for ICT, economy, security, public services, information society, judiciary, law making
	Project deliverables	• Cooperation regarding participation in STORK • Identified good practices and solutions • Modalities and solutions for mutual recognition of eSignature with the Eurasian Economic Union
	Total person-months (per country)	To be estimated
Policy support to eService development and benchmarking including capacity building for eProcurement sector	**Aims**	• Apply European approaches establishing and measuring e-services • Raise eService online maturity • Digitise public procurement • Exchange and implement best practices • Widen use of digital signature for and in public procurement
	Scope	Regional
	Rationale	• eServices and eGovernment are policy priority in each partner country • Obligation to implement relevant AA provisions • Availability of good practices for sharing between Partner Countries • Inadequate use of digital signature in eProcurement • Absent eService benchmarking methods • Lack of transactional e-services at higher levels of online maturity • Inadequate automation of eProcurement process • Impossibility of accessing e-services of other countries
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Lack of political will for closer cooperation with EU in non-AA partner countries
	Benefits/ Impact	• Will help expand digital services • Will facilitate implementation of AA agreements for signatory countries • Will strengthen security of eProcurement • Will increase economic transactions with the EU • Will facilitate trade and strengthen DSM
	Work required before launch	Awareness-raising, capacity and needs assessment, consultations, fact-finding missions

	Organisations involved	EC: DG Connect and other DGs Region: government agencies responsible for ICT, economy, security, public services, information society, judiciary, law making
	Project deliverables	• Roadmaps for increasing e-service maturity in each partner country • Roadmaps for full digitisation of public procurement process, especially at Award and post-Award stages • Policy papers on establishing national e-service benchmarking systems • Identified good practices
	Total person-months (per country)	To be estimated
Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre .	**Aims**	Improve knowledge exchange and exploit EU best practices and solutions in e-government Build capacities in e-government infrastructure and services Increase cooperation with
	Scope	Regional
	Rationale	• Lack of effectively functioning interoperability frameworks • Lack of effective knowledge exchange and adaptation mechanisms across borders
	Risks	• Lack of political will for closer cooperation with EU in non-AA partner countries • Lack of political will for closer cooperation with EU in non-AA partner countries
	Benefits/ Impact	• Will set up a regional mechanism for best practice sharing and adaptation • Will support and promote common interoperability solutions strengthen cyber security • Will increase compatibility of national e-government and state information systems • Will increase security of e-government services and transactions • Will facilitate trade and strengthen DSM
	Work required before launch	Awareness-raising, capacity and needs assessment, consultations, fact-finding missions
	Organisations involved	EC: DG Connect and other DGs Region: government agencies responsible for ICT, economy, security, public services, information society, judiciary, law making, Estonian e-Governance Academy
	Project deliverables	• Policy and working papers on e-government interoperability in each partner country

		• Identified good practices for transfer and adaptation • Strategy for establishing a Regional Demonstration and Knowledge Transfer Centre
	Total person-months (per country)	To be estimated

Table 2- pilot projects for Electronic identification and trust

eCustoms

The study has identified several aspects of mutual interest of the Region where it is possible to propose some pilot projects for individual Partner Countries or multi-country pilot projects for the ensemble of the Partner Countries. Term of implementation of the proposed small-scale pilot projects is between six to nine months.

Exchange of summary electronic declaration for pre-arrival and pre-departure information. The purpose is to implement information services for data exchange between customs information systems of some Partner Countries. After piloting with two or more countries, this project can be extended to the Region. Computerised customs systems for export, import, and transit as well as systems for the management of the data on economic operators, export, import, transit of Partner Countries would allow data exchange of summary electronic declaration for pre-arrival and pre-departure information. This project can be extended for the exchange of summary electronic declarations through electronic customs systems between some Partner Countries and then with the EU Member States through Common Communications Network / Common Systems Interface (CCN/CSI). A Technical infrastructure is required that enables automated data exchange between Member States' electronic customs systems and the Partner Countries that are not linked to CCN/CSI on the basis of EU bilateral or multilateral agreements. To support this initiative, a generic technical solution which permits each partner to connect to a system developed centrally has to be developed.

Set up an Anti-Counterfeiting and Anti-Piracy System. Such a system is intended to enhance intellectual property rights protection by improving the cooperation and sharing of information between right-holders and the national Customs administrations and between all the Customs offices of the Region. The pilot project can start by setting up national Anti-Counterfeiting and Anti-Piracy Systems in some Partner Countries. An electronic service provides traders with the possibility to submit a claim asking the intervention of customs in order to take measures against goods infringing certain intellectual property rights. At the

more advanced level, national Anti-Fraud Information System should allow exchange of data within the Partner Countries and be connected with the EU centralised Anti-Counterfeiting and Anti-Piracy System (COPIS), which is accessible by all Member States.

Create national segments for the Registered Exporters' System. This pilot project aims at the establishment of national Registered Exporters Systems for registered exporters established in non-EU countries (Generalised System of Preferences beneficiary countries) exporting goods to the EU under preferential trade arrangements. Exporters should be registered with the competent authorities of the beneficiary countries in order to be entitled to make statements on origin. The system should also allow an automated verification of the exporters' registration number from the declarations in the national customs declaration system. The Region can cooperate with the EU in order to automate registration of national exporters into the EU REX central database managed by the European Commission. The REX system is designated for economic operators from non-EU countries benefiting from preferential trade arrangements under the Generalised System of Preferences and exporting goods to the EU.

Pilot projects for the eCustoms priority area are summarised below and more detailed description is presented in Section 2.3.3:

Pilot project name		
Exchange of summary electronic declaration for pre-arrival and pre-departure information	**Aims**	Increase security of cross border trade
	Scope	Bilateral between individual EaP countries
	Rationale	Allow more accurate and quicker processing of customs declarations for goods arriving at border crossing points
	Risks	• Require bilateral agreements between countries • Difficulty of data exchange between heterogeneous information systems
	Benefits/ Impact	• Improved risk assessment • Provide more time to assess data against risk profiles • Automate process of input of data into customs systems
	Work required before launch	Sign bilateral agreements for data exchange between participating countries
	Organisations involved	• Customs services of the Partner Countries • Customs services of the EU Member States
	Project deliverables	Information service(s) that allows data exchange between information systems of customs services
	Total person-months (per country)	• Implementation period 3-6 months for 2 countries • Requires a small team of IT specialists from each country
Set up an Anti-Counterfeiting	**Aims**	• Enhance intellectual property rights protection

and Anti-Piracy System		• Take measures against goods infringing certain intellectual property rights
	Scope	Individual Partner country level or Regional level
	Rationale	Provide traders with the possibility to submit a claim asking the intervention of customs in order to take measures against goods infringing intellectual property rights
	Risks	• Use of this tool by traders for damaging of concurrent businesses • Need in additional specialised staff to check complaints
	Benefits/ Impact	• Enhanced intellectual property rights protection • Lawful traders get competitive advantage • Increase of trade volume of goods respecting intellectual property rights
	Work required before launch	-
	Organisations involved	• Government services responsible for intellectual property rights protection • Customs services • EU administration responsible for COPIS
	Project deliverables	• An electronic service providing traders with possibility to submit a claim • National Anti-Fraud Information Systems • Service for exchange of data within the Partner Countries and with the EU centralised system
	Total person-months (per country)	• Implementation period 6-9 months • Require a team of lawyers, business analysts, IT specialists
Create national segments for the Registered Exporters' System	**Aims**	Make up-to-date and complete information available on Registered Exporters established in non-EU countries exporting goods to the EU
	Scope	Regional level
	Rationale	Replace the current paper based certification process by an IT-supported self-certification process
	Risks	Little interest by traders due to small number of traders exporting to the EU
	Benefits/ Impact	• Simplify export procedures from the Partner Countries to the EU • Automate registration of national exporters into the EU REX central database
	Work required before launch	Revise and document preferential trade arrangements under the Generalised System of Preferences for each participating Partner country
	Organisations involved	• Ministry of Foreign Affairs of Partner Countries • Ministry of Economy • Customs Services • DG TAXUD
	Project deliverables	• National database of registered exporters • Checking of exporters' registration number from the declarations in the national customs declaration system • National segments for data exchange with the EU

		Registered Exporters' System
	Total person-months (per country)	• Implementation period 6-12 months • Require a team of lawyers, business analysts, IT specialists

Table 3- Pilot projects for eCustoms priority area

eCommerce for SMEs

The study has identified some actions that would have a significant impact on the Region. These are the aspects with the widest common gaps of the Region for harmonisation of eCommerce for SMEs. The common actions are also the ones with the biggest economic and political benefits within the Region. In eCommerce for SMEs, these are the areas which help in the creation of more accessible markets and facilitate a rapid boost in trade for SMEs. Pilot projects in information services development would show immediate benefit for SMEs and customers that use these services. The study proposes some most rewarding areas for harmonisation and the development of common pilot projects within the Region.

Develop an eCommerce trading platform that allows SMEs to conduct their digital trade activities across the Region and the EU. Such an interregional platform will significantly amplify market accessibility for SMEs, open new markets and assure a boost in trade. A pilot project can consist in setting up a platform in one or several individual Partner Countries. The initial scope can include some basic modules such as electronic catalogues of goods, e-payment tools, on-line trading, electronic documents exchange and repository, electronic signatures. More advanced modules can include electronic invoicing, electronic contracting, submission of requests for issuing of permits, customs declaration, etc. National segments can be then connected at the regional level in order to allow cross-border conducting of trading, administrative and customs procedures in electronic format.

Create online trustmark schemes for retail websites that will be common for the Region and harmonised with the EU scheme(s) for electronic identification and trust services of electronic transactions. This Pilot project would assure the trustfulness of qualified eCommerce service providers in a Partner Country. However, the Partner Countries get significant benefits from establishing a common trustmark scheme for the Region. For the harmonisation of digital markets, an important measure is joining the work in progress on the EU-wide trustmark schemes, which aims to reassure consumers on the reliability of accredited traders at the EU level. The trustmarks will facilitate the promotion of Regional eCommerce platforms for SMEs. Such certified sites help consumers to make informed decisions when using online retail services. The Partner Countries can start by

jointly developing specifications with regard to the implementation mechanisms, form, presentation, composition, size and design of the trust mark for qualified trust services.

A trustmark can be in the form of a logo published on certified websites and linked to an accreditation website (trustmark providing third-party website identity validation). It can be also assured through another mean of trusted electronic identification such as secure sockets layer (SSL) and electronic certificates.

Pilot projects for eCommerce for the SMEs priority area are summarised below and a more detailed description is presented in Section 2.4.3:

Pilot project name		
eCommerce trading platform for SMEs	**Aims**	Allow SMEs to conduct their trade activities across the Region and the EU in electronic format
	Scope	At the level of individual Partner Countries and regional level
	Rationale	National eCommerce platforms to conduct business in electronic format Cross-border electronic trade
	Risks	Technical complexity of mutual recognition of electronic signatures
	Benefits/ Impact	Amplify market accessibility for SMEs Open new markets and assure a boost in trade
	Work required before launch	-
	Organisations involved	National regulatory authorities of electronic signatures Banks (e-payments)
	Project deliverables	National eCommerce trading platforms for SMEs Interconnection between national platforms
	Total person-months (per country)	Implementation period 9-12 months Require national teams of business analysts, IT specialists
Common for the Region online trustmark scheme for retail websites	**Aims**	Assure the trustfulness of qualified eCommerce service providers from EaP countries at the regional and the EU levels
	Scope	At the level of individual Partner Countries and regional level
	Rationale	Create a common for the Region online trustmark schemes for retail websites harmonised with the EU scheme(s) for electronic identification and trust services
	Risks	EU has several concurrent projects aiming the development of online trustmark schemes. No single concept generalised
	Benefits/ Impact	Reassure consumers on the reliability of accredited traders at the national, regional and the EU level
	Work required before launch	Select between several existing EU online trustmark schemes for harmonisation
	Organisations involved	National administrations responsible for electronic commerce Associations of eCommerce traders
	Project deliverables	Online trustmark scheme for retail websites
	Total person-months (per country)	Implementation period 3-6 months Require national teams of lawyers, business analysts, IT specialists

Table 4 - Pilot projects for eCommerce for SMEs priority area

Digital Skills

It is recommended that all six Partner Countries join a Regional initiative to measure the Digital Skills gap in each country and for the Region overall, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap. Advice and best practices employed by EU countries to measure and monitor the Digital Skills gap will be an invaluable part of the proposed pilot.

The pilot project can be undertaken within the scope of a proposed "National Coalition for Digital Jobs" to be created in each country in conjunction with the EU's "Grand Coalition". The experience and advice from EU countries which have already established National and Local Coalitions will be invaluable. The first move would be a Regional seminar organised by the European Commission to present their published Toolkit for National and Local Coalitions.[10]

Pilot projects for Digital Skills are summarised below:

Pilot project name		
Introduction to the Grand Coalition for Digital Jobs	**Aims**	To raise the profile of Digital Skills
	Scope	Regional
	Rationale	Will accelerate the harmonisation process in this area
	Risks	Lack of priority given to the topic
	Benefits/ Impact	Will enable the countries to share experience and best practice
	Work required before launch	Preparation for a Regional Event
	Organisations	EC: Grand Coalition for Digital Jobs.

[10] See: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=913&PortalId=0&TabId=353

	involved	Regional: Representatives from Ministries of Economy and Education from each country.
	Project deliverables	Commitments from each country to launch National Coalitions
	Total person-months (per country)	Attendance by up to 5 persons per country at a 2 day Regional event
Assessment of the "Digital Skills Gap"	**Aims**	To measure and monitor the skills gap
	Scope	Regional
	Rationale	Will raise awareness of the digital skills gap and the need for co-ordinated action
	Risks	Current initiatives will stall whilst the project is being undertaken – awaiting results
	Benefits/ Impact	Quantification of the digital skills gap will raise the priority for creating consistent policies and initiatives for digital skills and jobs
	Work required before launch	1. High-level seminar fronted by EC (above) 2. Training for practitioners on how to measure and analyse the digital skills gap.
	Organisations involved	• EC: Grand Coalition for Digital Jobs. • Region: Representatives from Ministries of Economy and Education from each country
	Project deliverables	1st Report quantifying the Digital Skills Gap in each country
	Total person-months (per country)	Estimate to be provided by EC

Table 5 - pilot projects for Digital Skills

Telecom Rules

The overriding need is to harmonise telecoms rules among Partner Countries and h the EU, developing clear broadband policies and targets and implementing the regulatory frameworks that will guarantee investment and growth in the telecoms markets of the Partner Countries.

In the case of Georgia, Moldova and Ukraine, the basic steps and timescales for harmonization of the legal and regulatory frameworks have already been defined. In the cases of Georgia and Moldova, many of the harmonising steps have already been made, and the remainder will be undertaken, mostly within the next one to three years. In Ukraine, where fewer harmonising steps have been taken so far, the specific steps defined in the Association Agreement will take up to four years.

The common pilot projects for the Region should be focussed on the single most important infrastructure need – that of increasing high-speed broadband infrastructure to reach all parts of the Region. Without this universal high-speed broadband access, the basic aims of a single digital market simply cannot be achieved. The pilot projects should aim to install a firm policy commitment for the Region overall and within each country for universal high-speed broadband access. This policy should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, each country should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

These pilot projects for Telecoms Rules are summarised below:

Pilot project name		
Policy commitment for universal high-speed broadband	**Aims**	To harmonise telecoms sector policy for broadband
	Scope	Regional
	Rationale	Will provide overall policy direction for digital access and connectivity
	Risks	Lack of government priority
	Benefits/ Impact	Will increase connectivity and accelerate the closure of the "broadband gap" between the Region and the EU
	Work required before	Awareness-raising across the Region of the need

	launch	for clear policy statement for broadband access
	Organisations involved	EC: DG Connect Region: Ministries of ICT and Economy from each country
	Project deliverables	Clear policy statements for universal high-speed broadband access in each of the 6 countries
	Total person-months (per country)	To be estimated
Piloting rural broadband infrastructure investment projects	**Aims**	To provide a working model for high-speed broadband implementation in each country
	Scope	Regional – one pilot project in each country
	Rationale	Will define the best working model in each country for investment and implementation
	Risks	Lack of financing available
	Benefits/ Impact	Will accelerate broadband connectivity into a rural community, demonstrating feasibility
	Work required before launch	Clear policy statement (see above)
	Organisations involved	Region: Ministry and Regulator of ICT and Ministry of Economy from each country. Funding institutions
	Project deliverables	A documented working model for rural high-speed broadband infrastructure investment in each country
	Total person-months (per country)	To be estimated

Table 6 - pilot projects for Telecoms Rules

2.0.4 Overview of the individual Partner Countries

Armenia

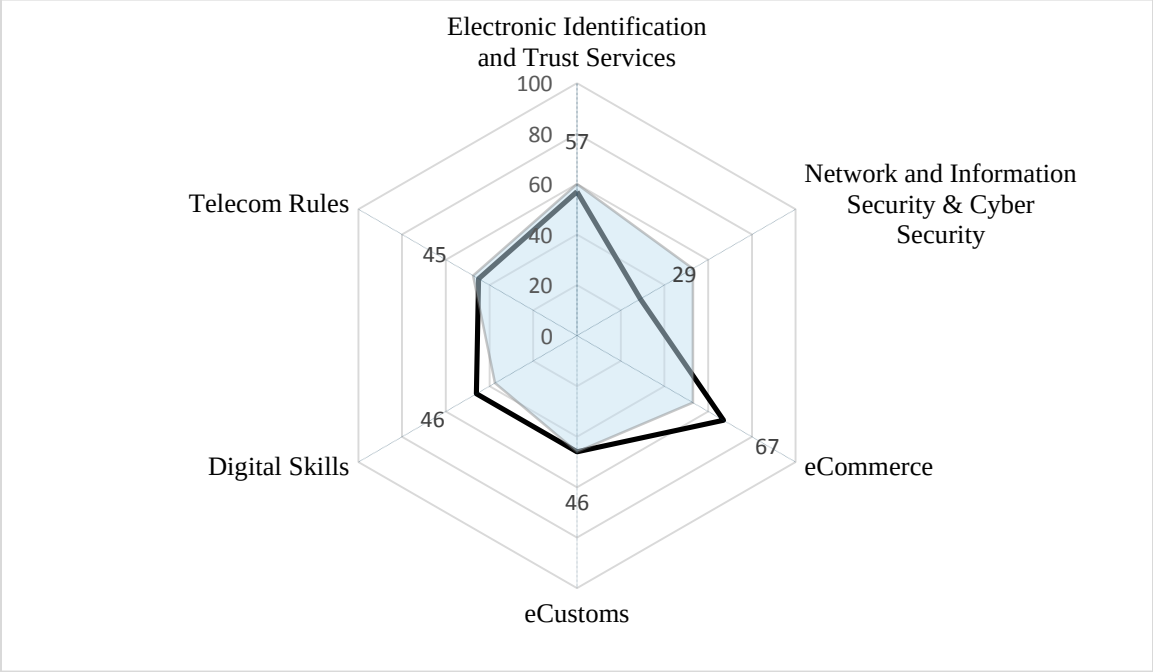

Exhibit 6 -HDM study findings on Armenia's digital economy, focusing on 6 priority topics

(100% represents the EU baseline, the shaded area represents the Regional average)

In the field of **network, information and cyber security**, Armenia displays the largest gap in relation to the EU baseline. It is significantly below the average gap for the Region. Armenia is the only Partner Country that has not established its government Computer Emergency Response Team although it joined the Cyber Crime Convention in 2001 and ratified it in 2006. Narrowing the gap requires preparing a national cyber-security strategy, developing procedures for reporting on security incidents in an open and transparent manner, defining minimal security levels and regularly practising cyber-attack simulations. The internet in Armenia is free and open.

For **electronic identification and trust services**, the country has reached the level of the EU baseline which is close to the Region's average. The biggest gaps are found in the area of e-services for businesses and citizens (provided at lower maturity levels) and insufficient legal certainty about licensing in the area of Public Key Infrastructure (PKI). It is important that electronic identification and trust services become interoperable across borders and be recognised in other countries. While Armenia's eProcurement system is almost on par with the EU baseline, digital signatures should be integrated into the entire tender process.

Armenia's score in **eCommerce for SMEs** is largely above the average for the Region. The country has achieved significant progress for instance on competition in eCommerce and electronic payments, but more work needs to be done notably in the areas of internet security and privacy, as well as in consumer rights protection. Specific follow-up activities are needed for setting-up a national trustmark scheme for eCommerce websites, defining out-of-court dispute settlement mechanisms, online dispute resolution system for consumers for eCommerce transactions and anti-spam regulation.

For **eCustoms**, Armenia's score is almost at the average of the Region. Progress has been made on the relevant legal framework and the eCustoms infrastructure, but more work needs to be done in the implementation of information services. Specifically, priority aspects include defining the status of an authorised Economic Operator, setting-up a registration system and organising exchange of data within the Region, creating anti-counterfeiting and anti-piracy systems, registered exporters status and system, and connection to the Single Point for Entry or Exit of Data portal (SPEED) of the EU.

For **Digital Skills**, the gap between Armenia and the EU baseline is less than the average for the Region. Progress has been made especially in introducing ICT for better education and there have been some independent initiatives for the development of ICT user skills for targeted groups. The Enterprises Incubator Foundation of Armenia published a report on the Digital Skills Gap in 2014 which should lead to increased awareness. Though the Government has announced that ICT is a priority sector for the country's economic development and for the creation of a knowledge-based economy, the strategies for the development of digital skills are not yet coordinated. Responsibilities are distributed among a number of institutions – notably the National Centre of Educational Technologies (NCED) (in education), the National Quality Assurance Organisation and the Ministry of Economy. Action has been led mainly by initiatives

in the private sector, using professional organisations and NGOs. These are not part of any special national agenda. Clear and coordinated policy is required and key components of action should be defined – awareness raising, long term co-operation, human resources investment, making ICT attractive, developing digital literacy for employability and e-inclusion and lifelong acquisition of digital skills. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, the gap between Armenia and the EU baseline is slightly larger than the average for the Region. Good progress has been made in exploiting spectrum to achieve universal mobile coverage. Even so, for all broadband services, overall penetration remains significantly below the EU average. The policy, legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecoms Rules. The largest gaps are in the elements that ensure competitive broadband markets, give better information to consumers and increase attractiveness to infrastructure investors. There is no clear policy for universal access to high speed (>30Mbps) broadband within an achievable deadline. The EU baseline contains this "Digital Agenda" target for 2020. Furthermore, the regulatory capacity in the sector is very limited and remains part of the Public Utilities Regulatory Commission which is dependent on state funding. The EU baseline requires far greater independent focus on this market sector. More resources are required to regulate this fast changing and dynamic market which is vital to the economy. Legal and regulatory change is required to give a better focussed regulator the tools to improve competition in the market and to provide more favourable conditions for infrastructure investors leading to better broadband choices for consumers.

Proposed pilot projects are presented in the detailed country's descriptions for each priority area.

Azerbaijan

For **network, information and cyber security** Azerbaijan is below the EU baseline and higher than the average for the Region. The largest remaining gap with the EU baseline is for the benchmarks describing the availability of strategic documents that spell out priorities and actions, especially regarding minimum security levels. There are also gaps in human resources capacity, lack of regular training and the persistent challenge of ensuring transparency in security issues. The country needs a comprehensive national cyber-security strategy to specify

minimal security levels, define rules for reporting and disclosure in security breaches and risks and enhance capacities.

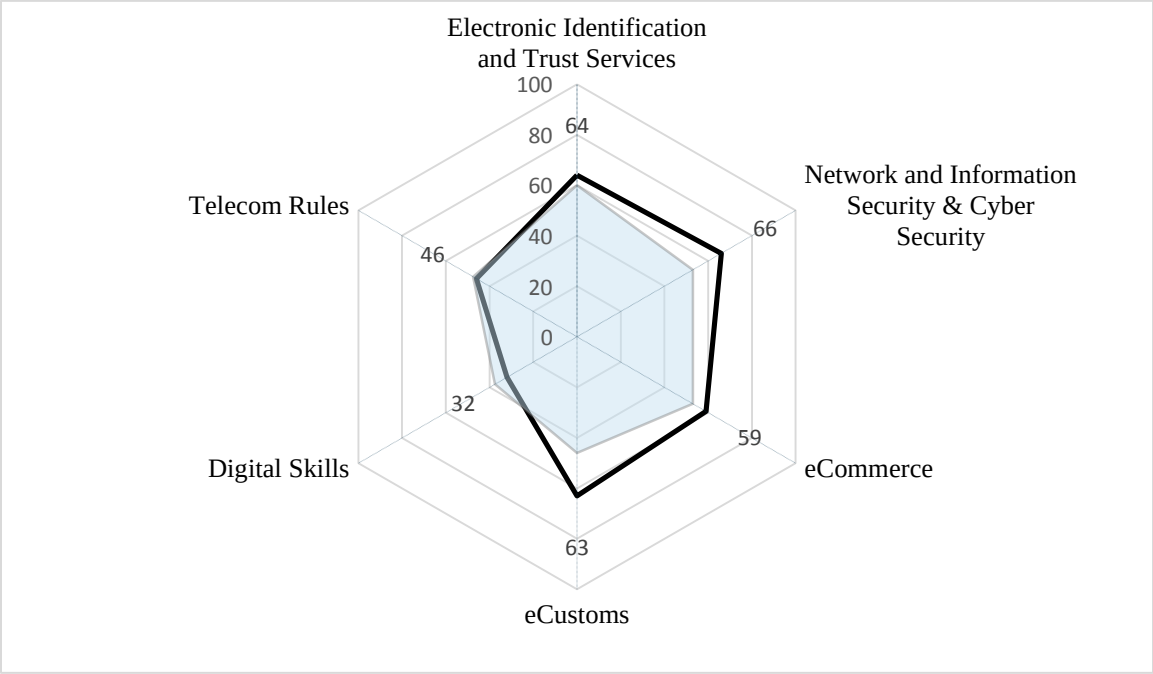

Exhibit 7 -HDM study findings on Azerbaijan's digital economy, focusing on 6 priority topics

(100% represents the EU baseline and the shaded area represents the Regional average)

Azerbaijan is making good progress in building infrastructure for **electronic identification and trust services.** It is higher than the average for the Region. The largest gaps are observed in the area of eProcurement, public confidence in eID, eGovernment interoperability and standards, The most important priority is to improve legal certainty (possibly with a new law) to make electronic identification services interoperable across borders and digitise public procurement at all stages of the tender process.

For **eCommerce for SMEs,** Azerbaijan scores a bit higher than half of the EU baseline, which is above the Region's average. The country has achieved significant progress for instance on openness for competition in eCommerce, consumer rights protection and eLogistics. More work needs to be done notably in the areas of electronic payments, internet security and privacy. Specific follow-up activities are needed for setting-up an online dispute resolution system for

consumers for eCommerce transactions, assuring equal treatment between paper and electronic invoices, defining a specific liability regime for intermediary service providers, and securing consumer protection international cooperation mechanisms.

On **eCustoms,** the score is significantly above the average achieved for the Region. While Azerbaijan has achieved progress, for instance in the relevant legal framework and the eCustoms infrastructure, more work needs to be done, particularly in the implementation of information services. Specifically, priority aspects are setting-up a registration system of Authorised Economic Operator and organising exchange of data within the Region, creating anti-counterfeiting and anti-piracy system and creating electronic interfaces to conduct all customs-related business.

For **Digital Skills**, the gap between Azerbaijan and the EU baseline is higher than the average for the Region. Progress has been made especially in introducing ICT for better education, but there are still significant gaps in comparison with the EU in policy formulation and the levels of coordination required to ensure an adequate supply of the necessary skills to create growth and jobs. As a vital first step, the extent of the "digital skills gap" should be systematically measured and monitored so that awareness of the need for action across all sectors can be raised. Clear and coordinated policy is required and key components of action should be defined – long term co-operation, human resources investment, making ICT attractive, developing digital literacy for employability and e-inclusion and lifelong acquisition of Digital Skills. Progress can be made by forming a national coalition for digital jobs, also local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, the gap between Azerbaijan and the EU baseline is higher than the average for the Region. Good progress has been made using state investment to build infrastructure for broadband services. However, the policy, legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecom Rules, particularly in the elements that ensure competitive markets and attractiveness to private investors. Furthermore, the regulatory capacity is very limited and remains part of the ministry structure, whereas the EU baseline requires far greater independence and separation. More regulatory resources are required to regulate a fast changing and innovative sector which is vital to the economy. Legal and regulatory change is required to give an independent regulator the tools to

improve competition in the market and to provide more favourable conditions for private investors and more consumer choice.

Proposed pilot projects are presented in the detailed country descriptions for each priority area.

Belarus

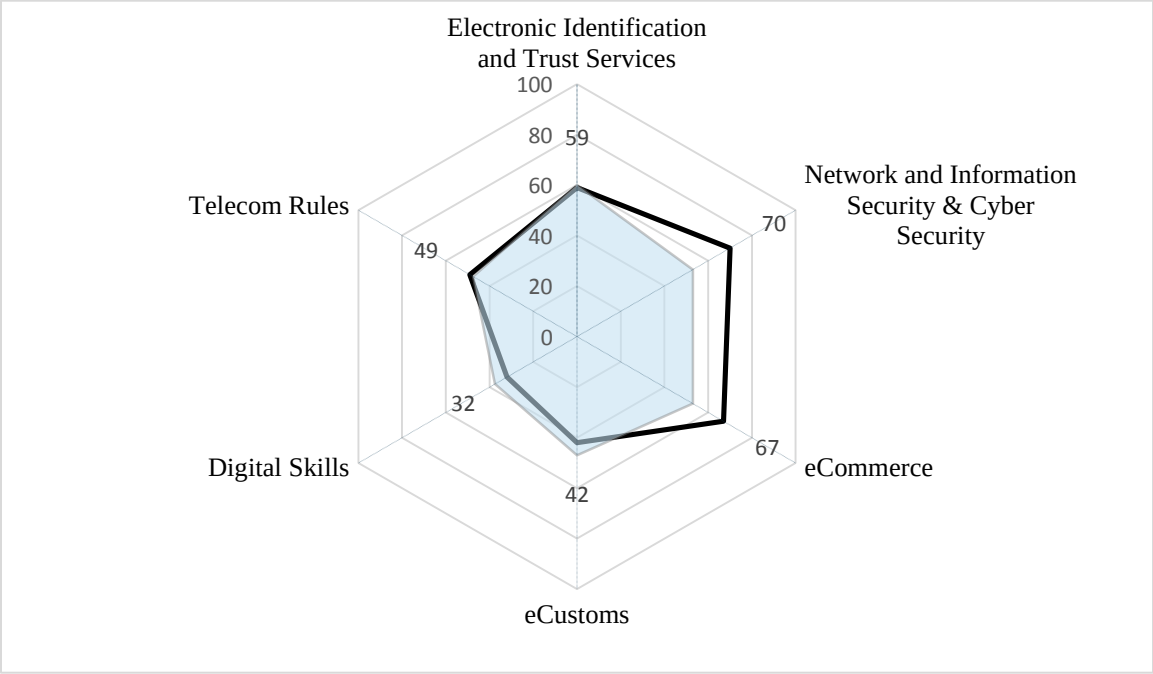

Exhibit 8 -HDM study findings on Belarus's digital economy, focusing on 6 priority topics

(100% represents the EU baseline, the shaded area represents the Regional average)

Belarus has not yet joined the Convention on Cybercrime, a major international agreement in **network, information and cyber security**. Yet its legislative and regulatory framework is generally adequate to respond to existing challenges. The country exhibits the smallest gap with the EU baseline. The legal and regulatory framework still needs improvement. Formulation of a national Cyber Security Strategy to address numerous challenges in a comprehensive way would be a step forward in this direction. Also, the country would need a new law to better

protect personal data and online privacy – a good European and international practice – and thus better balance internet openness with safety.

Belarus' score in **electronic identification and trust services** is at the level of the Region's average measured against the EU baseline. The country does not have display any clearly weak area, with the largest gap measured for e-services for citizens. eProcurement, common infrastructure and e-government interoperability, use of ICT standards and interoperability are at the medium level. While technically and legally it is not possible yet to use digital signature across borders, there are plans to overcome the existing obstacles. Belarus would benefit from making its national legislation more compatible with Europe's eIDAS Regulation to raise security of electronic transactions and to make eSignatures interoperable with EU.

Belarus' score in **eCommerce for SMEs** is above the average for the Region. The country has achieved significant progress for instance on openness for competition in eCommerce, consumer rights protection and eLogistics. More work needs to be done notably in the areas of electronic payments as well as Internet security and privacy. The priority follow-up activities are introducing a specific liability regime for intermediary service providers, defining online trustmark schemes for retail websites, setting-up online dispute resolution system for consumers for eCommerce transactions, and defining the rights on delivery of goods.

On **eCustoms** the score is slightly below the average for the Region. While Belarus has achieved progress, for instance in the relevant legal framework, more work needs to be done in the implementation of infrastructures and the development of information services. Specifically, the priority aspects for follow-up actions are automating exchange of data with the Region, creating electronic interfaces to conduct all customs-related business, setting up a Registered Exporters' system, setting-up a registration system of Authorised Economic Operators, and implementing a comprehensive national single window system for trade.

For **Digital Skills**, the gap between Belarus and the EU baseline is higher than the average for the Region. Progress has been made especially in using ICT for better education, and some policy context has been created for example using a formalised classifier for professions. There are still significant gaps with the EU in policy formulation and in the levels of coordination required to ensure an adequate supply of the necessary skills to create growth and jobs. As a vital first step, the extent of the "digital skills gap" should be systematically measured and monitored so that awareness of the need for action across all sectors can be raised. Neither

Ministry of Education nor the Ministry for Labour have a department in their structure that would be responsible for IT education and digital skills in general. Clear and coordinated policy is required and key components of action should be defined. Short-term priorities are to develop a curriculum and educational content standards for ICT skills based on the European e-Competence Framework, create the system of user-generated electronic content to be used for distance learning and promote activities within the EU and the Region to increase the popularity of ICT skills. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, the gap between Belarus and the EU baseline is slightly lower than the average gap for the Region. Particular progress has been made using state investment to build infrastructure for broadband services, giving Belarus the highest level of broadband penetration in the Region. However, there are no "state-aid rules" in place to ensure that this infrastructure provides the required competitive safeguards, including open access to alternative operators. The policy, legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecom Rules, particularly in the elements that ensure competitive markets and attractiveness to private investors. The electronic communications regulatory function remains part of the ministry structure, whereas the EU baseline requires far greater independence and separation. More resources are required to regulate a fast changing and innovative sector which is vital to the economy. Legal and regulatory change is required to give an independent regulator the tools to improve competition in the market and to provide more favourable conditions for private investors and more consumer choice. In particular, ex-ante market analysis procedures need to be introduced and market entry made easier by the simplification of the currently complex licensing regime.

Proposed pilot projects are presented in the detailed country descriptions for each priority area.

Georgia

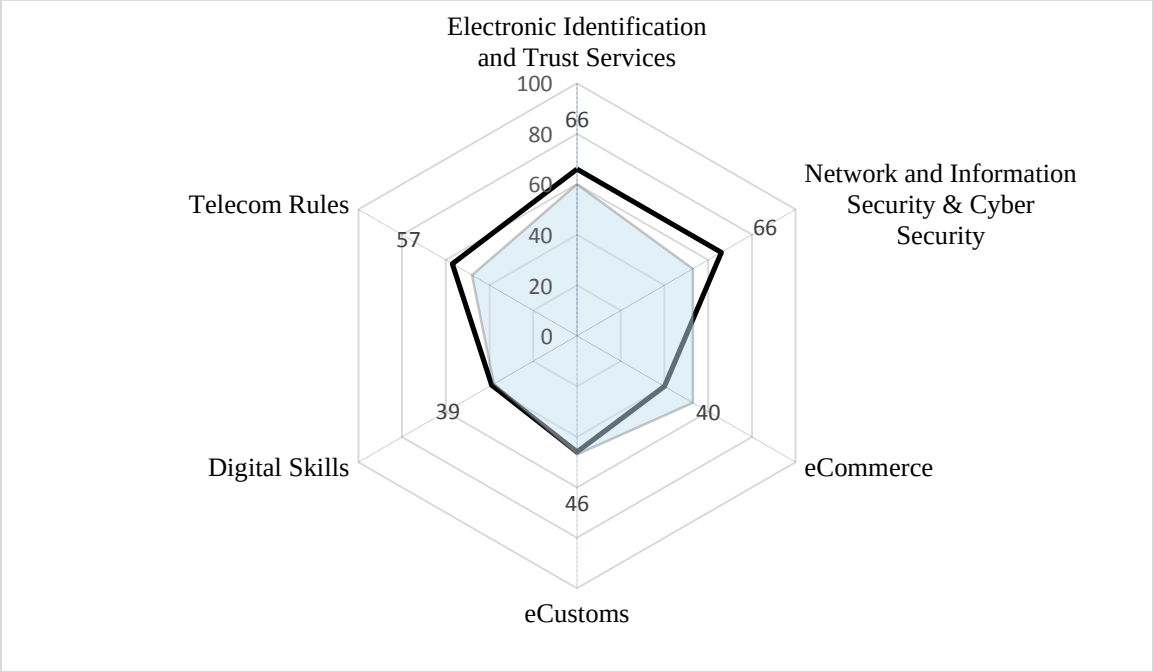

Exhibit 9 -HDM study findings on Georgia's digital economy, focusing on 6 priority topics

(100% represents the EU baseline, the shaded area represents the Regional average)

Following cyber-attacks on its electronic infrastructure and networks in 2008, Georgia takes **network, information and cyber security** seriously. After joining the Cybercrime Convention in 2008, the country has steadily advanced in applying European principles. This is significantly higher than the average gap for the Region. More progress is to be made in the field of private sector infrastructures, management of security breaches and reporting in a transparent and open manner. The country should continue aligning national legislation with that of the EU (e.g. by formulating a new national Cyber Security Strategy in line with the European Cyber Security strategy).

For **electronic identification and trust services** Georgia achieves the highest mark achieved within the Region. Adopting EU policies and practices have been the main driver of the

country's progress across the board. The current legal framework provides sufficient conditions for secure exchange of information between certification service providers, consumers and businesses. There is a plan to start international cooperation in the field of mutual recognition of electronic trust services across borders. The main attention should be devoted to e-services, a common e-government architecture and interoperability.

Georgia's score in **eCommerce for SMEs** is below the average for the Region. The country has achieved significant progress for instance on openness for competition in eCommerce, and in Internet security and privacy. The weakest areas are notably the protection of consumer rights and eLogistics. The specific follow-up activities are needed for defining online trustmarks for retail websites, assuring the transparency of commercial communications to be provided, requirements for distance contracts, setting-up online dispute resolution system for consumers for eCommerce transactions, and defining conditions for the risk of loss of or damage to the goods.

For **eCustoms** the score is just below the average for the Region. While Georgia has achieved progress, for instance in defining the relevant legal framework, more work needs to be done in implementation of information services. Specifically, the priorities for follow-up actions are setting-up a registration system of Authorised Economic Operators and organising exchange of data with the Region, creating anti-counterfeiting and anti-piracy systems, creating electronic interfaces to conduct all customs-related business and the implementation of uniform user management and digital signatures.

For **Digital Skills**, the gap between Georgia and the EU baseline is slightly less than the Regional average. Progress has been made especially in introducing ICT for better education and some policy development work has been initiated, together with actions on growth of digital skills and jobs. Georgia has not yet carried out a thorough survey to measure the "Digital Skills gap". The overall understanding of the importance of digital economy is in place and the government has initiatives to promote innovation and technology, including the creation of the Georgia Innovation and Technology Agency plus a technological park, with a planned opening in 2015. The E-Georgia initiative is not yet adopted. This includes e-inclusion and ICT skills development policies. Clear and coordinated policy is required and key components of action should be defined. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. Cooperation between Government and the private

sector on these issues, would increase trust and would have long term benefit. Progress can be made by forming a national coalition for digital jobs, also local coalitions to share best practices and link with Regional and EU initiatives under the “Grand Coalition for Digital Jobs”.

For **Telecom Rules**, the gap between Georgia and the EU baseline is less than the average for the Region. Good progress has been made in adopting the EU legal and regulatory framework by the well-resourced, independent regulator for electronic communications. Significant steps have included spectrum liberalisation, the removal of licensing in favour of a simple notification procedure and the use of ex-ante regulatory procedures based on market analysis to improve sector competitiveness. Even so, the overall penetration of broadband services remains significantly below the EU average. There is no clear policy for universal access to high speed (>30Mbps) broadband within an achievable deadline. The EU baseline contains this “Digital Agenda” target for 2020. Investment in infrastructure has been left largely to the private sector and the penetration of broadband services in rural areas is still very low. The legal and regulatory framework requires updating to include the latest ex-ante wholesale market and infrastructure enablers, co-ordination of civil works and simpler access to rights of way. Georgia has already used the EU Telecoms Rules model to create a competitive market for electronic communications and now the key challenge is to bring investment in high-speed broadband infrastructure out to the rural areas. Full support should therefore be given to the required analysis and planning for universal high-speed broadband, with public and private sector involvement to define and implement the required investments.

Proposed pilot projects are presented in the detailed country descriptions for each priority area.

Moldova

Since joining the Convention on Cybercrime in 2009 the country’s leadership has demonstrated strong political will to address new challenges of **network, information and cyber security** by aligning closely with Europe. The government has adopted a law to prevent and fight cybercrime, as well as to establish CERT. The National Strategy for Information Society Development ‘Digital Moldova 2020’ contains direct references to cyber-security in alignment with European principles. Yet the country needs to intensify its efforts to diminish the gap with the EU baseline which is substantial. Management of critical information infrastructure, alert

platforms, minimal security levels and cyber-attack simulations score even lower and need attention.

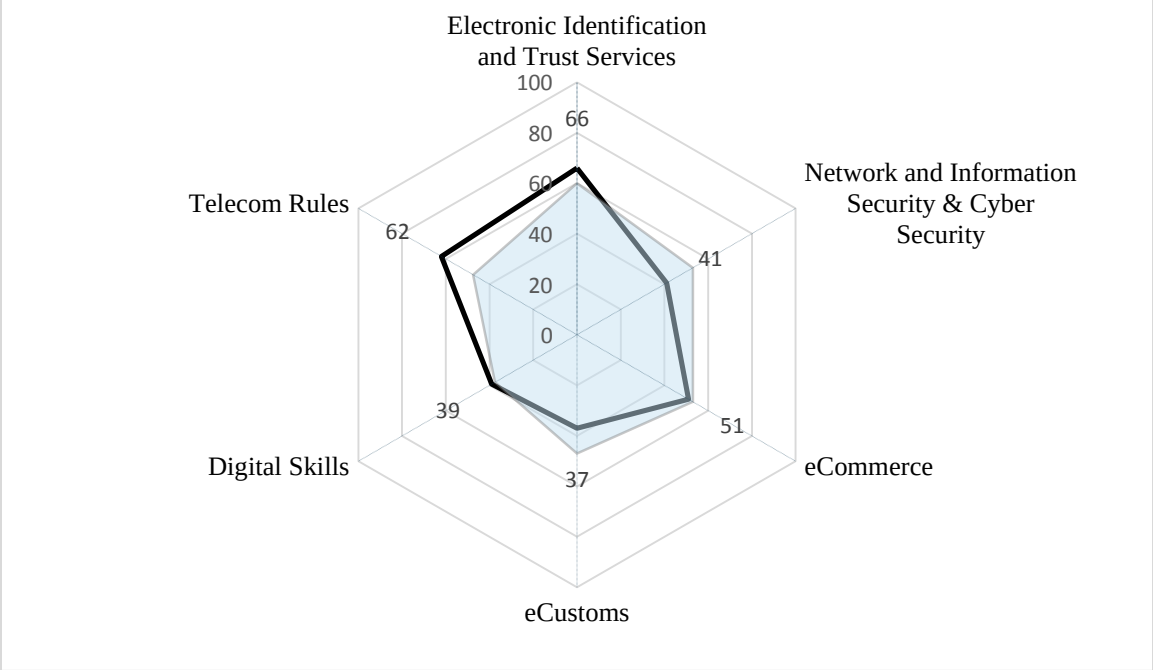

Exhibit 10 -HDM study findings on Moldova's digital economy, focusing on 6 priority topics

(100% represents the EU baseline; the shaded area represents the Regional average)

Moldova is one of the best performers in creating and using the **electronic identification and trust services** infrastructure scoring at a level above the average for the Region. Its strategy for a number of years has been to align with EU laws, regulations and practices. The government common technology platform M-Cloud, which is built on open architecture and European principles of e-government interoperability, is already at the level of the EU baseline. A number of mobile identification tools have been successfully implemented. Other required actions are the closing of the existing gaps in eProcurement and public confidence in eID, interoperability and digital signature.

Moldova's score in **eCommerce for SMEs** is slightly below the average for the Region. The country has achieved significant progress, for instance, on openness for competition in eCommerce and in assurance of Internet security and privacy. More work needs to be done

notably in the areas of eLogistics as well as protection of consumers rights. Specific follow-up activities are needed for defining the conditions for the risk of loss of or damage to the goods, introducing out-of-court dispute settlements for eCommerce, setting-up online dispute resolution system for consumers for eCommerce transactions, defining specific liability regime for intermediary service providers and securing consumer protection international cooperation mechanisms.

For **eCustoms** the score is significantly below the average for the Region. While Moldova has achieved progress, for instance in the relevant legal framework, more work needs to be done, in implementation of related infrastructures and setting up information services. Specifically, the priority aspects for follow-up actions are creating electronic interfaces to conduct all customs-related business, setting-up an integrated tariff information system, implementing an exporters' registered system and creating anti-counterfeiting and anti-piracy systems.

For **Digital Skills**, the gap between Moldova and the EU baseline is slightly less than the average for the Regional. Progress has been made especially in introducing ICT for better education. Awareness has been raised following a study on ICT industry skill requirements and actions have been defined for developing digital skills under "Moldova 2020" strategy. Clear and coordinated policy is required and key components of action should be defined. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. A clear institutional framework needs to be put in place and cooperation between Government and the private sector needs to be initiated. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, the gap between Moldova and the EU baseline is less than the average for the Region. Good progress has been made in adopting the EU legal and regulatory framework by the well-resourced, independent regulator for electronic communications. Significant steps have included spectrum liberalisation, the removal of licensing in favour of a simple notification procedure and the use of ex-ante market analysis regulatory procedures to improve sector competitiveness. The overall penetration of broadband services remains only at half of the EU average. Investment in infrastructure has been from both private sector and from the state-owned operator, but there is no universal access policy for high-speed (>30Mbps) broadband and no "state-aid" rules. The EU baseline contains this "Digital Agenda" target for 2020.

Penetration of broadband services in rural areas is still very low. The legal and regulatory framework in Moldova requires updating to include the latest ex-ante wholesale market and infrastructure enablers, co-ordination of civil works and simpler access to rights of way. Moldova has already used the EU Telecoms Rules model to create a competitive market for electronic communications and now the key challenge is to bring investment in high-speed broadband infrastructure to the rural areas. Full support should therefore be given to the required analysis and planning for universal high-speed broadband, with public and private sector involvement to select and implement the required investments.

Proposed pilot projects are presented in the detailed country descriptions for each priority area.

Ukraine

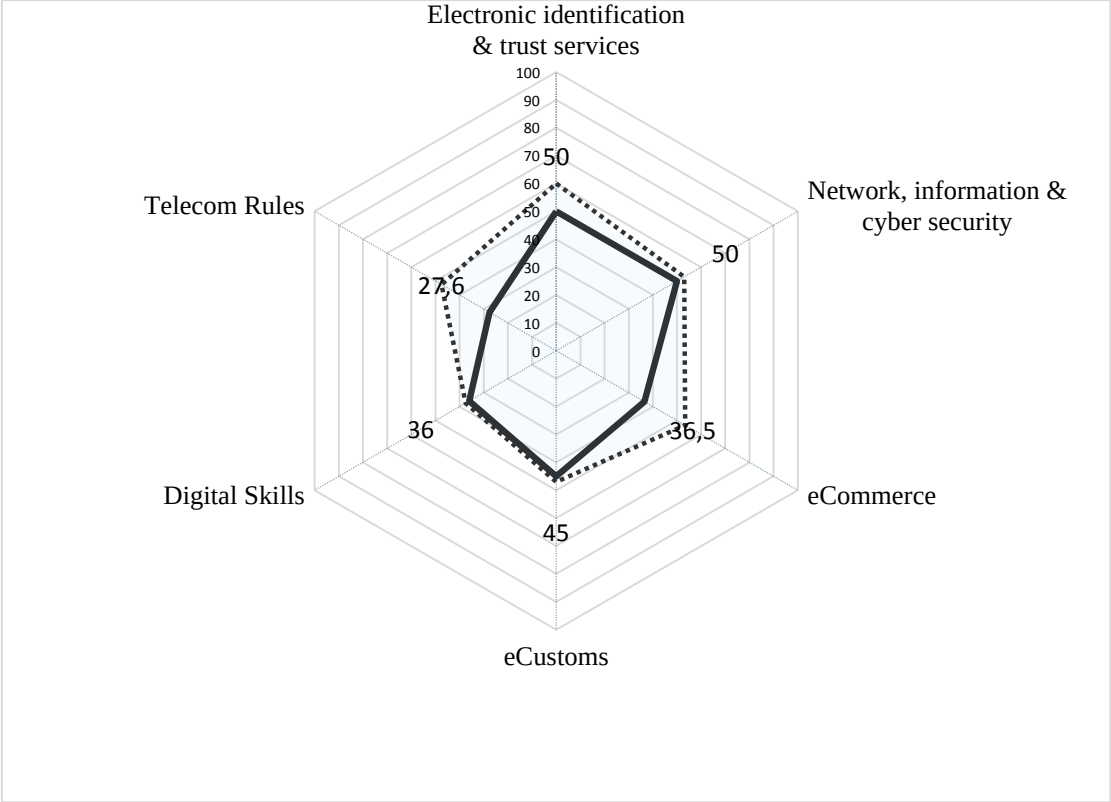

Exhibit 11 -HDM study findings on Ukraine's digital economy, focusing on 6 priority topics

(100% represents the EU baseline; the dotted / shaded area represents the Regional average)

While Ukraine's actual state of play in the area of **network, information and cyber security** is just above the EU average and close to the Region's average, the government leadership has been pro-active in adapting European principles and practices. There is a strong national CERT, well-developed and applied security standards, identified minimal security levels, open and free internet (the gaps are minimal in these areas). The weakest aspects include inadequate legal and regulatory frameworks defining the process of reporting on security incidents and breaches (including interaction with Telecom Regulator), vulnerable private sector critical infrastructure (its assessment and identification needs improvement), absence of a single national alert platform, lack of regular cyber attack simulations.

For **eCustoms** the score is close to the average for the Region. Progress has been made in the relevant legal framework and the eCustoms infrastructure. More work needs to be done, to obtain defined status of the authorised Economic Operator, uniform user management and limited usage of electronic signatures by government organisations, a national single window system, a registered exporters status and system and an anti-counterfeiting and anti-piracy system.

Ukraine's score in **eCommerce for SMEs** is below the average for the Region. While the country has achieved progress for instance on internet security and competition in eCommerce, more work needs to be done notably in the areas of eLogistics, ePayment and consumer rights protection. The priority aspects for specific follow-up actions are defining equal validity of electronic and offline contracts, defining the rights on delivery of goods, introducing equal treatment between paper and electronic invoices, limiting fees for the use of means of eCommerce payment, and setting up national trustmarks schemes for retail websites.

For **Digital skills**, Ukraine's score is close to the average for the Region. Action is required on increasing the awareness of the digital "skills gap" and developing a strong political will for prioritisation, co-ordination and support of relevant initiatives to promote digital skills and jobs.

For **Telecom Rules**, Ukraine scores much lower than the average for the Region. Broadband services penetration stands significantly below the average for the EU. Closing this significant "broadband gap" could add between €2.9Bn and €4.3Bn per annum to Ukraine's GDP. Harmonisation of spectrum exploitation would bring further economic benefits. This will require additional policies and Telecoms Rules that accelerate investments in high-speed broadband infrastructure, both in the private sector and using state-aid.

Proposed pilot projects are presented in the detailed country descriptions for each priority area.

2.1 Network, Information Security and Cyber-security

2.1.1 EU baseline

The core of the EU baseline in the field of NIS/Cyber-security consists of the following items:

EU Legislation/regulation:

- Articles 13a and 13b in page 55 of the Framework Directive
- Proposal for a DIRECTIVE concerning measures to ensure a high common level of network and information security across the Union - still under discussion with the European Parliament and the Council.
- Other relevant legal and regulatory acts (see below)

EU Agency (Institutions):

- European Union Network and Information Security Agency (ENISA) - current mandate is set out in Regulation 526/2013.

Most recent policy Communications:

- Cyber security strategy of the EU - Joint Communication JOIN(2013) 1
- Commission Communications on Critical Information Infrastructure Protection (CIIP): COM(2009) 149 and COM(2011) 163

The EU baseline is measured against 22 benchmarks:

- Leadership benchmark – Political will and commitment
- Policy benchmarks – International cooperation; Open and free internet; Capacity building
- Strategy benchmarks – Availability of a national strategy; National priorities and governing institutions
- Resources benchmark – Adequacy of resource base
- Implementation benchmarks – Cyber-attack simulations; Alert platforms, hotlines, public awareness; Cyber-security products and standards;
- Legal framework benchmarks – Regulatory and institutional environment; Minimal security levels; Management of security breaches; Transparency and openness;

Confidentiality of data and privacy protection; Attacks against information systems; Reporting on security incidents

- Infrastructure benchmarks – Understanding critical information infrastructure; Identifying critical information infrastructure; Private sector critical information infrastructures
- Services benchmarks – Services by Computer Emergency Response Team (CERT); Services to National Regulatory Authority (NRA)

Leadership, Policy, Legal Frameworks

- Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace (7/2/2013) and a Proposal for a Directive of the European Parliament and of the Council (part of a Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions of 7.2.2013) – setting out principles for cyber security; presenting the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks; demonstrating a clear mandate to ensure that the digital economy can safely grow and the European values of freedom and democracy are protected; defining measures to ensure a high common level of network and information security across the Union; proposing to establish legally binding common minimum requirements for NIS at a national level including the designation of national competent authorities for NIS, establishment of a well-functioning CERT, adoption of a national NIS strategy and a national NIS cooperation plan.
- Framework Directive (Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services) – establishes a common regulatory framework for the security and integrity of electronic communications networks and services.
- Directive on privacy and electronic communications (Directive 2002/58/EC) – enforces the personal data breach information and notification requirements for electronic communication services providers.
- Directive 2013/40/EU on attacks against information systems: Establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems, including through improved cooperation between judicial and other competent authorities to prevent such offences. The rules require that illegal

manipulation of and damage to information systems and computer data will be punishable as a criminal offence.

- Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the EU internal market: establishing minimum security requirements applicable to trust services
- Commission's Communication on Critical Information Infrastructure protection (CIIP) – defines policy measures and criteria for European critical information infrastructure to be prepared to prevent, detect, respond and mitigate disruptions, as well as to recover from them; makes international cooperation an integral part of the overall CIIP policy.
- Regulation No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) – empowers ENISA to carry out its tasks in the field of electronic communications and to contribute to an enhanced level of security of electronic communications as well as of privacy and personal data protection.
- The European Commission's proposal for a Directive of 2010 (COM (2010) 517 final) on attacks against information systems: aims to harmonise the criminalisation of specific types of conduct and further streamline the legal framework in the Member States in relation to the definition and punishment of certain cybercrime incidents (such as the creation, use and dissemination of cybercrime tools, the prosecution of illegal interception, the use of botnets, identity theft).
- Policy recommendations of the European Network and Information Security Agency (ENISA) – makes critical information infrastructure (CII) an integral part of a national social and economic policy agenda; helps empower CERTs with more authority to require telecom service providers and Internet Service Providers (ISPs) to implement security measures and changes; defines security measures and incident reporting procedures.

Strategy, Implementation, Resources

- Pillar III "Trust and Security of the Cyber security Strategy: enabling the implementation of policy and operational measures to:

(a) enhance cyber resilience of the EU's information systems, reduce cybercrime,

(b) strengthen EU international cyber-security policy and cyber defence,

(c) ensure a high common level of network and information security across the Union. Action 38: Member States to establish pan-European Computer Emergency Response Teams (CERTs); implementing Action 39 (Member States to carry out cyber-attack simulations), Action 40 (Member States to implement harmful content alert hotlines), Action 41 (Member States to set up national alert platforms).

- ENISA raising public awareness and developing public-private partnerships
- Europol, Eurojust and national data protection authorities have been active in raising awareness about cyber security
- Establishing CERT-EU to provide IT security services for EU institutions, agencies, bodies and implementing related projects
- All Member States have established and made operational national CERTs (best practices demonstrated by Finland, Portugal, and Belgium).
- Almost all Member States have carried out cyber-attack simulations, fully implemented hotlines and organised awareness raising campaigns on online safety for children (best practices demonstrated by Latvia. Luxemburg and UK)
- Over 50% of Member States have set up national alert platforms as one-stop-shops for the public which can play an active role in reporting illicit online activity and to collect statistics on alerts. Thus these platforms help to track the development of cybercrime at national level (best practices demonstrated by Luxemburg and Belgium).
- ENISA recommendations "Baseline Capabilities of National/Governmental CERTs": establishing an integrated risk management process for identifying and prioritising protective measures in cyber-security.
- Assessing and periodically reassessing the current state of cyber-security efforts and the development of programme priorities.
- ENISA's guidelines for the implementation of the security measures laid down in the EU telecom framework directive: Develop security measures and report on security incidents.

Infrastructures

- Commission's communications on Critical Information Infrastructure Protection (CIIP)[11]: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (2009) and "Achievements and next steps: towards global cyber-security" (2011), the European Parliament Resolution of 12 June 2012 on "Critical Information Infrastructure Protection: towards global cyber-security", and ENISA recommendations "Baseline Capabilities of National/Governmental CERTs": addressing all key aspects concerning the protection of Europe from cyber disruptions by enhancing security and resilience of critical information infrastructures.
- Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection (EPCIP) [COM (2006) 786 final – Official Journal C 126 of 7.6.2007]: aimed at both European and national infrastructure. Described a procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure. Also contained measures designed to facilitate the implementation of EPCIP, including an EPCIP action plan, the Critical Infrastructure Warning Information Network (CIWIN), the setting up of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes, and the identification and analysis of interdependencies. Support for EU Member States regarding their National Critical Infrastructures (NCIs) and related contingency planning also was envisaged by EPCIP.
- The European Commission staff working document of 2012 on the review of the European Programme for Critical Infrastructure Protection (EPCIP): presents the main preliminary findings of the review of the European Programme for Critical Infrastructure Protection (EPCIP) and in particular Directive 2008/114/EC on the identification and designation of European Critical Infrastructures.
- Council Directive 2008/114/EC on European critical infrastructures and their protection:

[11] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167

identifying and designating European critical infrastructures (ECIs) through a common assessment approach (especially in sectors with possible high casualties and economic and public effects such as energy and transport).

Services

- Computer Emergency Response Team (CERT-EU): providing IT security services for EU institutions, agencies, bodies including implementation of related projects and initiatives to ensure the coordinated approach to the application of such services.
- ENISA (European Network and Information Security Agency): providing services to improve capabilities of National/Governmental CERTs; encourages them provide additional services and demonstrate added value to their constituents by:

  (a) preparing national campaigns to raise awareness on cyber-security topics,

  (b) organising national cyber-security exercises together with relevant stakeholders,

  (c) identifying best practices, developing templates to comply with data protection regulations to empower CERTs with more authority to ensure that telecom service providers and ISPs implement security measures and changes,

  (d) guiding National Regulatory Authorities (NRAs) about reporting of significant incidents.

Box 1*:* Developing Cyber Security Strategies – ENISA Good Practice Guide on National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace.

The European Network and Information Security Agency (ENISA) is an EU body created to advance the functioning of the internal market by giving advice and recommendations and acting as a switchboard of information for good practices in network and information security. Several EU Member States have developed or are in the process of developing their national Cyber Security Strategies. Strategies of countries such as Estonia, Finland, and Slovakia, view Cyber Security from a socio-economic perspective in the broader context of information society development, with a focus on prevention, readiness and cooperation among major

stakeholders. Some other countries – e.g. the Czech Republic, France, and Germany, pay special attention to data integrity and confidentiality, while France stresses both the technical means needed to protect the security of information systems and fight against cybercrime and the establishment of cyber-defence.

The ENISA 'Practical Guide on Development and Execution' for National Cyber Security Strategies (2012) defines the strategy lifecycle, explains how to set the vision, scope, objectives and priorities; how to apply a risk assessment approach, identify and engage key stakeholders, and establish a clear governance strategies. Special emphasis is placed on the importance of public-private partnership and on striking the balance between security and privacy.

Source: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper; http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide .

Box 2: Lessons learned from cooperation between CERTs and law enforcement agencies.

In 2012, the European Network and Information Security Agency (ENISA) looked at key lessons learned from cooperation between Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) and law enforcement agencies (in the context of the Directive on attacks against information systems).The following three lessons can be learned from the study.

Lesson 1: Implementing legislation should be clear and explicit, and include clear carve-outs of the applicability of the provision for the normal activities of CERTs, academic institutions, researchers, network operators and security service professionals, and any actions undertaken should come from a lawful request of businesses, governments and end-users.

Lesson 2: There are limitations to the solutions based on legislation alone as the actual practice is always richer than abstract possibilities that might occur someday. Lawmakers or prosecutors are not able to define all the details through law or interpretative frameworks. Local expert communities should develop their own guidelines and recommendations on how to implement the law. That would help judges to identify workable criteria in relation to real-life cases at hand.

Lesson 3: Stronger security should include "economic incentivisation" in relation to the

responsibility and liability of service providers, e.g. operators of websites which run outdated software with known security vulnerabilities. Irrespective of technical awareness of the website operator, they should at least have some responsibility for choosing/maintaining/functioning unsecure systems. The owners of breached systems should be better motivated to implement proper security practices.

Source: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems

2.1.2 Overview of the state of play and gap analysis for the Region

The importance of network, information and Cyber Security (NIS) has grown rapidly worldwide reflecting upon the accelerated proliferation of digital information and communication technologies, especially the internet. To respond to this challenge, the European Union has undertaken a number of measures over the past several years culminating in the adoption in 2013 of the European Cyber Security Strategy: An Open, Safe and Secure cyberspace[12]. The Strategy proposed a new Directive to ensure a high common level of network and information security across the Union. The Strategy acknowledged that information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport. Many business models are now built on the uninterrupted availability of the Internet and the smooth functioning of information systems. It is estimated that the Digital Single Market will add as much as €1,000 per person to GDP. Citizens, organisations, and governments should trust information and communications technologies for economies to prosper. People want to be confident that their privacy and freedoms are protected.

The Region treats information and especially cyber-security seriously and all the countries have passed relevant laws and implemented other measures. Five countries (excluding Belarus)

[12] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

have signed and ratified the Council of Europe Convention on Cybercrime[13]. Protection of information, data, networks and entire infrastructures from internal and external threats has become a policy priority. Yet the Region lags substantially behind the EU baseline, as shown in the exhibits below.

Exhibit 12 demonstrates the existing gaps in relation to the EU baseline across main benchmark groups. Overall, there is a relatively sufficient legal certainty in NIS complemented by dedicated strategic plans and functioning infrastructures. The best progress is observed in policy and leadership, while the benchmarks reflecting the effectiveness of undertaken measures (implementation results, existing services and availability of adequate resources) reveal larger gaps.

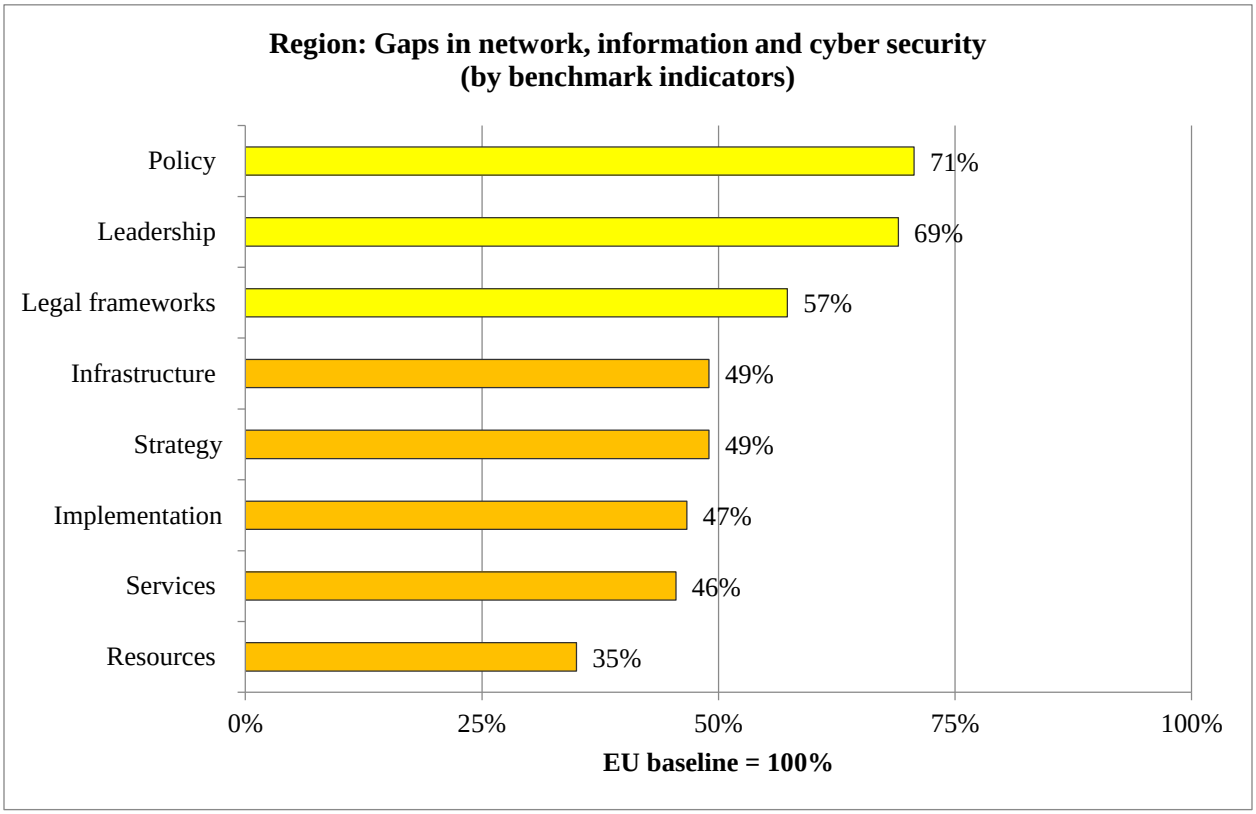

Exhibit 12 - State of play of the Region in network, information and cyber security (NIS) (by benchmark

[13] Open for signature since 23 November 2001 by the member and non-member States which have participated in its elaboration and for accession by other non-member States http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

indicators)

Exhibit 13 gives a more detailed picture by describing the status of each of the 22 individual benchmarks. The largest gaps are: absence of dedicated national cyber-security strategies, lack of services provided to National Regulatory Authority (NRA), inadequate resources allocated by governments to manage security threats, lack of laws and regulations ensuring that there is sufficient transparency and openness in reporting on security breaches and existing vulnerabilities of the private sector (critical) infrastructures. Also, most countries do not practise cyber-attack simulations on a regular basis, run alert platforms and hotlines for both experts and the general public.

The Region demonstrates strong political will to address NIS, including willingness to cooperate internationally. Whereas internet openness and confidentiality of personal data and privacy is protected by law, often the legal base is insufficiently represented by several different (and not infrequently) older laws, although this varies across the Region.

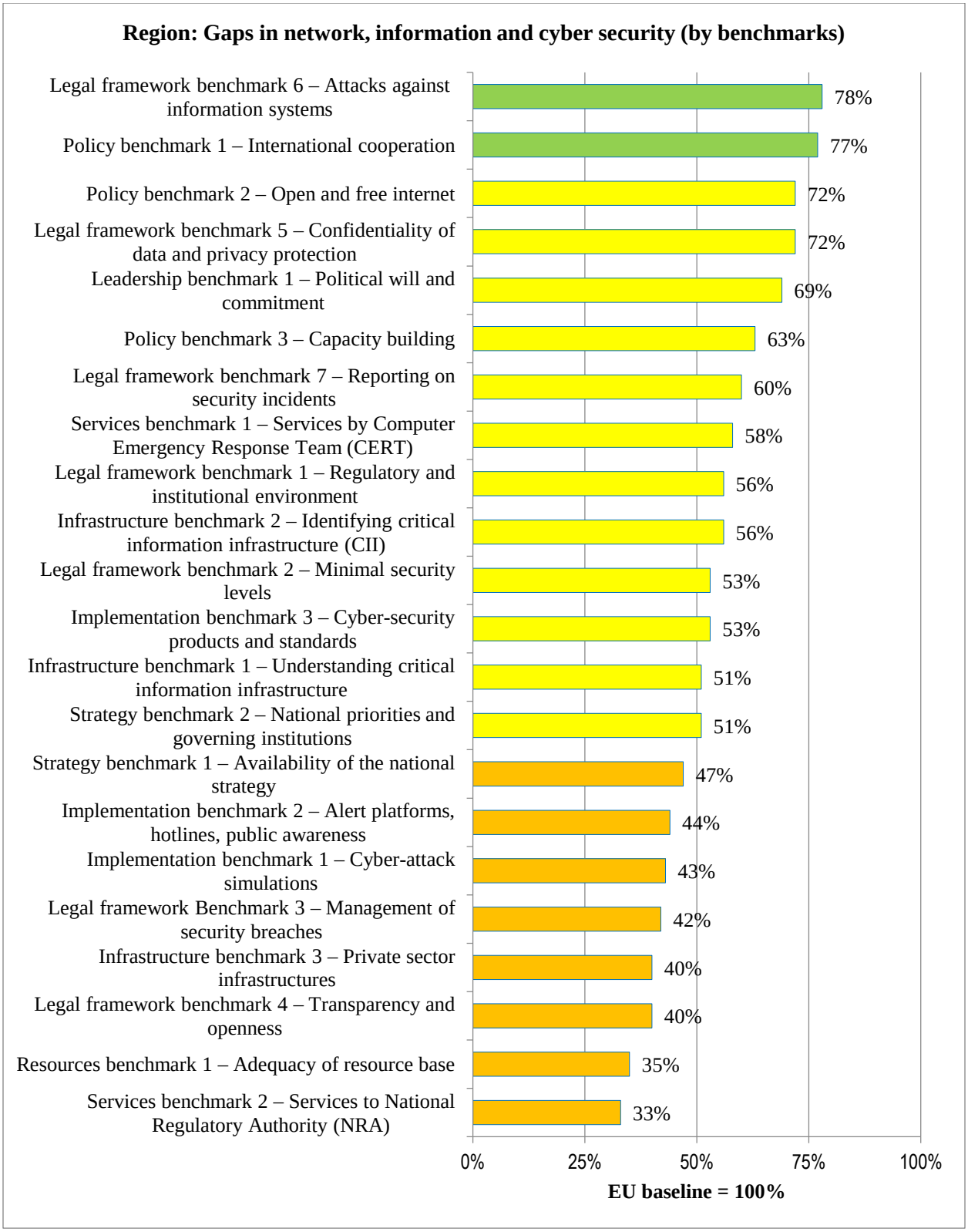

Exhibit 13- State of play of the Region in network, information and cyber security (NIS) priority area (by

benchmarks)

2.1.3 Overview of common actions for the Region

The following areas can be considered as common for the entire Region:

Leadership, Policy, Legal Frameworks

- Harmonisation of legislation and regulations with European standards in:

  (a) protecting personal data/online privacy,

  (b) confidentiality of electronic data,

  (c) Cyber Security policies.

- Ensuring strong leadership

Strategy, Implementation, Resources

- Ensuring transparency in reporting on security breaches and incidents
- Undertaking cyber attack simulations
- Raising public awareness about Cyber Security risks
- Development and implementation of national cyber strategies
- Identification of Critical Information Infrastructure including in the private sector
- Development of network, information and Cyber Security standards and products
- Ensuring internet openness
- Building capacities of national/government CERTS

Services

- Expansion of CERT services including to NRA; training CERT staff with ENISA's help

2.1.4 Benefits for and readiness analysis of the Region

Benefits of the Partner Countries from harmonisation with the EU

Closer harmonisation with the EU in the area of network, information and Cyber Security presents many benefits (as exemplified by Georgia). Cyber-attacks are borderless and require close cooperation between countries to protect their critical infrastructures, services and

increasingly citizens' well-being. All the countries of the Region already cooperate – although to a different degree – with the EU's institutions and bodies, in addition to collaboration with one another bilaterally and with international institutions.

While there are clear technological benefits, the Region is already quite strong on technically, using the latest software solutions. For example, Ukraine and Belarus produce home-grown cryptographic solutions in line with high international standards. The EU Association Agreement countries (Georgia, Moldova and Ukraine) are increasingly pro-active in learning from EU experiences, especially in the field of legal frameworks, and capacity building to replicate good practices including via cooperation with CERT-EU. Training courses offered by ENISA represent a particularly valuable asset in this regard. However, it is not necessarily easy to benefit from these cooperation opportunities (as reported by some countries which sometimes find it difficult to get access to such courses). This is a manifestation of a bigger challenge of access to the vast knowledge and competencies accumulated by the EU and individual Member States and institutions (national/government CERTs, for example). At the moment, there is no clear mechanism of tapping to such knowledge. Successful harmonisation would mean also getting benefits from effective knowledge sharing. Creating and putting into practice an on-demand knowledge exchange facility would be beneficial for the Region, which could choose from available options to meet specific needs.

There are numerous economic benefits that follow the mutual recognition of national trust services. These arise from an increase in the level of security of the exchanged information and documents across borders, thus generating significant economic gains for both the EU and the Region. As Belarus proposes, for example, this could be done via harmonising the national systems of accreditation of security (and cryptographic) solutions with best international standards. That would be the first step towards the mutual recognition of accreditation activities based on the principles of the Trusted Third Party (T3P) system to recognise digital signatures from the Region in the EU. Such a scheme is expected to become operational among the members of the Eurasian Economic Union (Armenia and Belarus). Creating a mechanism of developing bilateral agreements with particular EU countries might be another vehicle of harmonisation for mutual benefits depending on specific country contexts and needs.

Benefits from harmonisation between the Partner Countries

The benefits for the Partner Countries are not obvious (although it is assumed that they lie in the area of trade), except for the members of Eurasian Economic Union (EEU) whose members are expected to benefit in the future from an integrated system of cross-border exchange of legally binding electronic documents based on the Trusted Third Party services[14]. Linking the EEU and the EU system via T3P system, as proposed above, could be a mutually acceptable solution.

Conditions for the harmonisation of digital markets

The conditions for harmonisation include the current state of play in each Partner Country and future strategies (which are often closely linked to current progress and conditions). However, within the Region there are differences in the approaches towards handling NIS. While the EU Association Agreement (AA) countries have the policy of applying the European standards, norms and practices, the EEU countries rely either on their own national solutions or develop common approaches (as described above). It is believed that one approach should not exclude the other and compromises can be made.

The Region shares common problems and challenges that need to be addressed in order to create a level playing field with the EU to make stronger progress in NIS. The most typical challenges and tasks include the following:

- Get the legal basis right as a first step by establishing an enabling regulatory environment compatible with the European Cyber Security Strategy which would include the minimal level of requirements in relation to NIS, especially in the field of critical information infrastructure. At the moment the Region has a mix of (older) legacy and new laws/regulations that need to be streamlined and consolidated (assuming that having fewer good laws is better than having a fragmented legal basis consisting of several legal acts and secondary regulations).

[14] Decision of the Eurasian Economic Commission's decision №180 of 30 September 2014 On the order of keeping and exchanging electronic documents and data among the members of the Customs Union for foreign trade and a Decision of № 154 of 1 September 2014 on a Concept of using services and legally binding electronic documents in interstate information interactions.

- Establish effective multilateral cooperation mechanisms and channels of information exchange in the field of cybercrime. Five of the six Partner Countries have signed the Cybercrime Convention and accordingly aligned national legislation creates such opportunities.
- Develop and pass, where feasible, a dedicated, stand-alone national Cyber Security Strategy, which is a good European practice.
- Although the Region demonstrates a generally strong leadership to deal with NIS challenges, it is vital to continue maintaining sufficient political will for stronger progress in bridging the gaps with the EU.
- Empower national CERTs by building their capacities and expanding their competencies so that they are able to provide valuable services to other organisations; while CERTs are available, their competencies and resources are still limited.
- Establish alert-platforms and hotlines to seek the public's feedback, run regular cyber-attack simulations.
- Ensure greater transparency in reporting on NIS risks, incidents and breaches when the disclosure of such information is in the public interest.
- Guarantee confidentiality of personal data and privacy by passing a dedicated law on the protection of personal data in those Partner Countries that do not have such a law. Assistance in law drafting will be essential.
- Define, assess and specify critical information infrastructures, including in the private sector

Thanks to the EU support and cooperation initiatives, the Region has been successful in making Europe's physical borders safer over the past decade. The power of the internet lies in the lack of national frontiers in the borderless virtual world. The objective is to maintain a free and open internet for all regardless of official borders. From now on the cooperation between the EU and the Region in the field of cybercrime cannot be overestimated and will have a long-lasting impact on the internet and openness in general and Europe's economic growth in particular, as far as the DSM is concerned.

Impact of the EEU membership on the HDM with the EU

The expected impact from the enhanced harmonisation can be felt first of all in the improved economic opportunities thanks to the expanded cross-border trade and the creation of a level playing field with the EU. That may happen under condition of the mutual recognition of accreditation activities and interoperable digital signatures realised at the required security level. Political benefits might be significant as well, especially for civil society, provided that a secure and safe internet is also free and open.

2.1.5 Armenia

State of play and gap analysis

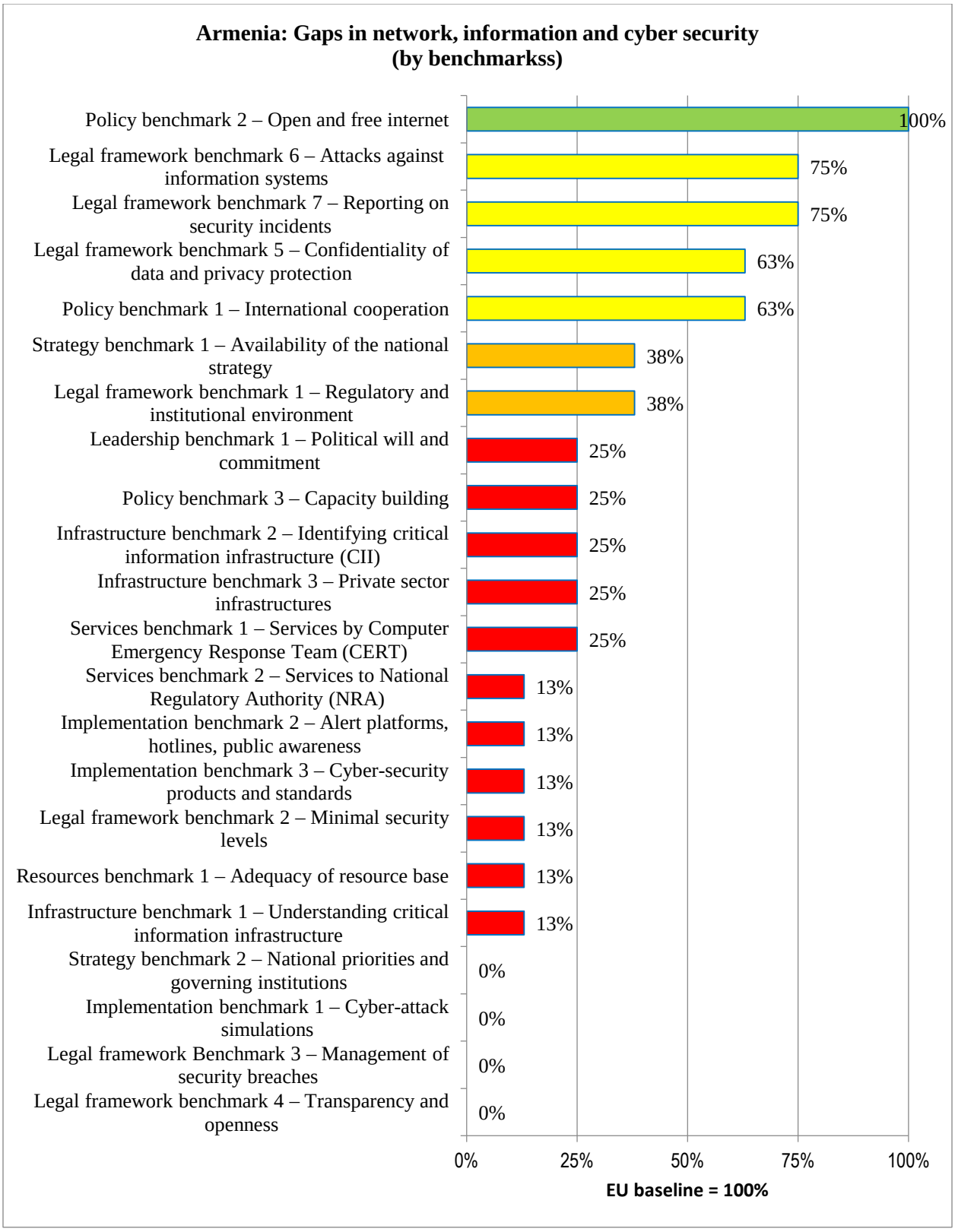

Exhibit 14- State of play and gap analysis of Armenia in NIS priority area

Armenia is the only Partner Country that has not established its government Computer Emergency Response Team CERT) although it joined the Cyber Crime Convention in 2001 and ratified it in 2006. Most of the initiatives undertaken so far relate to the Cybercrime Convention. Joining the Convention has prompted positive changes to the Civil Code to fully comply with the requirements of the Convention. All the legal requirements expressed by the Convention are included in the national legislation but the enforcement of the regulations is weak. There is a new draft law on personal data protection that addresses some key security-related issues in line with European standards.

The government's current approach distinguishes between security of networks and infrastructures, on the one hand, and information content, on the other. The first domain is supervised by the National Security Service, while the second one is under the Centre on Public Relations and Information. Technically, the government websites and internal networks are protected adequately.

There is a lot to be done to narrow the gap by passing a national cyber-security strategy, developing procedures for reporting on security incidents in an open and transparent manner, defining minimal security levels, and regularly practising cyber-attack simulations. The internet in Armenia is free and open.

Leadership, Policy, Legal Frameworks

Achievements

Availability of:

- Ratified CoE Cybercrime Convention
- Law on Personal Data
- Civil Code is fully aligned with the CoE Cybercrime Convention
- Draft Law on the Protection of Personal Data submitted to the Parliament and is fully in line with European standards
- Developed concept on IT Security
- Reporting on security incidents is regulated by the new Personal Data Protection law bill

Gaps

A need for:

- Cyber security law
- Clear and effective policies governing private sector critical information infrastructures
- Better protection of personal data and privacy
- More effective inter-agency cooperation and coordination
- Clarifying the role of the National Regulatory Authority in the field of NIS

Strategy, Implementation, Resources

Achievements

Availability of:

- Free and open internet (defamation and similar communications in social networks are not classified as criminal acts in Armenia as required by the CoE Cybercrime Convention)
- Existence of the internet governance forum and active civil society

Gaps

A need for:

- Government/national CERT
- National Cyber Security Strategy
- More effective enforcement of NIS-related laws and regulations
- Better public awareness raising, alert platforms, hotlines
- Stronger transparency and openness in reporting on security incidents
- Stronger leadership

Infrastructures

Achievements

Availability of:

- Well protected government information systems, communication networks and infrastructures websites including content.
- Well protected banking system from security threats

Gaps

A need for:

- NIS-related standards
- Security requirements for Trust Service providers
- Inclusion of the private sector critical infrastructures

Services

Achievements

Availability of:

- Non-governmental CERT is certified as a Trusted Introducer

Gaps

A need for:

- Cyber attack simulation services
- CERT's services to NRA

HDM roadmap

Leadership, Policy, Legal Frameworks

- Update and enforce existing and planned laws/regulations approximated with European standards. Develop, publicly discuss and approve national Cyber security strategy aligned with the European Cyber security strategy

- Raise the level of legal certainty and clarify definitions pertaining to the network, information and Cyber Security domain according to European standards (e.g. striking a balance between security and regulation of the internet)
- Improve enforcement effectiveness of legal and regulatory frameworks in NIS
- Create and operationalise a national/government CERT; ensure its adequate legal certainty and state funding
- Improve legal certainty and overall regulation level in network, information and cyber security
- Ensure that a new law on Personal Data Protection is in line with European standards
- Ensure sufficient legal certainty needed to empower competent NRA to manage and coordinate security incidents among public and private entities
- Ensure greater legal certainty in relation to reporting on security incidents and breaches
- Raise levels of legal certainty and develop procedures on reporting on security incidents in an open and transparent manner
- Ensure a high level of political will, leadership and commitment

Strategy, Implementation, Resources

- Improve enforcement effectiveness of legal and regulatory frameworks in NIS
- Create and operationalise a national/government CERT; ensure its adequate legal certainty and state funding
- Raise transparency of cyber-attack simulation
- Define clearly the role of the future government/national CERT (in light of the existence of the NGO-based CERT)
- Ensure sustainable financing of the government/national CERT from the state budget
- Start regular cyber-attack simulation activities; improve transparency

- Create dedicated hotlines and alert platforms (in addition to CERT information dissemination services)
- Consider expanding CERT services to provide services beyond the state sector
- Expand CERT cooperation with CERT-EU
- Run regularly and improve effectiveness of alert platforms/ hotlines
- Regularly undertake public awareness campaigns
- Deepen the dialogue with key actors/stakeholders on Cyber Security issues
- Practise new forms of engagement and participation of key stakeholders to raise transparency levels
- Regularly practise and improve performance and transparency of cyber attack simulations
- Practise new forms of engaging key actors in cyber attack simulation
- Develop and apply regulatory provisions governing the disclosure of information on security breaches of public importance
- Develop and apply dedicated regulatory provisions governing management and coordination of security incident with ISPs and providers of public electronic communication.
- Improve policies and practices on minimal security levels
- Improve policies to ensure regular update of standards for cyber-security products
- Expand and improve policies for greater effectiveness of international cooperation
- Maintain the adequacy of resource base
- Set up a capacity building plan for Cyber Security including for the future national/government CERT

Infrastructures

- Improve criteria to better understand and assess critical information infrastructures

- Decide how to handle the private sector infrastructures
- Define and apply procedures to include critical infrastructures owned/operated by private sector
- Analyse conditions, establish criteria and define CIIs (include relevant provisions into the future national Cyber security strategy)

Services

- Launch and intensify training and educational services in cooperation with ENISA
- Expand CERT's services to expert and business community, the general public, NRA

Conditions for harmonisation

The key conditions for harmonisation are as follows:

- An enabling legal and regulatory framework in general approximated with European standards as much as possible.
- Formulation and adoption of a national Cyber Security Strategy based on the principles of the European Cyber Security strategy.
- Defining minimal security levels.
- Establishment of the national/government CERT
- Strengthening the capacities of the government CERT and expanding its services.
- Ensuring strong leadership.
- Maintaining free and open internet while making it safe.
- Protection of personal data and privacy online.
- Identification and protection of critical information infrastructures.
- Pro-active public awareness raising and education.

Pilot Projects

It is recommended that Armenia joins all three proposed regional projects in the field of Network, information and cyber security, namely:

[1] Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation;

[2] Policy support to confidentiality of data processing, protection of personal data and online privacy;

[3] Capacity building plan for national/government CERTs, including through cooperation with ENISA.

2.1.6 Azerbaijan

State of play and gap analysis

Azerbaijn: Gaps in network, information and cyber security (by benchmarks)

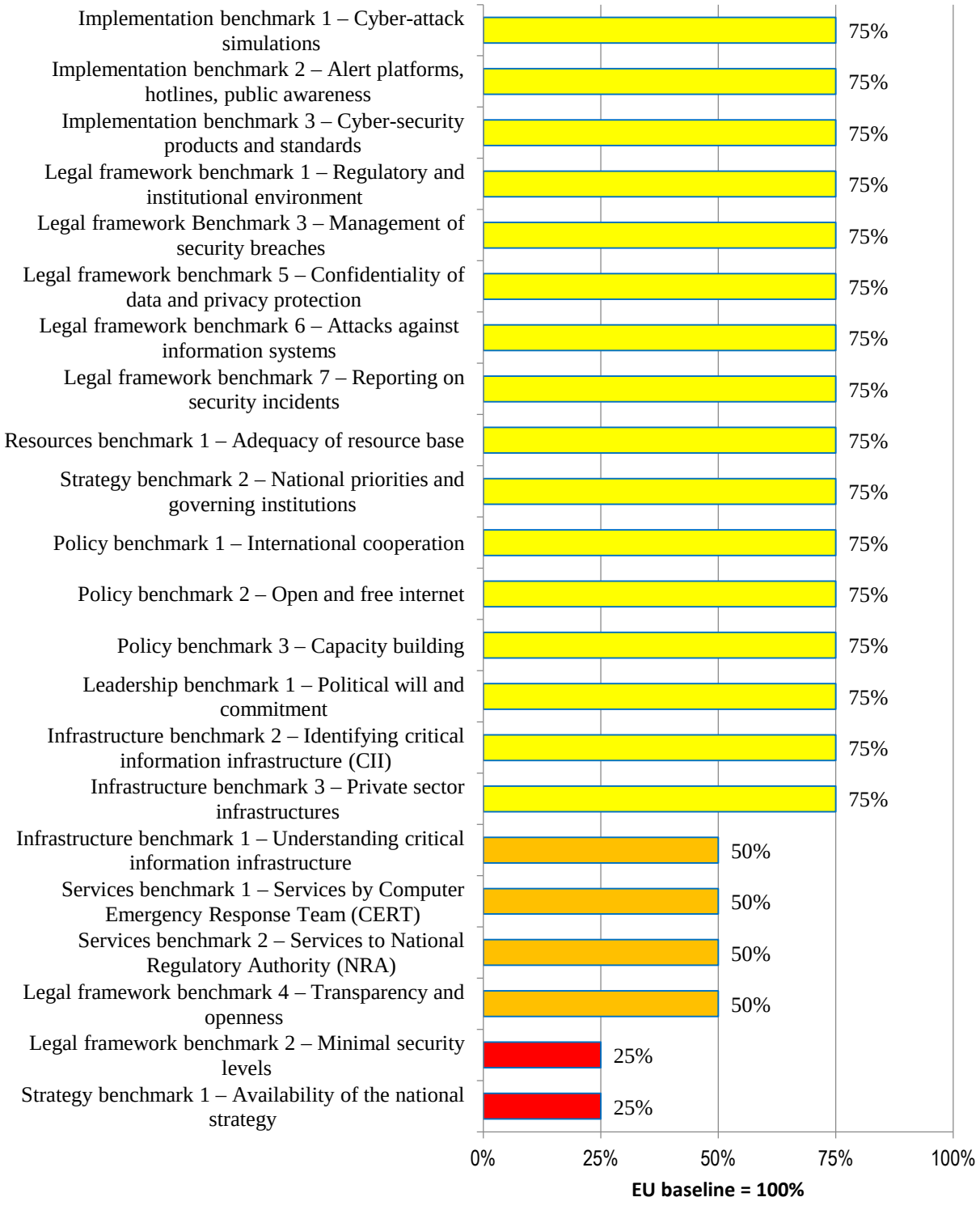

Exhibit 15 - State of play and gap analysis of Azerbaijan in NIS priority area

The government of Azerbaijan has been pro-active in addressing the growing number of network, information and Cyber Security challenges. After joining to Convention on Cybercrime in 2010, the legislative framework on combating cybercrime has been adapted to the requirements of the Convention. Appropriate changes have been made to the Criminal Code. Two Presidential Decrees (on the National Security Concept and the National Strategy for development of information society for 2014-2020) have created the necessary legal and institutional conditions for better regulation of the NIS area by establishing a Special Communication and Information Security State Agency (under the Special State Protection Service, CERT.GOV.AZ) and Cyber Security Centre (under the Ministry of Communication and High Technologies, CERT.AZ) as two key state bodies responsible for NIS supervision. In addition, there is a Computer Security Incident Group of Azerbaijan National Academy of Sciences (AzScienceCERT) that provides valuable services to a broad range of partners. The government of Azerbaijan sees many benefits in cooperation with the EU. As many as 14 national standards in the sphere of information are already identical to the existing international standards.

The largest gap with the EU baseline is observed for the benchmarks describing the availability of strategic documents that spell out priorities and actions. The Cyber Security Centre of the Ministry of Communication and High Technologies has already identified sectors with critically important information infrastructures. The lack of human resource capacity and the persistent challenge of ensuring greater transparency in security management reveal significant gaps as well. Lack of regular training is another barrier to overcome. To do so, the country needs a comprehensive national Cyber Security Strategy to specify minimal security levels, define clear rules for reporting and disclosure in security risks and further enhance institutional, administrative, technical and human resources capacities. There is also a need for a dedicated policy on cooperation with foreign CERTs and other counterparts, especially on cyber-attack simulations. The issue of stronger engagement with the public and industry demands investigation and support. The country would benefit from clearer guidance for evaluating the compliance of public telecommunications networks and service providers with existing legal requirements. It is paramount to ensure that the internet is both open and safe.

Leadership, Policy, Legal Frameworks

Achievements

Availability of:

- Ratified CoE Cybercrime Convention
- Three key agencies dealing with NIS issues: government CERT.GOV.AZ under Special Communication and Information Security State Agency; Cyber Security Centre (CERT.AZ) under the Ministry of Communication and High Technologies (established by Presidential Decree No 708 of 26.09.2012); Computer Security Incident Group of Azerbaijan National Academy of Sciences (AzScienceCERT)
- Effective inter-agency coordination
- Pro-active Cyber Security Centre (CERT-AZ) undertaking training and awareness raising activities, reporting on security incidents, participating in international cooperation, establishing a network of Cybercrime Centres of Excellence
- Key laws on: Individual data; Information provision; Telecommunication; e-Signature/e-Document; Information and informatisation
- National Strategy for Development of Information Society in the Republic of Azerbaijan for 2014-2020 includes components aimed at educating population and private organizations on cyber security, nurturing information security culture, and developing professional competencies
- Identified strategic priorities focused on developing the industrial and technological resources for cyber-security, reducing cybercrime, formulating Cyber Security policy, and supporting existing government CERT

Gaps

A need for:

- Cyber security law
- Greater legal clarity about the role of the National Regulatory Authority
- Clear and effective policies governing the security private sector critical information infrastructures

- More effective protection of personal data and privacy online through laws and regulations

Strategy, Implementation, Resources

Achievements

Availability of:

- Robust inter-agency cooperation and coordination
- State funding for CERTs

Gaps

A need for:

- National Cyber Security Strategy
- Strengthening capacities and resources of CERTs
- Effective enforcement of NIS-related laws and regulations
- Protection of personal data and privacy online in practice
- Clarification of the role of the National Regulatory Authority
- Procedures and principles for reporting on security incidents, public awareness raising, alert platforms, hotlines
- Stronger enforcement of transparency and openness in NIS-related matters
- Regular cyber-attack simulation
- Ensuring open and free internet
- Reporting on security incidents, public awareness raising, alert platforms, hotlines
- Better public awareness about alert platforms, hotlines

Infrastructures

Gaps

A need for:

- Developing NIS-related standards
- Security requirements for Trust Service providers
- Inclusion of the private sector critical infrastructures

Services

Achievements

Availability of:

- Non-governmental CERT is certified as a Trusted Introducer

Gaps

A need for:

- Cyber attack simulation services
- CERT's services to NRA

HDM roadmap

Leadership, Policy, Legal Frameworks

- Raise legal certainty and clarify definitions pertaining to the network, information and Cyber Security according to European standards
- Approximate as much as possible key legal and regulatory frameworks with European standards including those on Privacy and Personal Data Protection
- Ensure sufficient legal certainty needed to empower competent NRA to manage and coordinate security incidents in cooperation with public and private entities
- Raise levels of legal certainty and develop procedures on reporting on security incidents in an open and transparent manner
- Continue maintaining a high level of political will, leadership and commitment

- Develop and apply regulatory provisions governing the disclosure of information on security breaches of public importance
- Develop and apply dedicated regulatory provisions governing management and coordination of security incident with ISPs and providers of public electronic communication services.

Strategy, Implementation, Resources

- Formulate and approve a national Cyber security strategy approximated with the European Cyber security strategy
- Improve policies ensuring regular update of standards for cyber-security products aligned with best European and international standards
- Examine and use best international practices in creating effective legal/regulatory frameworks and in the field of cyber attacks
- Improve enforcement effectiveness of legal and regulatory frameworks in NIS
- Further develop capacities and competencies of the government CERT; ensure its adequate funding
- Strike a balance between internet security, regulation and openness
- Regularly practise and ensure high level transparency of cyber-attack simulations
- Improve effectiveness and outreach of existing and new hotlines and alert platforms (in addition to CERT information dissemination services)
- Consider expanding CERT services to provide services beyond the state sector
- Expand cooperation with CERT-EU
- Continue regular public awareness campaigns
- Launch and intensify training and educational activities in cooperation with ENISA
- Deepen the dialogue with key actors/stakeholders on Cyber Security issues
- Practise new forms of engaging key actors in Cyber Security including in cyber-attack simulation

- Improve policies and practices on minimal security levels
- Expand and improve policies for greater effectiveness of international cooperation
- Set up a capacity building plan for Cyber Security including for the government CERT

Infrastructures

- Develop guidelines for end-users regarding vulnerabilities of soft- and hardware
- Analyse conditions, establish criteria and define CIIs (include relevant provisions into the future national Cyber security strategy)
- Decide how to handle the private sector infrastructures
- Define and apply procedures to include critical infrastructures owned/operated by the private sector

Services

- Launch and intensify training and educational services in cooperation with ENISA
- Expand CERT's services to the expert and business community, the general public, and the NRA

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Creation of an enabling legal and regulatory framework in general approximated with European standards as much as possible.
- Formulation and adoption of a national Cyber Security Strategy based on the principles of the European Cyber Security Strategy.
- Defining minimal security levels.
- Strengthening capacities of the government CERT and expanding its services.
- Maintaining strong leadership.

- Maintaining free and open internet while making it safe.
- Protection of personal data and privacy online.
- Identification and protection of critical information infrastructures.
- Pro-active public awareness raising and education.

Pilot Projects

It is recommended that Azerbaijan joins all three proposed regional projects in the field of Network, information and cyber security, namely:

[1] Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation;

[2] Policy support to confidentiality of data processing, protection of personal data and online privacy;

[3] Capacity building plan for national/government CERTs, including through cooperation with ENISA.

2.1.7 Belarus

State of play and gap analysis

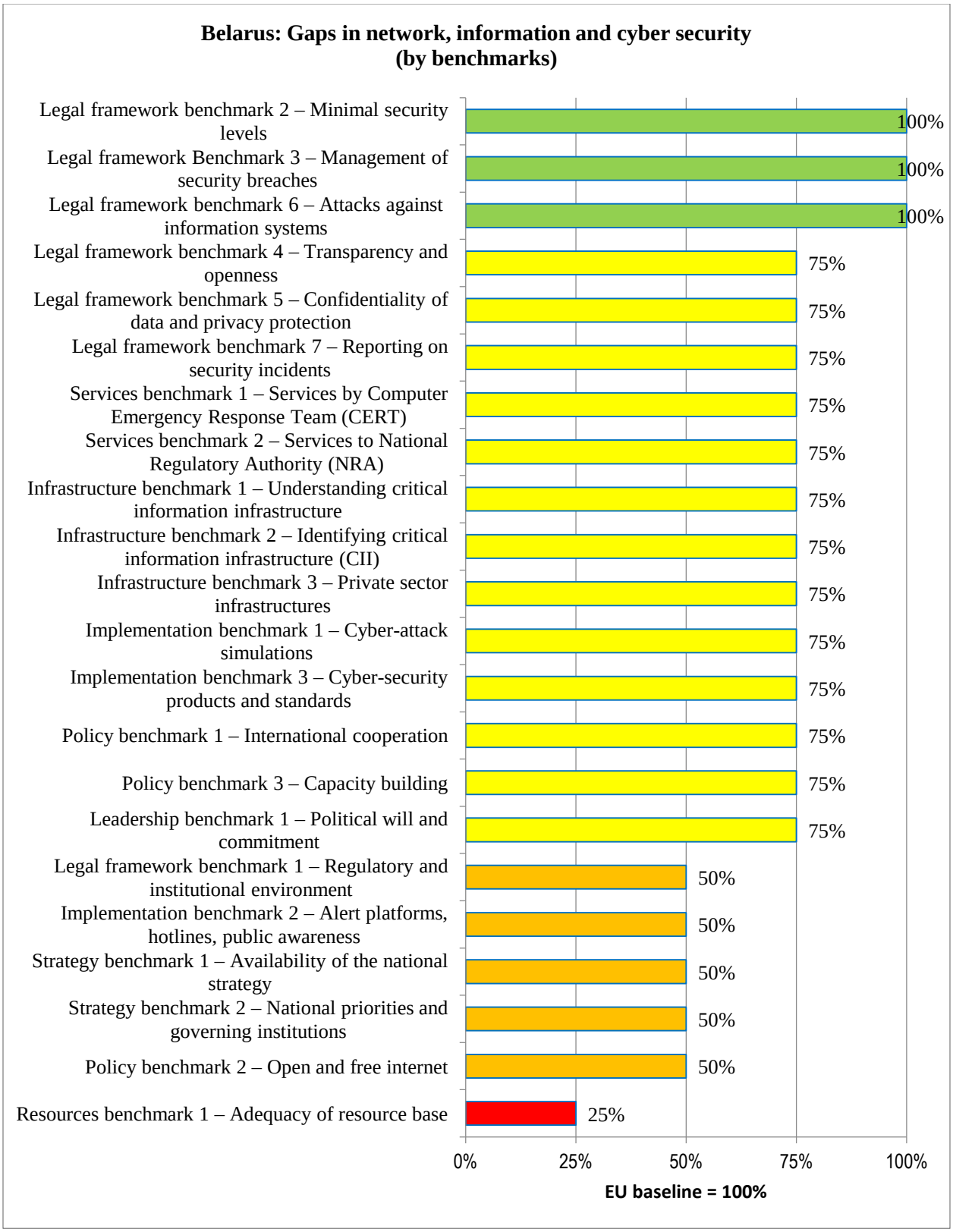

Exhibit 16 - State of play and gap analysis of Belarus in NIS priority area

While Belarus is the only Partner Country that has not joined the Convention on Cybercrime, it is ready to do so. The country's NIS-related legislative and regulatory framework is diverse and complex in an attempt to respond to many disparate challenges. There is a clear division of responsibilities between government agencies underpinned by strong inter-agency coordination. The country is open to cooperation with the EU in the field of network, information and Cyber Security by concluding bilateral agreements to exchange electronic signatures and documents in a secure way. There is a plan to pass a single dedicated law on personal data protection which would explicitly determine the requirements to protect personal data more effectively than it is done at present through a number of disparate legal acts and would take into account latest technological developments and international experience. There is a strong economic incentive to pass such a law due to the growing size of the national digital market and services that require trust in existing security measures to guarantee the protection of personal data and privacy online. Acceding the Cybercrime Convention will help better align national legislation with international standards, whereas formulating and implementing a national Cyber Security Strategy will help better define priorities and undertake actions in a more comprehensive and effective way. Such challenges include running effective and trustworthy alert platforms and hotlines, enhancing the NIS-related resource base, better balancing internet openness with safety and security, and providing new CERT services.

Leadership, Policy, Legal Frameworks

Achievements

Availability of:

- Extensive and complex legal basis that includes: Presidential Decree of1 February 2010 No 60 On Measures to Improve the Use of the National Segment of the Internet includes requirements to protect public sector information; Resolution of the Ministry of Communications and Informatisation No 6 of 18February 2015 approves Instruction on the procedure for shaping and storing data on the information resources (their constituents) of Internet-services, placed in the global computer Internet network (comes into force 1 January 2016);Sub-programmes Security of information and communication technologies and digital trust and Security of information and communication technologies and digital trust of the National Programme of accelerated development of services in the field of information and communication technologies (ICT) for 2011-2015;

State S&T Programme Development of methods and means of the comprehensive system for information protection for 2011-2015; Decree of Operations and Analytical Centre (OAC) № 48 On Approval of the order of attesting of managers responsible for ensuring the protection of state secrets, and other employees of government agencies and other organizations working with state secrets, as for application of technological measures protecting state secrets of 9 June 2011; Presidential Decree On some issues of the Information Society Development in the Republic of Belarus of 8 November 2011; Law No 455-Z On information, informatisation and protection of information of 10 November 2008; Law No 113-Z On electronic document and digital signature of 28 December 2009; Law On electronic communication No.45-3 of 19 July 2005; Resolution of the Council of Ministers No. 1055 On Procedures for rendering electronic communications services of 17 August 2006; Law on Mass Media No 427-З of 17 July 2008 (article 5 guarantees freedom of opinion and expression); Presidential Decree No 575 on National Security Concept of 9 November 2010 (amended 24 October.2014); Belarus-Russia Union State Programme Enhancing the system for protection of common information resources of Belarus and Russia on the basis of high technologies for 2011 – 2015; Council of Ministers' Decree No 2013/027/BY on Technical regulations Information technologies; several of OAC's regulations on Cyber Security standards and critical information infrastructures including Regulations on the procedure of technical protection of information in information systems designed for processing, distribution and (or) provision of data not classified as state secrets of 30 August 2013 approved by Order of the Operational and Analytical Centre under the President of the Republic of Belarus of 30.08.2013 (No 62, amended 16 January 2015, No 3) and Technical codes of practice TKP 483-2013 Information technology and security. Safe operation and reliable operation of critically important objects of informatisation. General requirements (No 47) of 17 July 2014; Criminal Code, Article 179, prohibits and defines punishment for illegal collection or dissemination of information about the private life; Presidential Decree No 486 of 25 October 2011 On some measures to ensure the security of critically important objects of informatisation; OAC's Order No 42 of 30 April 2012 on Instructions on how to conduct external monitoring of safety-critical objects of informatisation; Technical Regulations Information Technology. Means of information security. Information security (TR 2013/027 / BY)

- Strong political will and leadership to minimize security threats/incidents
- Readiness to raise legal standards in the area of personal data protection

Gaps

A need for:

- Ratification of the Cyber security Convention
- Dedicated Cyber security law
- Greater legal clarity about the role of the NRA
- Clear and effective policies governing the security of the private sector critical information infrastructures
- More effective protection of personal data and privacy online through laws and regulations

Strategy, Implementation, Resources

Achievements

Availability of:

- Government regulator in the area of information protection (Operational and Analytical Centre - OAC) which provides various services/training and actively cooperates with relevant bodies within the CIS
- CERT-BY is accredited by FIRST (Forum of Incident Response and Security Teams)
- Registry of information protection means includes 230 items as of 08.04.2015

Gaps

A need for:

- Protection of personal data and privacy in practice
- Policies aimed at safe but also open and free internet
- Free access to public sector information

- Effective enforcement of NIS-related laws and regulations
- Measuring progress in NIS/Cyber Security policies
- Stronger inter-agency cooperation and coordination
- Clarification of the role of the NRA
- Reporting on security incidents, public awareness raising, alert platforms, hotlines
- Cyber attack simulation
- Defining security requirements for Trust Service providers

Infrastructures

Gaps

A need for:

- Improving NIS-related standards
- Inclusion of the private sector critical infrastructures

Services

Gaps

A need for:

- Cyber attack simulation services
- CERT's services to NRA

HDM roadmap

Leadership, Policy, Legal Frameworks

- Raise legal certainty and clarify definitions pertaining to t network, information and Cyber Security according to European standards

- Approximate as much as possible key legal and regulatory frameworks with European standards including on Privacy and Personal Data Protection
- Ratify Cybercrime Convention of the Council of Europe
- Streamline, coordinate and consolidate NIS-related legal and regulatory framework governed by numerous laws and regulations
- Develop and pass a consolidated law guaranteeing the online protection of personal data and privacy in line with best European and international practices
- Develop and approve national Cyber security strategy approximated with the European Cyber security strategy
- Develop and pass a consolidated law guaranteeing free access to public information in line with best European and international practices (Freedom of Expression/Information acts)
- Ensure sufficient legal certainty needed to empower the competent NRA to manage and coordinate security incidents among public and private entities
- Ensure legal certainty for defining and classifying critical information infrastructures (CIIS)
- Continue maintaining a high level of political will, leadership and commitment
- Raise legal certainty and develop procedures on reporting on security incidents in an open and transparent manner
- Develop and apply regulatory provisions governing the disclosure of information on security breaches of public importance
- Develop and apply dedicated regulatory provisions governing management and coordination of security incidents with ISPs and public electronic communication service providers
- Update and enforce existing and planned laws/regulations in line with eIDAS

Strategy, Implementation, Resources

- Formulate and approve a national Cyber security strategy approximated with the European Cyber security strategy
- Improve policies ensuring regular update of standards for cyber-security products aligned with best European and international ones
- Examine and use best international practices in creating effective legal/regulatory frameworks and in the field of cyber attacks
- Develop easy-to-navigate guidelines for end-users regarding vulnerabilities of soft- and hardware
- Establish a requirement to notify the supervisory body within 24 hours after having become aware of a security breach
- Further develop capacities and competencies of the government CERT; ensure its adequate funding
- Regularly practise and improve performance and transparency of cyber attack simulations
- Consider expanding CERT services to provide services beyond the state sector
- Expand CERT cooperation with CERT-EU
- Regularly run and improve effectiveness of alert platforms/ hotlines
- Continue regular public awareness campaigns
- Launch and intensify training and educational activities in cooperation with ENISA
- Deepen the dialogue with key actors/stakeholders on Cyber Security issues
- Practise new forms of engaging key actors in cyber attack simulation
- Improve policies and practices on minimal security levels
- Expand and improve policies for greater effectiveness of international cooperation
- Set up a capacity building plan for Cyber Security including for the government CERT
- Improve enforcement effectiveness of legal and regulatory frameworks in NIS
- Strike a balance between internet security, regulation and openness

Infrastructures

- Improve criteria to better understand and assess critical information infrastructures
- Decide how to handle the private sector infrastructures
- Define and apply procedures to include critical infrastructures owned/operated by the private sector
- Develop guidelines for end-users regarding vulnerabilities of soft- and hardware

Services

- Launch and intensify training and educational services in cooperation with ENISA
- Expand CERT's services to the expert and business community, the general public, and NRA

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Acceding the Cybercrime Convention or fully aligning national legislation with the Convention
- Creation of an enabling legal and regulatory framework in general approximated with European standards as much as possible.
- Formulation and adoption of a national Cyber Security Strategy based on the principles of the European Cyber Security Strategy.
- Defining minimal security levels.
- Strengthening the capacities of the government CERT and expanding its services.
- Maintaining strong leadership.
- Maintaining free and open internet while making it safe.
- Protection of personal data and privacy online.
- Identification and protection of critical information infrastructures.

- Pro-active public awareness raising and education.

Pilot Projects

It is recommended that Belarus joins all three proposed regional projects in the field of Network, information and cyber security, namely:

[1] Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation;

[2] Policy support to confidentiality of data processing, protection of personal data and online privacy;

[3] Capacity building plan for national/government CERTs, including through cooperation with ENISA.

2.1.8 Georgia

State of play and gap analysis

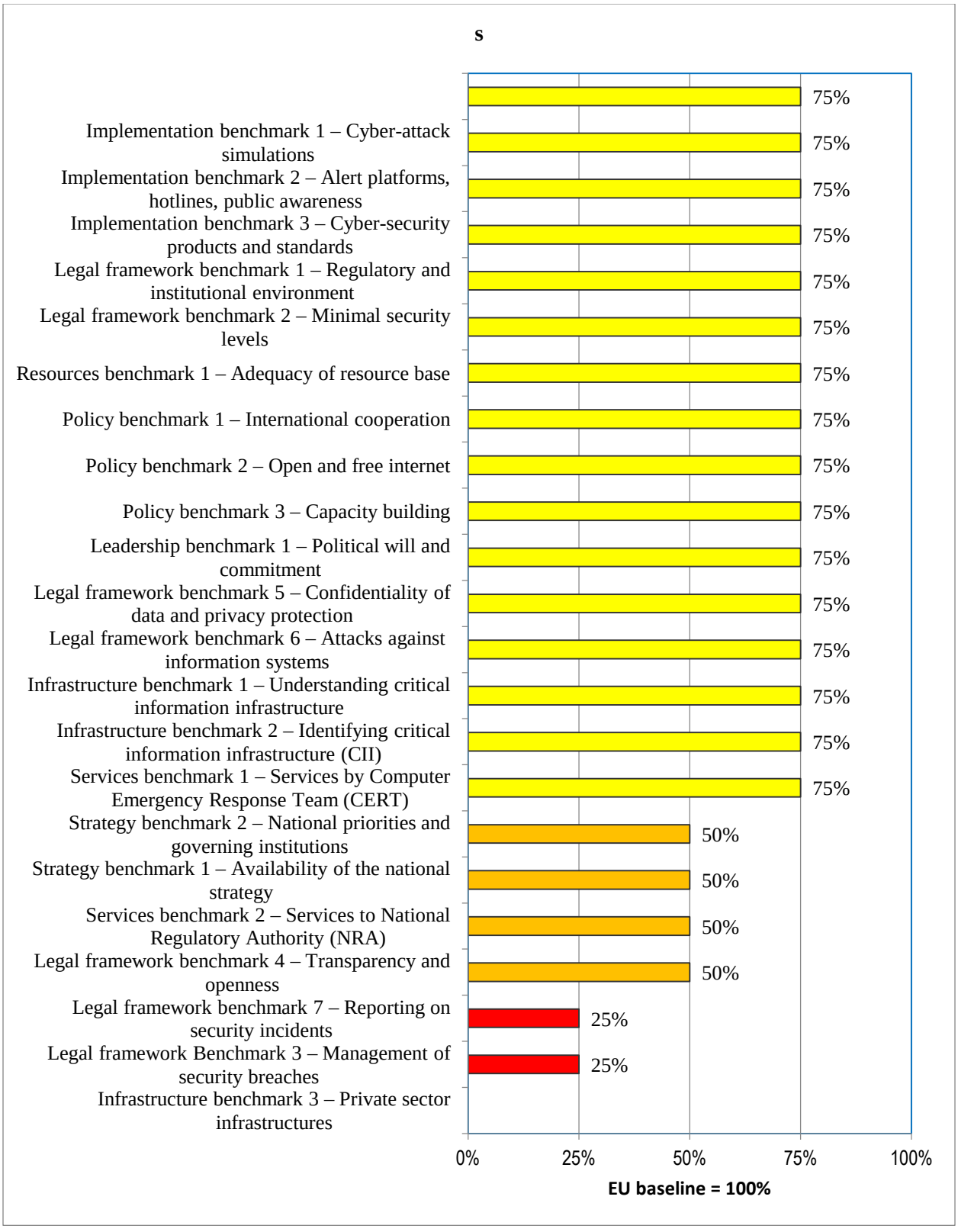

Exhibit 17 - State of play and gap analysis of Georgia in NIS priority area

The Government of Georgia allocates sufficient resources, especially financial, to ensure the adequate functioning of key institutions and critical infrastructures in the field of Network, information and Cyber-security. Having experienced cyber-attacks on its electronic infrastructure and networks in 2008, Georgia takes network, information and Cyber Security seriously. As a signatory of the Cybercrime Convention since 2008, it has thoroughly followed best international practices in NIS and cooperates extensively with the EU and other partners. As a result, the government regularly updates the national legal and regulatory framework and introduces novel approaches, such as implementing in 2012-2015 a national Cyber security strategy, which will be replaced by a new one.

Georgia has been active in cooperating with the EU to replicate best EU practices in the field of e-Policies, including in Network and information security (e.g. the development of A Digital Georgia: e-Georgia strategy and action plan 2014-2018 through a Twinning programme and EU-Georgia e-Governance Facility). Another example of cooperation is a Bilateral Project between Georgia and Estonia implemented since 2012 to increase the capacities of the Ministry of Internal Affairs to combat cybercrime and seizure of digital evidences. During 2008-2009, the Ministry of Interior was involved in the Council of Europe and European Commission's Joint Project on Cybercrime, which aimed to harmonize Georgian legislation with the Cybercrime Convention. Since March 2011, the Ministry of Internal Affairs participates in the CoE project "Cooperation against Cybercrime" for the Eastern Partnership countries.

The next challenge will be to pay more attention to critical information infrastructures operated by the private sector. Also, more progress is to be made in the management of security breaches and reporting on them in a transparent and open manner, as required by the Information Security law. CERT's services need to be expanded beyond the state bodies. The country should continue aligning its national legislation with that of the EU by formulating a new national Cyber Security Strategy in line with the European Cyber Security Strategy.

Leadership, Policy, Legal Frameworks

Achievements

Availability of:

- Ratified CoE Cybercrime Convention.
- Law On Information Security of Georgia contains provisions demanding from the

providers if critical information systems to report immediately in case of security breach or threat.

- Regulatory provisions governing reporting on security incidents/ breaches (Decrees of the Chairman of Data Exchange Agency on: Computer incident response group, Minimal Information Security requirements, Management rules of information assets, Rules of Information Security Audits, Rules of Authorization of Authorized persons and organizations and authorization fees, Minimal standards for information security managers of Critical Information Systems).
- Various secondary regulatory acts passed by relevant state entities in the field of Network, Information Security and Cyber Security.
- Cybercrime-related definitions in the Criminal Code, including computer interference or data interference is in line with 2001 Council of Europe) Cybercrime Convention.
- Plans to amend the Law on information Security to include special security requirements for Trust service providers (article 10).
- References in the Law On Information Security as well as in other secondary legislation acts underline the importance of enhancing security and resilience of critical information infrastructures
- Strong political will and leadership to minimize security threats/incidents.
- Readiness to raise legal standards in the area of personal data protection.

Gaps

A need for:

- Further alignment of the national legal and regulatory framework with European standards

Strategy, Implementation, Resources

Achievements

Availability of:

- A special Cybercrime Unit in the Ministry of Interior's Central Criminal Police Department that carries out the functions foreseen by the CoE' Convention on Cybercrime.
- A 24/7 hotline for cybercrime is open for the public at the Ministry of Internal Affairs. CERT.GOV.GE also operates hotline- incidents reporting mechanisms.
- Public education campaigns via social media, advertising on television, lectures for teachers, dissemination of leaflets and calendars undertaken by the Data Exchange Agency and the Ministries of Internal Affairs and Defence are key elements of Georgia's State Cyber Security Strategy.
- Cyber Security Discussion Forum as a form of engaging representatives of critical infrastructure systems Internet and other service providers, as well as financial institutions to simulate cyber attack simulations.
- Clear criteria for defining critical information infrastructures (CIIs) owned by 38 public entities.
- Clear CII approval procedure (Critical Infrastructure List approved by Decree of the President based on the proposal made by the Security Council of Georgia).

Gaps

A need for:

- New national cyber-security strategy aligned with the European Cyber Security Strategy
- Greater clarity regarding the services provided by the Computer Emergency Response Team (CERT) including to the National Regulatory Authority (NRA)
- Regular updates of cyber-security standards and products
- Addressing security of the private sector's critical information infrastructure

Infrastructures

Gaps

A need for:

- Maintain and improve criteria to better understand and assess critical information infrastructure

- Covering private sector critical information infrastructures
- Policies and procedures governing critical infrastructures owned/operated by private electronic service providers

Services

Gaps

A need for:

- Cyber attack simulation services
- CERT's services to NRA

HDM roadmap

Leadership, Policy, Legal Frameworks

- Raise the level of legal certainty and develop procedures on reporting on security incidents in an open and transparent manner
- Develop and apply regulatory provisions governing the disclosure of information on security breaches of public importance
- Develop and apply dedicated regulatory provisions governing management and coordination of security incident with ISPs and providers of public electronic communication service providers
- Raise legal certainty regarding attacks against information systems
- Update and enforce existing and planned laws/regulations in line with eIDAS
- Ensure a high level of political will and commitment to improve cyber security
- Maintain high level of political will and leadership

Strategy, Implementation, Resources

- Implement a new national Cyber security strategy approximated with the European Cyber security strategy

- Continue running and improving the effectiveness of alert platforms/ hotlines
- Regularly undertake public awareness campaigns
- Continue maintaining and deepening the dialogue with key actors on Cyber Security issues
- Practice new forms of engagement and participation to raise transparency levels
- Continue improving policies and procedures on reporting about security incidents
- Continue practicing and improving cyber attack simulations; practice new forms of engaging key actors in cyber-attack simulations
- Improve policies on minimal security levels
- Improve policies to ensure regular update of standards for cyber-security products
- Expand and improve policies for greater effectiveness of international cooperation
- Maintain the adequacy of resource base
- Set up a capacity building plan for Cyber Security
- Continue striking the balance between internet security and openness

Infrastructures

- Maintain and improve criteria to better understand and assess critical information infrastructure
- Decide how to handle the private sector infrastructures
- Define and apply procedures to include critical infrastructures owned/operated by private electronic service providers

Services

- Launch and intensify training and educational services in cooperation with ENISA
- Expand CERT's services to expert and business community, the general public, NRA

Conditions for harmonisation

- Creation of an enabling legal and regulatory framework in general approximated with European standards as much as possible.
- Formulation and adoption of a national Cyber Security Strategy based on the principles of the European Cyber Security Strategy.
- Defining minimal security levels.
- Strengthening the capacities of the government CERT and expanding its services.
- Maintaining strong leadership.
- Maintaining free and open internet while making it safe.
- Stepping up the protection of personal data and privacy online.
- Identification and protection of critical information infrastructures.

Pilot Projects

It is recommended that Georgia joins at least two of the proposed three regional projects in the field of Network, information and cyber security, for example:

[1] Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation;

[3] Capacity building plan for national/government CERTs, including through cooperation with ENISA.

2.1.9 Moldova

State of play and gap analysis

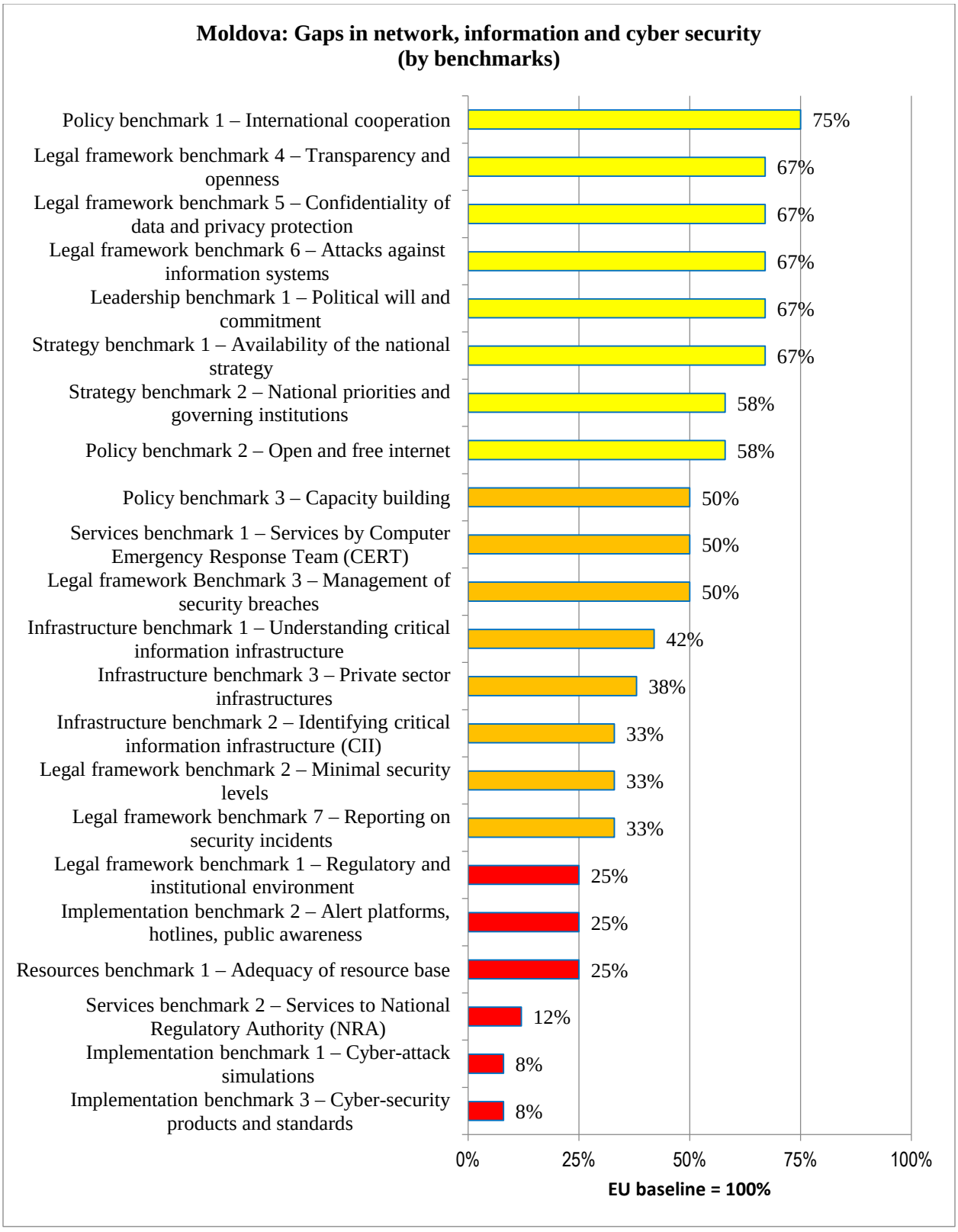

Exhibit 18 - State of play and gap analysis of Moldova in NIS priority area

Moldova demonstrates good progress in aligning with European standards, laws and best practices. While there is no stand-alone national strategy dedicated to cyber security, the national strategy Digital Moldova 2020 contains the action plan (chapter 4) aimed at “creation of conditions for increasing security level and trust in digital space”; the action plan addresses key Cyber Security issues including those related to internet safety and openness, personal data and privacy protection. Since 2009, when the country ratified the CoE Convention on Cybercrime, the government has been addressing the emerging Cyber Security challenges in a consistent manner. This is evidenced, in particular, by the adoption and implementation of the law to prevent and fight cybercrime, as well as by the establishment in 2010 of the government CERT (within the Individual Partnership Action Plan of the Republic of Moldova – NATO in 2010). The National Strategy for Information Society Development ‘Digital Moldova 2020’ (adopted in 2013) contains direct references to the European Cyber Security principles. In 2015, the Parliament’s Commission on national security and public order – having reviewed past and ongoing activities – asked the government to take further measures to improve the situation in the area of protection of Cyber Security and protection of personal data. There is also a National Centre for personal data protection, which should be informed (according to the existing legal framework) about all breaches of personal data security.

There is a plan of the Ministry of Information Technology and Communications to amend the Law on Electronic Communication in order to introduce a new chapter on security and integrity of networks and services of electronic communications; the chapter will regulate obligations of the provider of networks and/or public services on electronic communications to ensure security and integrity of the electronic network as well as the responsibilities of regulatory body which will evaluate measures taken by providers for guarantying security and integrity of networks and / or services with imposing respective measures.

The country’s priorities should include both the effective implementation of the security-related measures as formulated under the ‘Digital Moldova 2020’ Action Plan and further improving the existing legal and regulatory framework. Management of critical information infrastructure, alert platforms, minimal security levels, and cyber-attack simulations need additional attention. Moldova has a number of other challenges to meet, especially in the area of Cyber Security products and standards, critical information infrastructure (especially in the private sector) and reporting on security breaches and raising public awareness.

Leadership, Policy, Legal Frameworks

Achievements

Availability of:

- Ratified CoE Cybercrime Convention.
- Personal Data Protection Law No 133 of 2011
- Law No 305 of 2012 that regulates the re-use of public sector information held by the state (there is also a respective government directive passed in 2013, No 886).
- Law on digital signature and Government Decrees on mobile eSignature No 1090 of 2013 and No 405 of 2014 contain provisions requiring service providers protect personal data
- Criminal Code's provisions for prevention and combating cybercrime
- Plan amend the Law on Electronic Communication to step up NIS-related provisions

Gaps

A need for:

- Further alignment of the national legal and regulatory framework with European standards
- Greater legal clarity concerning reporting on security incidents/breaches, public awareness raising, alert platforms, hotlines

Strategy, Implementation, Resources

Achievements

Availability of:

- Government policy to disclose Public Sector Information and publish it on the government's Open Data portal www.date.gov.md
- Action plan on Cyber Security within the national strategy Digital Moldova 2020
- Free and open internet

- National CERT-GOV-MD with clearly formulated goals and policy statement
- A dedicated Cyber Security department at the Ministry of Interior of Moldova
- Action plan for NIS/Cyber Security under Digital Moldova 2020 strategy that includes Action 9.13 "Providing electronic identity management for cyber security", Action 9.11 "Strengthening CERT-GOV-MD team", Action 9.9 "Draw up User's Guide on minimum Cyber Security insurance with the provisions to institutionalise individual responsibility for cyber security", Action 9.5 "Encouraging mutual exchange of information between public and private sector concerning threats, weaknesses, risks, cyber incidents and attacks", Action 9.2 "Defining national critical infrastructure that is to be protected from cyber attacks", "Defining national critical infrastructure that is to be protected from cyber attacks", Action 9.12 "Develop and improve the Plan for M-cloud protective and security measures".

Gaps

A need for:

- Further alignment of the Digital Moldova 2020 Cyber security action plan with the European Cyber Security Strategy
- Clear policies governing the services provided by Computer Emergency Response Team (CERT) including to the National Regulatory Authority (NRA)
- Regular updates of cyber-security standards and products

Infrastructures

Gaps

A need for:

- Engaging with the private sector's critical information infrastructures

Services

Gaps

A need for:

- Cyber-attack simulation services
- CERT's services to NRA

HDM roadmap

Leadership, Policy, Legal Frameworks

- Raise legal certainty and develop procedures for reporting on security incidents in an open and transparent manner
- Reassess the progress of approximating national legal and regulatory framework with the EU legislation as far as the NIS-related issues are concerned
- Approximate national legislation to Directive 2002/58/EC (as amended by Directive 2009/136/EC) to ensure protection of fundamental rights and freedoms, in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and ensure the free movement of such data and of electronic communication equipment and services (before 2018)
- Raise legal certainty about confidentiality of personal data and online privacy
- Ensure that privacy is protected at design level by default
- Raise the level of legal/regulatory governing CERT's operations
- Ensure alignment with a Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, COM/2013/048 final - 2013/0027)
- Amend the Law on Electronic Communication on security and integrity of networks and services of electronic communications in line with the European Cyber Security Strategy
- Ensure alignment with a Proposal for a Directive of 2010 (COM (2010) 517 final) on attacks against information systems

- Expand the scope and breadth of international cooperation
- Update and enforce existing and planned laws/regulations in line with eIDAS
- Regularly run and improve effectiveness of alert platforms/ hotlines
- Regularly undertake public awareness campaigns
- Continue and intensify training and educational activities in cooperation with ENISA
- Deepen the dialogue with key actors/stakeholders on Cyber Security issues
- Practise new forms of engagement and participation to raise transparency levels
- Regularly practise and improve performance of cyber attack simulations
- Practise new forms of engaging key actors in cyber attack simulation
- Improving reporting procedures on security incidents
- Develop and apply dedicated regulatory provisions governing management and coordination of security incident with ISPs and providers of public electronic communication services
- Improve policies and practices on minimal security levels
- Maintain high level of political will and leadership

Strategy, Implementation, Resources

- Implement all planned actions of Digital Moldova 2020 in the area of cyber security, especially: define national critical infrastructure; establish and operationalise a national Cyber Security system; harmonise national legislation with that of the EU; establish and enforce minimum security requirements for national critical information infrastructure; encourage mutual exchange of information between public and private sector concerning threats, weaknesses, risks, cyber incidents and attacks; strengthen national CERT; strengthen security of the government M-Cloud network; undertake all planned training and awareness raising activities
- Ensure regular reporting on personal data breaches to the Centre for Personal Data Protection
- Raise effectiveness of policy monitoring and implementation by adding measurable

indicators to the action plan progress indicators (at the moment, a list of measurable indicators for Digital Moldova 2020 does not contain quantitative progress indicators related to NIS/Cyber security)

- Continue implementing policies guaranteeing open and free internet while making it more secure and safe
- Undertake a review of the implementation of the Cyber security action plan of Digital Moldova 2020
- Consider the rationale behind developing and adopting a dedicated national Cyber security strategy to better align with the European Cyber security strategy
- Implement the Program on Cyber Security (elaborated by the Ministry of Information Technology and Communications
- Continue running and improving the effectiveness of alert platforms/ hotlines
- Regularly undertake public awareness campaigns
- Continue maintaining and deepening a dialogue with key actors on Cyber Security issues
- Practice new forms of engagement and participation of key stakeholders to raise transparency levels
- Continue improving policies and procedures on reporting about security incidents
- Continue practicing and improving cyber attack simulations; engage key actors in cyber attack simulation
- Improve policies on minimal security levels
- Improve policies to ensure regular update of standards for cyber-security products and standards
- Expand and improve policies for greater effectiveness of international cooperation
- Set up a capacity building plan for Cyber Security including for CERT-GOV-MD
- Set up a capacity building plan for Cyber Security

Infrastructures

- Maintain and improve criteria to better understand and assess critical information infrastructure
- Decide how to handle the private sector infrastructures
- Define and apply procedures to include critical infrastructures owned/operated by private electronic service providers
-

Services

- Ensure that CERT possesses sufficient capacities to hire professional expertise in the field of cyber attack simulations
- Improve and expand CERT's services
- Define CERT's services to the NRA
- Launch and intensify training and educational services in cooperation with ENISA

Conditions for harmonisation

- Creation of an enabling legal and regulatory framework in general approximated with European standards as much as possible.
- Formulation and adoption of a national Cyber Security Strategy based on the principles of the European Cyber Security Strategy.
- Defining minimal security levels.
- Strengthening capacities of the government CERT and expanding its services.
- Maintaining strong leadership.
- Maintaining free and open internet while making it safe.
- Stepping up the protection of personal data and privacy online.
- Identification and protection of critical information infrastructures.

Pilot Projects

It is recommended that Moldova joins at least two of the proposed three regional projects in the field of Network, information and cyber security, for example:

[1] Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation;

[3] Capacity building plan for national/government CERTs, including through cooperation with ENISA.

2.1.10 Ukraine

State of play and gap analysis

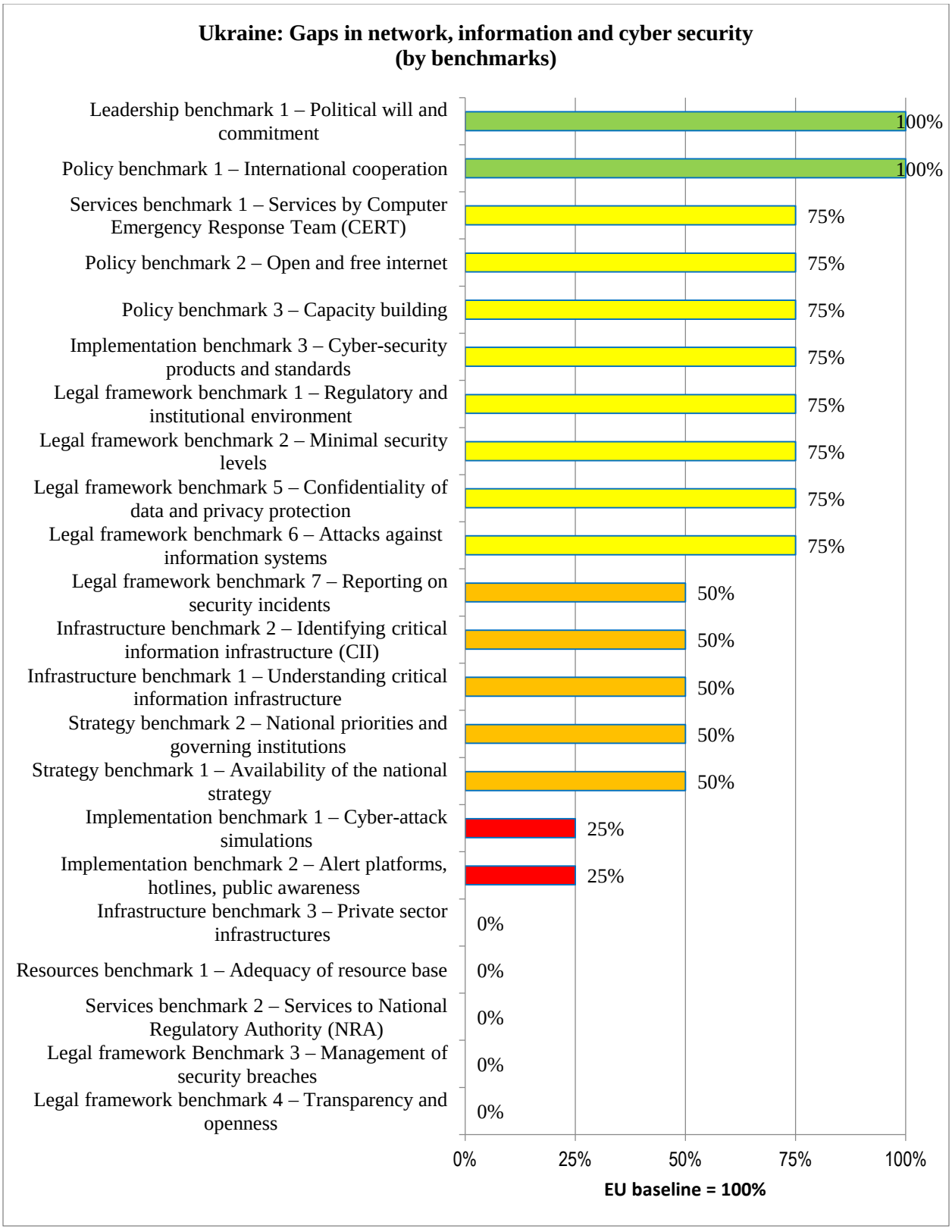

Exhibit 19 - State of play and gap analysis of Ukraine in NIS priority area

Ukraine was among the first Partner Countries to sign and ratify the Cybercrime Convention (signed in 2001, ratified in 2006), followed by the establishment in 2007 of the national CERT. The changed circumstances in 2014 witnessed hundreds of cyber-attacks, many of which targeted the Gov.ua domain. The country's legal and regulatory landscape in the area of network, information and Cyber Security is rapidly changing towards European standards, as is also spelled out in the Association Agreement.

There is a strong national CERT, well-developed security standards, and open and free internet. CERT provides various security alerts services on its webpage and disseminates text messages (in cooperation with mobile operators). Security standards are well-developed and applied, and minimal security levels and identified. The government's leadership in adopting European principles and practices is strong. The weakest aspects include inadequate regulations for reporting on security risks, incidents and breaches (including interaction with the regulatory agency for electronic communications). The lack of a single national alert platform and regular cyber-attack simulations, as well as vulnerable private sector critical infrastructure (its assessment and identification needs improvement) need serious attention. The major challenge will be to complete the legal reform by passing the already drafted new laws and enforce them effectively by allocating adequate resources and undertaking well-focused capacity building activities. The issues of critical information infrastructures, greater transparency in reporting on security breaches, better regulation of the private sector security, and enhanced services of the national CERT will be paramount to closing the gap with the EU which is significant at the movement.

Leadership, Policy, Legal Frameworks

Achievements

Availability of:

- Ratified CoE Cybercrime Convention.
- Draft Law on Cyber Security
- Draft law on National Regulatory Authority

- State information security is regulated by over 20 legal acts which include: Law on Information No 2658-XII of 2.10.92 (the last update in July 2012); Government Decree No 1135 of 05.11.2014 On the Action plan of resources protection 2014-2016; Presidential Decree On the Doctrine of information safety of Ukraine (No 514/2009 of 8 July 2009); Presidential Decree No 389 of 08.06.2012 On the Creation of the Cyber security strategy of Ukraine; Presidential Decree No 1229/99 of 27.09.1999 On Technical means of data protection (including cryptography-related provisions); Order of National Security and Defence Council of Ukraine, signed by President No 449/2014 of 28.04.2015 (includes provision for development and creation of the national wide Cyber Security system)
- Provisions of the Criminal Code of Ukraine No 2341-III of 05.04.2001 (the last update of 05.04.2015 defines illegal attacks against information systems that are considered (and punished) as criminal offences

Gaps

A need for:

- Further alignment of the national legal and regulatory framework with European standards
- Greater legal clarity concerning reporting on security incidents/breaches, public awareness raising, alert platforms, and hotlines

Strategy, Implementation, Resources

Achievements

Availability of:

- Draft Cyber Security Strategy
- National security strategy
- Action plan of resources protection 2014-2016 signed by the Cabinet of Ministers on 05.11.2014 No 1135-p (includes both legislative provisions and implementations such as modernization of CERT-UA, international cooperation etc)

- Availability of government supervisory authority – State Services of Special Communication and Information Protection of Ukraine (DSZZI)
- Diverse international cooperation activities
- Plans to modernize CERT-UA
- Experience of cooperation with private business on cyber attacks
- Free and open internet
- State programs in the area of Special Communication networks, Crypto Systems and means of information protection, National System of secure communication
- Requirement to report on security incidents within 24 hours (Administration Decree No143 of 24.07.2007 by DSSZZI)
- Government policy to disclose Public Sector Information and publish it on the government's Open Data portal

Gaps

A need for:

- Cyber security strategy
- Clear policies governing the services provided by the Computer Emergency Response Team (CERT) including to the National Regulatory Authority (NRA)
- Regular updates of cyber-security standards and products

Infrastructures

Achievements

Availability of:

- Criteria for defining critical information infrastructures

Gaps

A need for:

- Engaging with the private sector's critical information infrastructures

Services

Achievements

Availability of:

- Active CERT-UA in informing the public via its web site and social media

Gaps

A need for:

- Cyber attack simulation services
- CERT's services to NRA

HDM roadmap

Leadership, Policy, Legal Frameworks

- Raise legal certainty and develop procedures for reporting on security incidents in an open and transparent manner
- Ensure sufficient legal certainty needed to empower competent national regulatory authority to manage and coordinate security incidents among public and private entities
- Ensure relevant laws on personal data protection are approximated with the EU
- Ensure greater legal certainty in relation to reporting on security incidents and breaches (include relevant provisions into the national Cyber security law and strategy)
- Amend and pass the following laws in line with European standards: On bases of national safety of Ukraine; On information; On protection of information and electronic telecommunication systems; On national security service or, alternatively, consolidate what is at the moment a vast legal regulatory framework in the field of network, information and Cyber Security by having fewer but well focused laws
- Ensure a high level of political will, leadership and commitment
- Develop and apply dedicated regulatory provisions governing management and coordination of security incidents with ISPs and public electronic communication service providers
- Update and enforce the law in line with eIDAS

Strategy, Implementation, Resources

- Finalise, discuss and approve Cyber security strategy in line with European Cyber security strategy
- Start regular cyber-attach simulation activities
- Create dedicated hotlines and alert platforms (in addition to CERT-UA information dissemination activities)
- Align national standards with those of the EU
- Finalise, discuss and pass in line with European standards: Doctrine of information security; On Cyber security
- Regularly undertake public awareness campaigns
- Deepen dialogue with key actors/stakeholders on Cyber Security issues
- Practise new forms of engagement and participation to raise transparency levels; develop and apply regulatory provisions governing the disclosure of information on security breaches of public importance
- Improve policies and practices on minimal security levels
- Expand and improve policies for greater effectiveness of international cooperation

Infrastructures

- Analyse conditions, establish criteria and define CIIs (include relevant provisions into the national Cyber security law and strategy); include CIIs from private sector
- Improve policies to ensure regular update of standards for cyber-security products

Services

- Define clearly the role of CERT-UA; expand CERT-UA cooperation with CERT-EU; consider expanding CERT-UA services to provide services beyond state sector; ensure sustainable financing of CERT-UA from the state budget; set up a capacity building plan for Cyber Security including for CERT-GOV-UA
- Define CERT's services to National Regulatory Authority (NRA)

- Launch and intensify training and educational services in cooperation with ENISA

Conditions for harmonisation

- Creation of an enabling legal and regulatory framework in general approximated with European standards as much as possible.
- Formulation and adoption of a national Cyber Security Strategy based on the principles of the European Cyber Security Strategy.
- Defining minimal security levels.
- Strengthening the capacities of the government CERT and expanding its services.
- Maintaining strong leadership.
- Maintaining free and open internet while making it safe.
- Stepping up the protection of personal data and privacy online.
- Identification and protection of critical information infrastructures.

Pilot Projects

It is recommended that Ukraine joins all three proposed regional projects in the field of Network, information and cyber security, namely:

[1] Policy support to national Cyber Security Strategies: legal/ regulatory framework and implementation;

[2] Policy support to confidentiality of data processing, protection of personal data and online privacy;

[3] Capacity building plan for national/government CERTs, including through cooperation with ENISA.

2.2 Electronic identification and Trust Services

2.2.1 EU baseline

Electronic identification (eID) and Electronic Trust Services (eTS) are key enablers of secure cross-border electronic transactions and central building blocks of the Digital Single Market. The EU baseline for this HDM priority area sets a comprehensive general legal and technical framework for electronic transactions by regulating the mutual recognition of notified electronic identification schemes and means by provisioning electronic trust services (i.e. e-signature, e-seals, e-time stamp, e-registered delivery, and website authentication), as well as by ensuring the non-discrimination of electronic documents vis-à-vis their paper equivalent and thus ensuring the legal validity of electronic transactions. The baseline comprises relevant EU legislation, best practices, standards and ICT platforms as appropriate for eID/eTS.

The core of the EU baseline in the field of eID/eTS consists of the following items.

EU Legislation

- Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (replacing the preceding E-Signature Directive 1999/93/EC)
- Decision 2004/387/EC (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC)
- Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package"

EU Standardisation initiatives/cross border tools

- Mandate M460 given by the Commission to CEN and ETSI (to be revised and extended)

EU Strategies

- Digital Agenda for Europe (DAE)

EU Best practices

- Large Scale Pilots (such as STORK, STORK 2.0, PEPPOL, SPOCS, e-SENS), Country-specific good practices (e.g. Estonian interoperability e-Road solution)

The baseline is measured against 11 benchmarks:

- Leadership benchmark 1 – Political will and capacity
- Legal framework benchmark 1 – Legal certainty about secure electronic transactions
- Legal framework benchmark 2 – eSignature including across borders
- Legal framework benchmark 3 – Confidence in eID and privacy protection
- Legal framework benchmark 4 – Use of eID in public procurement online
- Infrastructure benchmark 1 – Common infrastructure and services
- Infrastructure benchmark 2 – Interoperability, ICT standards
- Services benchmark 1 – Services for citizens
- Services benchmark 2 – Services for businesses
- Services benchmark 3 – eProcurement uptake
- Services benchmark 4 – eProcurement sophistication

<u>Legal framework</u>

- Regulation No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (including the preceding E-Signature Directive 1999/93/EC) – demonstrating clear mandate and of political will to enhance trust in electronic transactions in the internal market by providing a common pan-European foundation for secure electronic interaction between citizens, businesses and public authorities across borders, and increase the effectiveness of public and private online services, electronic business and electronic commerce in the EU; establishing rules and legal certainty for developing and applying electronic identification and trust services via the creation of a common

foundation for secure electronic interaction between citizens, businesses and public authorities; encouraging the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes and for online services or electronic transactions in order to make it easier for businesses and citizens to access their online services from other countries; removing barriers to the cross-border use of electronic identification means used in the Member States to authenticate public services.

- Mandate M460 (a Rationalised Framework for Electronic Signature Standardisation) – establishing a standardisation mandate to the European Standardisation Organisations in the field of Information and Communication Technologies applied to Electronic Signatures; ensuring legal certainty for the application of ICT standards and specifications by regulating the EU standardisation initiatives and cross border tools; creating conditions for the interoperability of eSignature at intra-community level through a rationalised European eSignature standardisation framework; ensuring policy consistency in developing EU Standards on Electronic Signatures and PKIs (Public Key Infrastructure).
- Directive 95/46/EC of the European Parliament and of the Council (Data Protection Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, part of the "Telecom Package") – preventing the unauthorised and excessive access to personal data online; guaranteeing confidentiality and security of personal data processing; require EU Member States to protect the fundamental rights and freedoms of natural persons, and in particular the right to privacy with respect to the processing of personal data; guaranteeing the "right to privacy in the electronic communication sector" and free movement of data, communication equipment and services; ensuring personal data is accessed only by authorised persons; protecting personal data from being destroyed, lost or accidentally altered; requiring service providers to inform the person concerned, including the National Regulatory Authority (NRA), in case of the infringement of personal data.
- Directive 2004/18/EC of the European Parliament and Council of 31.3.04 on the

coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Directive 2006/123/EC of the European Parliament and Council of 12.12.06 on services in the internal market, Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement (notified under document C(2014) 2120) (2014/188/EU; Official Journal of the European Union 5.4.2014) – ensuring economic operators fully enjoy fundamental freedoms in the competition for public procurement contracts via transparent and non-discriminatory procedures; facilitating freedom of provision of services between Member States to improve the quality of services both for consumers and businesses using these services; identifying ICT specifications to be adopted after consultation of the European multi-stakeholder platform on ICT standardisation set up by Commission Decision 2011/C 349/04 (1) complemented by other forms of consultation of sectoral experts .

Leadership, Strategy, Policy

- Digital Agenda for Europe (DAE) (Communication from the Commission to the Council, The European Parliament, the European Economic and Social Committee and the Committee of the Regions, 19.05.2010) – helping citizens and businesses in Europe to get the maximum benefit from digital technologies as the drivers for EU's smart sustainable and inclusive growth by implementing 7 actions under Pillar II on ICT interoperability and standards including in the field of public procurement; defining and implementing a common list of key cross-border services to enable entrepreneurs to set up and run a business anywhere in Europe independently of their original location, and to allow citizens to study, work, reside and retire anywhere in the European Union.
- i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All (Communication from the Commission to the Council, Method paper 2010: Preparing the 9th Benchmark Measurement (Capgemini, Rand Europe, IDC, Sogeti and DTi for European Commission Directorate General for Information Society and Media).

Infrastructures

- Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA)

including Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services' of 16 December 2010 (part of the Digital Agenda for Europe (DAE) Action 21 aimed at proposing legislation on ICT interoperability and Action 24 aimed at adopting a European Interoperability Strategy (EIS) and European Interoperability Framework (EIF) – establishing for the period 2010-2015 a programme on interoperability solutions for European public administrations and institutions and bodies of the Union by providing:

(a) common and shared solutions facilitating interoperability and

(b) legal support for ICT interoperability to reform the rules on implementation of ICT standards in Europe; identifying ICT technical specifications to encourage the development of Europe-wide standards for stronger interoperability of digital applications and devices working across borders; ensuring seamless interaction of digital devices, applications and services anytime and across borders.

- Decision 2004/387/EC (Corrigenda) of the European Parliament of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), Interoperability of European public services – maintaining infrastructure services in a sustainable manner; enabling efficient, effective and secure interchange of information between public administrations at all appropriate levels, as well as between such administrations and the EU institutions or other entities; extending the benefits of the interchange of information to facilitate the delivery of e-services to businesses and citizens taking into account their needs; supporting the European decision-making process and facilitating communication between European institutions by developing the related strategic framework at the pan-European level; promoting the spread of good practice and encouraging the development of innovative telematics solutions in public administrations; ensuring pan-European eGovernment services rely on the market-oriented approaches so as the selection of suppliers is done on a competitive basis in a multi-vendor environment, while ensuring, whenever appropriate, the operational and financial sustainability of measures.
- European Interoperability reference Architecture and European Cartography of Interoperability solutions and European federated Interoperability Repository (EFIR) –

developing a common vision for a European Interoperability Architecture (EIA) to ensure compatibility of different services and data registers used by public administrations for cross-border cooperation and services; deciding how the architectural building blocks fit together and determine which interface standards can link-up such building blocks; assessing the need for and relevance of having common infrastructure services as part of this architecture with the help of Conceptual Reference Architecture aimed at defining the conceptual reference building blocks needed to build systems in support of public services; disseminating interoperability solutions; making EFIR a valuable information source; providing access to a set of interoperability assets that can be further re-used in the National Interoperability Framework (NIF).

Services

- Directive 2004/18/EC of the European Parliament and Council of 31.3.04 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Directive 2006/123/EC of the European Parliament and Council of 12.12.06 on services in the internal market, Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement (notified under document C(2014) 2120) (2014/188/EU; Official Journal of the European Union 5.4.2014) – ensuring economic operators fully enjoy fundamental freedoms in the competition for public procurement contracts via transparent and non-discriminatory procedures; facilitating freedom of provision of services between Member States to improve the quality of services both for consumers and businesses using these services; identifying ICT specifications to be adopted after consultation of the European multi-stakeholder platform on ICT standardisation set up by Commission Decision 2011/C 349/04 (1) complemented by other forms of consultation of sectoral experts .
- Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers. Final Report (A study prepared for the European Commission DG Communications Networks, Content and Technology by Capgemini, Tech4i2, Time.lex, Universiteit van Antwerpen, 2011).
- Large Scale Pilots (STORK, STORK 2.0, PEPPOL, SPOCS, e-SENS) – defining technical definitions and descriptions of assurance levels for establishing minimum

technical requirements, standards and procedures in the context of Regulation No 910/2014 and ensuring its consistent application with regard to identity proofing for issuing qualified certificates.

Box 1: x-Road in Estonia – Seamless and secure interoperability solution.

Started in the early 2000s by the e-Government in Estonia, x-Road (or Tree in Estonian) has become a recognized European Best Practice – a working model of the Interoperability Architecture (IA). This is a backbone of the e-government architecture that includes:

- secure data transport backbone (x-Road per se)
- distributed software systems and different hardware components like portals
- elements of public key infrastructure (PKI) – eID, eAuthentication, eAuthorization facilitated by the X-Road Service Layer governmental databases and information systems

x-Road facilitates the transfer of dozens of e-services that have been created for Estonian citizens, civil servants and businesses. It ensures data integrity, authenticity and authentication, encryption, reliable, verifiable, scalability and availability, neutrality towards different technical solutions, transparency in data models through the loosely coupled services, enhanced security thanks to a two-level authorization model and XML-based compatibility.

Source: Various sources

Box 2: STORK 2.0 – European e-services without borders.

The large-scale pilot project STORK develops interoperable solutions for electronic identity (eID) that work on a distributed e-government architecture platforms regardless of different specifications and infrastructures existing in EU Member States so as to fully integrate EU e-services. The STORK platform will obtain the required guarantee (authentication) from national e-government platforms when requesting an access to e-services requiring personal data (national eID).

It will be possible to start a company, get tax refund, or obtain university papers without physical presence; all is needed is to access these services by entering personal data using national eIDs, while the STORK platform will obtain the required guarantee (authentication) from the national government.

Source: STORK 2.0 https://www.eid-stork.eu/

2.2.2 Overview of the state of play and gap analysis for the Region

The market for electronic communications in the six Partner Countries reached a level of about €8.3Bnin 2013. In geographical terms, the largest market was Ukraine with a share of close to 55%, followed by Azerbaijan and the Republic of Belarus[15]. Broadband is becoming the main channel of internet access to the population and thus access to electronic services provided to citizens and businesses. All Partner states are active in building their digital markets implementing eID/eTS initiatives, progressing to a different but similar degree in relation to the established EU baseline.

The best progress has been achieved in the field of creating the eID/eTS infrastructure and implementing eSignature. Legal certainty about eID is sufficient and leadership is relatively strong. However, digital signature as a main tool of electronic identification is not used widely

[15] EaPeReg Benchmarking Report – Benchmarking Electronic Communications Markets in EaP countries, 2015.

and is not interoperable across borders. E-Government interoperability in general and e-services for citizens in particular are the weakest among other indicators.

Achieving the EU baseline lies in the national interest of all the Partner Countries given the new trade opportunities that may emerge as a result of making digital signature working across borders. All countries express their readiness to change legislation in order to eliminate this barrier., although solutions for the EU Association Agreement countries and the members of the Eurasian Economic Union differ.

The availability of e-services requiring electronic identification is not sufficient at the moment. Until now, electronic signature has served better the business community than citizens. In general, eProcurement has been among the key drivers of building relevant infrastructure and services closely linked with eCommerce. All countries plan to move public procurement online (Armenia has already done so). The Region's digital markets are still closed markets. Yet, the first signs of their opening are coming through. EU experiences and best practices are barely known in the Region (except Estonia whose x-Road interoperability solution is applied in Georgia, Moldova, Azerbaijan and Ukraine). Access to the European knowledge in eID and eTS is still rather restricted. There must be much better knowledge sharing and solution adaptation mechanisms created in the region so as to expose the Partner Countries to the rich expertise of the EU.

Exhibit 20 demonstrates that the best progress has been achieved in the field of creating eID/eTS infrastructure and implementing eSignature. Also, leadership and political will to create digital infrastructure is usually strong. eServices for citizens appear to be the weakest. Otherwise, the revealed discrepancies between the countries measured across benchmarks are not significant, which points out the commonality of challenges the Region is facing.

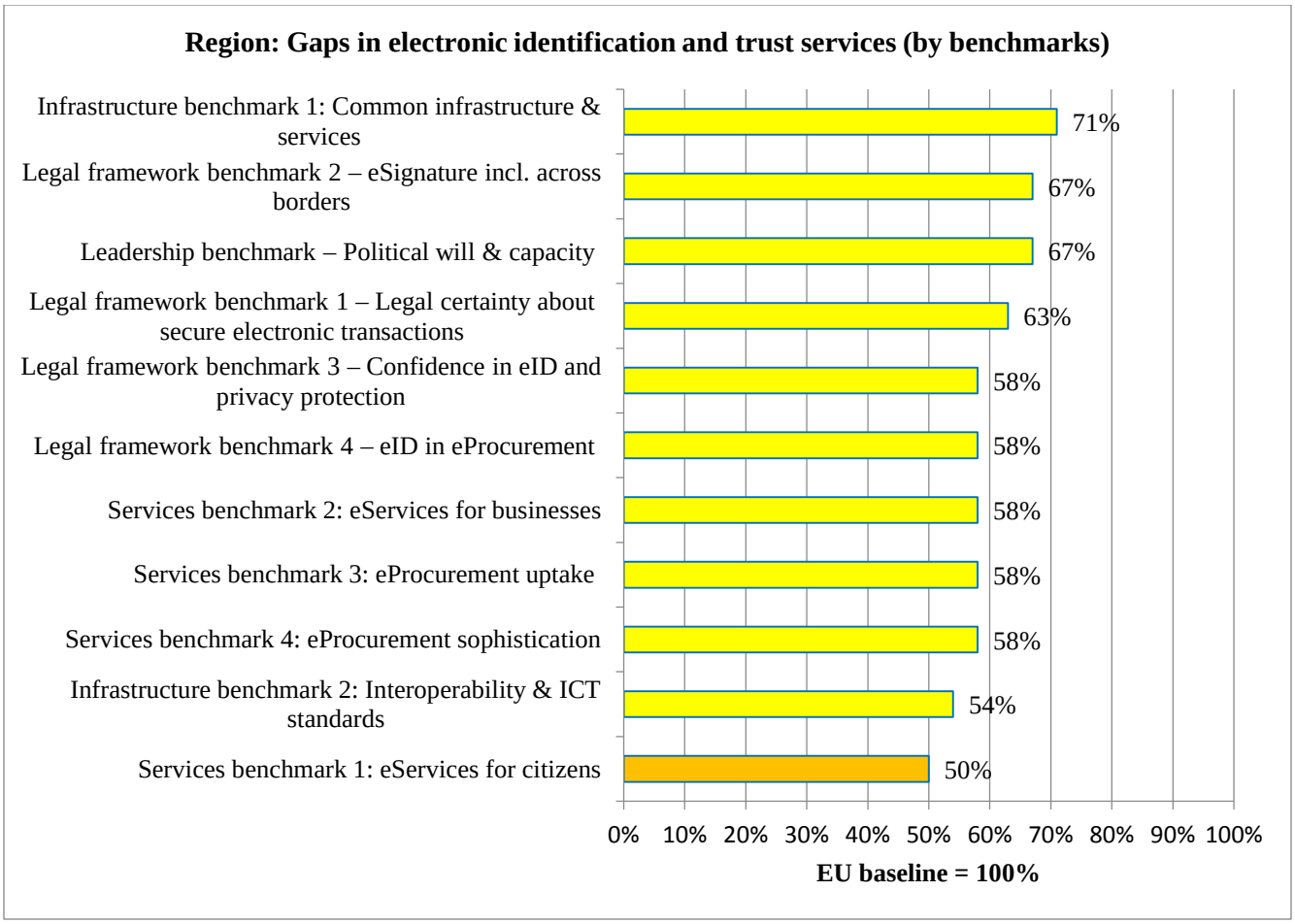

Exhibit 20 - State of play of the Region in electronic identification and trust services (eID/eTS)

2.2.3 Overview of common actions for the Region

Electronic identification and trust services are at the heart of building national digital markets and the Region is aware of this imperative need. There are multiple benefits – economic, technological and political – of closer harmonisation with the EU which is seen as a technological leader in building digital markets. Technological benefits are the most straightforward ones to modernise and advance eID/eTS schemes and tools. The issues of trade – which becomes increasingly borderless – and economic development requires faster implementation to stay economically competitive or to gain new comparative advantages by being able to trade across borders and regions. The EU is among the largest trading partner for the Region. Therefore possessing key digital market technologies is of paramount importance for a broader development.

On one hand, eProcurement is seen as an area with clear opportunities for economic benefits through cross-border trade and eventually participation in public procurement tenders. On other hand, this is one of the most problematic areas suffering from insufficient use of electronic identification and trust technologies in practice, undermining international transactions. At the moment, the Region's digital markets are still closed markets. Yet, the first signs of their opening are coming through.

For some Partner Countries, the EU in general and individual Member States in particular are important sources of good practice and knowledge. Estonia is a case in point especially in infrastructure, services and e-government interoperability. Its experience is widely known and often adopted in practice (such as the x-Road interoperability and e-government architecture solution). Other EU experiences and best practices are less known in the Region. There must be much better knowledge sharing and solution adaptation mechanisms created in the region so as to expose the Region to the EU expertise. Access to the European knowledge in eID/eTS is still rather restricted. This is an important conclusion of the study based on the interview results held with government officials.

2.2.4 Benefits for and readiness analysis of the Region

Mutual benefits within the Region are not obvious as yet, although there are cases of inter-country cooperation, such as between Moldova and Ukraine on the interoperability of infrastructure services. Another case has a broader regional dimension and applies to the Eurasian Economic Union whose members (Armenia and Belarus) will get access to national public procurement tenders. That has prompted the work on the mutual recognition of trust services and would, most likely, lead to further progress towards the use of eID/eTS technologies. It is not clear whether or not the increased openness in these digital markets (thanks to eProcurement) would facilitate greater openness towards the EU as well. There are signs that that might be the case, for most Partner Countries are considering changes in the current legislation to allow for that. Still, a lot of practical work would lie ahead to realise these changes in practice and where the EU could provide significant help in making this transition shorter and more successful through knowledge sharing and regional and/or inter-country pilots.

2.2.5 Armenia

State of play and gap analysis

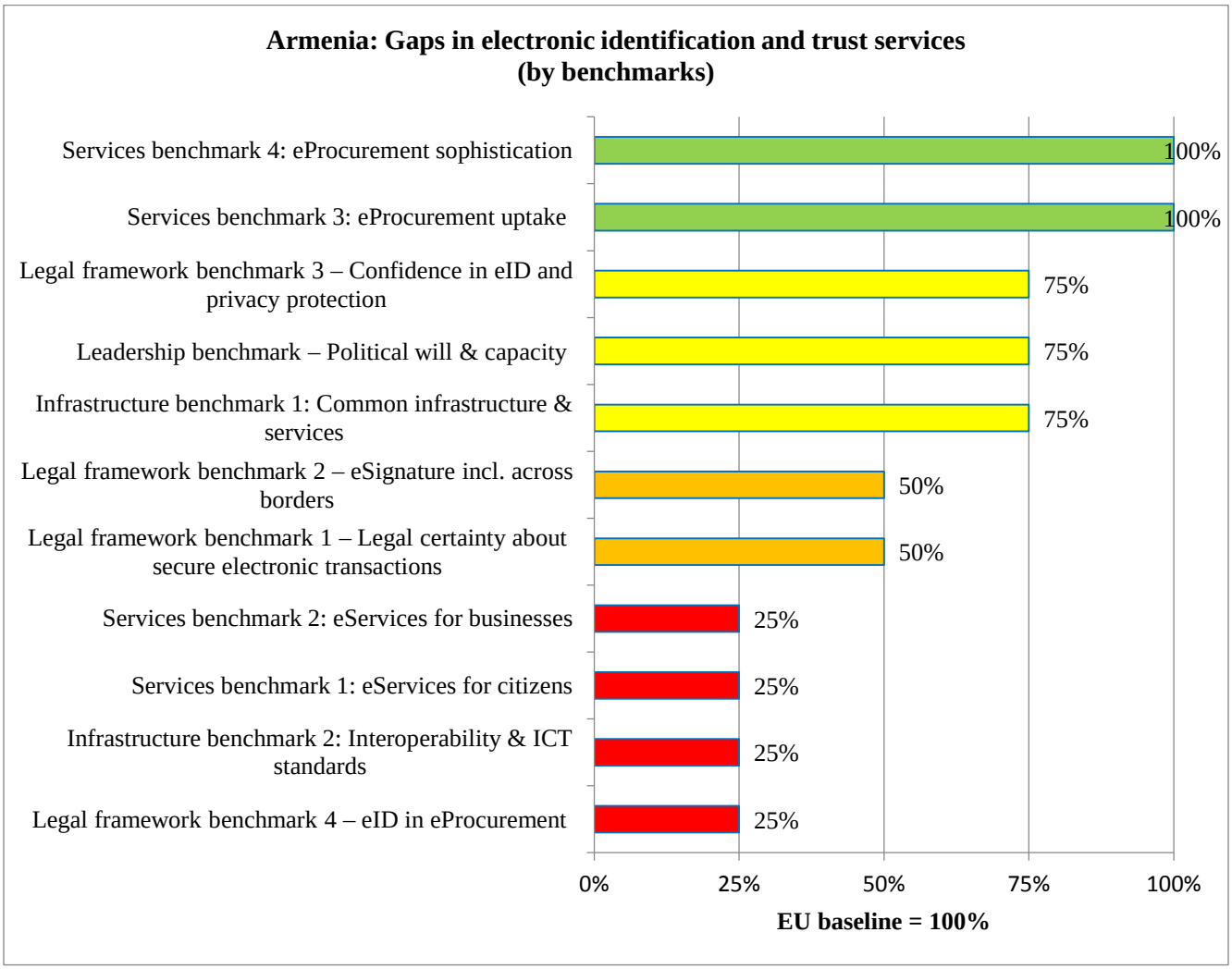

Exhibit 21 - State of play and gap analysis of Armenia in eID/eTS priority area

The area of eID/eTS has been an important focus of Armenia's e-government strategy since 2008, with the adoption of the President's order "On the Conception for Migration System" and "On the Introduction of the System of Electronic Passports and Identification Cards with Biometric Parameters". The country has passed two specific laws on electronic identification – on Identity Cards and on Electronic Documents and Electronic Signature. The Ministry of Economy and the Staff of the Government are the state agencies responsible for policy making and strategy development. The Ministry's eGovernance Infrastructure Implementation Unit "EKENG" is the key execution agency in eID/eTS. It is actively involved in developing rules,

regulations and procedures. There has been a visible uptake of eID recently, with "EKENG" preparing the launch of mobile eID. All the tenders are mandatory for online submission. In 2015, some 2,500 tenders announced by state agencies were administered online. While there is a good infrastructure in place to provide trust services across borders, no legislation exists to permit recognition of eID/eTS from other countries.

The biggest gaps are found in the area of e-services for businesses and citizens (provided at lower maturity levels), insufficient legal certainty about licensing in the area of Public Key Infrastructure (PKI). It is important that electronic identification and trust services become interoperable across borders and recognised in other countries. While Armenia's eProcurement system is almost on a par with the EU baseline, digital signature should be integrated into the entire tender process.

Leadership, Strategy, Policy, Legal Frameworks

Achievements

Availability of:

- Key legal and regulatory frameworks include: Presidential Decree On the Conception for Migration System of the Republic of Armenia and for Introduction of the System of Electronic Passports and Identification Cards with Biometric Parameters in the Republic of Armenia; On Identity Cards; On Electronic Documents and Electronic Signature; Law on Procurement; Government Decree on eProcurement; Law on Identity Cards; Law on Electronic Documents and Electronic Signature; Government Decree No 116-Ն of 2008 defines the licensing procedures of certification services; Government Decree On the Interoperability design and model is under preparation
- Ministry of Economy and the Government Office are the key state agencies responsible for policy making and strategy development in e-government
- Significant progress is creating an enabling legal and regulatory environment for e-government development and services
- Experience in experimentations in under the EU Guillotine programme

Gaps

A need for:

- Legal and regulatory framework for cross-border certification and digital signature services (no mutual recognition of trust services for legal reasons while technical infrastructure is adequate)
- Bilateral and multilateral agreements for cross-border recognition of digital signature
- Participation in the EU large-scale pilots (such as STORK)

Infrastructures

Achievements

Availability of:

- eID/TS technical infrastructure that meets necessary standards
- Shared e-government infrastructure
- Interoperability system (under development)
- E-governance Infrastructure Implementation Unit (EKENG) of the Ministry of Economy is e-Government operator

Gaps

A need for:

- Whole-of-government interoperability

Services

Achievements

Availability of:

- e-Services for businesses are well developed
- Full penetration of e-procurement services at Pre- and Post-award stages are (mainly administered via by e-commerce tools)

- Mandatory submission of tenders online. In 2015 alone, 2,500 tenders announced by state agencies were administered online
- Available access control tools to trace the use of personal data by government agencies

Gaps

A need for:

- e-Services requiring electronic identification
- Mobile eID/TS
- Harmonisation of basic e-services with the EU
- Higher e-service maturity (low at the moment at 1-2 stages)
- Wider use of eID in public procurement

HDM roadmap

Leadership, Strategy, Policy, Legal Frameworks

- Define clear procedures of the licensing institution more clearly
- Complete the design and setup of an interoperability model/framework for Armenia's e-government system.
- Issue Government Decree on the interoperability model design
- Prepare and implement an e-Government Interoperability Action Plan
- Create an enabling legal and regulatory framework for secure identification in mobile environment
- Approximate national legal and regulatory framework as much as possible with the respective EU laws and regulations, especially the most recent ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation)
- Examine and adopt relevant EU best practices
- Discuss with the European Commission possible options and cooperation modalities for

implementing eID/TS between Armenia and EU Member States (including mutual recognition of certification services and digital signatures via the mediation of the Trusted Third Party mechanism)

- Ensure strong leadership and political will

Infrastructures

- Implement mobile eID/TS solutions including mobile digital signature
- Consider possibility of joining STORK's (Secure identity across borders linked) eID platform for interoperable solutions for electronic identity and authentication across borders

Services

- Harmonise basic e-services for citizens and businesses with those of the EU
- Identify a number of e-services for cross-border access along with relevant trust services
- Raise e-service maturity (from current situation of mostly one-way information provision and downloadable forms)

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Making national legislation compatible with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) as much as possible so as to raise security of electronic transactions and make eSignature interoperable across borders
- Raising confidence in eID among ordinary citizens by harnessing personal data and privacy protection
- Adopting the European model of e-service maturity for citizens and businesses and approximating the list of such services with that of the EU
- Offering a number of e-services for cross-borders access

- Making all key stages of public procurement available online and integrating eID into tender processes
- Adopting a viable e-government interoperability strategy as closely as possible aligned with the principles of the European Interoperability Framework
- Maintaining strong leadership.

Pilot Projects

It is recommended that Armenia joins all four proposed regional projects in the field of Electronic identification and trust services, namely:

[1] Policy support for mutual recognition of eID/TS

[2] Piloting digital signature across borders

[3] Policy support to eService development and benchmarking including capacity building for eProcurement sector

[4] Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre

2.2.6 Azerbaijan

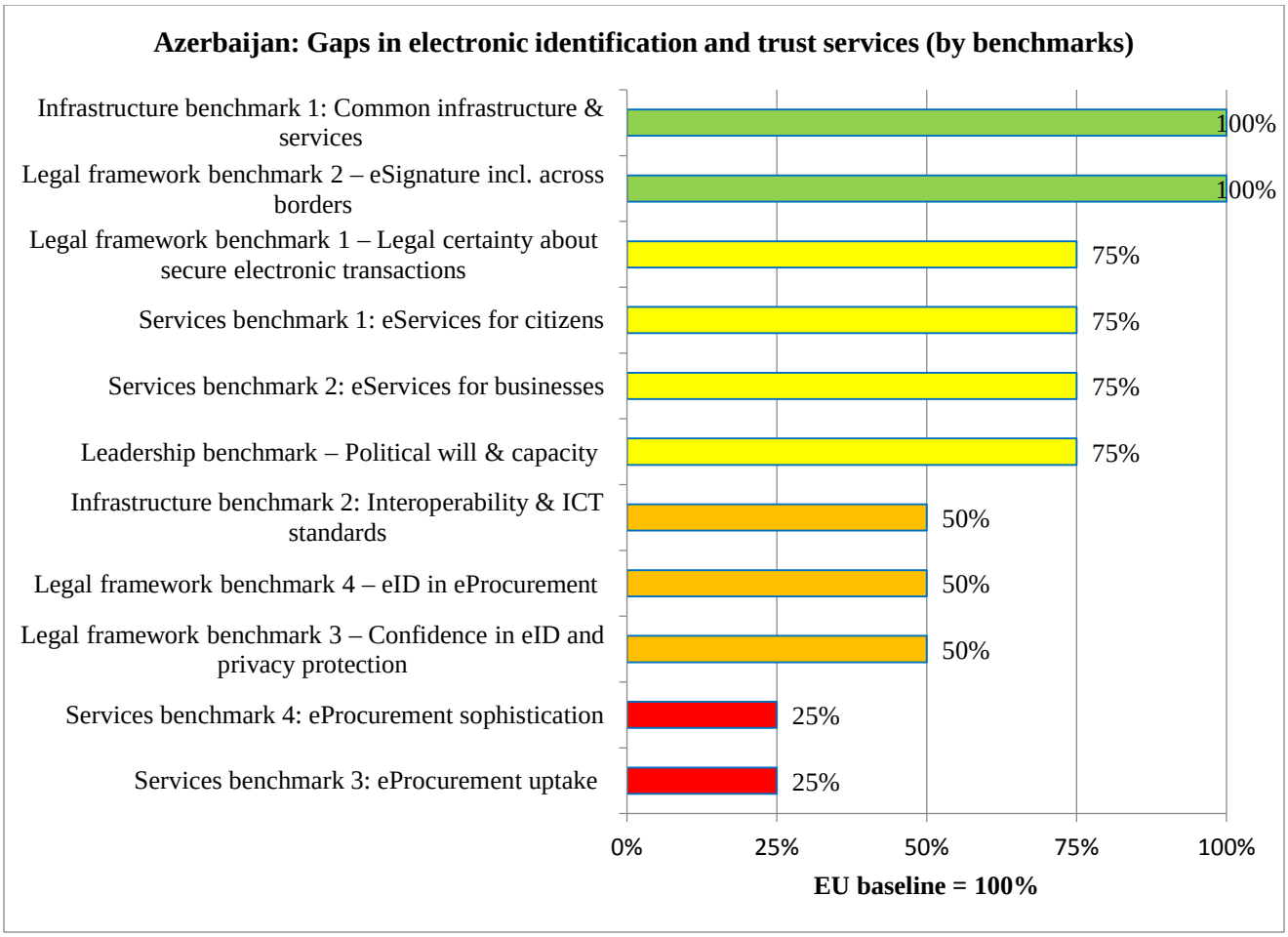

Exhibit 22 - State of play and gap analysis of Azerbaijan in eID/eTS priority area

Azerbaijan has built a modern electronic signature infrastructure and advanced in developing eSignature-based solutions. The Government demonstrates strong political will and leadership for effective functioning of electronic identification and trust services. A number of State Programmes on the "Development of ICT" (including electronic services) have been implemented over the past several years.

A new National Strategy for the Development of the Information Society in Azerbaijan for 2014-2020 has been recently adopted. The government is aware of positive economic benefits of electronic identification in the globalised e-commerce services. The social benefits are seen in facilitating and simplifying international travel, human contacts, border and customs control checks.

In legal terms, the eID/eTS area is governed by the Law on “E-signature and e-document”, Presidential Decree on “Implementation of e-signatures,” the Law on “Individual data” and the Law on “Information, informatisation and information exchange”. Electronic signature is obtainable via smart cards and mobile SIM cards. Both the Ministry of Communication and High Technologies (MCHT) and the Ministry of Taxes issue their own electronic identification tools. MCHT provides eID services mostly to citizens and government officials, while the Ministry of Taxes targets the business sector. As of 1 September 2014, MCHT issued some 23,000 e-signature certificates demonstrating a monthly growth rate of nearly 1,200 users. The Ministry of Taxes issued almost 50,000 mobile signatures (an ASAN eSignature). A SIM-card based e-identification – or mobile ASAN (Easy) eSignature issued by the Certification Service of the Ministry of Taxes – was introduced in Azerbaijan in cooperation with an Estonian company. Mobile ASAN eSignature enables users to register for e-services and issue e-signatures on documents.

The largest gaps are observed in the area of eProcurement, eGovernment interoperability and standards, and public confidence in eID. The number one priority would be to improve legal certainty about eID (possibly with a new law) to make electronic identification services interoperable across borders and digitise public procurement at all stages of the tender process.

Experience from other countries needs to be studied and applied taking into account best international standards through international cooperation within a short period of time. That especially concerns eProcurement. However, there is a shortage of local specialists and engineers in the field of security electronic identification and trust services. The main challenge is to bring the legal and regulatory framework closer to international standards. Creating trust on public e-services is also an ongoing challenge.

Leadership, Strategy, Policy, Legal Frameworks

Achievements

Availability of:

- Certification Services Centre established in 2011 under the Ministry of Communication and High Technologies (MCHT); the Ministry of Taxes (MT) issues its own e-identification tools (for business mostly)

- Draft law on information resources under preparation
- Successful implementation of the National Strategy on Information-Communication Technologies for the Development of the Republic of Azerbaijan 2003-2012 within the e-Azerbaijan framework programme
- Adoption of a New State Programme on the Development of ICT and the National Strategy for the development of information society in Azerbaijan for 2014-2020
- Key laws and regulations include: Presidential Decree On Implementation of e-signatures; Law On e-Signature and e-document; Law on Individual data; Law On Information, informatisation and information exchange; Law On Obtaining of information; Law On Freedom of Information
- Availability of State Procurement Agency (www.tender.gov.az)

Gaps

A need for:

- International harmonisation of information protection standards
- Bilateral and multilateral agreements for cross-border recognition of digital signature via Trusted Third Party mechanism
- Participation in the EU large-scale pilots (such as STORK)
- Use of eID in public procurement
- Harmonisation of basic e-services policies with the EU

Infrastructures

Achievements

Availability of:

- Choice of electronic identification tools comprising:

  (a) smart card and

  (b) SIM card based e-signatures (although not widely used yet)

- Affordability of e-Signature (15 Euro for three years for citizens)
- National infrastructure for e-document and e-government data centre is under construction

Gaps

A need for:

- Interoperability of sectoral information systems

Services

Achievements

Availability of:

- eID cards that are linked to a bank account (as a means of payment service)
- Rising uptake of e-Government services (in 2014, some 12% of the population used them)
- Eight procurement-related e-services (information provision mostly) available on e-Government portal (www.e-gov.az)
- Relatively well-developed e-services for business (three to four stages of service maturity)
- Specialized ASAN Service Centre (State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan)

Gaps

A need for:

- Stronger uptake and use of eID/TS
- Rapid rise in online services among those over 400 services that are published on e-Government portal and higher e-service maturity (most e-services for citizens are at stage 1 to 3 of online maturity)
- Online public procurement

- Electronic identification for e-services including eProcurement

HDM roadmap

Leadership, Strategy, Policy, Legal Frameworks

- Pass a new law on information resources (under preparation)
- Develop and implement action plans for the introduction of eProcurement tools
- Harmonise data/information protection standards with those of the EU
- Approximate national legal and regulatory framework as much as possible with the respective EU laws and regulations, especially the most recent ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation)
- Examine and adopt relevant EU best practices
- Discuss with the European Commission possible options and cooperation modalities for implementing eID/TS between Azerbaijan and EU Member States (including mutual recognition of certification services and digital signatures via the mediation of the Trusted Third Party mechanism)
- Continue maintaining strong leadership and political will

Infrastructures

- Complete the creation of the national infrastructure for e-document
- Establish and operationalise e-Government Data Centre
- Consider possibility of joining STORK's (Secure identity across borders linked) eID platform for interoperable solutions for electronic identity and authentication across borders

Services

- Harmonise the list of basic e-services for citizens and businesses with those of the EU

- Improve uptake of e-government services
- Identify a number of e-services for cross-border access along with relevant trust services
- Raise levels of e-service maturity
- Automate the full cycle of public procurement services online

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Making national legislation compatible with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) much as possible, so as to raise security of electronic transactions and make eSignature interoperable across borders in line
- Raising confidence in eID among ordinary citizens by harnessing personal data and privacy protection
- Adopting the European model of e-service maturity for citizens and businesses and approximating the list of such services with that of the EU
- Offering a number of e-services for cross-borders access
- Making all key stages of public procurement available online and integrating eID into tender processes
- Adopting a viable e-government interoperability strategy aligned with the principles of the European Interoperability Framework as closely as possible
- Maintaining strong leadership.

Pilot Projects

It is recommended that Azerbaijan joins all four proposed regional projects in the field of Electronic identification and trust services, namely:

[1] Policy support for mutual recognition of eID/TS

[2] Piloting digital signature across borders

[3] Policy support to eService development and benchmarking including capacity building for eProcurement sector

[4] Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre

2.2.7 Belarus

State of play and gap analysis

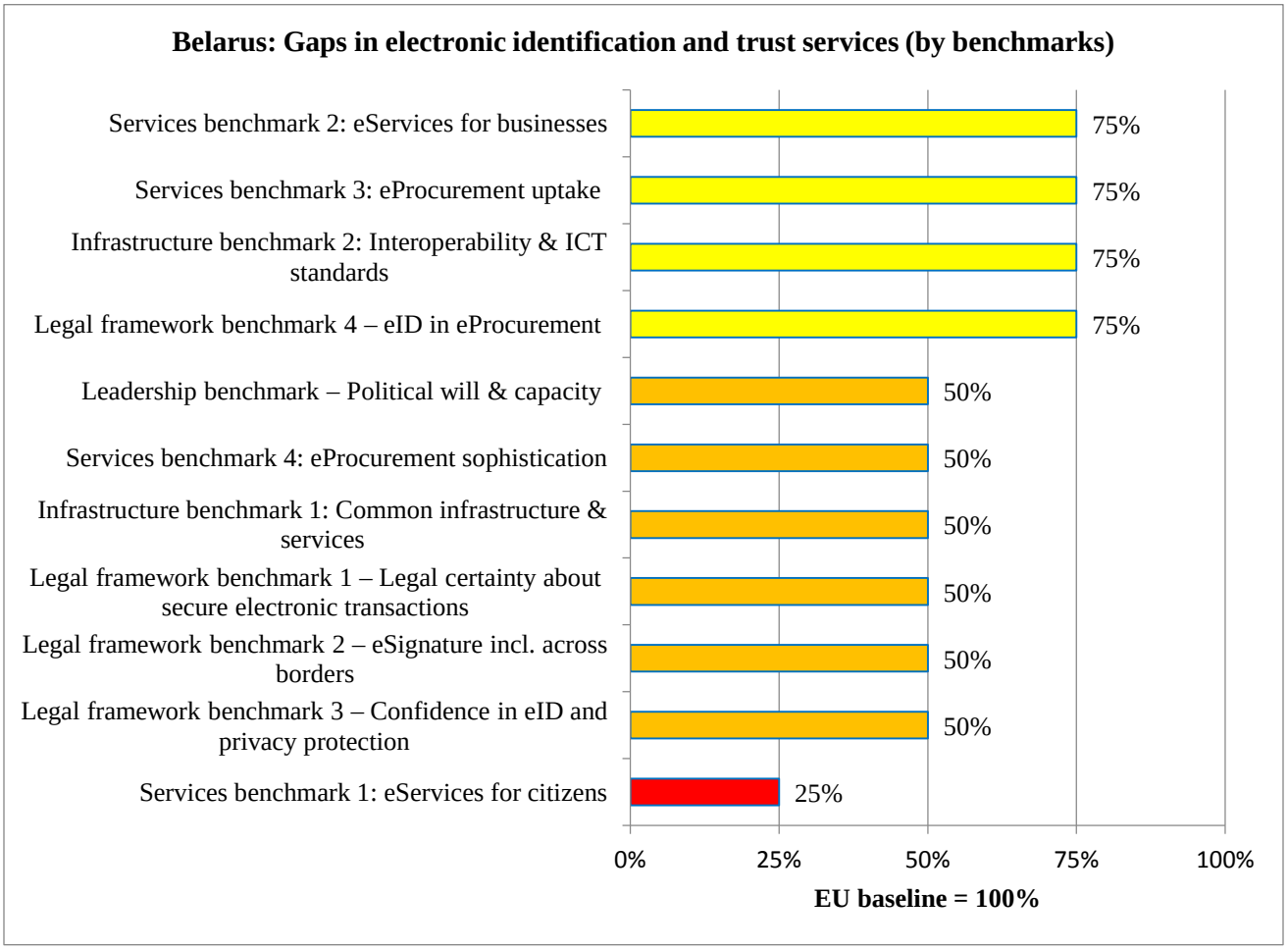

Exhibit 23 - State of play and gap analysis of Belarus in eID/eTS priority area

The country's government demonstrates strong leadership and sufficient operational capacity to:

(a) timely propose laws/adopt regulations needed for the effective functioning of electronic identification and trust services and to assign/create an agency in charge with sufficient powers for inter-agency coordination,

(b) effectively enforce laws and regulations by elaborating relevant action plans,

(c) put in place effective implementation mechanisms to support the efficacy of policies and strategies. Yet the allocated financial resources are insufficient to attract the best IT specialists from the private sector.

Until recently, Belarus has not recognized digital signatures of other countries, just as its eSignature solutions could not be used outside the country's national borders. With the adoption of the eID-related legislation within the Eurasian Economic Union (EEU), it will become legally and technically possible to mutually recognise other EEU members' certification services and thus use eSignature in those countries (e.g. in Armenia) via a Trusted Third Party mechanism. Belarus proposes using this approach to conclude bilateral or multilateral agreements with EU Member States to make eSignature interoperable with the EU as well. However, to do so the country needs to make its national legislation more compatible with Europe's eIDAS Regulation to raise security of its trust service providers. The major gaps are observed in the field of e-services for citizens. There is also lack of formally adopted e-government interoperability strategy framework so as to expand transactional services at a high maturity level.

Leadership, Strategy, Policy, Legal Frameworks

Achievements

Availability of:

- Electronic Document and Signature Law of 2009 is aligned with European and international standards and provides sufficient legal certainty to render certification services and sign documents electronically but only within the country (other countries' electronic signatures and certificates cannot be used)
- Operative Analytical Centre under the President's Office as e-Government Regulator as the key operator performing supervisory functions in the field of eID/TS by issuing relevant regulatory acts, such as: Order No 79 of 16 October 2012 On the State Public Key Infrastructure (PKI) Management System for digital signature verification (includes a Concept of PKI management); Order No 53 of 1 August 2013 On Approval of the Statute

of the Core Certification Centre; Order No 42 of 30 April 2012 On the Control rules in relation to the critically important information assets; Order No 49 of 29 July 2013 On the Reporting rules regarding the state of technical protection of information;

- Other key laws, regulations and programmes including: Law No 455-З of 10 November 2008 On Information, Informatisation and Information Protection; Presidential Decree No 515 of 8 November 2011 On Information Society development in Belarus; e-Government component of the National Programme of the accelerated development of ICT services for 2011-2015; Government Decree No 1074 of 9 August 2011 On e-Service provision via the State Automated Information; Presidential Decree No 200 of 26 April 2010 on Administrative procedures carried out by public bodies upon citizens' request; Law No 433-3 of 28 October 2008 On the Basics of administrative procedures; Presidential Decree No 708 of 30 December 2010 On Conducting electronic auctions; Presidential Decree No 618 of 17 November 2008 On Public procurement in the Republic of Belarus

Gaps

A need for:

- Bilateral and multilateral agreements for cross-border recognition of digital signature via Trusted Third Party mechanism

Infrastructures

Achievements

Availability of:

- A well-functioning and secure national system of electronic identification via digital signature access to which is affordable for citizens and entrepreneurs (the cost is 45 Euro for two years)
- National eID/TS standards based on international standards
- A National Public Key Infrastructure system established in 2012 to encompass certification service providers (certification centres) headed by the Core Centre; in 2014, a Republican Certification Centre started providing certification services under the supervision of the National e-Services Centre

-

Gaps

A need for:

- Wider use of Digital Signature as a key enabler of creating a national interoperability system (many sectoral information systems are interoperable as yet)
- Interoperability of sectoral information systems
- eID passport/card
- Participation in EU large-scale pilots (such as STORK)

Services

Achievements

Availability of:

- Mandatory electronic submission of tax declarations for legal entities paying VAT
- State Automated Information System serving as a platform and Portal (portal.gov.by) for e-service provision (e-Government System is in early stages of development and does not require digital signature for accessing e-services)
- 65% of public procurement processes realized online
- 50% of online procurement automated (mostly a Pre-award stage, Post-awards stage is not automated but can be realised via other services)
-

Gaps

A need for:

- Wider use of digital signature by private persons
- e-Services requiring electronic identification
- Mobile eID/TS

- Higher e-service maturity
- Use of eID in public procurement
- Expanded public procurement online at Award- and Post-Award stages

HDM roadmap

Leadership, Strategy, Policy, Legal Frameworks

- Develop plans for introducing digital signature for accessing e-services for greater security (at the moment, the national e-Government System is in early stages of development and does not require strong identification/ authentication)
- Create enabling legal and regulatory framework for secure identification in mobile environment
- Approximate national legal and regulatory framework as much as possible with the respective EU laws and regulations, especially the most recent ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation)
-
- Examine and adopt relevant EU best practices
- Discuss with the European Commission possible options and cooperation modalities for implementing eID/TS between Georgia and EU Member States (including mutual recognition of certification services and digital signatures via the mediation of the Trusted Third Party mechanism)
- Continue maintaining strong leadership and political will

Infrastructures

- Implement mobile eID/TS solutions including mobile digital signature
- Implement eID passport/card
- Harmonise data/information protection standards with those of the EU

- Ensure that national data/information protection standards are recognised internationally (e.g. by ISO)
- Consider possibility of joining STORK's (Secure identity across borders linked) eID platform for interoperable solutions for electronic identity and authentication across borders

Services

- Identify a number of e-services for cross-border access along with relevant trust services
- Raise levels of e-service maturity (from current situation of mostly one-way information provision and downloadable forms)
- Automate the full cycle of public procurement online

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Making national legislation compatible with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) as much as possible, so as to raise security of electronic transactions and make eSignature interoperable across borders in line
- Raising confidence in eID among ordinary citizens by harnessing personal data and privacy protection
- Adopting the European model of e-service maturity for citizens and businesses and approximating the list of such services with that of the EU
- Offering a number of e-services for cross-borders access
- Making all key stages of public procurement available online and integrating eID into tender processes
- Adopting a viable e-government interoperability strategy aligned with the principles of the European Interoperability Framework as closely as possible
- Maintaining strong leadership.

Pilot Projects

It is recommended that Belarus joins all four proposed regional projects in the field of Electronic identification and trust services, namely:

[1] Policy support for mutual recognition of eID/TS

[2] Piloting digital signature across borders

[3] Policy support to eService development and benchmarking including capacity building for eProcurement sector

[4] Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre

2.2.8 Georgia

State of play and gap analysis

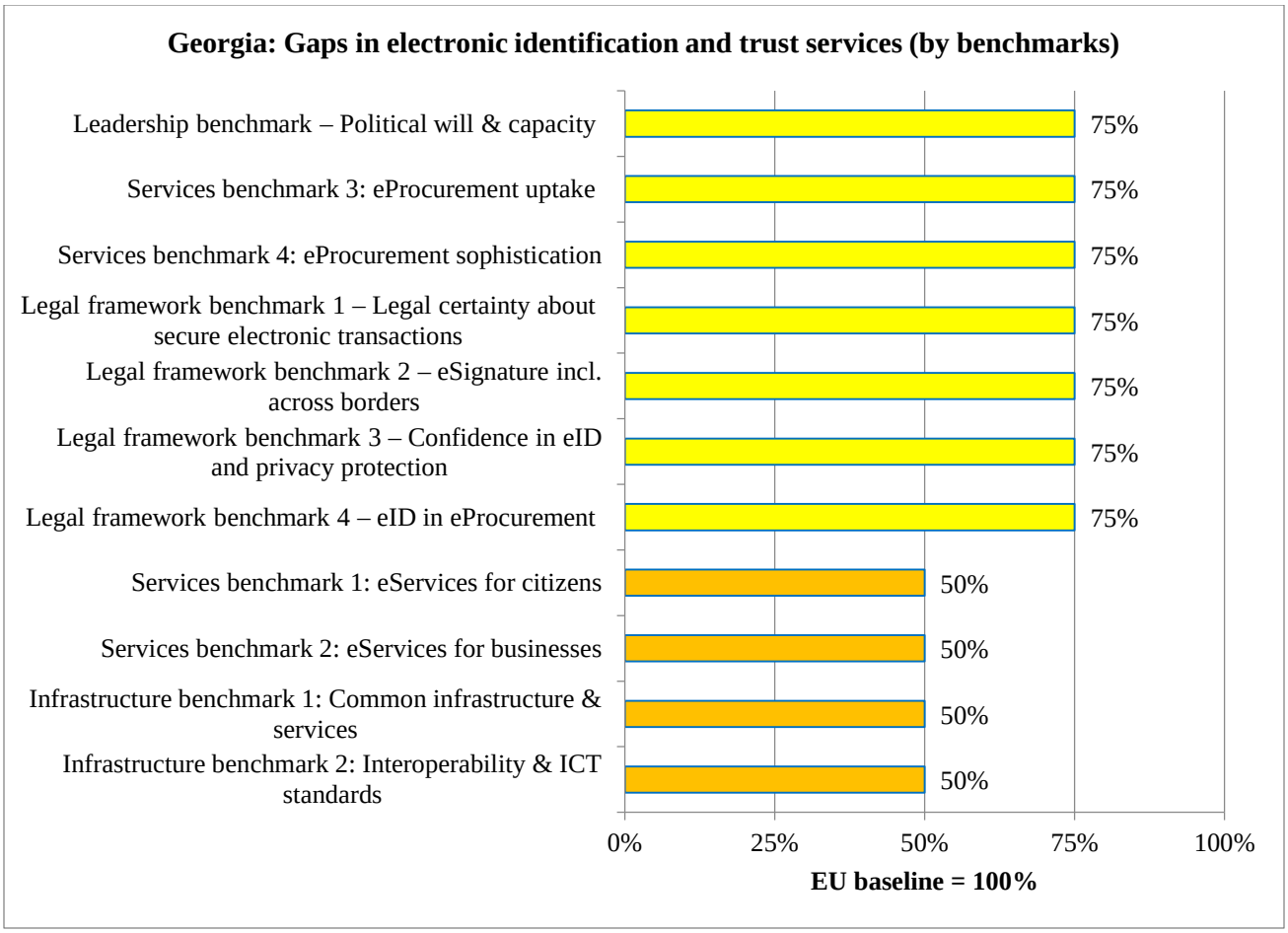

Exhibit 24 - State of play and gap analysis of Georgia in eID/eTS priority area

Georgia's progress in electronic identification and trust services has been consistent and smooth. The gap with the EU baseline across major benchmarks is moderate. Adopting EU policies and practices have been the main driver of the country's progress across the board. The current legal framework provides sufficient conditions for secure exchange of information between certification-service providers, consumers and businesses. There is a plan to start international cooperation in the field of mutual recognition of electronic trust services across borders. Strong and active institutional leadership has been demonstrated by the Data Exchange Agency of the Ministry of Justice in key e-government areas and ensured international attention and funding. Public e-services for citizens and businesses, coupled with common interoperable infrastructure, constitute key challenges to bring the country's state of play closer to that of the EU, especially as far as the legal and regulatory framework is

concerned. The main attention should be devoted to e-services, common e-government architecture and interoperability.

Leadership, Strategy, Policy, Legal Frameworks

Achievements

Availability of:

- Sufficient legal background and certainty in the provision of electronic identification and trust services including: Laws on Electronic Signature and Electronic document; Law on Personal data protection and online privacy; Law on Unified state register (Portal of Registry of Registries)
- Strong political will and adequate operational capacity on the government side; active leadership of Data Exchange Agency in eGovernance and related international cooperation activities including in interoperability
- Legal and regulatory framework for certification including the existence of the State Service Development Agency as an official certified authority
- Successful experience of international cooperation on mutual recognition of electronic identification (e.g. with Austria)
- Key institutions including Data Exchange Agency, Office of Personal Data Protection Inspector, State Procurement Agency to enforce respective laws
- National e-governance strategy that includes establishment of an interoperable environment for e-services by Data Exchange Agency that defines data standards and principles of the interoperability of state information systems

Gaps

A need for:

- Better approximation of national legal and regulatory framework with that of the EU
- Legal recognition of cross-border certificates of certification services and electronic signatures with EU Member States including via international agreements recognising eID/TS services across borders with non-EU states

- Capacity and competency building for successful approximation of respective legal and regulatory frameworks and adoption of best practice

Infrastructures

Achievements

Availability of:

- National eProcurement system with 100% of public procurement at Pre-award and Award stages done online
- Enterprise Architecture framework applied to build eGovernment infrastructure

Gaps

A need for:

- Full-fledged interoperability framework for common infrastructure (now part of the eGovernment strategy)
- Cross-border interoperability of electronic identification and trust services
- Participation in EU large-scale pilots (such as STORK)

Services

Achievements

Availability of:

- e-Services portal (my.gov.ge); Georgian Government Gateway (G3) as data exchange infrastructure for public bodies; Register of Registries and e-Catalogue (Service Catalogue)
- 100% take-up of online property tax declaration
- High impact e-services for citizens and businesses are estimated to be at maturity stages between 3 and 5 including e-services for getting passport/ID, changing of

residency address; registering marriage, divorce, birth adoption, change of name, death, power of attorney etc.

Gaps

A need for:

- Higher level of e-service maturity for citizens and businesses aligned with the EU maturity model
- Stronger take-up of e-services for businesses
- Cross-border recognition of open online tendering
- Mobile eID/TS

HDM roadmap

Leadership, Strategy, Policy, Legal Frameworks

- Identify discrepancies between (current and planned) national and EU legislation; approximate national legal and regulatory framework as much as possible with the respective EU laws and regulations, especially the most recent eIDAS ***Regulation No 910/2014*** ; discuss with the European Commission possible options and cooperation modalities for implementing eID/TS between Georgia and EU Member States
- Approximate national legislation governing public procurement in general and electronic procurement in particular with that of the EU
- Consider concluding international agreements to mutually access public services online including mutual recognition of digital signature, certification, identification/authentication and trust services across borders (in the letter and spirit of the eIDAS Regulation)
- Introduce relevant amendments to existing laws (e.g. Electronic signature) in line with European standards and practices
- Continue maintaining strong leadership of the Data Exchange Agency
- Align national e-Governance Strategy as much as possible with the Digital Agenda for Europe (DAE)

- Examine and adopt relevant EU best practices

Infrastructures

- Develop and implement a dedicated national interoperability framework based on best European and international practices (e.g. European Interoperability Framework)
- Implement the Registry of Registries within the EU-funded Public Administration Improvement programme
- Consider joining STORK's (Secure identity across borders linked) eID platform for interoperable solutions for electronic identity and authentication across borders

Services

- Start discussion with the European Commission on mutual recognition or cross-border eID/TS services for easier and more secure cross-border transactions
- Establish a trusted list of supervised/accredited certification service providers issuing certificates to the public
- Adopt EU's e-service maturity model and apply the same method
- Develop and expand basic sets of e-services for citizens and businesses similar to the EU's
- Automate the full cycle of public procurement, especially the Post-award stage; consider using electronic identification services (e.g. electronic signature) in the public procurement process to ensure the legislation assurance level for stronger security required by the EU eIDAS
- Ensure cross-border recognition of open online tendering
- Improve take-up of e-services for businesses
- Harmonise basic e-services for citizens and businesses with those of the EU
- Identify e-services for cross-border access along with relevant trust services
- Implement mobile eID/TS solutions including mobile digital signature

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Making national legislation compatible with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) as much as possible, so as to raise security of electronic transactions and make eSignature interoperable across borders in line
- Raising confidence in eID among ordinary citizens by harnessing personal data and privacy protection
- Adopting the European model of e-service maturity for citizens and businesses and approximating the list of such services with that of the EU
- Offering a number of e-services for cross-borders access
- Making all key stages of public procurement available online and integrating eID into tender processes
- Adopting a viable e-government interoperability strategy aligned with the principles of the European Interoperability Framework as closely as possible
- Maintaining strong leadership.

Pilot Projects

It is recommended that Georgia joins all four proposed regional projects in the field of Electronic identification and trust services, namely:

[1] Policy support for mutual recognition of eID/TS

[2] Piloting digital signature across borders

[3] Policy support to eService development and benchmarking including capacity building for eProcurement sector

[4] Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre

2.2.9 Moldova

State of play and gap analysis

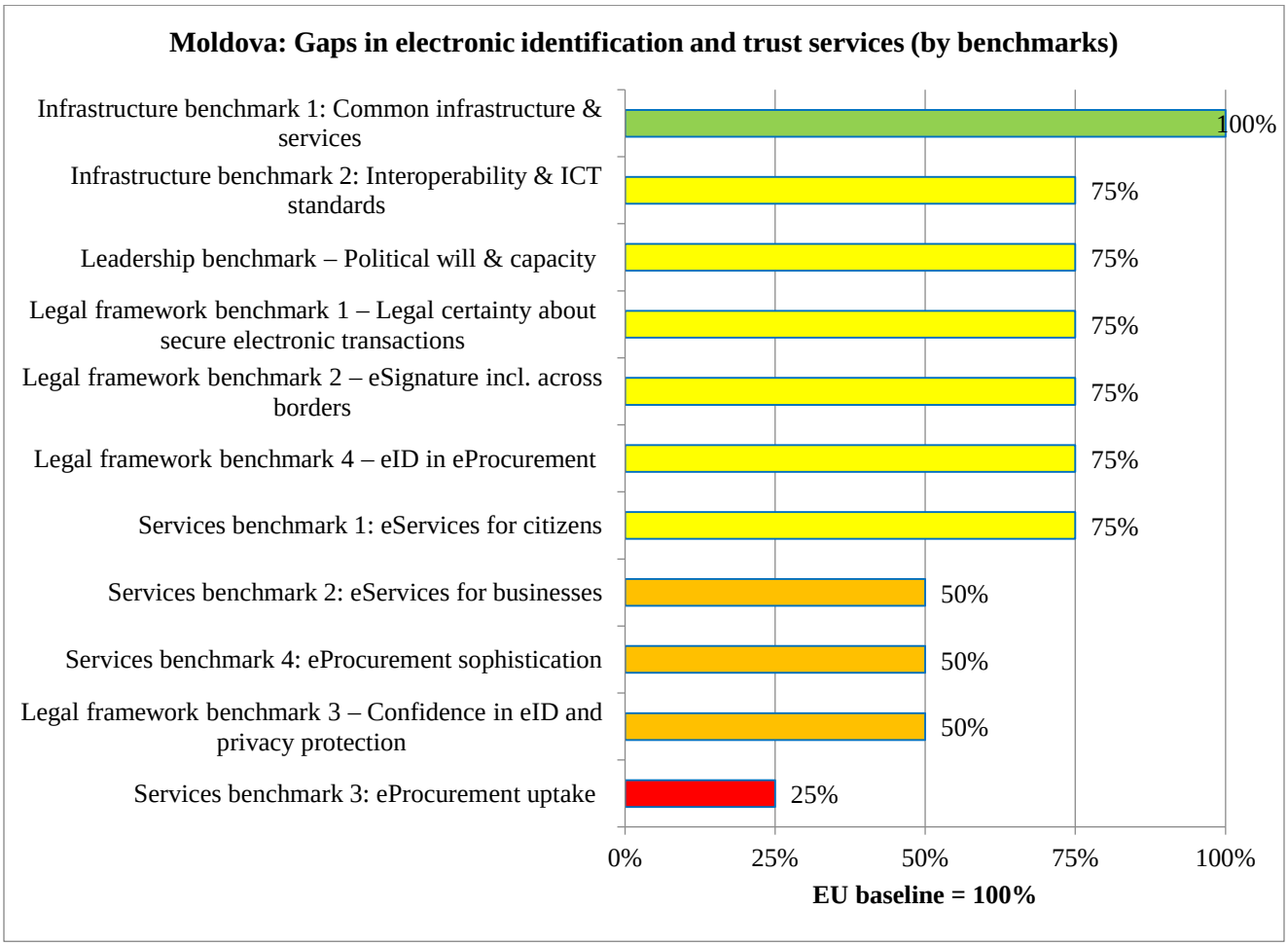

Exhibit 25 - State of play and gap analysis of Moldova in eID/eTS priority area

Moldova has demonstrated an impressive progress in aligning its legislation and actual practices with those of the EU. During a short period of time, the government has implemented a number of successful initiatives such as introducing mobile identification tools (MPass, MSign, MConnect, MPay)– key instruments for safe electronic transactions and for the development of the digital economy in general in compliance with the eIDAS Regulation[16]. Government

[16] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

platforms offer safe electronic interaction between companies, citizens and public authorities. e-Business and electronic trading is now possible both inside the country and abroad. The government has implemented the mobile signature infrastructure in a private-public partnership mode, at no cost for the government. All standards and technical specifications that are used in Moldova are in full conformity with the EU Interoperability Framework .

Moldova is one of the best performers in building digital market infrastructure and services. The government's common technology platform M-Cloud was built on the open architecture and European principles of e-government interoperability. Other initiatives are closing the existing gaps, especially in interoperability and digital signature. eProcurement remains a problematic area with the largest gap at the moment.

Leadership, Strategy, Policy, Legal Frameworks

Achievements

Availability of:

- National e-Government Strategy Moldova 2020 is aligned with the Digital Agenda for Europe 2020
- Strategic Programme for Governance Technological Modernization, described as Governance eTransformation approved by Government Decision No 710 of 20 September 2011
- Law No 91 of 29 May 2015 on Electronic Signature and Electronic Document is aligned with Directive 1999/93/EC as required by Annex XXVIII-B of the Association Agreement; the law contains Article 6 that legally recognises digital signatures issued in other countries and relevant certificates issued by foreign certification service providers under certain conditions and restrictions
- Law No 173 of 28.07.2011 On Ratification of the Financing Agreement between the Republic of Moldova and the International Development Association for implementation of the "Governance e-Transformation" Project
- Other key Government Decisions and resolutions include: No 198 of 23 April 2015 On Amending and supplementing the Government Decision No 122 of 18 February 2014 On the Programme on Public Service Reform for 2014-2016; No1090 of 31.12.2013 on

electronic service on control and authentication of access (M-PASS) to facilitate secured authentication and control of access of users in information system, including access to e-services; No 700 On Policy Concept on the principles of the open government data; No 405 of 02.06.2014 On Integrated Governmental Electronic Service Digital Signature (MSign); No 1096 of 31.12.2013 On Approval of the 2014 Action Plan for the implementation of the Strategic Programme for Technological Modernization of Governance (e-Transformation); No 1090 of 31.12.2013 On Government electronic service of access authentication and control (MPass); No 573 of 06.08.2013 On the Strategy for the Development of Public Finance Management for 2013-2020; No 972 of 21.12.2012 On Approval of the Action Plan for 2013 in terms of implementing the technological modernisation of the Government (e-Transformation);No 499 of 06.07.2012 On the e-Transformation unit within central public administration authorities; No 656 of 05.09.2012 On Approving the Interoperability Framework Programme; No 499 of 06.07.2012 regarding the e-Transformation unit within central public administration authorities; No 709 of 20.09.2011 On Some measures in the field of Governance e-Transformation; No 330 of 28.05.2012 On Creation and administration of unique governmental public services portal; No 195 of 04.04.2012 On Approval of the Action Plan on Open Government for 2012-2013 years; No 44 of 26.01.2012 On Approval of the Action Plan for 2012 for implementation of the Strategic Program for Governance Technological Modernization (e-Transformation); No. 222 of 01.04.2011 on the creation of the e-Transformation Coordinators Council; No 760 of 18.08.2010 On Approval of the statute of the public institution Electronic Government (e-Government) Centre

- Strong political will and adequate operational capacity on the government side; active leadership of e-Government Centre (State Chancellery)

Gaps

A need for:

- Comprehensive legal and regulatory framework for mutual recognition of eID/TS services across borders synchronized with eIDAS
- Cross-border interoperability of electronic identification and trust services
- Capacity and competency building for successful approximation of respective legal and

regulatory frameworks and best practice adoption

Infrastructures

Achievements

Availability of:

- Mobile signature in addition to the traditional e-signature ensuring secure identification in the mobile environment
- Integrated Government electronic service of the digital signature (M-sign) allowing the use of digital signature via eID card as well access to all e-services
- Moldova's interoperability standards and technical specifications in conformity with the EU Interoperability Framework
- Draft Concept "Development of the Private Cloud Platform (MCloud) for Government of Moldova developed by the e-Government Centre, in the context of the Governance eTransformation Agenda and Government Decisions No 710 of 20.09.2011 and No 128 of 20.02.2014
- State Register for Public Procurement that uses authentication and identification issued by digital certificates of the State Enterprise Centre of Special Telecommunication

Gaps

A need for:

- Participation in EU large-scale pilots (such as STORK)
- Adopting the draft regulatory framework for the implementation of the interoperability platform (M-Connect) during 2015-2020

Services

Achievements

Availability of:

- Over 100 various e-services on Servicii.gov.md; 40% of customs declarations (export) submitted online through e-Customs at stage 4; the majority of existing e-services for businesses are at stage 3 of service online maturity
- Order of the Fiscal Service No1223 of 26.08.2014 On Approval of instructions on mode of use of electronic fiscal services to regulate electronic services for citizens in fiscal area

Gaps

A need for:

- Digitisation of 500 public services for citizens and business by 2020 (Government Decision No 710 of 20.09.2011)
- Raising online maturity of basic public services
- Expand the online functionality of the public procurement process (less than 1/3 procurement procedures are realised online; electronic auctions, online submission of bids, automatic evaluation of tenders are not possible at the moment)
- Intensify take-up of e-services for businesses
- Consider open cross-border online tendering

HDM roadmap

Leadership, Strategy, Policy, Legal Frameworks

- Identify discrepancies between national (current and planned) and EU legislation; further amend the Digital Signature law to align with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) for easier and more secure cross-border transactions
- Ensure mutual recognition of trust services with the EU by eliminating existing restrictions with regard to the mutual recognition of certification service providers
- Consider concluding international agreements for mutual access to public services online including mutual recognition of digital signature, certification, identification/authentication and trust services across borders (in the letter and spirit of

the eIDAS Regulation)

- Approximate national legislation governing public procurement in general and electronic procurement in particular as per the Association Agreement and other EU laws and regulations
- Continue maintaining strong leadership and political will
- Examine and adopt relevant EU best practices
- Discuss with the European Commission possible options and cooperation modalities for implementing eID/TS between Moldova and EU Member States

Infrastructures

- Extend the validity of public key certificates for more than one year
- Ensure effective implementation of the Interoperability Strategy and adopt an enabling regulatory framework for the implementation of the interoperability platform (M-Connect) during 2015-2020
- Automate the full cycle of public procurement online starting with online electronic auctions integrated with e-invoice service; include e-Ordering and e-Payment functions
- Ensure effective implementation of the national interoperability framework
- Consider joining STORK's (Secure identity across borders linked) eID platform for interoperable solutions for electronic identity and authentication across borders

Services

- Start discussion with the European Commission on mutual recognition or cross-border eID/TS services
- Establish a trusted list of supervised/accredited certification service providers issuing certificates to the public
- Create adequate legal certainty for all existing and planned e-services for citizens and businesses
- Adopt EU's e-service maturity model and apply the same service benchmarking method

- Approximate basic, high-impact e-services for businesses and citizens with those in the EU at a high level of service maturity online (stages 4 and 5)
- Ensure cross-border recognition of open online tendering
- Ensure that digital signature can be used for identification and authentication purposes in online procurement processes
- Harmonise e-services for citizens and businesses with those of the EU
- Identify a number of e-services for cross-border access along with relevant trust services

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Making national legislation compatible with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) as much as possible to raise security of electronic transactions and make eSignature interoperable across borders in line
- Raising confidence in eID among ordinary citizens by harnessing personal data and privacy protection
- Adopting the European model of e-service maturity for citizens and businesses and approximating the list of such services with that of the EU
- Offering a number of e-services for cross-borders access
- Making all key stages of public procurement available online and integrating eID into tender process
- Adopting a viable e-government interoperability strategy aligned with the principles of the European Interoperability Framework as closely as possible
- Maintaining strong leadership.

Pilot Projects

It is recommended that Moldova joins all four proposed regional projects in the field of Electronic identification and trust services, namely:

[1] Policy support for mutual recognition of eID/TS

[2] Piloting digital signature across borders

[3] Policy support to eService development and benchmarking including capacity building for eProcurement sector

[4] Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre

2.2.10 Ukraine

State of play and gap analysis

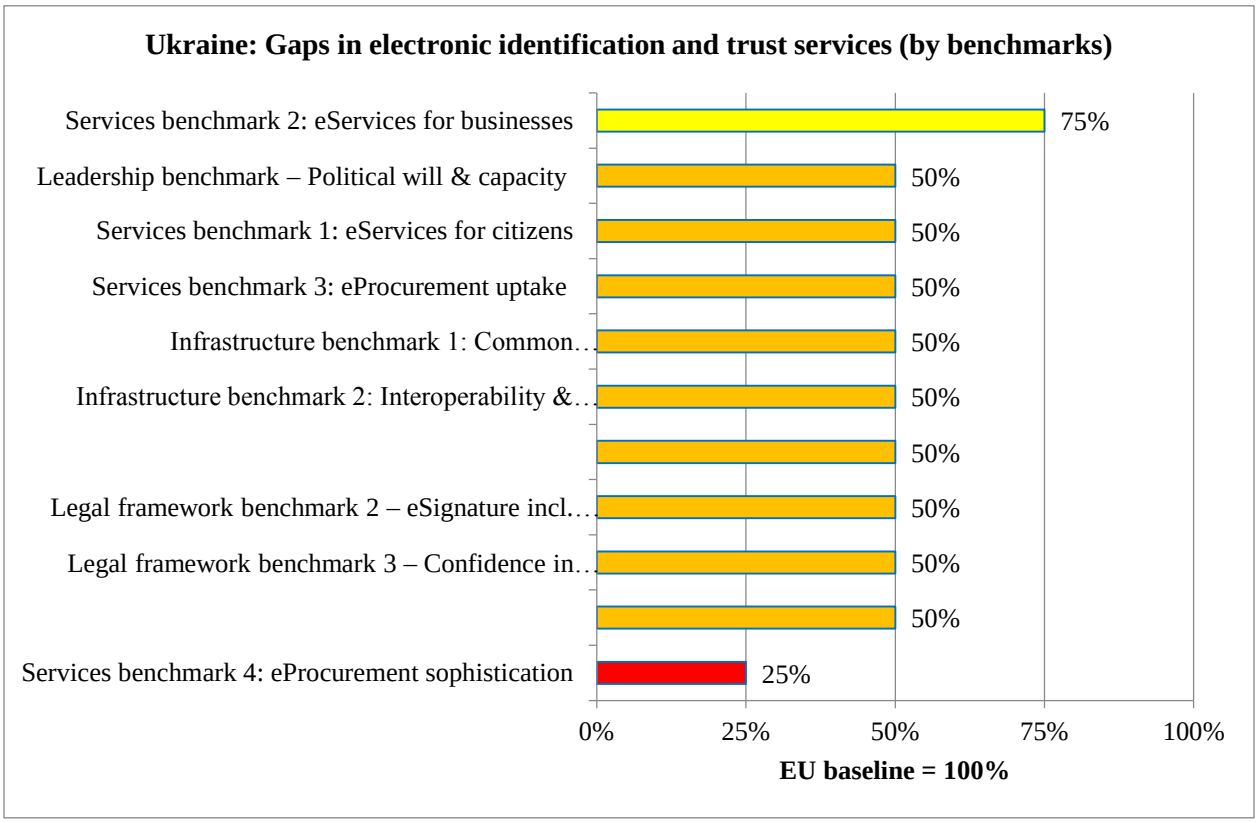

Exhibit 26 - State of play and gap analysis of Ukraine in eID/eTS priority area

The Ukrainian digital market has a vast potential estimated at the level of some 4 billion Euros[17]. However, e-Government developments for many years have lacked consistent national policies to integrate many disparate central and regional information systems unconnected through a common interoperability system. At present, Ukraine considers e-government development as is an important instrument for creating its digital market in line with the European standards, as envisaged by the Ukraine-EU Association Agreement. The country's leadership understand the importance of digital market technologies and provides necessary support. In 2014, the State Agency for e-government was created to implement relevant policies and develop adequate electronic infrastructure. A major recent breakthrough in aligning closer with European practices has been the elaboration of a draft Law on Trust services and its public discussion[18].

The gap with the EU baseline is significant for almost all benchmarks related to the field of eID/eTS. New institutions and laws should help facilitate bridge the gap. These substantial gaps are the result of the lack of strong political will and leadership to follow an information society agenda in the past.

To advance, the country needs to improve the provision of interactive, transactional online e-services for citizens (e-services for businesses, e.g. in customs and tax administration) that require secure electronic identification on the basis of the interoperable e-government architecture. eProcurement (typically, the most corruption-prone area) is the most problematic scoring significantly below the EU baseline.

At the moment, the use of electronic signatures is possible within Ukraine only (with some exceptions in the area of railroad-related exchange of information and data between Russia and Belarus). There are two trust services available within Ukraine – issuance of qualified certificates for electronic signatures and for electronic seals, including qualified time-stamping. The cross-border aspects of electronic identification are addressed in new law drafts on interoperability and trust services. Other alternative personal identification instruments are not available due to lacking legislation.

[17] EaPeReg Benchmarking Report – Benchmarking Electronic Communications Markets in EaP countries, 2015.

[18] http://etransformation.org.ua/2014/07/16/117/

The first priority will be to ensure that the new law is aligned with the EU eIDAS regulation.

Leadership, Strategy, Policy, Legal Frameworks

Achievements

Availability of:

- Fast progress over the past two years in accelerating e-government development (including Open Government) – the Ministry of Economics was charged to deal with digital services and e-Procurement while the Ministry of Justice is responsible for legal aspects of eID and trust services
- A new State Agency for Electronic Governance (under the Ministry for Regional Development, Building and Housing) established in 2014 to create an enabling legal environment and set new policies by passing new laws on Single Demographic Register (No 5492-17 of 1 January 2013) and Open Data
- A new law on Electronic identification and trust services in line with eIDAS Regulation including a White Book on the National Strategy of electronic identification
- Draft law on e-government interoperability framework (electronic interaction system)
- Other relevant laws and regulations include: On electronic documents and electronic document workflow (No 2599-IV of 31 May 2005); On the Concept of National information development programme (No 75/98-BP); On Digital Signature (No 852-15 of 15 January 2009); Resolution of Cabinet of Ministers N 930O of 13 July 2004 On Accreditation procedure of certification authority; Resolution On Approval of the central certification authority (No 1451 of 28 October 2004); Resolution On approval of the action plan for implementation of the Partnership and Open government initiative in 2014 – 2015 years (N 1176-p of 26 October 2014)

Gaps

A need for:

- Legal and regulatory framework for mutual recognition of eID/TS services inside the country and across borders

- Capacity and competency building for successful approximation of respective legal and regulatory frameworks and best practice adoption

Infrastructures

Achievements

Availability of:

- 60 IT-related standards approved in 2014 by the Ministry of Economics including for e-signature and cryptography (effective January 2016)

Gaps

A need for:

- Core registers
- Participation in EU large-scale pilots (such as STORK)
- Use of eID in public procurement
- Cross-border interoperability of electronic identification and trust services
- Mobile eID/TS

Services

Achievements

Availability of:

- 100% online service availability for submission of: Income tax declaration/ notification of assessment; Social contributions (for employees);Corporate tax (declaration, notification); VAT declaration/notification; Statistical data; Custom declaration
- White Book on e-services and a single portal on e-services (Ministry of Economics)
- Public procurement online pilots on eTendering under the threshold of 100,000 UAH

Gaps

A need for:

- Higher online maturity of basic public services for citizens and businesses
- Online public procurement
- Cross-border online tendering and electronic access to public procurement markets

HDM roadmap

Leadership, Strategy, Policy, Legal Frameworks

- Start discussion with the European Commission on mutual recognition or cross-border eID/TS services; identify discrepancies between national (current and planned) and EU legislation; discuss with the European Commission possible options and cooperation modalities for implementing eID/TS between Ukraine and EU Member States; - approximate national legal and regulatory framework as much as possible with the respective EU laws and regulations, especially the most recent ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation)
- Amend, as needed a Digital Signature law to align with eIDAS
- Ensure that the new law bills are in line with European standards (especially eIDAS regulation) for easier and more secure cross-border transactions
- Enforce effective implementation of the newly passed laws
- Review the relevance of other existing laws and amend them as needed
- Ensure mutual recognition of trust services with the EU by eliminating existing restrictions with regard to the mutual recognition of certification service providers
- Consider concluding international agreements for mutual access to public services online including mutual recognition of digital signature, certification, identification/authentication and trust services across borders (in the letter and spirit of the eIDAS Regulation 910/2014)

- Approximate national legislation governing public procurement in general and electronic procurement in particular
- Continue maintaining strong leadership and political will
- Examine and adopt relevant EU best practices

Infrastructures

- Streamline, rationalise and simplify the public procurement system (aligned with relevant provisions of the Association Agreement) and automate the entire procurement cycle
- Elaborate detailed action plans to implement e-government interoperability framework
- Ensure effective implementation of the national interoperability framework
- Consider joining STORK's (Secure identity across borders linked) eID platform for interoperable solutions for electronic identity and authentication across borders
- Implement mobile eID/TS solutions including mobile digital signature

Services

- Establish a trusted list of supervised/accredited certification service providers issuing certificates to the public
- Decide on priority e-services (develop a plan)
- Ensure effective implementation of the Interoperability Strategy
- Create adequate legal certainty for all existing and planned e-services for citizens and businesses
- Adopt the EU's e-service maturity model and apply the same service benchmarking method
- Approximate basic, high-impact e-services for businesses and citizens with those in the EU at a high level of service maturity online (stages 4 and 5)
- Automate the full cycle of online public procurement services

- Ensure cross-border recognition of open online tendering
- Ensure that digital signature can be used for identification and authentication purposes in online procurement processes
- Harmonise e-services for citizens and businesses with those of the EU
- Identify a number of e-services for cross-border access along with relevant trust services

Conditions for harmonisation

The key conditions for harmonisation are seen as follows:

- Making national legislation compatible with ***Regulation No 910/2014*** of 23 July 2014 on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation) as closely as feasible to raise security of electronic transactions and make eSignature interoperable across borders in line
- Raising confidence in eID among ordinary citizens by harnessing personal data and privacy protection
- Adopting the European model of e-service maturity for citizens and businesses and approximating the list of such services with that of the EU
- Offering a number of e-services for cross-borders access
- Making all key stages of public procurement available online and integrating eID into tender process
- Adopting a viable e-government interoperability strategy aligned with the principles of the European Interoperability Framework as closely as possible
- Maintaining strong leadership.

Pilot Projects

It is recommended that Ukraine joins all four proposed regional projects in the field of Electronic identification and trust services, namely:

[1] Policy support for mutual recognition of eID/TS

[2] Piloting digital signature across borders

[3] Policy support to eService development and benchmarking including capacity building for eProcurement sector

[4] Policy support to creating national e-government interoperability frameworks including setting up a Regional Demonstration and Knowledge Transfer Centre

2.3 eCustoms

The European Commission and the Member States have undertaken the task of setting up and operating secure, integrated, interoperable and accessible electronic Customs systems. Its purpose is the facilitation end-to-end supply chain logistics and customs processes for the movement of goods into and out of the European Union, as well as the reduction of risks of threats to citizens' Safety and Security by minimising the remaining differences between the Member States' customs processes.

The Community Customs Code has been providing the necessary legal basis (Legal framework) for the computerisation of customs procedures, declarations and data exchange (Infrastructure and Services).

For the purposes of this study, eCustoms includes not only the aspects directly related to the legislation, infrastructure and information systems of the customs administration, but also comprises aspects of cross border trade, and interaction between different government and non-government authorities involved in the procedures of issuing permits and certificates for external trade.

2.3.1 EU baseline

The EU baseline comprises the relevant EU legislation, best practices, standards and ICT platforms as appropriate for each HDM area. This EU baseline has been defined in consultation with DG TAXUD.

The following main sources are proposed for the definition of the EU baseline for eCustoms:

- The EU legal and regulatory framework related to eCustoms
- Infrastructures and information systems developed or planned for implementation by the

European Commission and the Member States

- Strategy and plans for the implementation of new projects
- Examples of best practice already implemented in the EU and EU Member States

Table 5 below summarises the relevant legal basis, infrastructure and systems of the EU baseline for eCustoms, together with the principal benchmarks (components) that are required to meet the baseline. The Annex contains the detailed description of the EU baseline for eCustoms[19].

EU Baseline[20]	Principal components required to achieve the baseline

Regulation (EC) n° 648/2005 - security amendment to the Community Customs Code	• Common criteria and priority areas for risk assessment
	• Risk Information Form (RIF)
	• Authorised economic operators status
	• Interoperating of systems for import, export and transit
	  ○ Automated Import System
	  ○ Automated Export System (AES)
	  ○ New Computerised Transit System (NCTS), NCTS – TIR
	• Authorised Economic Operators mutual recognition
	• Summary electronic declaration for pre-arrival and pre-departure information
	• Information systems interconnection for lodging Summary Declarations and their communication to other countries systems

Decision N° 70/2008/EC - Decision on the paperless environment for customs and	• Interoperating of systems of identification and registration for economic operators with the authorised economic operators system

[19] *Annex / EU best practice / eCustoms - Detailed description of the EU baseline*

[20] See Annex A for full references to the EU legal and regulatory references where not otherwise referenced

trade - 'Electronic Customs Decision'	• Single Electronic Access Points (SEAP)
Council Regulation (EEC) No 2913/92 - establishing the Community Customs Code	• Paperless environment for customs and trade
Council Regulation (EEC) No 2658/87 of 23 July 1987 - The legal base of the TARIC on the tariff and statistical nomenclature and on the Common Customs Tariff	• Integrated tariff environment and interconnection between the tariff related IT systems
Regulation (EU) No 952/2013 - The **Union Customs Code (UCC)** Commission Implementing Decision of 29 April 2014 establishing the **Work Programme for the Union Customs Code** **Regulation (EEC) No 2454/93** laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code	• Single Point for Entry or Exit of Data (SPEED) portal • Uniform user management and digital signatures • EU Single Window • System for management of electronic trade certificates • The electronic customs systems of the Community and the Member States • Registered Exporters System
Regulation (EC) No 312/2009	• Economic Operators Registration and Identification

- Economic Operators' Registration and Identification system	system
REGULATION (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights	• Anti-Counterfeiting and Anti-Piracy System

Table 7- Baseline and components required for eCustoms harmonisation

The Table 6 presents a set of indicators and the corresponding benchmarks that describe the enablers towards meeting the baseline defined in Table 7. From these indicators, a set of questions has been prepared so that when the answers to these questions are collected in the six Eastern Partner Countries.

Indicator	Benchmarks to achieve the Harmonised Digital Market in eCustoms
Legal framework	• Common criteria and priority areas for risk assessment • Risk Information Form (RIF) • Authorised economic operators status • Interoperating of systems of identification and registration for economic operators with the authorised economic operators system • Provisions for the paperless environment for customs and trade

Infrastructure	• Single Electronic Access Points (SEAP)
	• Interoperating of systems for import, export and transit
	  ○ Automated Import System
	  ○ Automated Export System (AES)
	  ○ New Computerised Transit System (NCTS), NCTS – TIR
	• Integrated tariff environment and interconnection between the tariff related IT systems

	• Single Point for Entry or Exit of Data (SPEED) portal • Uniform user management and digital signatures
Services	• Registered Exporters System • Economic Operators Registration and Identification system • Authorised Economic Operators mutual recognition • Electronic customs, management of electronic trade certificates systems • National Single Window for trade • Anti-Counterfeiting and Anti-Piracy System

Table 8 - Indicators and benchmarks for eCustoms

The Annex contains the detailed description of the EU baseline for three main dimensions:

- Legal framework
- Infrastructure
- Information systems

2.3.2 Overview of the state of play and gap analysis for the Region

The Region has some strong and weak aspects in relation to the EU baseline. The Region has made significant progress in some areas of the EU baseline.. The identified common gaps point to the required measures and indicate the projects that can be proposed at the Region level.

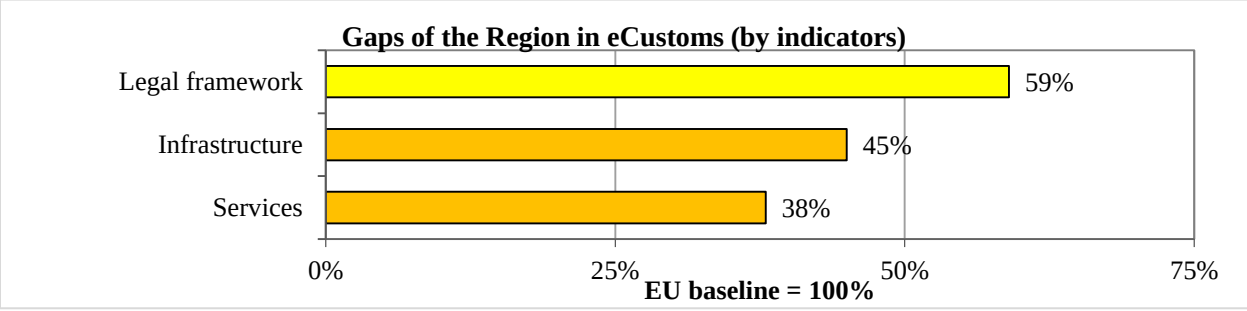

Exhibit 27 - State of play and gaps of the Region in eCustoms

The legal framework in eCustoms in the Partner Countries is the most advanced aspect towards harmonisation with the EU. The overall legal framework and several major regulatory provisions related to the eCustoms area are in line with the EU baseline.

The weakest aspect is information services. Several key information services have not yet been developed and implemented in the Region. Information exchange with the EU or even with other neighbouring countries is very limited, with the exception of Belarus and Armenia where an automated information exchange is organised.

The detailed gap analysis of the Region at benchmarks level shows more precisely, where progress on harmonisation in the eCustoms area could be achieved, as shown in Exhibit 28.

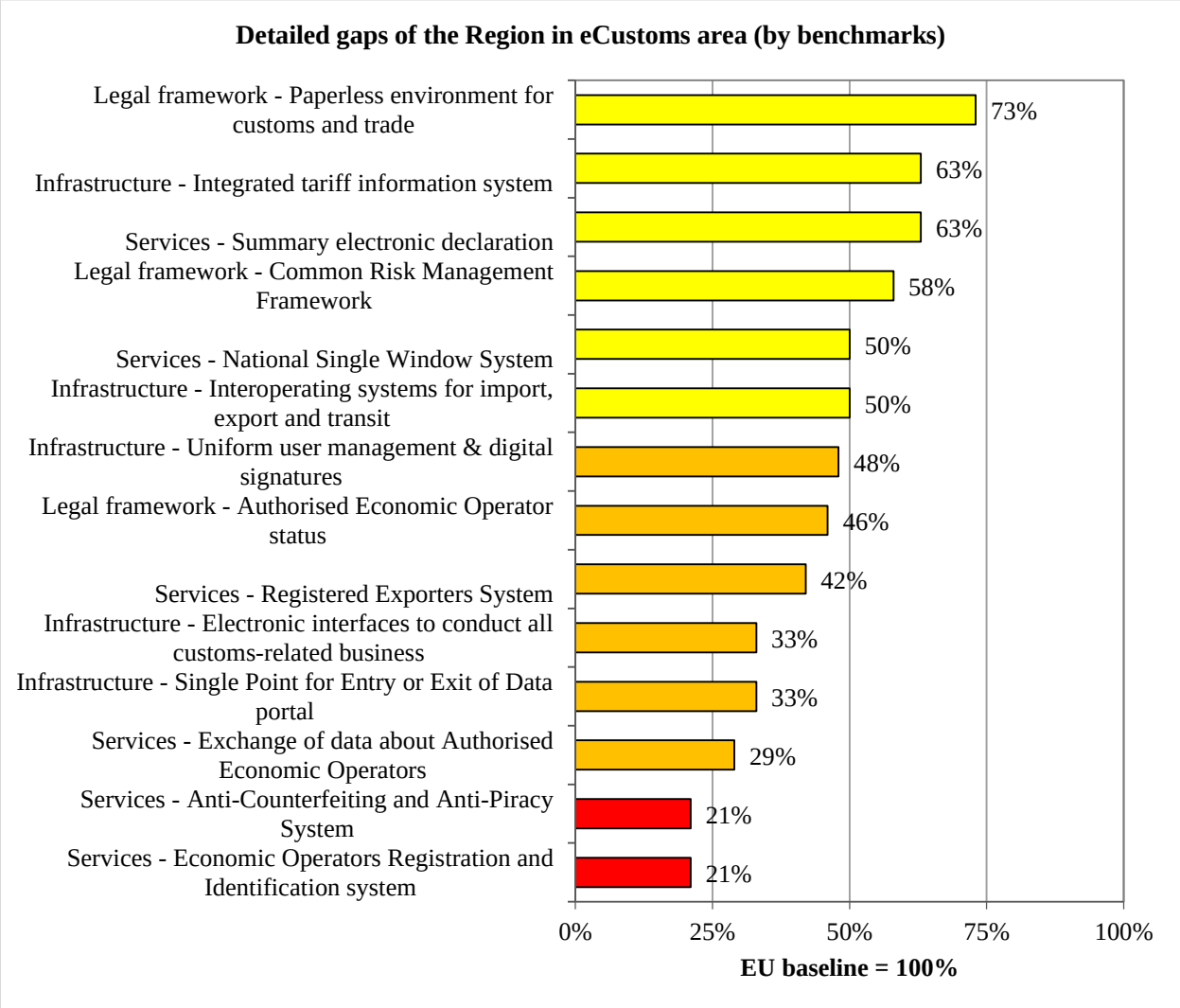

Exhibit 28-Detailed gap analysis of the Region in eCustoms

All Partner Countries have formulated a legal framework defining the paperless environment for customs and trade. The framework requires the use of data processing techniques for lodging summary declarations and for the electronic exchange of data between customs authorities, with a view to basing customs controls on automated risk analysis systems. Nevertheless, there is a gap in defining the interoperability of electronic customs systems with the customs systems of EU and third countries (with the exception of Armenia and Belarus, for which the international paperless environment is defined). The issue of accessibility of electronic customs systems to economic operators in third countries obstructs the creation of a paperless environment at the Regional level.

Most of the Partner Countries have implemented an integrated tariff information system. The next step toward harmonisation would be interconnection between the already existing tariff related IT systems aiming to achieve re-use of data and functionality of one system to another.

The biggest common gaps in the Region are in the implementation and use of information services such as a system for registration and identification of authorised economic operators. Most of the Partner Countries have introduced the status of Authorised Economic Operator(AEO). The countries where this status is operational (Azerbaijan, Moldova, Belarus and Ukraine) indicate that traders do not always realise any real benefit of getting this status because exports towards the EU are small. Implementation of information systems for the management of AEO profiles and exchange with the EU of data on authorised economic operators is at its beginning. In the Region, there are no countries that have concluded AEO Mutual Recognition Agreement with the EU.

None of the Partner Countries has set up an anti-counterfeiting and anti-piracy system that allows right holders to submit online claims and to ask the intervention of Customs in order to take measures against goods infringing certain Intellectual Property Rights (IPR). No information exchange has been undertaken with internationally or with EU centralised Anti-Counterfeiting and Anti-Piracy System (COPIS).

At the level of infrastructures, little has been done to implement electronic interfaces for economic operators so as to enable them to conduct all customs-related business, even if other countries are involved, with the customs authorities of the country where they are established. Belarus can act through the Partner Countries' customs systems, but there is no possibility for

traders of the Partner Countries to submit electronic documents to the customs authorities of other countries.

The usage of the Registered Exporters registration established in non-EU countries (Generalised System of Preferences beneficiary countries) exporting goods to the EU under preferential trade arrangements is only defined in Azerbaijan. Other countries still do not fully use this status. None of Partner Countries have organised a service of registration of their national exporters to the EU Registered Exporters System (REX).

Only the customs system of Ukraine is connected to the Single Point for Entry or Exit of Data portal (data exchange for New Computerised Transit System-NCTS between the EU and countries which are not a candidate for EU membership e.g. Ukraine, Russian Federation, Albania), the secured network infrastructure that is provided by the European Commission to facilitate the exchange of information between the National Administrations of the Customs and Taxation area. This kind of system allows secure data exchange between the EU and countries, which are not candidates for EU membership. Ukraine exchanges data on transit within the New Computerised Transit System (NCTS).

2.3.3 Overview of common actions for the Region

The following priority actions have been formulated on the basis of analysis of the biggest gaps identified for the ensemble of the Partner Countries.

Electronic services

Set up an Economic Operators' Registration and Identification system. Authorised economic operators benefit from facilitations with regard to customs controls relating to security and safety and/or from simplifications based on the criteria for granting such status that are recognised in the EU Member States. Economic Operators' System – Authorised Economic Operator subsystem (EOS-AEO) is an existing and operational information system that interconnects the authorities of the EU Member States and DG TAXUD. The EaP countries can consider negotiating AEO Mutual Recognition Agreement with the EU. The AEO Mutual Recognition (AEO MR) project aims to ensure the exchange of AEO data among Member States, DG TAXUD and third countries in a uniform way to increase security and facilitation.

Set up an Anti-Counterfeiting and Anti-Piracy System. The system is intended to enhance intellectual property rights protection by improving the cooperation and sharing of information

between right-holders and the national Customs administrations and between all the Customs offices of the Region. An electronic service provides traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. The national Anti-Fraud Information System can exchange data within the Partner Countries and be connected with the EU centralised Anti-Counterfeiting and Anti-Piracy System (COPIS), which is accessible by all Member States.

Automate the exchange of data about Authorised Economic Operators with the EU. The Partner Countries should implement national information systems for registration and identification of economic operators using the Economic Operators Registration and Identification (EORI) numbering approach. These systems contain data about economic operators' profiles. Based on the profiles, the country's authorities can attribute different trust level status to different economic operators. A Centralised Economic Operators Registration and Identification information and communication system supporting the concept of the Authorised Economic Operators, enables the national administrations of the Member States to grant AEO status (including online consultations) and provides access to the list of the AEOs for business needs. The Partner Countries can then conclude mutual recognition agreements with the EU and ensure the exchange of AEO data in a uniform way to increase security and facilitation. The economic operators of the Region will benefit from reduced physical and document based controls as well as priority treatment.

Create national segments for the Registered Exporters' System. The Region should establish a Registered Exporters System (REX) that allows automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The Region can cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission. The REX system is designated for economic operators from non-EU countries benefiting from preferential trade arrangements under the Generalised System of Preferences and exporting goods to the EU.

Infrastructures

Create Electronic interfaces to conduct all customs-related business (single point). The service of single access points enables economic operators to use one single interface to lodge electronic customs declarations, even if the customs procedure is carried out in another country. It allows traders to lodge their electronic pre-arrival/pre-departure, summary and full customs

declarations via one single interface of their choice that connects their system with other countries' customs systems. The data is automatically made available to any customs office responsible for the place at which goods have been, or are to be, presented, irrespective of the country concerned. Then the national segments of the Partner Countries can be connected with the EU Single Electronic Access Point (SEAP) which provides the framework environment where traders can be connected in order to interact with EU Customs.

Implement infrastructure for data exchange of electronic customs systems within the Region. The Region's computerised transit, export, import and economic operators systems have to allow data exchange with electronic customs systems between each country and the EU Member States. In the EU, a Common Communications Network / Common Systems Interface (CCN/CSI) operational infrastructure consists of a closed and secured network infrastructure that is provided by the European Commission (DG TAXUD) to facilitate the exchange of information between the National Administrations of the Customs and Taxation area. A Technical infrastructure solution that enables automated data exchange between Member States' electronic customs systems and the Partner Countries that are not linked to CCN/CSI on the basis of EU bilateral or multilateral agreements should be developed and implemented. To support this initiative, a generic technical solution which permits each partner to connect to a system developed centrally has to be developed.

Implement uniform user management and cross-border usage of electronic signature signatures. A common solution for electronic signatures (or a system based on mutual recognition of existing solutions) has to be operational in the Region to enable the economic operators to send electronically signed documents not only to administrations other than customs inside each country, but also to other countries. This system should enable these administrations to verify the authenticity of the author, of the sender and of the information. An advanced level of uniform user management and digital signatures system would allow economic operators to send information to administrations of the Region and to some neighbouring countries.

Common projects between the Partner Countries

The study has identified several aspects of mutual interest for the Region where it is possible to propose several multi-country projects for the ensemble of the Partner Countries:

- Exchange of summary electronic declaration for pre-arrival and pre-departure information.

- Exchange of data on Authorised Economic Operators.
- Uniform user management and the digital signatures framework.
- System for exchange of electronic trade certificates.
- Common Anti-Fraud Information System.
- Systems interconnection for lodging preliminary and summary declarations.
- Single Window – interconnected paperless environment for customs and trade.

2.3.4 Benefits for and readiness analysis of the Region

Benefits for the Partner Countries from harmonisation with the EU

- The Region would benefit from the usage of common Community risk profiles that help to spot priority control areas, and indicate suitable measures as required under the rules concerning a Community Risk Management Framework. An example of the use of Risk Information Forms is the dissemination by the Commission to all Member States and to Candidate Countries risk analysis centres of information regarding protection measures relating to avian influenza in Thailand. The EU customs have been given detailed information to include in their risk assessment strategies to support their controls in the fight against the possible illegal importation of prohibited poultry products from Thailand.
- The status of authorised economic operator granted by one Partner Country or one EU Member State should be recognised by the other Partner Country and by any EU Member State, so that an authorised economic operator shall benefit from facilitations with regard to customs controls relating to security and safety and/or from simplifications provided for under the customs rules in the ensemble of the countries.
- Provisions for the paperless environment for customs and trade (use of data processing techniques for lodging summary declarations and for the electronic exchange of data between customs authorities, with a view to basing customs controls on automated risk analysis systems) offer to economic operators a wide range of electronic customs services enabling them to interact in the same way with the customs authorities of any Member State or of any Partner Country.
- Uniform user management and digital signatures mutual recognition allows traders to

access electronic services in the ensemble of the EU and the Region. This enables the provision of a unique interface to a number of central services implemented by the EC for traders (SPEED for the Region and others); therefore, effectively addressing the lack of harmonised interfaces for trade and the redundant implementations of services of common functionality for Member States and the Region. For example, economic operators from the EU or the Region can use a service jointly developed by the Region (such as submission of transit declaration). It would mean that customs administrations will not implement functionality (or systems) offering the same service. It will contribute to effectively addressing the lack of harmonised interfaces for Trade and the redundant implementation of services of common functionality in the EU and the Region.

- The use of the Economic Operators Registration and Identification system by economic operators from the Region simplifies the procedures for them in the EU countries. On the other side, the customs authorities in the EU have easy and reliable access to operators' registration and identification data. Economic operators not established in the customs territory of the Community should be registered if they perform one of the following main activities: lodge a summary in the Community (e.g. a summary declaration for temporary storage), lodge an exit or entry summary declaration in the Community; operate a temporary storage facility; apply for an Authorised Economic Operator certificate.
- Harmonisation in the area of requirements for submission of summary electronic declaration for pre-arrival and pre-departure information allows implementation of appropriate risk-based controls both for the EU Member States and for the Region.
- Harmonisation of EU Customs Single Window and Single Windows brings benefits to enable economic operators to lodge electronically, and only once, all the information required by customs and non-customs legislation for EU and cross-border movements of goods. The national single windows can be connected to one another and will be supported by the Single Electronic Access Point (SEAP).

Benefits for the EU from harmonisation with the Region

- Common criteria and priority areas for risk assessment establish an equivalent level of protection in customs controls for goods brought into or out of the customs territory of the Community extended by the territories of the Region.

- An increasing number of authorised economic operators in the Region will reduce the expenses in the EU Member States for the procedures related to customs controls, security and safety measures.
- A system of identification and registration for economic operators interoperating with the authorised economic operators system and enabling those economic operators to register only once for all their interactions with customs authorities throughout the Region will reduce operational expenses for customs and trade procedures both in the EU and the Region.
- Deployment of the Single Electronic Access Points (SEAP) in the Region and implementation of electronic interfaces for economic operators enable them to conduct all customs-related business, even if several EU Member States and/or Partner Countries are involved, with the customs authorities of the Member State where they are established (or Partner Country).
- Systems for import and export interoperating with the system for transit enable the seamless flow of data from one customs system to another throughout the whole of the Community and the Region. This creates an advantage in reducing submissions in every country inside the Region with the harmonised rules through which goods are passing.
- A Computerised and operational transit system working in all Member States and the Region (the UCC Transit System including extended NCTS) would allow the temporary suspension of duties, taxes and commercial policy measures that are applicable at import, thereby allowing customs clearance formalities to take place at the destination rather than at the point of entry into the customs territory. The objective is to provide full control of the EU+Regional leg of TIR movements and to facilitate the termination/discharge of TIR operations within the Community and the Region by replacing the return of Voucher No 2 with the sending of NCTS messages
- The Registered Exporters System aims to make up-to-date and complete information available on Registered Exporters established in non-EU countries (Generalised System of Preferences beneficiary countries) exporting goods to the EU under preferential trade arrangements. Exporters should be registered with the competent authorities of the beneficiary countries in order to be entitled to make statements on origin if the total value

of originating products in a consignment exceeds €6,000. In addition, the registration of exporters will facilitate targeted ex-post controls. In order to register exporters, each beneficiary country should use the REX established by the European Commission. Through the system, put in place for the benefit of administrations and Economic Operators in the EU and in beneficiary countries, the Economic Operators should be able to check – before declaring goods for release for free circulation – that their supplier is a registered exporter in the concerned beneficiary country. Similarly, EU economic operators should be registered with the competent authorities in the Member States for the purpose of bilateral accumulation of origin and splitting of consignments to be sent to beneficiary countries.

- The Authorised Economic Operators Mutual Recognition aims to ensure the exchange of AEO data among Member States, DG TAXUD and third countries in a uniform way to increase security and facilitation. The economic operator from the Region benefits from reduced physical and document based controls and priority treatment by the customs authorities in the EU Member States.

Conditions for the harmonisation of digital markets

Challenges

- The harmonisation of digital markets requires important financial resources, especially for the implementation and upgrading of information systems. The Partner Countries have limited financial resources for it. Costs and benefits analysis should be carefully performed for every potential project in order to select the most valuable with the highest economic impact.
- A Rapidly changing legal framework in the Region related to the harmonisation with the EU will create a challenge for economic operators to understand this rapidly changing environment and operate in it.
- For mutual recognition of Authorised Economic Operators, the Region needs to have a single residency scheme. For some of the Partner Countries (Armenia and Belarus), this will be established in the EEU by 2017. In addition, mutual recognition will require harmonisation of all current requirements for AEOs between countries.

Risks

- Common criteria and priority areas for risk assessment in EU countries can be inappropriate for the Partner Countries
- Risk information forms cannot be openly shared with other states for national security reasons.
- Risk of abuse and non-respect of the procedures for granting the status of authorised Economic Operator.
- For the implementation of the paperless environment for customs and trade, the complexity and multiple stakeholders of the process could delay the launch of pilot projects. System effectiveness significantly depends on the involvement of private companies that operate in the transportation and logistics sectors.

Obstacles

- Economic operators currently realise little practical benefits from the status of Authorised Economic Operator.
- Successful implementation of the eCustoms environment needs implementation of the electronic procedures in all state authorities related to control of goods crossing the border.

Conditions

- In case of further integration with the EU eCustoms, a full and detailed gaps analysis between the Common Risk Management Framework and the Partner Countries risks frameworks should be performed. Implementation of any measures shall be done with gradual and carefully timed approach taking into account the difference in the nature of risks faced by individual countries.
- Successful harmonisation requires learning from the experience of other countries in this sphere, such as the experience of the new EU Member States or countries at the pre-accession stage.
- Strong political support and leadership in the EU and the Partner Countries.

Opportunities

- Further facilitation of trade development between the Region and the EU
- Unique opportunity for the administrations of the Region to improve their operational practices within implementation of collaboration projects with their counterparts.
- Countries will benefit from technological development related to opportunities for creation of new approaches, tools and systems.

Impact of EEU membership on the HDM with the EU

The Eurasian Economic Union (EEU) has a significant impact on eCustoms development, not only in Belarus and Armenia, but also throughout the Region due to historical economic linkages between these countries. At present, the EEU also focuses on the development of paperless trade, risk management approaches, uniform user management and interconnection of national information systems.

Several aspects reflected in the eCustoms EU baseline have been implemented or under implementation in the EEU with its own approach and perspective. The cooperation between the Region and the Eurasian Economic Union would bring significant benefit to both parties. The most critical aspect is assuring seamless flow of information and data to facilitate cross border trade between the EU, the Region and the EEU.

The detailed description of the role and the benefits of the Eurasian Economic Union's membership on the HDM with the EU is presented in the Appendices (Detailed state of play description of the Partner Countries / eCustoms).

2.3.5 Armenia

The Ministry of Finance, which has recently combined the national tax and customs authorities, is responsible for the sector of external trade. Armenia has been harmonising towards the EU regulations in the area of eCustoms. Significant achievements have been recorded in ensuring paperless environment for customs clearance, access to national single window, single databases of operators of foreign trade, etc. However, interoperability with other internal state systems and especially with international counterparts is quite limited. The Ministry of Finance is already working on policies to harmonise Armenia's regulations to the EEU standards.

State of play and gap analysis

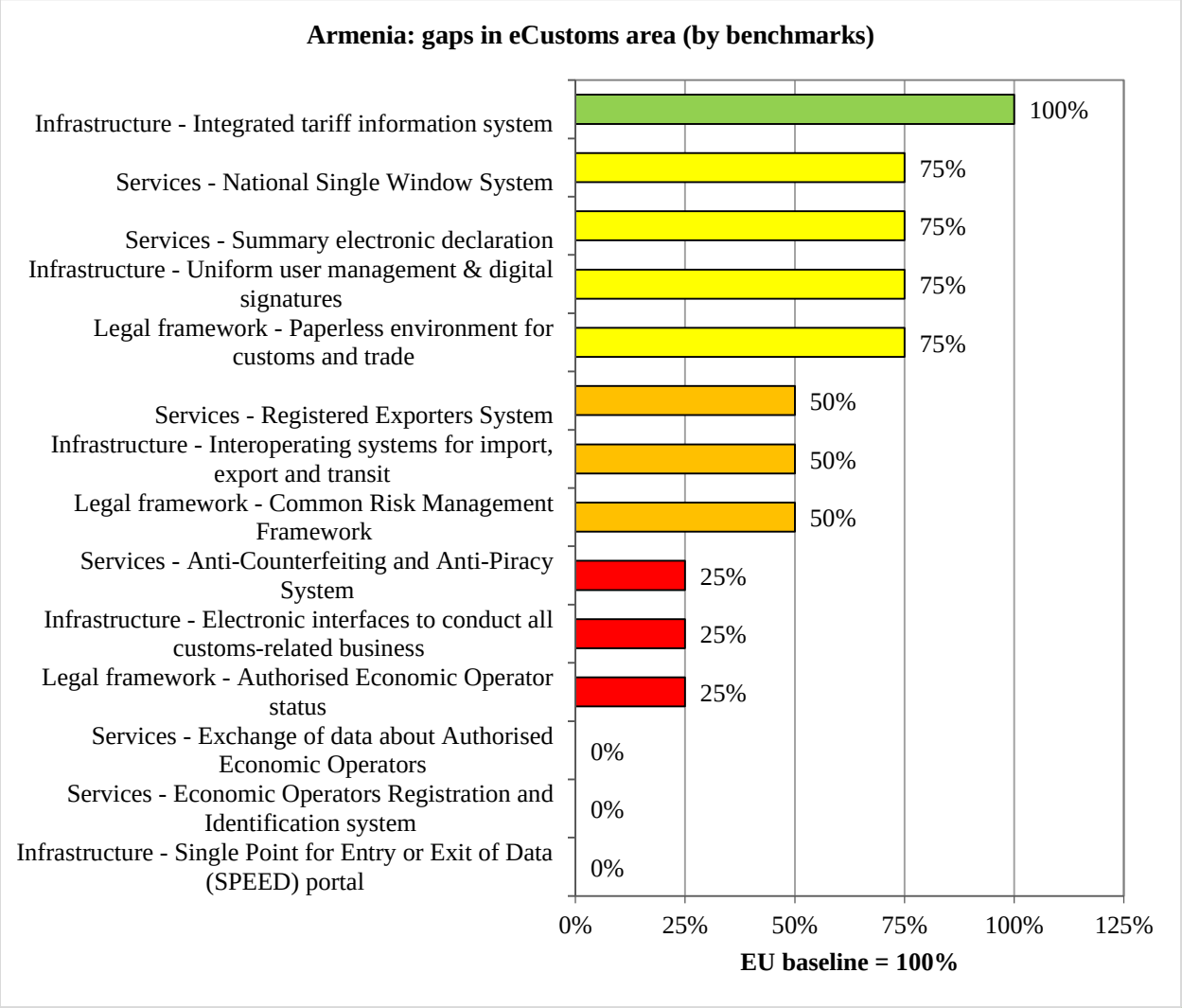

Exhibit 29- Armenia: state of play and gap analysis in eCustoms

Legal framework

Armenia's national risk management system is developed based on the WTO requirements. According to a recent programme/ study Armenia's regulations in this area are almost 100% in accordance with EU regulations. In relation to the integration with the Eurasian Economic Union, the legal framework of the latter stipulates that the currently deployed risk management systems in the member states are not subject to change. The Eurasian countries will continue using their national risk management systems. The exchange of risk information is currently carried out based on requests through the Ministry of Foreign Affairs or the Ministry of Finance. The risk

analysis uses automated data processing techniques but is not fully automated. There is no single interface or platform available with other countries. Armenia has defined the national risk management framework in customs controls for goods brought into or out of the country. The framework is harmonised with the EU common criteria and priority control areas. The Risk Information Form currently cannot be exchanged electronically with customs offices of the EU countries.

The Law defines the requirements, procedures and benefits of the authorised economic operators. Despite the amended version of the regulations, there are no registered AEOs in Armenia. There is a certain lack of motivation for local enterprises to become AEOs. The customs authorities of the country apply common criteria and harmonised requirements for granting the status of authorised economic operators (with fewer restrictions comparing to the EU criteria), allow the use of simplifications by authorised economic operators and recognise the status of AEOs registered in the EU Member States or other countries. The National system of identification and registration for economic operators does not interoperate with the Authorised Economic Operators EU system.

National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information. The electronic customs system does not currently allow the exchange of data between the customs authorities of Armenia and customs authorities of any other country, economic operators, other administrations or official agencies involved in the international movement of goods.

Indicator 2: Infrastructure

Economic agents in Armenia can declare their goods at any cross border point within the country independently of the exact point of exit of the product. However, the examination (if needed) is done only in one centre – in Yerevan. The country's single access point is not connected to the access points of other countries.. There is no single information infrastructure in place. The existence of a single platform will require integration of corresponding legislations and regulations in one place which is a significant effort and requires considerable time. By 2017 Armenia will have a legislative framework in agreement with the EEU requirements in place. The information systems of the country do not have a single access point so as to enable

economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries (EU Member State or others). This work within the Eurasian Economic Union has been planned to start from the development of the required legal framework.

The customs system is almost 100% electronic. The interfaces for the export, import and transit areas are different but they operate in the same environment and can exchange information among each other. The systems are fully interoperable within the country but are not connected to other countries' systems. There is no service that can currently ensure transfer of data between the national customs systems to/from customs system of the EU Member States.

All information sources refer to the Law on Customs for reference about binding classification. Currently the Ministry of Finance works with the Eurasian Economic Union on harmonising 18 components in this area. The country has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is interconnected with other tariff related IT systems to facilitate re-use of data and functionality of one system to another.

The country's computerised transit, export, import or economic operators systems are not connected to the Single Portal for Entry and Exit of Data portal which allows data exchange for electronic customs systems between the country and the EU. SPEED has the key objective to facilitate trade of the EU with third countries and/or exchanges with non-Customs systems.

The e-signature system is in place in Armenia. The system is based on mutual recognition of solutions for electronic signatures and enables the national economic operators to send information to administrations other than customs, and to enable these administrations to verify the authenticity of the author, of the sender and of the information. The national electronic signature framework is not interoperable with e-signature frameworks of other countries.

Services

As soon as a company is registered in the state registry, the data about the company is automatically entered into the database of the Ministry of Finance. When the company begins to export, its activities are recorded in the same database. The regulatory framework does not allow registering the data of local companies in the European REX database. There are no efforts undertaken in registering local exporters in European REX. Armenia has a national

database of legal entities that also include data on their export activities. This cannot be considered as a proper Registered Exporters System. There is no possibility for automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country does not cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

Registration and Identification numbering system is not operational in the country. The national systems containing profiles of traders are not interconnected with the EORI central database managed by the EC.

Economic operators are registered in different registries, including the state registry, tax payers' registry and customs registry. The AEO status is regulated by the law, however there are not registered AEO in Armenia yet. The country does not have a dedicated information system for registration and Identification of economic operators. It has not concluded an agreement of mutual recognition of the country's registers of economic operators and the Authorised Economic Operators in the EU. There is not system-to-system interface allowing the economic operators' data received from the country to be disseminated to the EU Member States or the country's AEO status in the EU transaction systems to be validated.

An electronic summary declaration containing the required pre-arrival or pre-departure information will be ready by the end of 2015. Currently the information is exchanged via the Ministry of Finance. The Ministry of Foreign Affairs provides the information without any limitation in the countries. By the end of 2015, it will be possible to lodge an electronic summary declaration containing the required pre-arrival or pre-departure information before any goods are brought into or out of the territory of the country. All information will be provided to the customs and other authorities in electronic format. Existing national infrastructure allows such information to be shared electronically with third countries where an international agreement provides so.

According to corresponding order by the President of the Republic of Armenia, the single window principle is implemented in various areas, such as pharmaceuticals, food safety, etc. In a number of areas the introduction of Single Window is underway according to the planned timeline (Government Decree 2015-2017). The national single window and one-stop shop in the area of external trade (different degree of readiness for different applications) is in place and allows submission of all required information and documents in electronic format (application for

certificates, customs declaration, required documents, permits). Administrations or agencies will be able to deliver certificates required for import or export authorisation in electronic format.

Armenia is part of intellectual property agreements (IPM). No other exchange of information is taking place. There is no electronic service in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. There is no exchange of electronic information with the EU centralised Anti-Counterfeiting and Anti-Piracy System information system, which is accessible by all Member States.

HDM roadmap

Legal framework

Common Risk Management Framework. Develop information system and interface to permit the secure electronic transmission and secure exchange of risk information forms with the electronic Risk Information Form (RIF) system.

Authorised Economic Operator status. Create and promote incentives for the authorised Economic Operator status in the country. Create an interoperating system for exchange of data between the national system of identification and registration of economic operators and the Authorised Economic Operators EU system.

Infrastructure

Electronic interfaces to conduct all customs-related business. Plan the development of a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to customs systems of the EU member state through Single Electronic Access Point (SEAP).

Interoperating systems for import, export and transit. Design and develop a service for transfer of data between the national interoperating customs systems of export, import and transit to/from customs system of the EU Member States and the systems of the Region.

Single Point for Entry or Exit of Data (SPEED) portal. Initiate cost/benefits study for the development of an interoperability and mutual recognition frameworks for electronic signatures of Armenia and the EU Member States, and the Region. Assess the benefits of development of a common framework for mutual recognition of electronic signatures for the Region.

Services

Registered Exporters System. Create a regulatory framework for the status of registered exporter that can bring benefits of simplification for some administrative procedures for eligible legal and natural persons. Extend the functionalities of the existing database of the Ministry of Finance to accommodate data related to the registered exporter status. Cooperate with the European Commission in order to organise registration of national exporters into the EU REX central database.

Economic Operators Registration and Identification system. Conduct a feasibility study about the introduction of economic operators' registration and identification numbering system in Armenia. Implement the EORI approach based on EORI number that serves as a common reference in the relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. Conduct costs/benefits analysis for interconnection of the national system with the EORI central database managed by the European Commission.

Exchange of data about Authorised Economic Operators. Update one of the existing registers' information systems containing data on economic operators (state register, customs, and tax payers) to contain data on authorised economic operators. Promote the registration of qualified economic operators. Conclude mutual recognition agreements with the EU to ensure the exchange of AEO data in a uniform way to increase security, facilitation of reduced physical and document based controls, and priority treatment.

Anti-Counterfeiting and Anti-Piracy System. Create a national Anti-Fraud Information System - an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Connect the national Anti-Fraud Information System with the EU centralised Anti-Counterfeiting and Anti-Piracy System and similar systems of the Region.

2.3.6 Azerbaijan

The State Customs Committee of Azerbaijan is the central executive body responsible for formation, execution and regulation of state policy on Customs in Azerbaijan. Relevant legislation:

- Customs Code
- Resolution of the Cabinet of Ministers on the “Approval of the Rules for rendering of electronic services by central executive bodies on specific spheres” and on the “Approval of the list of e-services’ types”, dated 24.11.2011, #191

According to the Cabinet of Ministers’ Resolution dated 24.112011, on approval of “Rules for rendering of e-services on specific spheres by central executive bodies” and on approval of “List of e-services’ types” a number of e-services to be rendered by the State Customs Committee were incorporated into the E-Gov portal.

Currently the following 14 e-services are rendered by the State Customs Committee:

- e - Customs Declaration / Goods
- e - Pre-arrival Information
- e - Customs Declaration / Passengers
- e - Monitoring
- e - Imports / Exports
- e - Customs Examination
- Goods Nomenclature
- Submission of application and documents to get, terminate or annihilate the license for operating as customs broker and customs carrier
- Submission of application and documents to get, terminate or annihilate the license for establishing customs warehouses and warehouses of temporary storage
- Online monitoring of application and inquiries submitted to the State Customs Committee
- e - Customs Payments, calculation of customs payments for import of light vehicles

State of play and gap analysis

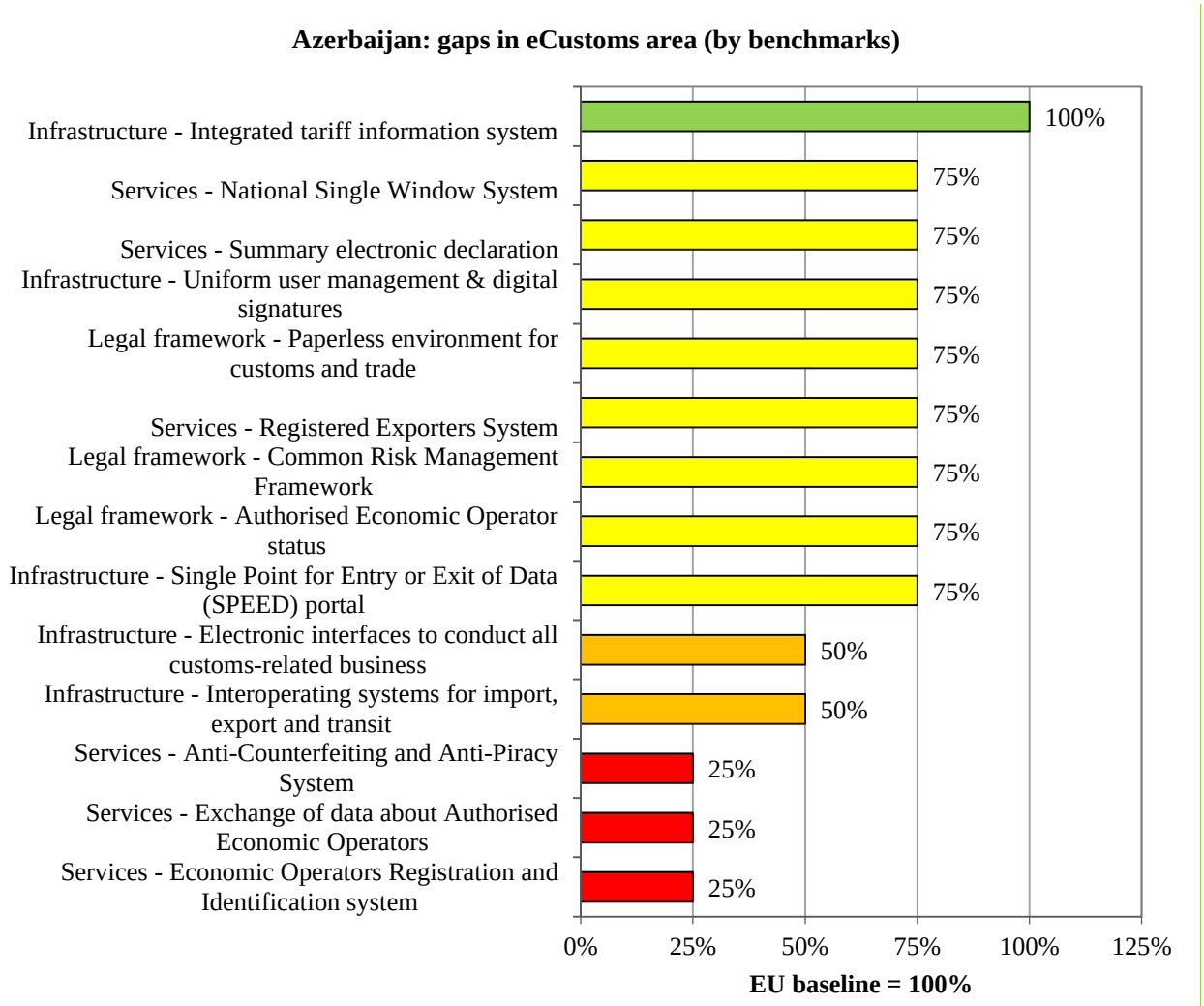

Exhibit 30- Azerbaijan: state of play and gap analysis in eCustoms

Legal framework

A risk management system operates as a module of the Unified Automated Management System (UAMS). A clearly defined national risk management framework in customs controls for goods brought into or out of the country is in place and is automated. It is harmonised with the WTO international criteria (WTO Risk Management Compendium) which also covers the EU common criteria and priority control areas. Risk Information Forms cannot be exchanged electronically with customs offices of EU countries.

The legislative base of the Institute of the Authorised Economic Operator (AEO) is fully developed in the country. Chapter 5 of the Customs Code and Decree # 230 of the Cabinet of

Ministers, 27 August 2013 set forth rules on how to get a status of AEO for legal entities, including requirements on AEO's operations. These legal acts provide simplified procedures in line with the best international practices. Implementation of the project on AEO is at a stage of development and currently there is no registered AEO in the country. The customs authorities of the country apply common criteria and harmonised requirements for granting the status of authorised economic operators, allow the use of simplifications by authorised economic operators and recognise the status of AEOs registered in the EU Member States or other countries. However, currently there are no registered AEOs in the country.

Data exchange contained in customs declarations, corresponding documents, certificates and exchange of other relevant information can be carried out within the framework of international treaties. National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information.

Infrastructure

UACS is in a position to provide one-stop access for electronic customs declarations and data exchange. The information systems of the country have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations. However, there is no current possibility of submission to the customs systems of other countries (EU Member States or others).

Import, export and transit subsystems are interoperating and completely integrated under the Unified Automated Management System of the Customs Service. Nevertheless, at the moment the Customs Service does not carry out any electronic data exchange on import, export or transit to EU.

The country has implemented a national centralised binding tariff information system within the UACS that allows getting tariff classification for goods. The system is interconnected with other tariff related components to facilitate re-use of data and functionality of one system to another.

The computerised transit system of the State Customs Committee (SCC) is one of the components of the UACS. The system can be accessed based on the Single Sign-On concept. Electronic data exchange with EU countries is not being carried out. The country's computerised

transit system is not connected to the SPEED portal. There is no data exchange between the electronic customs systems of Azerbaijan and the systems of the EU countries.

A common solution for electronic signatures is operational and enables the national economic operators also to send information to administrations other than customs, and enables these administrations to verify the authenticity of the author, of the sender and of the information. No interoperability for mutual recognition of electronic signatures with other countries has been established.

Services

The registration of foreign economic activity participants is carried out through the Taxpayer identification number in the UACS system, which allows automatic verification of registration numbers from declaration. There is no registration of national exporters in the central database Registered Reporters System (REX) being carried out. The country does not currently cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

Azerbaijan does not use a system of economic operators' registration or identification numbers assigned to economic operators. There is no common reference numbering system in the country to organise relations of economic operators with customs authorities throughout the country or for the exchange of information between the customs authorities and other authorities.

Azerbaijan has a registration and identification information system of economic operators. It has not concluded any agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU. There is not system-to-system interface that could allow the economic operators' data received from the country to be disseminated to the EU Member States or allow the validation of the country's AEO status in the EU transaction systems.

The Customs legislation of the Republic of Azerbaijan allows filing of summary e-declarations, specifically stipulated in Articles 113-116 of Customs Code. This is possible if there is an international legal mechanism in place. An electronic summary declaration containing the required pre-arrival or pre-departure information is lodged before any goods are brought into or out of the territory of Azerbaijan. All information can be provided to the customs and other

authorities in electronic format. The country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

To modify the Customs service and provide more favourable conditions for businesses and international trade, a "Single Window" (One-Stop-Shop) system was introduced in accordance with Presidential Decree dated 11.11.2008. The authority of regulatory state body on state borders was given to the State Customs Committee. It was achieved by transferring of some functions of the Ministries of Health, Transport, Agriculture and Veterinary Service to the State Customs Committee. This project was also beneficial for improving Azerbaijan's rating in the World Bank "Doing Business" report and helped to make significant steps for creating National Single Window System.

There is no Anti-Counterfeiting and Anti-Piracy System in the country. A basic electronic service is in place which provides traders with the possibility to submit a claim to the State Customs Committee about goods infringing certain intellectual property rights. There is no national Anti-Fraud Information System.

HDM roadmap

Legal framework

Common Risk Management Framework. Assess feasibility for electronic exchange of Risk Information Forms with customs offices of EU countries

Infrastructure

Electronic interfaces to conduct all customs-related business. Conduct technical feasibility study for connection of the UAMS information systems through the service of single access point to the customs systems of the EU Member States and the Region. Assess the cost/benefits of enabling economic operators to use one single interface to lodge electronic customs declarations

Single Point for Entry or Exit of Data (SPEED) portal. Conduct feasibility and cost/benefits studies for connection of the national systems to the Single Portal for Entry and Exit of Data that enables automated data exchange between Member States' electronic customs systems and Azerbaijan.

Uniform user management and digital signatures. Initiate cost/benefits study for development of interoperability and mutual recognition frameworks for electronic signatures of Azerbaijan and the EU Member States, and the Region. Assess the benefits from development of a common framework for mutual recognition of electronic signatures for the Region.

Services

Registered Exporters System. Assess the feasibility of cooperation with the European Commission in order to organise registration of national exporters into the EU REX central database

Economic Operators Registration and Identification system. Conduct a feasibility study about introduction of economic operators' registration and identification numbering system in Azerbaijan. Implement the EORI approach based on EORI number that serves as a common reference in the relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. Conduct cost/benefit analysis for the interconnection of the national system with the EORI central database managed by the European Commission.

Exchange of data about Authorised Economic Operators. Conduct a gap analysis between the existing information system containing data on economic operators and the EU requirements for the Authorised Economic Operator status. Conclude mutual recognition agreements with the EU to ensure the exchange of AEO data in a uniform way to increase security, facilitation of reduced physical and document based controls and priority treatment. Develop a system-to-system interface allowing the economic operators' data received from Azerbaijan to be disseminated to the EU Member States and the country's AEO status in the EU transaction systems to be validated

National Single Window System. Conduct a feasibility study for the development of a fully integrated National Single Window System that allows submission, processing and delivery of all required information and documents in electronic format.

Anti-Counterfeiting and Anti-Piracy System. Create the national Anti-Fraud Information System - an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Connect the national Anti-Fraud Information System with the

EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of information sharing and connect the national Anti-Fraud Information System with similar systems of the Region.

2.3.7 Belarus

The State Customs Committee (SCC) of the Republic of Belarus acts as a leading body developing and implementing state policy in the eCustoms sector. When elaborating the Customs IT projects to be carried out within the framework of the National Programme for Accelerated Development of ICT for the years 2011-2015, the SCC interacted with other state bodies such as the Ministry of Economy and the Ministry of Communications and Informatisation.

In the structure of the SCC, the issue of the implementation of information technologies in customs procedure is entrusted to the Administration for the Development of Customs Infrastructure and Administration for Information Technologies, Customs Statistics and Analysis. Information systems are used by the Administration for the organisation of customs control, the administration for counter-contraband operations and infringement of administrative customs offences, the administration for tariff regulation and customs payments, the management of risk analysis and operational control.

State of play and gap analysis

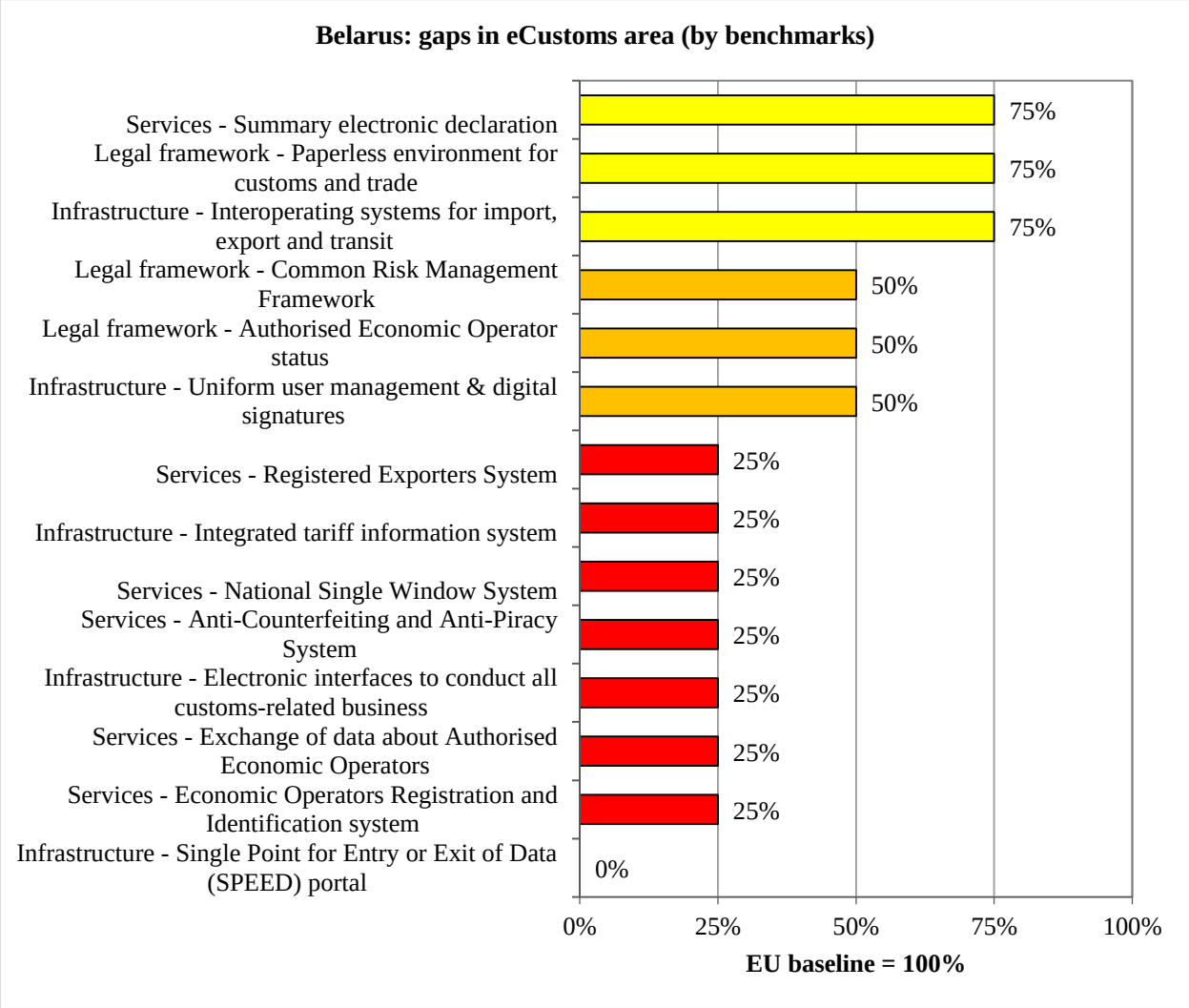

Exhibit 31- Belarus: state of play and gap analysis in eCustoms

Legal framework

The SCC has formed a legal and methodological framework of risk analysis and management system (RAMS), a corresponding organisation structure has been created, and the Concept of risk analysis and management system for the years 2010-2015 and up to 2020 has been elaborated and approved. The existing system has not been harmonised with the principles of the EU. Priority areas of control in Belarus were outlined, but these are different from those applicable in the EU due to the specific structure of economic system and peculiarities of legislation in the Customs Union countries. Within the framework of the project “Assistance in

creation of electronic system of preliminary information exchange between the customs authorities of Belarus and Ukraine (PRINEKS)", financed by the European Union in the end of 2015, a new risk management system will be implemented, which will enhance security of the countries in relation to illegally moved goods. Automatic data processing is implemented. This system is not harmonised with the general principles of the EU and the priority areas for EU control. Common standards and criteria are not harmonised with those of the EU. Customs offices of the country cannot exchange information about the risk in electronic form with the customs services of the EU. Data exchange is carried out only with the countries of the EEU (data exchange, not a "system to the system" interaction).

The Decree of the President "On some issues of customs regulation, on the implementation of activities in the field of customs and the authorised economic operator" includes provision for the issue of a certificate on entering the Register of Authorised Economic Operators and its withdrawal. The status of authorised economic operator is assigned to the concerned person by the State Customs Committee by issuing a certificate. For all the authorised economic operators still in Belarus, similar simplifications are applied. There exists a tendency towards categorising business units and depending on such categorisation various methods of customs control will be applied. The customs authorities of the country allow the use of simplified procedures by authorised economic operators. The status of AEOs registered in EU Member States or other countries (also Russia and Kazakhstan) is not recognised. There is a national system of identification and registration for economic operators (not using EORI). It does not interoperate with the Authorised Economic Operators EU system. The approach to risk assessment and accreditation of economic operators, and the criteria for granting the AEO status are different from the criteria applied in the EU.

The regulatory basis for the issues of e-declaration, the structure of electronic copies of documents, as well as the requirements set to the foreign information systems are elaborated. Interaction between state bodies according to the principle "system to system" on the whole is not fully developed in Belarus. The SCC and taxing authorities exchange information, but they do not cooperate. On the whole, the SCC electronically cooperates with about 40 state organisations. But with each department such cooperation is implemented separately, as each of them has their own departmental information systems, and requirements regarding the composition and format of the document may vary. There is no single format of data exchange between state bodies. To solve this problem SAIS is being built in Belarus, and through this

system the state will make cooperation between state organisations obligatory. This system is built on web-services with standard format of data transfer in XML. There is no specific requirement to certain customs systems in Belarus. There are regulatory acts governing flow of e-documents within information systems, including state bodies.

The SCC has started to implement the principle of “integrated border management”. There is no common regulatory act governing the interaction procedure with the EU. A set of the international contracts has been signed by the Government and the governments of the corresponding EU countries on interaction in customs issues that gives a legal platform for interaction between customs administrations. The SCC discusses issues and establishes the corresponding technology and technical regulations with each country that Belarus signed such agreements with. For each country today entirely different format composition, and method of information exchange can be applied.

General national legal acts define integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information. Available electronic customs systems are safe, integrated, accessible and interoperable. The exchange of data contained in customs declarations, accompanying documents, certificates and other relevant information also takes place between the customs authorities of the countries-members of the Customs Union. No data exchange is carried out with the EU, or between customs authorities and economic operators, the Commission and other bodies involved in the international movement of goods

Infrastructure

Belarus uses the National Automated Information System of Electronic Declaration (NAISED) – a system that provides information support and automation of customs operations carried out by customs officials and concerned parties (declarants) using written and electronic documents. It also provides informational interaction of Customs authorities with concerned parties and Customs of other countries. The information systems of electronic customs declaration do not have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries. The National Automated System of Electronic Declaration (NASED) is available and functionally compatible with other electronic customs systems for the exchange of data contained in customs

declarations. This system can communicate with EAEC (not "system to system," but individual data exchange), but cannot communicate with the EU. Within Belarus, the data of NASED is automatically available to any customs office but is not automatically available to any customs office outside Belarus irrespective of the country.

The Customs authorities use around 40 various information systems. Most of these systems are integrated into a Single automated information system. The country systems for import and export interoperate with the system for transit and enable the seamless flow of data. The service cannot ensure transfer of data between the national customs systems to/from customs system of EU Member States.

An integrated tariff environment enables the reuse of data across the connection of systems of export and import to the National System for Customs declarations and to the National control system (within the customs information systems, the tariff system is integrated separately). For the tariff classification, the economic operator must determine the commodity code. In Belarus there is no automated system for economic operators that would allow them get to know the tariff of goods. In Belarus, the economic operators are responsible for the commodity code identification – they should correctly identify it in the customs declaration. For this purpose, the declarant may use the Uniform tariff FEACC codes classifier which operates in three countries of the Customs Union. The country has implemented a national, not centralised tariff information system that allows getting tariff classification for goods (it is integrated only in some systems of declarations submission). However, it does not assist economic operators to obtain the correct tariff classification for goods they intend to import or export. The system is not interconnected with other tariff related systems to facilitate re-use of data and functionality of one system to another.

The country's computerised transit systems (or other systems such as export, import or economic operators systems) are not connected to the EU SPEED portal and do not allow data exchange for electronic customs systems between the country and the EU.

Electronic digital signature (EDS) is used by the declarants when submitting electronic documents into the National Automated Information System of Electronic Declaration (NAISED). Economic operators are able to send information to administrations other than customs to verify the authenticity of the author, of the sender and of the information (not via NASED but individually to these authorities). Belarus introduced in 2014 a State Public Keys Management

System (SPKMS) in order to solve the problem of interagency electronic documents. The Root Certification Authority and the National Certification Authority were put into operation. Now the country and the customs authorities also begin to use SPKMS, and it will allow the transmission of documents not only to the customs but also to other public authorities. EDS are not applied for the information exchange between customs authorities within the country because other means for information security protection in the system are used, the system is not available to external users. A common solution for electronic signatures (or a system based on mutual recognition of existing solutions) is not yet operational in the country (it was launched in 2014). For interdepartmental electronic document exchange within the country, the State System of Open Keys (ГосСУОК) is introduced. National economic operators are not currently able to send information to other countries' customs authorities (EU Member States, EEU countries) neither to other administrations, or to enable these administrations to verify the authenticity of the author, of the sender and of the information.

Services

There is no separate comprehensive register of registered exporters in the country. There is a portal for export information support (operator - National Centre for Marketing and Price Study of the Ministry of Foreign Affairs), containing a database of Belarusian enterprises-exporters, a database of exported goods and services, and a database of commodity distribution network objects. The country does not have an information system containing the data of registered exporters. There is no possibility of automated verification of the exporters' registration number from the declarations in the national Customs declaration system. Belarus does not currently cooperate with the EU in order to register national exporters in the EU REX central database managed by the European Commission. This does not allow the economic operators from Belarus to benefit from preferential trade arrangements under the Generalised System of Preferences.

An electronic system for storing and exchanging Economic Operators Registration and Identification (EORI) numbers is not yet operational in the country. Non-residents (Russia, Kazakhstan, Poland, Lithuania, and others.) do not get additional numbers (numbers are used, taken for the identification of business entities in these countries, including EORI).

Belarus maintains a separate register of authorised economic operators, which contains data on the number of business entities, whom the customs trust and accord certain simplifications. The

criteria for granting this ”trusted” operators’ status do not align with those applied in other countries, be it in the EU or the EEU. There are no agreements on mutual recognition of authorised economic operators either with the EU or the EEU. In principle, there is no system-to-system interface either with the EEU or the EU. Based on the profiles of economic operators registered in the national system, the country’s authorities can attribute different trust level status to different economic operators. Now, the gradation "normal" and "authorised" is used. More detailed gradation is planned under the Customs Code of the Customs Union. The country has not yet concluded an agreement of mutual recognition of the country’s register of economic operators and the Authorised Economic Operators in the EU. There is no system-to-system interface that would allow the economic operators’ data received from the country to be disseminated to the EU Member States and the country’s AEO status in the EU transaction systems to be validated.

The Belarusian legislation has two different terms - pre-declaration and preliminary information. The preliminary declaration, which is filed electronically, is used mainly for export and contains a minimum set of data for risk assessment, after which complete information is submitted. An electronic summary declaration containing the required pre-arrival or pre-departure information is lodged before any goods are brought into or out of the territory of the country (preliminary declaration). All information is provided to the customs and other authorities in electronic format. The existing national infrastructure allows information to be shared electronically with third countries where an international agreement so provides (now only within the Customs Union, and not in the form of "system to a system" interaction but in the form of individual data exchange). Submission of preliminary information is carried out electronically by means of interaction of the information system of the customs authorities of the Member States of the Customs Union (CU) and the information systems of concerned parties or via web-portals of the CU.

The country has a unified system for filing e-declarations, but it is available only to the customs services; economic entities submit documents into the system electronically via the automated workstations of a number of complementary software products developed by different developers. For the time being, there is no system, which is able to provide all the necessary information and documents in electronic format. The national single window and one-stop shop for trade is not in place. There is no possibility (except for the customs service) of submission of all required information and documents in electronic format (application for certificates, customs

declaration, required documents, and permits). Administrations or agencies do not deliver certificates required for import or export authorisation in electronic format

It is possible to submit via email a request asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. However, there is no website where this could be done. As a preventive measure, the Customs authorities may render fee-based services upon the importer's/ exporter's request to monitor compliance with their intellectual property rights when goods are crossing the borders. The customs body enters the request into a specific register and monitors it. If any economic entity tries to import counterfeit goods, the Customs will reveal this fact and prevent importation. However, this register is not shared with the EU. Each national body has a register of intellectual property items, which is maintained on a central basis (in Belarus it is represented by the National Centre of Intellectual Property). To protect their intellectual property rights post factum, the exporter or the importer must lodge an application and notify of infringement on their rights (the Law of the Republic of Belarus dated 18 July 2011 "On Application of Citizens and Legal Bodies" allows for lodging an e-application with indication of all identification details).

For a long time, Belarus has successfully applied the system for labelling of goods with control identification marks. In the near future, there will be a transition to a higher quality system, i.e. to labelling of goods with control (identification) marks containing RFID tags, and entry of data on produced and imported goods into the interdepartmental distributed information system known as "Data Bank of Electronic Goods Certificates". Interaction with the system of electronic certificates of goods via barcodes is also not included in current plans.

There is no electronic service in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights (it is possible to submit a request by e-mail). There is no national Anti-Fraud Information System and no exchange of information with the centralised EU information system.

HDM roadmap

Infrastructure

Electronic interfaces to conduct all customs-related business. Develop a service of single access point enabling economic operators to use one single interface to lodge electronic

customs declarations to the customs systems of other countries (through NASED or a dedicated portal). Conduct a feasibility study for the extension of the single access point to interface customs systems of other countries. Conduct technical feasibility for connection of the information systems through the service of Single Electronic Access Point (SEAP) to the customs systems of the EU Member States

Integrated tariff information system. Develop and integrate into the tariff information system a tool to assist economic operators to obtain the correct tariff classification for goods they intend to import or export. Conduct a feasibility study for the use of an integrated tariff information system and its interconnection with the already existing tariff related IT systems (not only the systems of the Customs service, but of other administration within the single window) aiming to achieve re-use of data and functionality of one system to another.

Single Point for Entry or Exit of Data (SPEED) portal. Conduct feasibility and cost/benefits studies for connection of the national Single automated information system of the Customs authorities to the Single Portal for Entry and Exit of Data portal that enables automated data exchange between Member States' electronic customs systems and Belarus (specifically for data exchange for New Computerised Transit System - NCTS).

Uniform user management and digital signatures. Assess economic benefits, conduct technical study for defining a concept of mutual recognition of electronic signatures within the Region. Conduct a feasibility study for introduction of uniform user management and usage of digital signatures based on a mechanism of mutual recognition for electronic signatures for the customs and other authorities related to external trade between Belarus and the EU countries (main trading partners of Belarus). Conduct technical study for defining a concept of mutual recognition of electronic signatures between the CU and the EU countries.

Services

Economic Operators Registration and Identification system. Implement the EORI approach based on EORI number that serves as a common reference in the relations of national economic operators with customs authorities of the EU countries. Conduct feasibility study for interconnection of the national system with the EORI central repository managed by the European Commission.

Exchange of data about Authorised Economic Operators. Conduct a gap analysis between the

Belarusian register of authorised economic operators and the EU requirements for the Authorised Economic Operator status. Conclude AEO Mutual Recognition Agreement with the EU to ensure the exchange of AEO data in a uniform way to increase security, facilitation of reduced physical and document based controls and priority treatment. Develop system-to-system interface allowing the economic operators' data received from Belarus to be disseminated to the EU Member States and the country's AEO status in the EU transaction systems to be validated.

National Single Window System. Develop a service for submission of electronic customs declarations through the nationwide automated information system NAIS portal (XML or web forms). Develop individual services for automation of the submission of applications for some key permits (certificate of origin, veterinary, phytosanitary, pharmaceuticals). Prepare terms of reference for the development of fully integrated National Single Window System that allow submission, processing and delivery of all required information and documents in electronic format

Anti-Counterfeiting and Anti-Piracy System. Create a national Anti-Fraud Information System with an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs. Develop a service for submission of electronic claims through the nationwide automated information system NAIS portal. Integrate the Anti-Fraud Information System with "Data Bank of Electronic Goods Certificates", the system of RFID tags and barcodes. Study the feasibility of connecting the national Anti-Fraud Information System with the EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of information sharing and connect the national Anti-Fraud Information System with similar systems of the Region.

2.3.8 Georgia

State of play and gap analysis

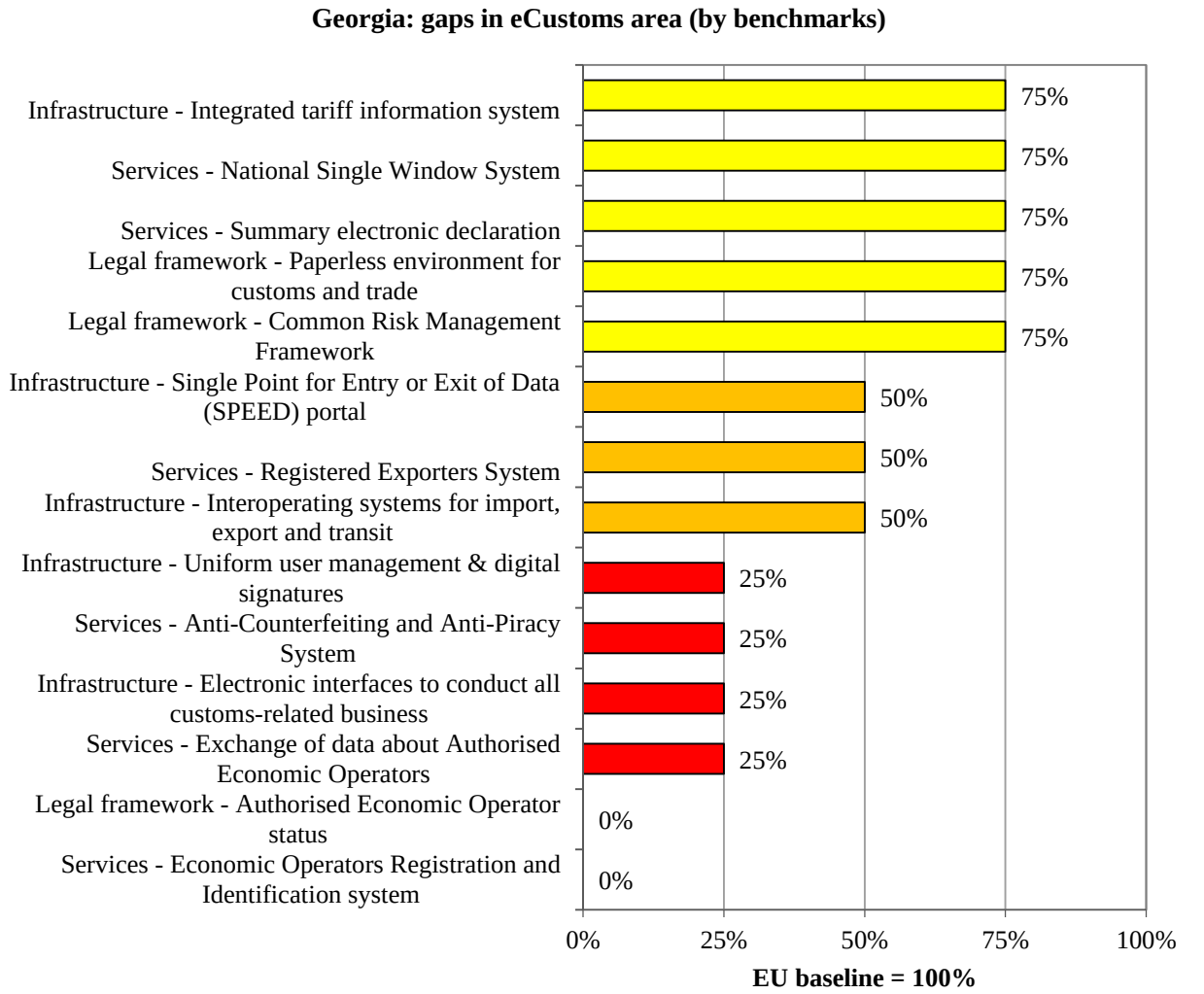

Exhibit 32- Georgia: state of play and gap analysis in eCustoms

Legal framework

A National Risk Management System has been established and is automated since 2007. The formal study or comparison of risk criteria established in Georgia with the Common Risk Management Framework established in the EU has not been performed. The management of customs operational risks is automated. Both the eCustoms (ASYCUDA World) and Oracle systems support the automation of risk management procedures. All tariff risks (import and export operations) are fully supported by the eCustoms system, while the Oracle system

provides support for management of non-tariff risks related primarily to border-crossing and transit operations. In addition to managing risk profiles, Customs maintain a database of qualified traders (a so-called “Golden List”). Companies included in the list are allowed to process consignments through simplified procedures. The “Golden List” (alternative programme for the Authorised Economic Operators programme) is a part of the eCustoms system and is mainly used for processing import operations. The national risk management framework in customs controls for goods brought into or out of the country is harmonised with the EU common criteria and priority control areas. Risk Information Form’s are currently not exchanged electronically with customs offices of EU countries.

AEO status implementation is part of the strategy for the Association Agreement between the European Union and Georgia. The Customs authorities do not currently apply common criteria and harmonised requirements for granting the status of authorised economic operators, allowing the use of simplifications by authorised economic operators. Recognition of the status of AEOs registered in the EU Member States or other countries has not been implemented yet.

Implementation of a paperless environment has already been launched. The automation of customs operations in Georgia is organised through two independent and fragmentally integrated information systems; eCustoms (built on ASYCUDA World) and “Oracle”. While the eCustoms system is dedicated entirely to support customs operations, the “Oracle” system represents a unified integrated platform that processes all revenue collection-related data and operations. Both the eCustoms and “Oracle” systems are web-based applications, providing interfaces for external users using secure communication channels. The systems are integrated. Further steps are planned though Trade Facilitation System Project, launched in 2012 (the pilot will be launched summer 2015) which is the system aiming at harmonisation of the electronic flow of information among key participants in the logistics, shipping, and transport industries, both public and private. Data exchange is provided between different agencies within Georgia. Currently, Georgian Customs exchanges electronic information with the customs authorities of two countries: Turkey and Ukraine.

Indicator 2: Infrastructure

Information systems of the country do not have a single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries. Data exchange agreements have been signed and are operational

with Turkey and Ukraine.

Georgian systems for import and export interoperate with the system for transit and enable the seamless flow of data, but are not integrated with EU systems, such as AIS, AES or NCTS. The service does not currently ensure transfer of data between the national customs systems to/ from systems of the EU Member States.

National Goods Nomenclature for External-Economic Activities has been adopted in 2002, and the last update was adopted in 2012. Nomenclature is publicly available and is used for estimation of tariffs for goods for import and export purposes. Nomenclature is based on the International Convention on the Harmonised Commodity Description and Coding System. Nomenclature is integrated for active and real-time re-use by National Declaration Processing Systems, but is not integrated with national surveillance systems. The country has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is integrated for active and real time re-use by National Declaration Processing Systems, but is not interconnected with other tariff related IT systems to facilitate re-use of data and functionality of one system to another.

Integration or connection is not part of the Association Agreement agenda. Georgia's computerised transit system and other systems such as export and import systems are not connected to SPEED portal and do not allow data exchange for electronic customs systems between the country and the EU. However, the current level of development of automated eCustoms information system allows data exchange with two countries.

Georgia has introduced eSignatures with a Law on electronic Signatures and electronic documents in 2008. Electronic signatures are not used in customs operations and therefore are not exchanged with other countries, including EU Member States. A common solution for electronic signatures (or a system based on mutual recognition of existing solutions) is not operational in the country.

Services

Georgia has not established or harmonised a Registered Exporter System for preferential trade arrangements with EU countries. The Revenue Service has established a unified database of taxpayers combined with exporters' registration data. The database (equivalent of registered exporters' system) should allow an automated verification of the exporters' registration number

from the declarations in the national eCustoms declaration system. Georgia currently does not cooperate with the EU on registration of national exporters into the EU REX central database managed by the European Commission.

Georgia has not implemented a system for registration and identification of economic operators based on an equivalent of EORI number that serves as a reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. There are no interconnections with the EORI central database managed by the European Commission.

Georgia has a registration and identification information system of economic operators. It has not concluded any agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU. System-to-system interface allowing the economic operators' data received from the country to be disseminated to the EU Member States and the validation of the county' AEO status in the EU transaction systems has not been implemented.

Summary electronic declarations are used in Georgia, while relevant authorities (Revenue service) undertake information exchange with the republic of Turkey as per agreement of joint use of Land Crossing Points. Information is filed and provided in electronically and is equal to Entry Summary Declaration. Through established information exchange with Turkey, an electronic summary declaration containing the required pre-arrival or pre-departure information could be lodged before any goods are brought into or out of the territory of the country. All information is provided to the customs and other authorities in electronic format. Existing infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

A single window is managed by Revenue Service and Ministry of Finance of Georgia. The national single window and one-stop shop is in place and allows submission of all required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits). It has not been confirmed that the administrations or agencies deliver certificates (permits) required for import or export authorisation in electronic format.

Under the framework of the Association Agreement, Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of

intellectual property rights and repealing Council Regulation (EC) No 1383/2003 shall be implemented. The approximation with the provisions of the above mentioned Regulation, with the exception of Article 26, shall be carried out within three years following the entry into force of this Agreement. Therefore, a national information system on IPR has not yet been established and no information exchange has been undertaken with internationally or with EU centralised Anti-Counterfeiting and Anti-Piracy System. An IPR oriented National Anti-Fraud system has not been implemented. In Georgia there is no electronic service in place that provide traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain IP rights.

HDM roadmap

Indicator 1: Legal framework

Common Risk Management Framework. Assess feasibility for electronic exchange of Risk Information Forms with customs offices of the EU countries

Authorised Economic Operator (AEO) status. Implement the status of the authorised Economic Operator compliant with the EU requirements (part of the Association Agreement between the European Union and Georgia's implementation plan). Promote incentives of the authorised Economic Operator status

Indicator 2: Infrastructure

Electronic interfaces to conduct all customs-related business. Plan the upgrading of the current systems of data exchange with other countries (Turkey, Ukraine) to integrate a single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of these countries. Conduct a feasibility study for the extension of the single access point to interface the systems of the Region. Conduct technical feasibility for connection of the information systems through the service of Single Electronic Access Point (SEAP) to the customs systems of EU Member States.

Interoperating systems for import, export and transit. Design and develop a service for transfer of data between the national interoperating customs systems of export, import and transit to/from customs system of the EU Member States and the systems of the Region.

Integrated tariff information system. Interconnect the national nomenclature system with other tariff related IT systems to facilitate active and real time re-use of data and functionality of one

system to another, notably with the National Declaration Processing Systems and National Surveillance systems.

Single Point for Entry or Exit of Data (SPEED) portal. Conduct feasibility and cost/benefits studies for connection of the national automated eCustoms system to the Single Portal for Entry and Exit of Data portal that enables automated data exchange between Member States' electronic customs and Georgia.

Uniform user management and digital signatures. Conduct a technical study and cost/ benefit analysis for upgrading of the eCustoms system to use electronic signatures. Conduct a feasibility study for introduction of uniform user management and usage of digital signatures based on a common solution for electronic signatures (or a system based on mutual recognition of existing solutions) for the customs and other authorities related to external trade.

Indicator 3: Services.

Registered Exporters System. Assess the feasibility of cooperation with the European Commission in order to organise registration of national exporters into the EU REX central database

Economic Operators Registration and Identification system. Conduct a feasibility study about introduction of economic operators' registration and identification numbering in Georgia. Implement the EORI approach based on EORI number that serves as a common reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. Conduct a cost/ benefit analysis for interconnection of the national system with the EORI central database managed by the European Commission.

Exchange of data about Authorised Economic Operators. Conduct a gap analysis between the existing information systems (eCustoms and Oracle-based) containing data on economic operators and the EU requirements for the Authorised Economic Operator status. Conclude AEO Mutual Recognition Agreement with the EU to ensure the exchange of AEO data in a uniform way to increase security, facilitation of reduced physical and document based controls and priority treatment. Develop system-to-system interface allowing the economic operators' data received from Georgia to be disseminated to the EU Member States and the validation of the county' AEO status in the EU transaction systems.

Summary electronic declaration. Conduct a technical study on the mutual possibility for lodging of summary customs declaration between Georgia and the EU.

Anti-Counterfeiting and Anti-Piracy System. Create a national Anti-Fraud Information System with an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Connect the national Anti-Fraud Information System with the EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of information sharing and connect the national Anti-Fraud Information System with the similar systems of the Region.

Conditions for harmonisation

Challenges. Within the frameworks of development of the paperless environment for customs and trade, to enable electronic connections not only between public sectors institutions (customs, railway, border police), but as well with private sector bodies (sea ports, shipping lines, airlines, post transporters, airports, terminals, expeditors, freight forwarders, railway, brokers, banks, insurance companies).

Risks. A paperless environment for customs and trade; complexity and multiple stakeholders in the process could delay launch of pilot projects. System effectiveness significantly depends on the involvement of private companies that operate in transportation and logistics sector.

Conditions. In case of further integration with EU eCustoms, a full and detailed gap analysis between the Common Risk Management Framework and risk frameworks of the Region should be performed. Implementation of any measures shall be done with a gradual and carefully timed approach, taking into account the difference in the nature of risks faced by individual countries.

Benefits. According to the survey carried out in Poti Port, a paperless trade environment will substitute 1 million paper documents annually. TFS streamlined procedures will save 3.7 hour of an operator’s working time and 26 printed pages on each container, the total annual estimated savings related to the containers management would be GEL 4,530,000.

Parties connected to TFS will be able to optimise logistic processes and improve their competitive position. By adopting the system, 24-hour-service will be accessible from any place, management and administration expenses will be reduced, information availability will increase and probability of errors will decrease.

2.3.9 Moldova

State of play and gap analysis

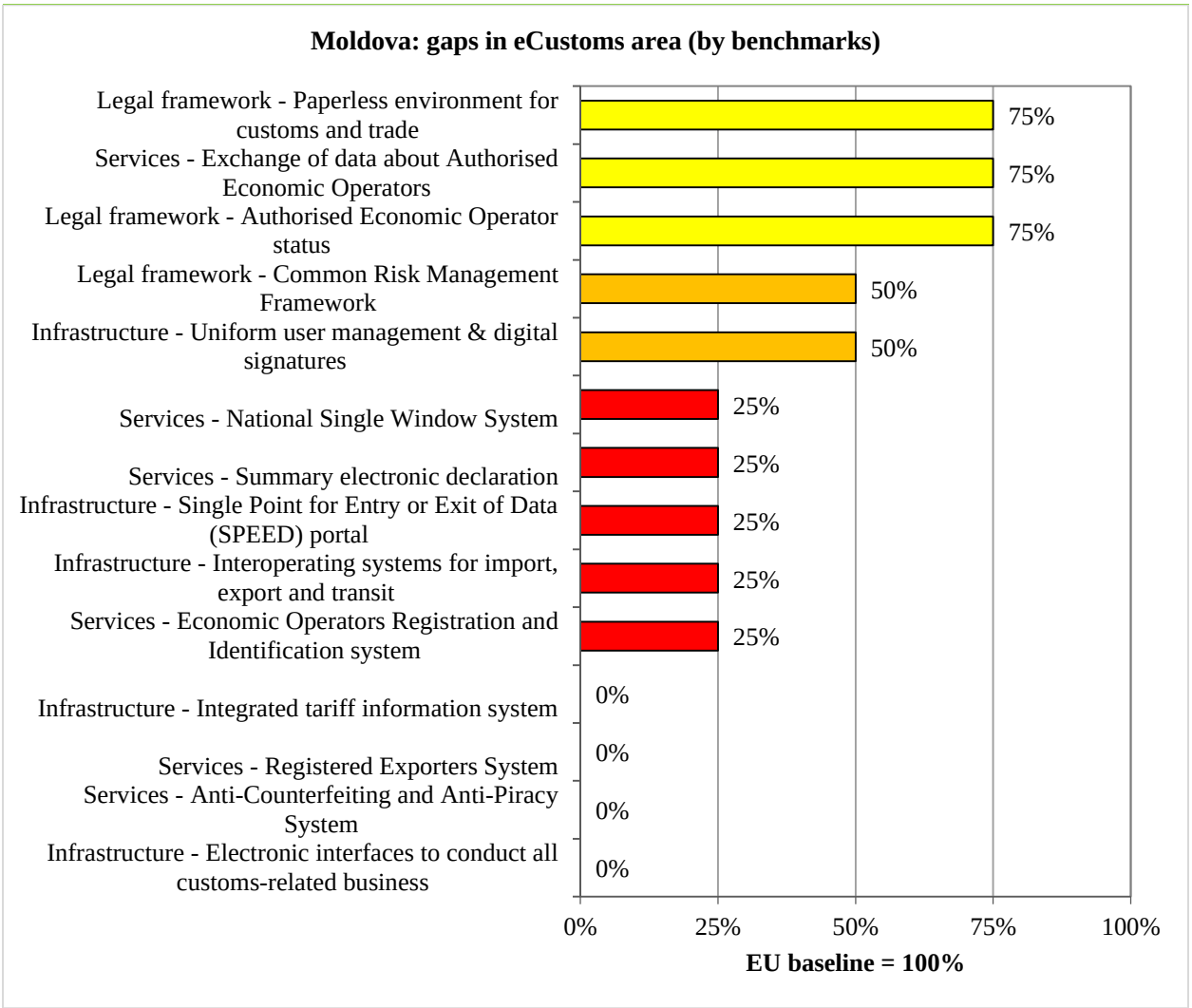

Exhibit 33- Moldova: state of play and gap analysis in eCustoms

Indicator 1: Legal framework

The Moldovan legal framework in this area is in accordance with the EU legal framework. More than 53.3% of exports from Moldova are oriented towards the EU market. A Moldovan Customs risk management system is based on the automated selectivity system in ASYCUDA World. The Customs Service is willing to exchange customs data with the EU for the purposes of risk

management. Currently, Moldova is negotiating with the European Commission the implementation of a pilot project on the pre-arrival of exchange of customs data. The pilot project is planned to be launched in 2015 at the border crossing point with Romania at Leuşeni - Albiţa. The Customs Service has consulted the EU Legal Framework, in particular, the Community Risk Management Framework laid down in the Regulation (EC) 648/2005 while developing its national Risk Management System. In this process, Moldova benefits from expertise offered by international experts, including EUBAM, EUHLPAM, BRITE and USAID. Moldova has implemented a national risk management framework in customs controls for goods brought into or out of the country that is harmonised with the EU common criteria and priority control areas. Risk Information Forms cannot be currently exchanged electronically with customs offices of the EU countries.

The relevant EU legal framework is transposed to the national legal provisions[21], including requirements for granting the statement of AEO and simplified declarations. Until today, the Moldovan Customs Service has issued 59 certificates for AEO. The AEO Register is published on the web portal of the Customs Service (customs.gov.md). The customs authorities of Moldova apply common criteria and harmonised requirements for granting the status of authorised economic operators, allowing the use of simplifications by authorised economic operators and recognising the status of AEOs registered in the EU Member States or other countries. A national system of identification and registration for economic operators does not interoperate with the Authorised Economic Operators EU system.

As from March 2013, Moldovan customs implemented electronic export declaration and the share of eExport submissions grew by 42% by January 2015. As from September 2014, an electronic import declaration has been also been implemented. At present a number of projects are being implemented which will permit electronic exchange of information within the public sector. The Customs Service participates in this process. The Government has adopted the Government Decision no.656/2012 on Interoperability framework [22] and is currently implementing the technical layer of interoperability (pilot project) in accordance with

[21] Customs Code, section 27 indices 1 and 28 indice 1, Government Decision no.647 of 7.8.2014 to apply the provisions of the Customs Code, section 27 index 1 and 28 index1

[22] http://egov.md/images/normative/Moldova_Interoperability_Framework_Program.pdf

Government Decision no.404 of 2.06.2014. National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information. Appropriate system applications are in the process of implementation.

Indicator 2: Infrastructure

There is no single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries. Interoperability of systems for import, export and transit is not currently in place. However, a Twinning Project Fiche for Moldovan Customs for implementing NCTS has been drafted by the European Commission and it is expected to be launched in 2015.The country systems for import and export do not interoperate with the system for transit and do not enable the seamless flow of data. There is no service that ensures transfer of data between the national customs systems to/ from customs system of the EU Member States.

Currently this procedure is paper-based and it is not supported by an IT tool. The country has not yet started the implementation of a national centralised binding tariff information system that allows getting tariff classification for goods.

Moldova is negotiating with the European Commission for the implementation of a pilot project on the pre-arrival of exchange of customs data. The pilot project is planned to be launched in 2015 at the border crossing point with Romania at Leuşeni - Albiţa. The country's computerised transit system (or other such as export, import or economic operators systems) is not connected to SPEED portal and there is no data exchange for electronic customs systems between the country and the EU.

E-signatures used for customs operations are issued for other operations as well as and can be accepted by other institutions. There is a lack of financial means to ensure the necessary developments in the customs information system by the UNCTAD developer of ASYCUDA World. The implementation is based on the developed legal framework: Law no 91 of 27.06.2014 on e-signature and electronic document, Regarding Government Decision no.904 of 13.11.2013 on procedure on eDeclaration of goods, a common solution for electronic signatures is operational in the country and enables the national economic operators to send information to other administrations than customs, and to enable these administrations to verify the

authenticity of the author, of the sender and of the information. No mutual recognition frameworks of e-signatures with other countries have been implemented.

Indicator 3: Services

A draft concept paper on automatic procedures has been prepared. Moldova has not established a Registered Exporters System (or similar) that allows an automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country currently does not cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

There is a centralised system for registration of the economic operator in ASYCUDA World. There is no special registration and identification numbering for customs unique registration in place. An electronic system for storing and exchanging Economic Operators Registration and Identification numbers is partially operational. The national system is not interconnected with the EORI central database managed by the European Commission.

Draft terms of reference have been prepared for a pilot project on unilateral recognitions of the EU AEO at Leuşeni - Albiţa border crossing point between Moldova and Romania. Moldova has a registration and identification information system of authorised economic operators and is in process to conclude an agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU within a pilot project. There is no system-to-system interface that allows the economic operators' data received from the country to be disseminated to the EU Member States and the validation of the county' AEO status in the EU transaction systems.

The Moldovan Customs Service implemented a pre-arrival exchange of data with Ukrainian customs in electronic format from 2008 with the support of the EUBAM. The exchange is done in separate system. This system has an interaction with ASYCUDA but is not integrated in it. An electronic summary declaration containing the required pre-arrival or pre-departure information can be lodged before any goods are brought into or out of the territory of the country. All information is provided to the customs (and other authorities) in electronic format. Existing country's infrastructure allows such information to be shared electronically with third countries where an international agreement so provides.

A Twinning Fiche has been drafted by the European Commission for supporting the Moldovan

Customs in developing a single window approach. The national single window and one-stop shop is not yet implemented. There is no possibility to submit required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits).

An Anti-Counterfeiting and Anti-Piracy System has not been established. There is no electronic service providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights.

HDM roadmap

Indicator 1: Legal framework

Common Risk Management Framework. Implement a pilot project funded by the EC on the pre-arrival of exchange of customs data at the boarding crossing point with Romania at Leuşeni Albiţa (starting 2015). Assess the results of the pilot project and extend it into development of electronic exchange of Risk Information Forms with customs offices of EU countries.

Authorised Economic Operator status. Create an interface for exchange of data between the national system of identification and registration for economic operators and the Authorised Economic Operators EU system.

Indicator 2: Infrastructure

Electronic interfaces to conduct all customs-related business. Conduct a technical feasibility for connection of the customs declaration information system through the service of single access point to the customs systems of the EU Member States and the Region. Assess cost/ benefit of enabling economic operators to use one single interface to lodge electronic customs declarations.

Interoperating systems for import, export and transit. Implement the twinning pilot project financed by the EC. Upgrade the customs systems to allow exchange of data between the components of import/ export. Interoperate it with the system for transit and enable the seamless flow of data for facilitates the exchange of data contained in customs declarations, documents accompanying customs declarations and certificates and the reuse of other relevant information.

Integrated tariff information system. Implement a national centralised binding tariff information

system that allows getting tariff classification for goods and interconnected with other tariff related IT systems to facilitate re-use of data and functionalities of one system to another.

Single Point for Entry or Exit of Data (SPEED) portal. Implement a pilot project at the cross border point with Romania financed by the EC. Based on the results, conduct cost/ benefit and technical studies for connection of the national systems to the Single Portal for Entry and Exit of Data portal that enables automated data exchange between Member States' electronic customs systems and Moldova.

Uniform user management and digital signatures. Initiate cost/benefits study for development of an interoperability and mutual recognition frameworks for electronic signatures of Moldova and the EU Member States, and the Region. Assess the benefits of development of a common framework for mutual recognition of electronic signatures for the Region.

Indicator 3: Services

Registered Exporters System. Create a regulative framework for the status of registered exporter that can bring benefits of simplification for some administrative procedures for qualified legal and natural persons. Extend the functionalities of the existing database of the ASYCUDA World to accommodate data related to the registered exporter status. Conduct a feasibility study on the development of an inter-systems interface. Cooperate with the European Commission in order to organise registration of national exporters into the EU REX central database

Economic Operators Registration and Identification system. Conduct a feasibility study about enhancement of the usage of Economic operators' registration and identification numbering. Implement the EORI approach compliant with the EU requirements based on EORI number that serves as a common reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. Conduct a cost/benefit analysis for interconnection of the national system with the EORI central database managed by the European Commission

Exchange of data about Authorised Economic Operators. Implement the pilot project on unilateral recognitions of the EU AEO at the Leuşeni - Albiţa Moldova-Romanian border crossing point. Conclude mutual recognition agreements with the EU to ensure the exchange of AEO data in a uniform way. Based on the results of the pilot project, develop a system-to-system interface allowing the economic operators' data received from Moldova to be

disseminated to the EU Member States and the validation of the county' AEO status in the EU transaction systems

National Single Window System. Implement the pilot project initiated previously. Prepare terms of reference for the development of fully integrated National Single Window System that allow submission, processing and delivery of all required information and documents in electronic format.

Anti-Counterfeiting and Anti-Piracy System. Create the national Anti-Fraud Information System with an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Connect the national Anti-Fraud Information System with the EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of information sharing and connect the national Anti-Fraud Information System with the similar systems of the Region.

2.3.10 Ukraine

State of play and gap analysis

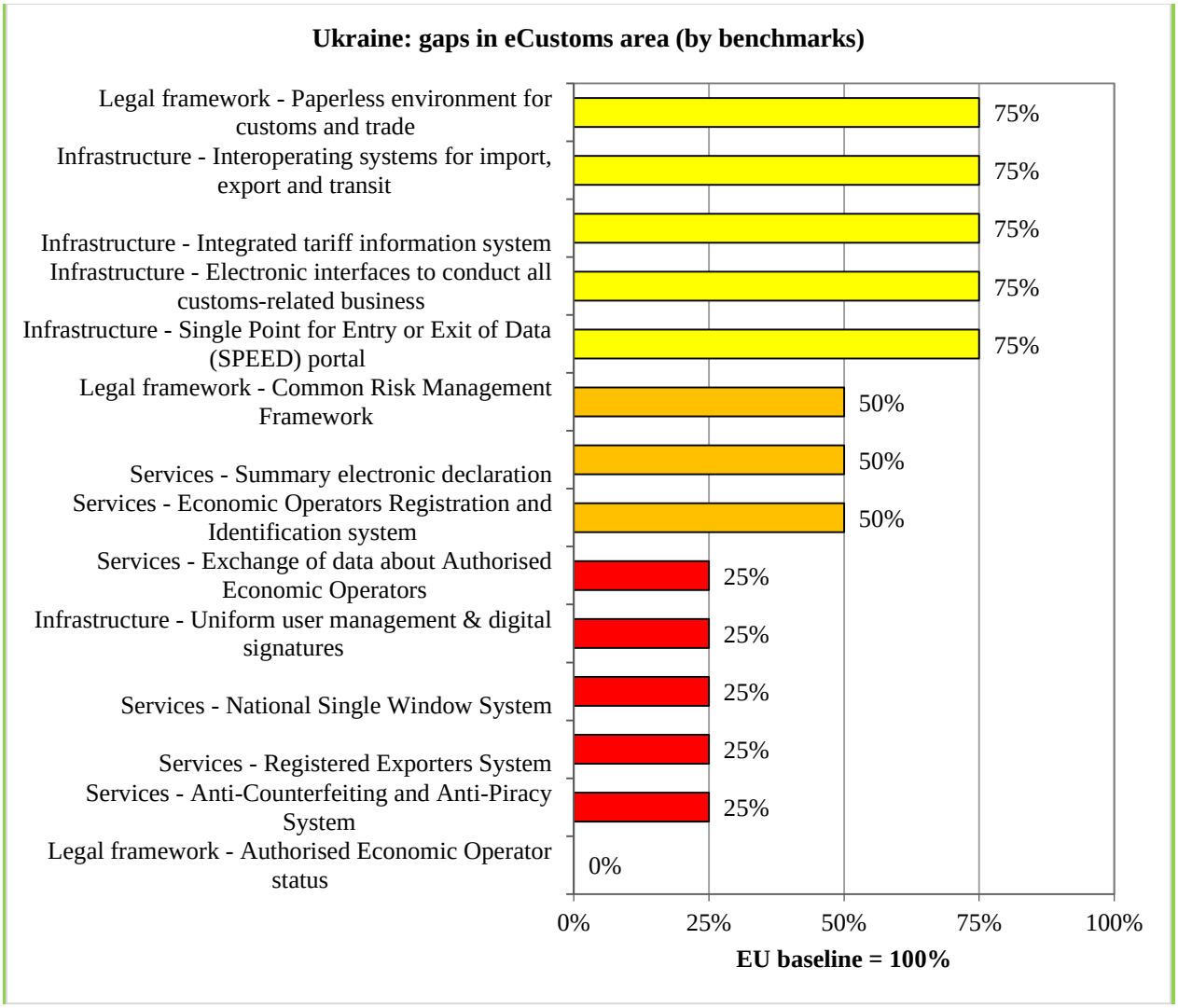

Exhibit 34- Ukraine: state of play and gap analysis in eCustoms

Indicator 1: Legal framework

Ukraine has an internally developed risks management system (risk profiles are developed and confirmed by a special Commission – the data is internal and confidential). The framework is regulated by the Tax Code, and specifics orders in case of changes and for risks specification. For the exchange of related data, there is functionality of data exchange, but not exchange of risks profiles. Ukraine has a clearly defined national risk management framework in customs controls for goods brought into or out of the country. It is not harmonised with the EU common criteria and priority control areas. Risk Information Form cannot be exchanged electronically with customs offices of EU countries.

The Tax Code provides the required basis for authorised economic operator status, but there is no implemented mechanism and no regulations for implementation. The Customs authorities of the country do not apply common criteria and harmonised requirements for granting the status of authorised economic operators due to absence of the regulations.

A unified Automated Information System assures a paperless environment and exchanges of data with many state bodies. 92 % of tax declarations are paperless. Data exchange between other State bodies and the Customs Service is very limited. National legal provisions are defined for secure, integrated, interoperable and accessible electronic customs systems for the exchange of data contained in customs declarations, documents accompanying customs declarations, certificates and the exchange of other relevant information (see more information in the Annex).

Indicator 2: Infrastructure

Customs information systems of Ukraine have a service of single access point enabling economic operators to use one single interface to lodge electronic customs declarations to the customs systems of other countries (the EU member state or others) only for the transit (NCTS).

The country systems for import and export interoperate with the system for transit and enable the seamless flow of data. The service can partially ensure transfer of data between the national customs systems to/from customs system of the EU Member States (NCTS and TIR).

The subject is regulated by Law of Ukraine on Customs Tariff. Ukraine has implemented a national centralised binding tariff information system that allows getting tariff classification for goods. The system is connected with the customs system to facilitate re-use of data and functionality of one system to another.

There is currently no solution based on single service bus for data exchange. Exchange of data is assured by online one-to-one systems exchange. Periodically, exchange of emails is practiced for about 50 customs declarations per day. State Agency for E-Governance in Ukraine currently develops a solution of single service bus. The country’s computerised transit systems (or other such as export, import or economic operators systems) is not connected to SPEED portal. There is some data exchange for electronic customs systems between the country and the EU by semi manual procedures.

Country-wide electronic identification principles are defined in the draft of Law on electronic

identification. The digital signatures provided by State Fiscal Service are applicable in most of cases inside of Ukraine. An alternative digital signature solution is used within the banking system. For external exchanges, the Customs Services are using MSAT–RSA signatures because of the requirement for RSA certification/ ESI compatibility. There is no common solution for electronic signatures. There is a partial system based on mutual recognition of existing solutions (digital certificates delivered by 2 authorities) operational in the country and enables the national economic operators to send information to the customs. National economic operators cannot submit information digitally signed to other countries. Cross-border submissions are operational with International Road Transport Union (two-sided exchange for TIR books/data – RSA standard), and Railroads of Ukraine with Russian and Belarus (transportation data, including fiscal for goods - protected with double-standard e-signature).

Indicator 3: Services

The procedure on Registered Exporters is defined by the Ministry of Finance in its order from 07.10.2014 № 1013 in application since 23.12.2014. The development of technical solutions is in progress. The country has not yet established a Registered Exporters System that allows an automated verification of the exporters' registration number from the declarations in the national Customs declaration system. The country does not cooperate with the EU in order to register national exporters into the EU REX central database managed by the European Commission.

The Tax Code of Ukraine (Section 1, part 2 – some amendments done in 2012, 2013) identifies the requirements for national Economic Operators. An electronic system for storing and exchanging Economic Operators Registration and Identification numbers is operational in the country since 1996. The national system is not interconnected with the EORI central database managed by the European Commission.

Centralised Economic Operators Registration and Identification information and communication system supporting the registration of the Authorised Economic Operators is not implemented in Ukraine. The country does have a registration and Identification information system of economic operators (based on principle of AEO in the EU) and has not concluded an agreement of mutual recognition of the country's register of economic operators and the Authorised Economic Operators in the EU.

Summary declaration is not currently used. The submission of a preliminary customs declaration is implemented since 1998 (fully electronic since 2011). It requires providing all information

available prior to border crossing. Submission of an electronic summary declaration containing the required pre-arrival or pre-departure information is not currently lodged before goods are brought into/out of Ukraine.

The single window application is available but due to lack of integration with other involved ministries, it cannot serve as a fully integrated single window. The technical readiness of related state bodies to connect to single Customs system is low. There is no of single bus solution that could resolve the potential obstacle (it is currently developed by State Agency for E-Governance in Ukraine). The national single window and one-stop shop is only partially in place (customs services). For most of involved state bodies, it does not allow submission of all required information and documents in electronic format (application for certificates, customs declaration, required documents, and permits).

Anti-Fraud requests are submitted and managed based on paper applications, an electronic system is available only for internal use. The internal system does not exchange data with the EU information system. The legislation needs to be updated. There is a reference to the Ukraine-EU Association Agreement Action Plan, approved by Cabinet of Ministers of Ukraine dated 17.09.2014 № 847-p – Action 116, in reference to Article 84, Amendment XV: legislation development in reference to EU Decree № 1383/2003 dated 22.07.2003 on customs activities in reference to intellectual property rights. No electronic service is in place providing traders with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights.

HDM roadmap

Indicator 1: Legal framework

Common Risk Management Framework. Develop a service and an interface to permit the secure electronic exchange of risk information forms with the electronic Risk Information Form (RIF) system and with the Region.

Authorised Economic Operator (AEO) status. Implement the status of the authorised Economic Operator compliant with the EU requirements. Promote incentives of the authorised Economic Operator status. Create an interface for exchange of data between the national system of identification and registration for economic operators and the Authorised Economic Operators EU system.

Indicator 2: Infrastructure

Electronic interfaces to conduct all customs-related business. Extend the current systems of data exchange for NCTS to use one single interface to lodge electronic customs export declarations to the customs systems of EU countries. Conduct a feasibility study for the extension of the single access point to interface the systems of the Region. Conduct a technical feasibility for connection of the information systems through the service of Single Electronic Access Point (SEAP) to the customs systems of the EU Member States.

Single Point for Entry or Exit of Data (SPEED) portal. Conduct feasibility and cost/benefit studies for connection of the national Unified Automated Information System to the Single Portal for Entry and Exit of Data that would enables automated data exchange between Member States' electronic customs systems and Ukraine. Design an interface based on service bus technology.

Uniform user management and digital signatures. Conduct a feasibility study for introduction of uniform user management and usage of digital signatures based on a common solution for electronic signatures (or a system based on mutual recognition of existing solutions) for the customs and other authorities related to external trade. Conduct technical study and cost/benefits analysis for a framework of mutual recognition of electronic signatures between Ukraine and the EU Member States. Conduct technical study, cost/ benefit analysis for a framework of mutual recognition of electronic signatures between Ukraine and the Region with the EU.

Indicator 3: Services

Registered Exporters System. Extend the functionalities of the existing customs systems to accommodate data related to the registered exporter status. Conduct a feasibility study on development of interoperability systems interfaces with the EU REX. Cooperate with the European Commission in order to organise registration of national exporters into the EU REX central database

Economic Operators Registration and Identification system. Implement the EORI approach compliant with the EU requirements based on EORI number that serves as a common reference in relations of economic operators with customs authorities throughout the country and for the exchange of information between the customs authorities and other authorities. Conduct

technical analysis for interconnection of the national system with the EORI central database managed by the European Commission.

Exchange of data about Authorised Economic Operators. Conduct a gap analysis between the existing information systems used for registration of economic operators and the EU requirements for the Authorised Economic Operator status. Conclude mutual recognition agreements with the EU to ensure the exchange of AEO data in a uniform way to increase security, facilitation of reduced physical and document based controls and priority treatment. Develop system-to-system interface allowing the economic operators' data received from Ukraine to be disseminated to the EU Member States and the validation of the county' AEO status in the EU transaction systems.

Summary electronic declaration. Implement electronic summary declarations compliant with the EU requirements. Conduct a technical study on creating a mechanism of lodging of summary customs declarations between Ukraine and the EU. Conduct a technical study on creating a mechanism of lodging of summary customs declarations between Ukraine and the Region.

National Single Window System. Fulfil the organisational measures and prepare technical terms of reference for the remaining development to ensure operations of the fully integrated national single window system that allows submission, processing and delivery of all required information and documents in electronic format (including for foreign traders). Implement the integration of the national single window with the single window.

Anti-Counterfeiting and Anti-Piracy System. Create an electronic service that provides economic operators and citizens with the possibility to submit a claim asking the intervention of Customs in order to take measures against goods infringing certain intellectual property rights. Upgrade the current national Anti-Fraud Information System (internal) to allow automated processing of claims. Connect the national Anti-Fraud Information System with the EU centralised Anti-Counterfeiting and Anti-Piracy System. Conclude agreements, define formats of data exchange and connect the national Anti-Fraud Information System with the similar systems of the Region.

2.4 eCommerce for SMEs

By fostering a digital single market, the EU expects to create up to €250 billion in additional growth, hundreds of thousands of new jobs, and a vibrant knowledge-based society. Why does the EU need a Digital Single Market and what are the main benefits of the harmonisation of digital markets with the Eastern Partnership countries?

2.4.1 EU baseline

With the growth of the B2B sectors in all industries, eCommerce for SMEs is one of the sectors that have witnessed a rapid increase. eCommerce platforms for SMEs (B2B eMarketplaces) to

Box 1: EU Digital Single Market for eCommerce

315 million Europeans use the Internet every day

The Digital Market today is made up of:

- By national online services (39%)
- US-based online services (57%)
- EU cross-border online services (4%)

The priority areas of the Digital Single Market are:

1. Better access for consumers and businesses to digital goods and services across Europe

- EU consumers could save €11.7 billion each year if they could choose from a full range of EU goods and services when shopping online
- 15% of consumers bought online from other EU countries in 2014, while 44% did so domestically

2. Unlocking eCommerce potential

- Only 7% of SMEs in the EU sell cross-border
- Small online business wishing to trade in another EU country face around €9,000 extra costs for having to adapt to national laws
- If the same rules for e-commerce were applied in all EU Member States, 57% of companies would either start or increase their online sales to other EU countries

3. Affordable parcel delivery costs

- More than 85% of e-shoppers say delivery price is the most important factor when buying online
- 62% of companies that are willing to sell online say that too high delivery costs are a problem

4. Tackling geo-blocking

- In 52% of all attempts at cross-border orders the seller does not serve the country of the consumer

Source: EU Digital Single Market factsheet

assist their day-to-day digital trading activities exist since 1999 with the commercialisation of the Internet.

An interregional platform for SMEs in the Eastern Partnership would significantly enhance market accessibility for SMEs both of the EU and the Partner Countries. As there are several eCommerce operational platforms at the EU level and covering several member states, the EU baseline defines the key components and aspects that are required for harmonisation with the DSM in eCommerce.

The EU baseline has been defined in consultation with DG MARKET/CONNECT. The key aspects of the EU baseline for eCommerce harmonisation are the following: Internet security and privacy, consumer rights, competition, ePayments and eLogistics.

The main sources for the proposed description of the EU baseline for eCommerce are the following:

- The EU legal and regulatory framework related to eCommerce
- Infrastructures and information systems developed or planned for implementation by the EU Commission and the Member States
- Cases of best practice already implemented in the EU and EU Member States

Table 7 below summarises the most relevant legal basis of the EU baseline for eCommerce, together with the principal enablers that are required to meet the baseline:

EU Baseline[23]	Principal enablers required to achieve the baseline
Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on	• Free movement of information society services • Principle excluding prior authorisation to pursuit the activity of an information society service provider • Minimum general information to be provided by information society service provider

[23] See Annex A for full references to the EU legal and regulatory references where not otherwise referenced

electronic commerce)	• Transparency requirement of commercial communications information to be provided • Requirements for sending of unsolicited commercial communication • Requirement for commercial communication on-line by regulated professions • Equal validity of electronic contracting and contract concluded offline • Specific liability regime for intermediary service providers • No general obligation for providers to monitor transmitted or stored information • Non obstruction to out-of-court dispute settlement • Availability of court actions concerning information society services
Directive 2011/83/EC on Consumer Rights	• Information required for distance contracts and off-premises contracts • Consumer Protection Cooperation Network between government agencies • Rights on delivery of goods • Rules on the fees for the use of means of payment • Passing of risk - rules on the conditions for the risk of loss of or damage to the goods • Limitation of rate for communication by telephone
Regulation (EU) N°910/2014 on electronic identification and trust services for electronic	• Online trustmarks for retail websites • Non -discrimination of electronic documents vis à -

transactions in the internal market (eIDAS Regulation)	vis paper documents as evidence in legal proceedings
Directive 2007/64/EC on payment services in the internal market	• Legal framework in the area of eCommerce payments
Directive 2010/45/EU on the common system of value added tax as regards the rules on invoicing	• Equal treatment between paper and electronic invoices
Directive 2013/11/EU on alternative dispute resolution for consumer disputes	• Online Dispute Resolution system for consumers for eCommerce transactions
Directive 2002/58/EC on privacy and electronic communications	• Authorised recording of communications and the related traffic data in the course of lawful business practice / confidentiality of the communication • Allowance to process user traffic data by the provider of an electronic communication service

Table 9-Legal basis and enablers required for eCommerce harmonisation

Table 8 lists a set of indicators and corresponding benchmarks towards meeting the defined baseline in Table 7. The indicators exhaustively describe the main aspects required for the implementation of an interregional eCommerce platform for SMEs. From the benchmarks, a set of questions has been prepared so that when the state of play have been collected in the 6 Eastern Partner Countries;

Indicators	**Benchmarks to achieve Harmonised Digital Markets for eCommerce**
Internet security and privacy	• Allowance to process user traffic data by the provider of an electronic communication service

	• Specific liability regime for intermediary service providers • No general obligation for providers to monitor transmitted or stored information • Authorised recording of communications and the related traffic data in the course of lawful business practice / confidentiality of the communication
Consumer rights	• Online trustmarks for retail websites • Minimum general information to be provided by information society service provider • Transparency requirement of commercial communications information to be provided • Minimum pre-contractual information required for distance contracts and off-premises contracts • Consumer Protection Cooperation Network between government agencies of EU Member States • Non obstruction to out-of-court dispute settlement • Online Dispute Resolution system for consumers for eCommerce transactions • Requirements for sending of unsolicited commercial communication • Limitation of rate for communication by telephone
Competition	• Free movement of information society services • Principle excluding prior authorisation to pursuit the activity of an information society service provider • Mini One-Stop-Shop for exchanges of data on VAT

ePayments	• Legal framework in the area of eCommerce payments and rules on the fees for the use of means of payment • Equal treatment between paper and electronic invoices
eLogistics	• Equal validity of electronic contracting and contract concluded offline • Passing of risk - rules on the conditions for the risk of loss of or damage to the goods • Rights on delivery of goods

Table 10-Indicators and corresponding benchmarks defining the baseline for eCommerce

Table 3 in the Annex presents the detailed description of the EU baseline. The annex also includes the identified references to the EU legal and regulatory framework related to eCommerce area.

2.4.2 Overview of the state of play and gap analysis for the Region

The Eastern Partnership countries have collectively some strong and weak aspects in relation how far they are from the EU baseline. Due to historical reasons, the state of play of some Partner Countries could be similar. However, most of the Partner Countries have done significant progress in areas described by one, two or several indicators and their state of play in these areas approaches the EU baseline level. The identified common gaps are indicators of common measures and potential projects that can be proposed at the Region level.

The following exhibit shows the overall state of play and gaps of the Region by the main broad indicators:

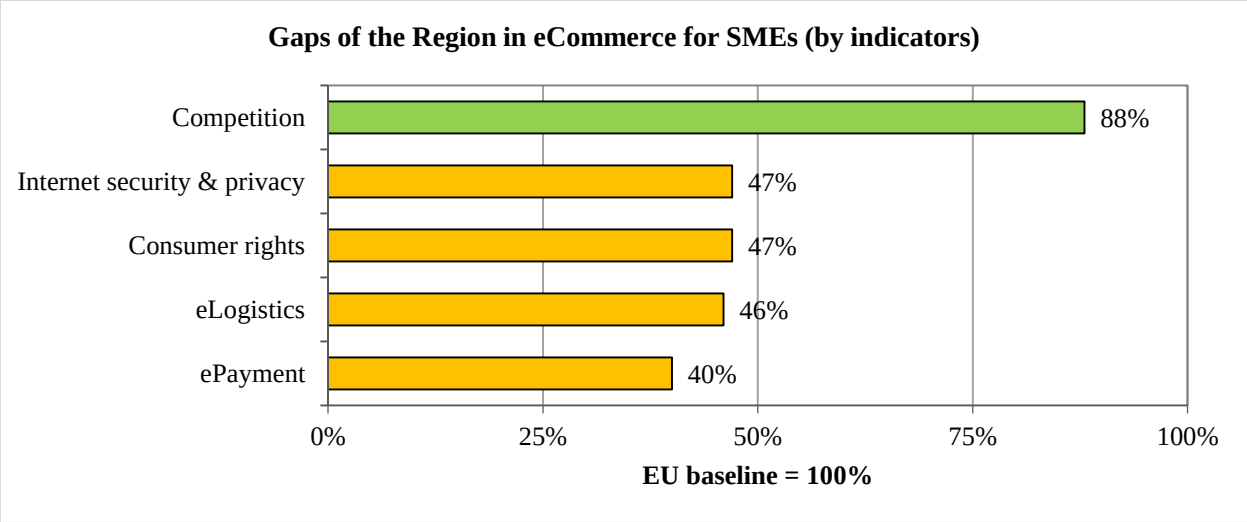

Exhibit 35 - State of play and gaps of the Region in eCommerce for SMEs

The aspect of competition in eCommerce for SMEs in the Region is that the most have advanced towards the harmonisation with the EU Member States. This means that the countries are open for the competition on eCommerce market and have no generalised obstacles for its access by SMEs from other Eastern Partnership countries.

The weakest aspect is electronic payments for eCommerce transactions where a number of aspects obstruct the implementation of a seamless approach for cross border payments. The average level for three other indicators, internet security and privacy, consumer rights and eLogistics, have a similar state of play. Their score indicates that the Region has defined basic aspects of their national legal frameworks in relation to eCommerce. The required national components for the implementation of information systems of eCommerce platform have been initiated.

The detailed gap analysis of the Region at benchmarks level shows more precisely, where progress on harmonisation of eCommerce for SMEs could be done. The following exhibit shows the overall state of play and gaps of the Region by the detailed benchmark:

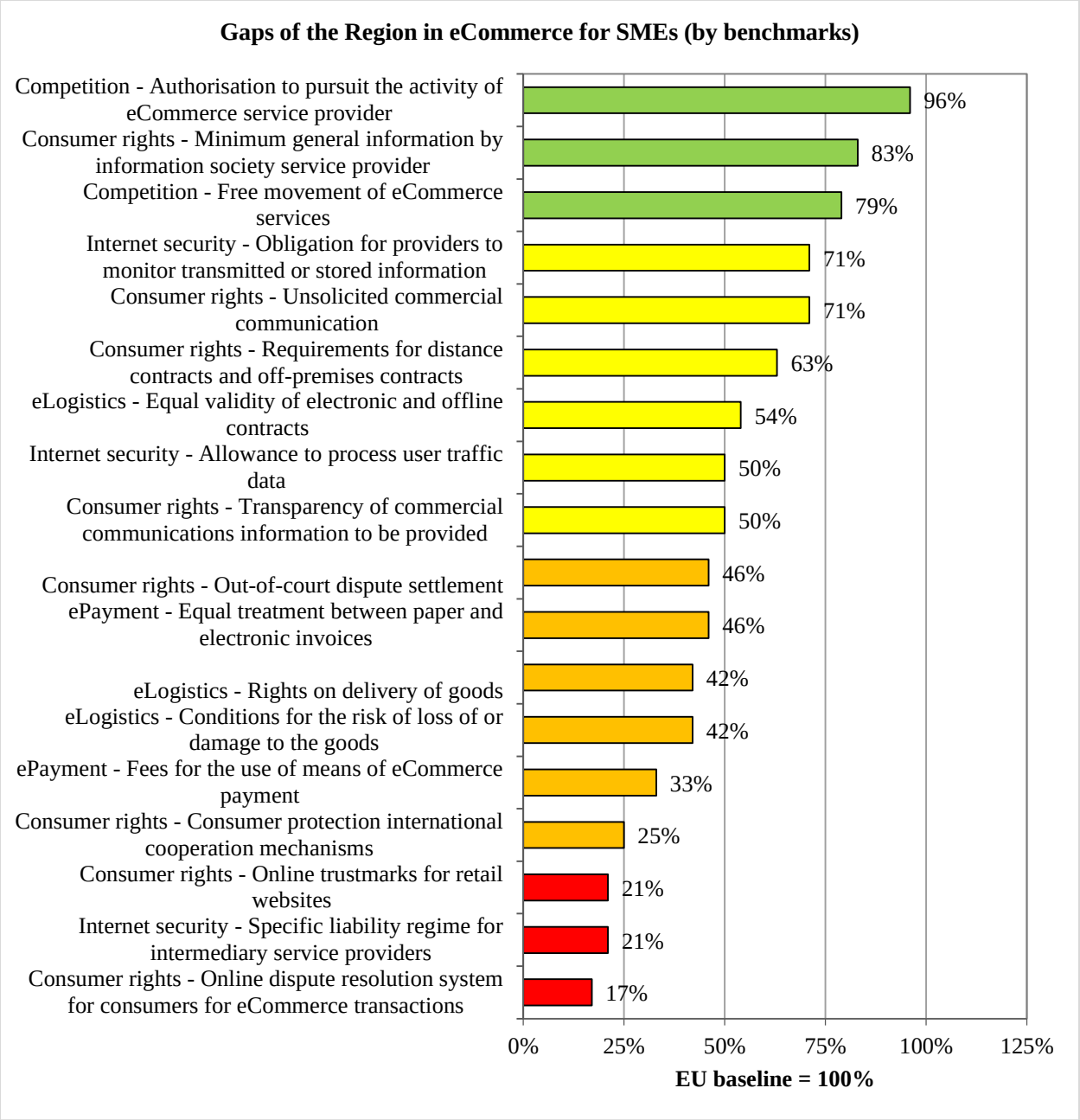

Exhibit 36-Detailed gap analysis of the Region in eCommerce for SMEs

The legal framework of the most of the Partner Countries applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. Another aspect in the state of play of the Region which compiles well with the EU baseline is that of eCommerce service providers render easily, directly and permanently accessible to the recipients of the service and competent authorities minimum general information that may be vital for customers claiming

their rights. The Partner Countries do not restrict the freedom to provide information society and eCommerce services by service providers from another country.

The biggest common gaps of the Region are in the legal provisions and frameworks assuring consumer rights. None of the Partner Countries has established an on-line dispute resolution system for customers of eCommerce transactions. In the EU, the Alternative Dispute Resolution system is supplemented by an Online Dispute Resolution mechanism involving the setting up of a European online dispute resolution platform - an interactive website free of charge in all languages of the Union Accessible through "Your Europe" portal.

This gap is linked to another important gap in harmonisation between the EU and the Region, and namely the weak international cooperation mechanisms on consumer protection . The Consumer Protection Cooperation (CPC) Network brings together the public authorities in all the EU Member States (and other EEA countries) which are responsible for the enforcement of EU consumer protection laws. A national authority in the EU country where consumer interests are harmed can call on their counterpart in the Member State where the trader is located and ask for action to stop the infringement. Enforcement authorities can also alert each other to malpractices that they have spotted which may spread to other countries.

eCommerce websites in the Region use online trustmarks provided by a few international companies. However, there are no national schemes of online trustmarks for retail website in the Partner Countries. The usefulness and benefits of the trustmark schemes are in the reassurance of consumers on the reliability of accredited traders. The aim is to encourage the establishment of eCommerce platforms with price comparison functionalities.

In most of the Partner Countries, the national legislation does not define specific liability regimes for three categories of essential services assuring the provision of eCommerce online services: transmission conduit operators, caching providers and hosting services providers.

Rules on the fees for the use of certain means of eCommerce payment (e.g. credit or debit cards, electronic valets) should prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment. However, the national legislation of most of the Partner Countries does not define the requirements for eCommerce payments and does not limit the fees for the use of means of electronic payment.

Only Armenia and Belarus have introduced the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved. The same is applied to the definition of the rights on delivery of goods. The national legislations do not always define the requirements for time of delivery of goods purchased through eCommerce transactions. These limitations seriously obstruct to the willingness of the consumers to make online purchases, especially from eCommerce websites established outside the territory of their countries.

2.4.3 Overview of common actions for the Region

The study has identified some actions that would have a significant impact on the Region. These are the aspects with the widest common gaps of the Region for harmonisation of eCommerce for SMEs. The common actions are also the ones with the biggest economic and political benefits within the Region. The priority actions could be divided in two categories. The first category includes infrastructures and service development projects. The second category concerns the harmonisation of the legal frameworks within the Region.

Set up of an online dispute resolution platform (an interactive website free of charge) that facilitates and speeds up resolution of disputes related to eCommerce transactions. This tool can provide reassurance to both sides, service providers and consumers, and build trust in eCommerce transactions. Through this website, parties can initiate an alternative dispute resolution procedure in relation to disputes concerning online transactions without going through traditional court legal procedures that are time and resources consuming. National entities responsible for settling alternative disputes receive the complaint electronically through the online platform and seek to resolve the dispute through existing legal alternative dispute resolution mechanisms.

Create online trustmark schemes for retail websites for electronic identification and trust services of electronic transactions which assure the trustfulness of qualified eCommerce service providers. The Partner Countries would get significant benefits from establishing a common trustmark scheme for the Region. Another step is joining the work in progress on the EU-wide trustmark schemes, which aims to reassure consumers on the reliability of accredited traders at the EU level. The trustmarks will facilitate the promotion of Regional eCommerce platforms for SMEs. Such certified sites help consumers to make informed decisions when using online retail services. The Partner Countries can start by jointly developing specifications with regard to the

implementation mechanisms, form, the presentation, composition, size and design of the trust mark for qualified trust services.

Enhance consumer protection international cooperation mechanisms within the Region. The Region should establish cooperation mechanisms between the national public authorities and the authorities of the EU who are responsible for enforcement of consumer protection laws, including for eCommerce. Especially for consumer protection in eCommerce field, the authorities can establish information systems for the exchange of information between competent authorities of different countries.

Legally define a specific liability regime for intermediary service providers. These are the conditions for network operators (transmission in a communication network), caching providers (temporary storage of information) and hosting services.

Limit fees for the use of means of eCommerce payment. Comprehensive national legislations for eCommerce payments by credit or debit card, on the internet, by phone, using mobile and other electronic payments presents a substantial benefit for eCommerce development and market integration in this field at European level. Also, the Partner Countries should think about the synergies in defining a similar rule for the Region in order to facilitate the international expansion of SMEs.

Define in the legislation conditions for the risk of loss of or damage to the goods. These legal provisions of eLogistics should define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. It also should stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

Define rights on delivery of goods. The national legislations should be amended to define the time of delivery when the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer. It also should clearly define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

Develop an eCommerce platform that assists SMEs in their digital activities across the Region and the EU. Such an interregional platform will significantly amplify market accessibility for SMEs, open new markets and assure a boost in trade.

Common priority projects within the Region

In eCommerce, these are the areas which help in the creation of more accessible markets and facilitate a rapid boost in trade for SMEs. Pilot projects in information services development would show immediate benefit for SMEs and customers that use these services. The study proposes some most rewarding areas for the harmonisation and the common projects within the Region:

- Setting-up an eCommerce platform for SMEs
- Common online trustmark scheme for eCommerce websites
- Harmonised semantic data model and format of electronic invoice
- Harmonised semantic data model and format of electronic contract
- Consumer Protection Cooperation Network between government agencies

Legal harmonisation within the Region

Another important area for the common actions for the Partner Countries is the harmonisation of the legal frameworks within the Region. The following aspects have been identified as the most important for the harmonisation in eCommerce for SMEs:

- Minimum general information to be provided by eCommerce service provider
- Transparency requirement of commercial communications information
- Minimum pre-contractual information required for distance contracts
- Requirements for sending of unsolicited commercial communication
- Rules on the conditions for the risk of loss of or damage to the goods
- Rights on delivery of goods

2.4.4 Benefits for and readiness analysis of the Region

Benefits of the Partner Countries from the harmonisation with the EU

Allowance to process user traffic data within the EU and the Region would significantly increase opportunity for SMEs to use traffic data for personalised marketing of their eCommerce services and for development of new value added services.

Harmonisation of the conditions of a specific liability regime for three categories of essential service provider can bring transparency for SMEs in the requirements to provide eCommerce services in foreign markets. They would have less uncertainties and better understanding about their rights and obligations. The harmonisation would increase international opportunities for hosting service providers and Cloud computing services providers. Increase competition brings better and cheaper services to users. Saved money can be reinvested into better infrastructure and in development of new services.

For the development of eCommerce, there is a definitive usefulness and benefits of the country-wide trustmark schemes that help to reassure consumers on the reliability of accredited online traders and service providers, especially for SMEs. This will lead to increase in eCommerce sales.

Minimum general information to be provided by information society service provider is important and may even be vital for customers claiming their rights. The country of origin of the web trader can have major consequences, for example, for their right of withdrawal.

The requirements for transparency of commercial communications information to be provided will give a boost for development of advertisement services on Internet and new business opportunities for SMEs.

Conditions for the harmonisation of digital markets

Challenges and risks

- Introduction of a specific liability regime for three categories of services providers requires clear definition of their responsibilities in the technological environment that rapidly changes and is in some aspects different in the EU and the Region.
- Harmonisation regarding specific liability regime for caching and hosting intermediary service providers can create disputes in interpretation of conditions that the provider does not have actual knowledge of illegal activity or information by a recipient of the

service. In regard of claims for damages, it could be challenging to justify that it is not aware of facts or circumstances from which the illegal activity or information is apparent.

- Implementation of trustmarks schemes normally requires the usage of SSL certification for web servers. Establishment of a common trustmark scheme by the Region will require mutual recognition of national SSL certificates providers.
- Establishment of a Regional trustmark (or joining EU-wide trustmark) schemes will require putting in place effective cooperation mechanisms and platforms for the governance of such national trustmark systems.
- Harmonisation in the rules of transparency of commercial communications information to be provided wider open possibility for well-established international companies to dominate local markets of online advertisement.

Obstacles

- Authorisation to process user traffic data can be limited by the requirement of some national legislations to keep the citizens' data on the territory of their countries. This increases the cost of communication services because service providers would need to maintain additional infrastructures in foreign countries.
- Trustmark schemes require the usage of cutting edge technologies for eCommerce website seals which are currently quite expensive.
- Additional requirements for transparency of commercial communications information to be provided will impose new rules and regulations on SMEs which can create additional burden.
- There will be resistance and limited trust by number of legal and natural persons for conclusion of distance contracts using electronic signature means.

Conditions

- The current legislative framework in the Region has to be deeply analysed and approximated with the EU legal requirements from the perspective of benefits from harmonisation. The private sector should be involved from the initial phase in proposals development. Proposed changes have to be presented for public consultation.
- To review the existing legislation and make changes to improve the legislation on

processing of user traffic data, set appropriate regimes for online service providers,

- Implementation of a trustmark scheme require the definition of clear rules applied to the process of assessment of candidate eCommerce service providers and the explicit conditions for the attribution of the trustmark. This creates a threat of possible corruption of the decision making authority. Creation of a code of conduct and transparent procedures are the critical conditions.
- Transparency requirement of commercial communications information to be provided emphasises the need for transparency when advertisements are displayed on the Internet. It obliges eCommerce service providers to ensure that online commercial communications (including promotional offers, discounts, premiums, promotional competitions or games) meet certain transparency requirements. Both the commercial communication and the natural or legal person responsible for it must be clearly identifiable, and any conditions attached to the offers, discounts etc. must be easily accessible.
- Implementation of distance contracts requires simple and accessible technical tools for verifying of electronically signed contracts, their signatories and timestamps. With the harmonisation of digital markets, these tools have to allow verification of electronic documents and signatures issued in other countries. This imposes a strong condition on the interoperability of the required tools.

Opportunities

- The requirement on intermediary services providers to inform the competent public authorities in case of detection of illegal activities can provide additional reassurance to certain categories of consumers to use eCommerce. This can particularly important for eCommerce services for children and teenagers (online education, media content sharing, and social networks).
- With a number of eCommerce websites that have trustmarks, there is an opportunity to establish national price-comparison websites, and later of pan-EU/Regional price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services.
- The fact there are no national trustmark schemes in the Region creates an opportunity to

design them in Harmonisation with the future common trustmark scheme of the EU Member States. The European Commission is in the process of elaborating different policy options for EU-wide trustmark schemes and cooperation platforms in the governance of such trustmark systems.

- Instead of creating national trustmark schemes, the Region can establish a common trustmark scheme.

Impact of the EEU membership on the HDM with the EU

The membership of Belarus and Armenia in the Eurasian Economic Union has an impact on the consumer protection and international cooperation mechanisms. The harmonisation of eCommerce for SMEs should take into account the current engagements of these countries and find mutual benefits from the coordination of development of eCommerce in the Region and in the EEU.

A consumer protection cooperation agreement is set up within the Eurasian Economic Union and the CIS. A similar body has being created to affiliate to Eurasian economic commission. The Memorandum on cooperation between the CIS Consumer rights protection advisory council and the Interstate antimonopoly policy council has been signed. Agreement on the main lines of cooperation of the CIS member-states in the area of consumer rights protection has come into force. Information exchange on the laws and financial literacy is in process within the CIS. Executive authorities can alert each other to malpractices that can affect the other countries even though it mostly covers big infringements. Public councils on consumer rights protection are a part of the international consumer system CI.

In its work on the harmonisation in eCommerce, the Region can gain from the syndicated activities with the EEU and benefit from the progress already achieved by the EEU. Instead of concluding consumer protection cooperation agreements for eCommerce with individual Partner Countries, an agreement at the level of the Region and the EEU could be considered, including involving other members of the EEU.

2.4.5 Armenia

State of play and gap analysis

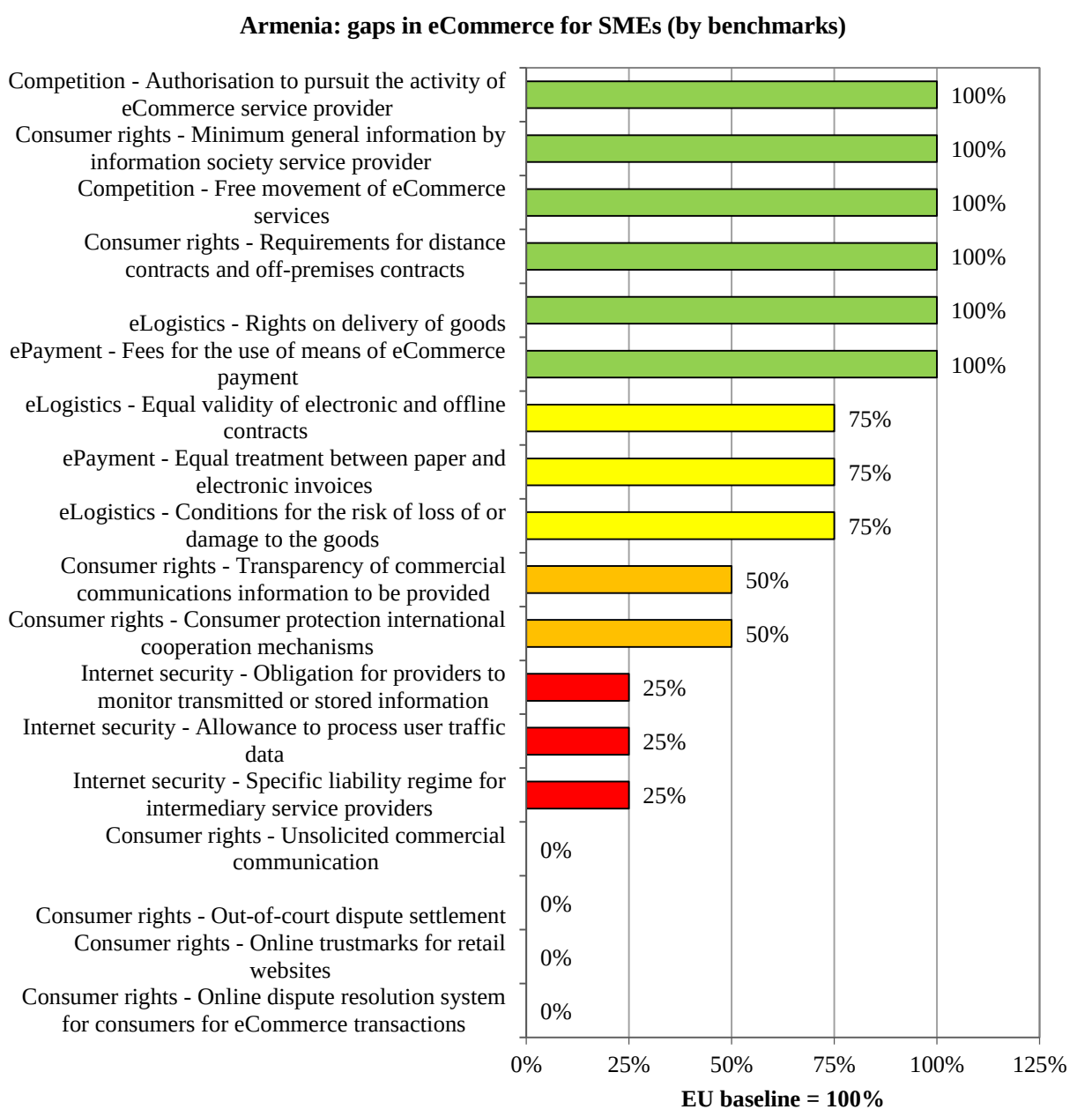

Exhibit 37- Armenia: state of play and gap analysis in eCommerce

Internet security and privacy

The proposed Law on the Protection of the Personal Data defines the necessity of the consent

of the individual to process or use their personal data. The national legislation does not define any rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

The caching and hosting services are defined as telecom services in the Armenian regulation. After the amendments to this law, the telematics services were excluded from the list of activities subject to licensing and are not defined in any way in any of the laws. Apart from the gap in the definition of the services, there is also an uncertainty regarding the liability regimes of the service providers. For example, the court can convict a hosting service provider in disseminating pornography (which is a cyber-crime according to the Criminal Code). The decisions are made case-by-case. The national legislation does not clearly define specific liability regimes for three categories of online service providers -transmission conduit operators, caching providers and hosting services providers.

The providers of transmission services, such as mobile operators, do not have the right to monitor the content of the information transmitted through their networks and are not liable for this information as defined by the Law on Electronic Communications. Obligations of information transmission service providers to monitor information are regulated. In compliance with the EU baseline, the national legislation does not include requirements for providers of caching and hosting information services to monitor the information which they transmit or store in order to detect any illegal activity.

Consumer rights

There are no established country-wide trustmark schemes for electronic identification and trust services for electronic transactions that help to reassure consumers on the reliability of accredited online traders and service providers. Trustmarks of foreign providers are used by individual eCommerce websites for electronic identification and trust services for electronic transactions.

By the proposed changes in the Law of Trade and Services (article 4.1) the eCommerce service provider is required to place information about the company legal name, status, address and contacts details, state registration and VAT numbers, licensing information. The amended Trade Law will impose the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined

scope of information about the service provider.

The area is regulated by the Law on the Advertisement and the Law on the Television and Radio. However, no specific regulations are available for internet advertising and internet marketing. There is no explicit obligation to ensure that online commercial communications such as promotional offers, discounts, premiums, promotional competitions or games, meet certain transparency requirements. Both the commercial communication and the natural or legal person responsible for it should be clearly identifiable, and any conditions attached to the offers, discounts etc. must be easily accessible.

The current legislation and proposed amendments include the requirements for distance contracts and off-premises_contracts with indication of minimum of legally defined pre-contractual information.

The international consumer protection cooperation brings together the public authorities in different countries who are responsible for the enforcement of consumer protection laws. Cooperation is done in the frame of IPM. The country has established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

A working group of the Ministry of Justice has initiated the process, and has commenced the work on drafting of proposed amendments to the laws. However, no official documents or drafts are presented to the public yet. The national legislation does not currently allow the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

The country does not have an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.

Unsolicited commercial communications (spam) sent by e-mail is considered as a fundamental way of commercial promotion of products and services, and is an important factor for the development of eCommerce. The legal framework of Armenia is not specific on this matter. It does not explicitly prohibit nor allow the sending of unsolicited commercial communications.

Competition

The proposed changes in the Law on Trade and Services (Article 4.1) defines that “eCommerce services can be provided by legal entities or individual entrepreneurs based on invoicing forms

and documentation as defined by the tax regulations in Armenia". No other restrictions or requirements are defined in the Law. The national legislation does not restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country.

The current legislation does not explicitly restrict the freedom to provide eCommerce services by a provider from another country. In the information service sector, authorisation may be required only in telecom and TV services sectors, where the operator requires numbering or frequency. The country applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider.

ePayment

Any rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) that can prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment have not been identified in the current legislation. The regulations of the Central Bank of Armenia define the requirements for online payments for the use of means of electronic payment[24].

The vast majority of invoicing in Armenia is processed through electronic platforms. The latter is favoured compared to the paper invoicing. The proposed changes in the Law on Electronic Document and Electronic Signature define that the electronic document/invoice which does not hold electronic signature but can validate that it is submitted by the consumer can fully replace the paper invoices with handwritten signatures. The national legislation assures equal treatment between paper and electronic invoices (e-invoices). The framework of a common national data model of e-invoicing format has not been defined.

eLogistics

The regulations for eContracting are in place. The electronic contracts signed by electronic signatures have equal validity as the paper contracts. In addition, trade deals/contract concluded at distance can be considered valid even without electronic signature.

[24] For example, private payment system iDram[24] applies the following conditions applied to legal persons: receiving online payments for products and/or services, sold by legal persons - 2.5-5% commission. It takes 2-5 days to connect to the system.

By the proposed changes in the Law on the Consumer Rights (article 23), the customers of distance trade (including eCommerce) will also have the right to give back or change the purchased good during 14 days of the purchase. The necessary preconditions for the change are defined in the Law. The proposed amendments to the current legislation will define some conditions for the risk of damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved. However, these legal provisions should also define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier.

By the proposed changes in the Law on the Consumer Rights (article 24) the time of delivery of distant trade items is defined maximum 30 days, if the contract does not say otherwise. The proposed amendments to the current legislation will define the requirements for time of delivery of goods purchased through eCommerce transaction.

HDM roadmap

The following sections present the aspects where progress on HDM can be made, the objectives and individual follow-up actions of the country for the priority area:

Internet security and privacy

Allowance to process user traffic data - assure to users their rights to manage online privacy. Amend the national legislation with the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

Specific liability regime for intermediary service providers - increase the transparency of rules for provision of cross border eCommerce services by SMEs. Amend the national legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

Obligation for providers to monitor transmitted or stored information - improve the security of users online. Clearly extend the allowance to other categories intermediate service providers such as cashing and hosting. Not impose a general obligation on providers, when providing the services of transmission, caching and hosting, to monitor the information which they transmit or store. Not to require to actively seek facts or circumstances indicating illegal activity.

Consumer rights

Online trustmarks for retail websites - reassure consumers on the reliability of accredited online service providers, especially across borders. For the development of eCommerce, there is a definitive usefulness and benefits of the country-wide trustmark schemes that help to reassure consumers on the reliability of accredited online traders and service providers. A trustmark can be in form of a logo published on certified websites and linked to an accreditation website (trust mark providing third-party website identity validation). It can be also assured through another mean of trusted electronic identification (SSL, electronic certificate). Another aim is also to encourage the establishment of price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services. The next step would be harmonisation of national trustmarks schemes with EU Member States.

Transparency of commercial communications information to be provided. Amend the legislation with the requirements emphasising the need for transparency when advertisements are displayed on the Internet for the types of the online commercial communications such as promotional offers, discounts, premiums, promotional competitions or games.

Consumer protection international cooperation mechanisms - create a mechanism for international user protection between the Region and the EU. Establish consumer protection cooperation with the public authorities in different countries who are responsible for the enforcement of consumer protection laws with neighbouring countries, countries with main trading volumes, EU Member States. Especially for consumer protection in eCommerce field, the authorities can establish an information system for efficient exchange of information between competent authorities of different countries for action to stop infringements.

Possibility for out-of-court dispute settlement - facilitate dispute resolution for cross-border purchases. Amend the national legislation allowing the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

Online dispute resolution system for consumers for eCommerce transactions - provide reassurance to service providers and consumers, and build trust in eCommerce transactions. Set up an online dispute resolution platform (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions.

Requirements for the sending of unsolicited commercial communication (spam) - improve the effectiveness of promotion of products and services assuring consumer rights. Improve the

relative legislation by defining requirements applied to unsolicited commercial communication. It must notably ensure that such communication is clearly and unambiguously identifiable. Unsolicited commercial communications sent by e-mail is an important way of commercial promotion of products and services, and is an important factor for the development of eCommerce between the Region and the EU.

ePayment

Equal treatment between paper and electronic invoices - reduce costs and delays of international eCommerce transactions. Amend the national legal framework that should assure equal treatment between paper and electronic invoices. Define national technical standards by promoting the development of interoperable e-invoicing solutions based on common with the EU standards, paying particular attention to the needs of small and medium-sized enterprises. Define a single and clear semantic data model and a common eInvoicing format compatible with the EU best practices to facilitate semantic interoperability, ensure technology neutrality and facilitate the uptake of e-invoicing for eCommerce transactions for SMEs.

eLogistics

Conditions for the risk of loss of or damage to the goods - reassure consumers and increase the attractiveness of cross-border eCommerce services. Amend legislation to define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. Stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

2.4.6 Azerbaijan

State of play and gap analysis

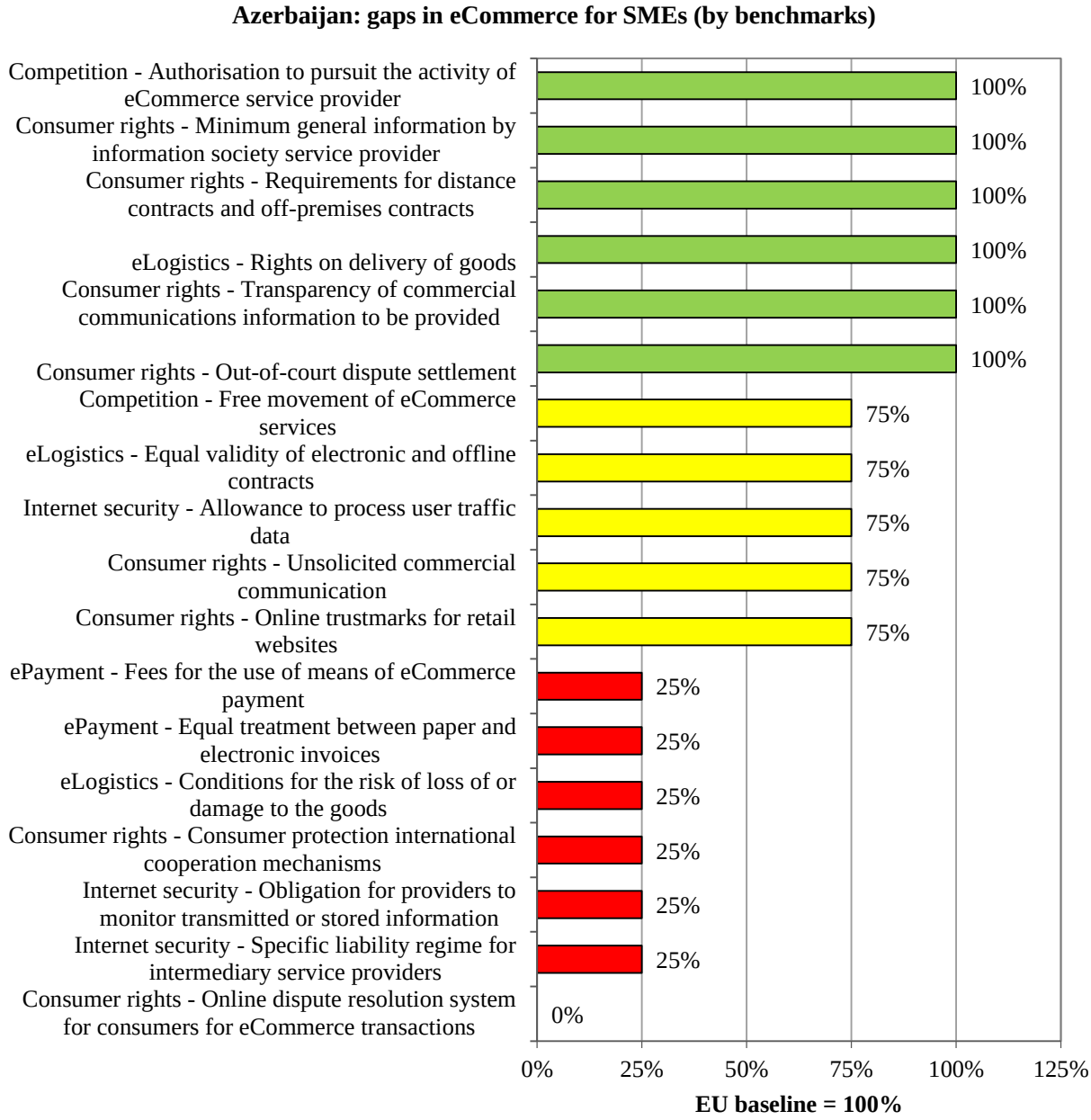

Exhibit 38- Azerbaijan: state of play and gap analysis in eCommerce

Internet security and privacy

The national legislation defines that for the purpose of marketing electronic communications

services or for the provision of value added services, the provider of an electronic communications service may process user traffic data to the extent and for the duration necessary for such services or marketing. This is conditioned by the requirement that the subscriber or user to whom the data relate has given his/her consent. In general, the Law on eCommerce is compliant with the EU best practice in this aspect. Still, the legislation is not explicit about possibility for users or subscribers to withdraw their consent for the processing of traffic data. In addition, it is not indicated if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

There is no provision in the national legislation on the regimes for online service providers. In Azerbaijan, the conditions for mere conduit operators (transmission in a communication network), caching providers and hosting services are not defined. This can create uncertainty for some service providers, especially foreign companies, to provide eCommerce services. The aspect is important for services of streamed video and audio, hosting of different types of user data and information, Cloud computing, SaaS.

The national legislation does not have any provisions about the requirements for information services providers on monitoring information transmitted to detect illegal activities. Cases when information service providers have obligations to inform the competent public authorities of alleged illegal activities are not defined. By the decision of court, the activities of e-commerce parties, as well as information services providers can be checked to detect illegal activities. The absence of neither the general obligation on providers, when providing the services of transmission, caching and hosting, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity is fully compliant with the recommendations of the EU legislation.

Consumer rights

Azerbaijan has not yet established its national eCommerce trust mark as an indication that the online shops displaying the national trustmark offer a high level of service. However, individual eCommerce service providers use international online trustmark services. This practice however is not widely used.

The national legislation should impose the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined scope of information about the service provider. The Law on

eCommerce (Article 5.3-The requirements for eCommerce service provider) sets the requirement for the supplier to give the information on its registration details, contacts, registration number of register or other identification information, tax ID, etc. This provision is fully compliant with the EU baseline and with the requirements of the Directive 2000/31/EC on electronic commerce Article 5.

The national legislation imposes that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers. Article 6 of the Law on eCommerce (Commercial notification) defines the rules of transparency in the commercial communication for eCommerce. According to the Law, the seller using commercial notification to advertise the goods should meet certain terms. This aspect is compliant with the requirements of the Directive 2000/31/EC on eCommerce Article 6.

For a distance contract (concluded online or by electronic means) or an off-premises contract, the national legislation requires that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms. The Article 8 of the Law on eCommerce on (Requirements for concluding a contract) stipulates that the seller (supplier) must provide specified information before the buyer (customer) orders. This aspect is compliant with the requirements of the Directive 2011/83/EC on Consumer Rights.

The consumers' rights are protected by the State Service for Antimonopoly Policy and Consumer Rights Protection under the Ministry of Economy and Industry. However, the international cooperation with its foreign counterparts is not so developed. On the Ministry level, it is limited to general economic activities[25].The country has not yet established international cooperation mechanisms with the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

The Law on eCommerce stipulates that disputes between parties can be solved by out-of-court means, as well as by electronic means. However, an appropriate platform for settlement of disputes using electronic means is not yet developed. According to the national legislation, the parties can agree for the dispute to be settled by the Court of arbitration. Azerbaijan is also a party to the New York Convention 1958, on the Recognition and Enforcement of Foreign Arbitral Awards. This aspect is compliant with the requirements of the Directive 2000/31/EC on

[25]www.economy.gov.az

eCommerce Article 17.

Even though the national legislation provides provisions for dispute settlement, including eCommerce transactions, using electronic means, there is no platform developed for this. The ministry of Justice currently works on development of the platform for online claims.

The Law on eCommerce allows sending unsolicited commercial communications by email or mobile communication means, but few requirements for this are defined. The Law on eCommerce indicates that service providers have to respect the opt-out registers to which natural persons not wishing to receive such commercial communications can sign up. Also, the legislation stipulates that absence of an answer to an unsolicited commercial communication does not mean acceptance of its commercial offer. Additional amendments to local legislation to set the requirements for sending unsolicited commercial communications are planned to make by the Parliament. The framework is compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 7.

Competition

The national legislation of Azerbaijan does not restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country. The general rule is that in order to be engaged in entrepreneurial activities on the territory of Azerbaijan foreign registered company should be registered locally. The Law on eCommerce (Article 4 – General principles of electronic commerce) stipulates the principle of free movement of services, goods and financial resources. In these terms, the legislation in Azerbaijan is partially compliant with the EU best practices (Directive 2000/31/EC on electronic commerce Article 3) because it does not explicitly define the conditions of provision services or sales of goods in the territory of Azerbaijan by a service provider established abroad.

According to the Law on eCommerce, except for activities requiring special consent (licence) according to legislation of the Republic of Azerbaijan, legal person from the date of registration and physical from the date of getting right to deal with business activity not creating legal person can start e-commerce activity. The country applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. This principle is without prejudice to the authorisation schemes of Azerbaijan which are not specifically and exclusively targeted at information society services, or which are covered by another legislation (activities in the areas of financial, insurance and securities markets). The provision is fully compliant with the EC

Directive on electronic commerce that defines the principle excluding prior authorisation (Directive 2000/31/EC on electronic commerce Article 4).

ePayment

A Draft Law on Payment Services in under consideration at the Parliament. The national legislation does not yet define the requirements for eCommerce payments and does not define the rules on the fees for the use of means of electronic payment. The rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean(Directive 2011/83/EC on Consumer Rights).

The practice of eInvoicing is not widely spread in Azerbaijan even though there is no any limitation for this. There is no solid technical platform for eInvoicing. The national legislation does not explicitly assure equal treatment between paper and electronic invoices and does not define the framework of a common national data model of eInvoicing format.

eLogistics

The Law on eCommerce (Article 7 on Signing the contract and Article 8 on Requirements for signing the contract) stipulates the requirements for the contract between seller and buyer of eCommerce can be signed in the form of an eDocument. The rules applied for placing of orders are defined. The national legislation of Azerbaijan does not establishes the universal equal validity of electronic contracting and contract concluded offline that is not compliant with the recommended by the EC Directive 2000/31/EC on electronic commerce Articles 9-11.

Even though there are some provisions in the law on eCommerce on the delivery of goods, the national legislation does not define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. It also does not stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply (The Directive 2011/83/EC on Consumer Rights).

The Law on eCommerce (Article 10 - Fulfilment of contract) sets the period of 30 days for implementation by the seller of the order, from the day of ordering by customer. If seller can’t

supply the goods order due to the impossibility of supply, the seller should inform the customer and return the sum paid by customer within 7 days. The national legislation is compliant with the EU baseline Directive 2011/83/EC on Consumer Rights.

HDM roadmap

The following sections present the aspects where progress on HDM can be made, the objectives and individual follow-up actions of the country for the priority area:

Internet security and privacy

Allowance to process user traffic data - assure to users their rights to manage online privacy. In addition to the Law on eCommerce, the legislation should give to users or subscribers the possibility to withdraw their consent for the processing of traffic data. The traffic data can be processes without users' consent based on decision of court. The Law on e-Commerce does not regulate this issue. This can also concern processing of traffic data necessary for the purposes of subscriber billing and interconnection payments. The legislation should indicate if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

Specific liability regime for intermediary service providers - increase the transparency of rules for provision of cross border eCommerce services by SMEs. The legislation should be amended to define the degree of liability of the service provider for the information transmitted in a communication network of information provided by a recipient of the service. The liability of a service provider should be defined for the automatic, intermediate and temporary storage of that information, performed for making more efficient the information's onward transmission to other recipients of the service upon their request. Liability of the hosting service providers should be defined for the information stored at the request of a recipient of the service, with some clearly defined liability exceptions (does not have actual knowledge of illegal activity or information, and others).

Obligation for providers to monitor transmitted or stored information -improve the security of users online. The legislation may establish obligations for information society service providers to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service

with whom they have storage agreements.

Consumer rights

Online trustmarks for retail websites - reassure consumers on the reliability of accredited online service providers, especially across borders. For the development of eCommerce, there is a definitive usefulness and benefits of the country-wide trust mark schemes that help to reassure consumers on the reliability of accredited online traders and service providers.

Consumer protection international cooperation mechanisms - create a mechanism for international user protection between the Region and the EU. Consumer protection cooperation agreement can be set up by the State Service for Antimonopoly Policy and Consumer Rights Protection with the public authorities in different countries who are responsible for the enforcement of consumer protection laws, in priority, with neighbouring countries, countries with main trading volumes, EU Member States. Especially for consumer protection in eCommerce field, the authorities can establish an information system for efficient exchange of information between competent authorities of different countries for action to stop infringements.

Online dispute resolution system for consumers for eCommerce transactions -provide reassurance to service providers and consumers, and build trust in eCommerce. Set up an online dispute resolution platform (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions.

Requirements for sending of unsolicited commercial communication (spam) - improve the effectiveness of promotion of products and services assuring consumer rights. The country should improve its relative legislation by defining in the Law on eCommerce some additional requirements applied to unsolicited commercial communication. It must notably ensure that such communication is clearly and unambiguously identifiable. Unsolicited commercial communications sent by e-mail is an important way of commercial promotion of products and services, and is an important factor for the development of eCommerce between the Region and the EU.

ePayment

Legal framework in the area of eCommerce payments and rules on the fees for the use of means of payment - make payments online more attractive to consumers and increase the competitiveness of SMEs. A comprehensive national legislation for eCommerce payments by

credit or debit card, on the Internet, by phone, using mobile and other electronic payments will present a substantial benefit for eCommerce development and market integration in this field with the EU. The Law on Payment Services which is under consideration at the Parliament, should include the rules on the fees for the use of certain means of payment (e.g. credit or debit cards, electronic valets) and prohibit traders from charging consumers fees that exceed the cost borne by trader for the use of such mean.

Equal treatment between paper and electronic invoices -reduce costs and delays of international eCommerce transactions. Reduce costs and delays of international eCommerce transactions. Amend the national legal framework that should assure equal treatment between paper and electronic invoices. Define national technical standards by promoting the development of interoperable e-invoicing solutions based on common with the EU standards, paying particular attention to the needs of small and medium-sized enterprises. Define a single and clear semantic data model and a common eInvoicing format compatible with the EU best practices to facilitate semantic interoperability, ensure technology neutrality and facilitate the uptake of e-invoicing for eCommerce transactions for SMEs.

eLogistics

Equal validity of electronic and offline contract - Extend possibilities of cross-border trade by facilitating conclusion of contracts. Amended the national legislation to assure the same validity of the contracts concluded by electronic means and contracts concluded offline by "traditional" means and not only in case of eCommerce sales as it is now in the law on eCommerce. The principle should be extended for other types of activities, such as provision of distance services. This should apply to all stages and acts of the contractual process, such as the contractual offer, the negotiation and the conclusion of the contract by electronic means. Legal provisions obliging hand-written contracts should be no longer allowed.

Conditions for the risk of loss of or damage to the goods - Reassure consumers and increase the attractiveness of cross-border eCommerce services. Amend legislation to define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. Stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

2.4.7 Belarus

In 2014, there were about 3,000 on-line shops in Belarus that are responsible for 1.5% (or approx. USD 430m) total retail turnover. Belarus' eCommerce is assumed to reach USD 500m by the end of 2014. About a million users in Belarus make on-line purchases. 65% of Belarusian internet users have never made online purchases. Average on-line purchase costs are USD 290.00 approximately. 60% of the customers paid for their orders in cash against delivery. About 12% of the buyers used their bank cards on site, 8% paid by bank transfer, 7% paid by "client-bank" system, 4% used e-money, and only 3% paid by bank cards against delivery.

State of play and gap analysis

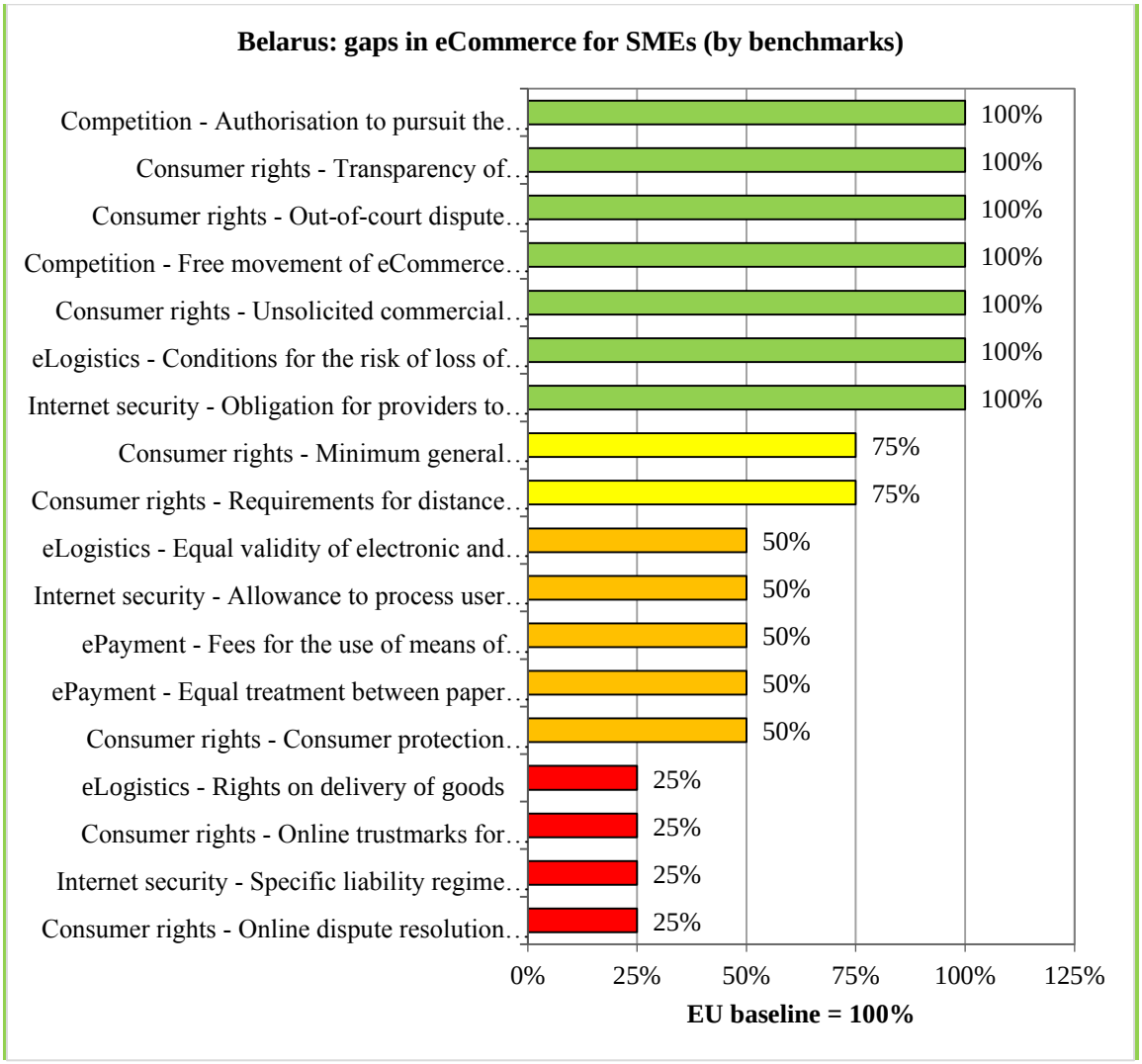

Exhibit 39- Belarus: state of play and gap analysis in eCommerce

Internet security and privacy

The regulation of the Department of Commerce regulates that within 2 years from the date of sale of goods, information about the act of sale have to be kept by the seller. The national legislation does not explicitly define the rules of processing of user traffic data by the provider of an electronic communication service. The types of allowed data to be stored by service providers do not include any kind of traffic data.

Liability of the communication service providers is regulated by the basics of security regulations that are given in the Law No.455-P "On information, informatisation and information security" and the Resolution No.1055 of the Council of Ministers dated August 17, 2006 "On Approval of the procedures for rendering electronic communications services" in 2012. There are no clearly defined specific liability regimes for three categories of essential intermediary services assuring the provision of eCommerce online services - transmission conduit operators, caching providers and hosting services providers.

The national legislation does not explicitly include requirements and conditions on providers of eCommerce and other information services of transmission, caching and hosting, to monitor the information that they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. The services providers have to give access to the information collected to the competent government bodies in order to detect any illegal activity. Therefore, the legislation of the Republic of Belarus is generally compliant with the EU baseline (Directive 2000/31/EC on electronic commerce Article 15).

Consumer rights

Regulatory bodies have worked through the issue of introducing a voluntary certification for activities of eCommerce that require endowing one of the governmental bodies with such a function. The country has not yet established a country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers.

In case of trade carried out without or outside of a retail facility (distance trade)[26], the trader is

[26] Resolution No. 31 of the Council of Ministers of the Republic of Belarus of 15 January 2009 "On the Rules of selling goods in retail trade by sample"

obliged to bring to the consumer's knowledge the defined scope of information. The national legislation imposes the obligation on the information service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities the defined scope of information about the service provider that is compliant with the EU best practices. The legislation of Belarus does not impose a requirement to establish an effective direct communication channel with its customers (Article 5 (Directive 2000/31/EC on electronic commerce). This information is important and may even be vital for customers claiming their rights.

The Law No. 225-327 "On advertisement" defines commercial communications information to be provided by advertisements. Requirements of this clause do not apply to the advertisement distributed through the Internet that contains a link where the mentioned above information is published. The legislation also imposes a number of requirements about conditions attached to the offers advertised online. However, the legislation does not state the requirements for advertising originating from the operator of an online marketplace and displayed by a search operator. Directive 2000/31/EC on electronic commerce Article 6 recommends that this type of advertising must always disclose both the identity of the online marketplace operator and the fact that the trademarked goods advertised are being sold through that online marketplace.

For a distance contract, the national legislation requires that the trader provides the consumer with comprehensive and legally defined pre-contractual information. Information about the complaints and claims policy, information about after-sale service, and consideration period do not qualify by the law as required to be provided before the contract conclusion. Directive 2011/83/EC on Consumer Rights also asks the trader provides the consumer with the information required about obligation to pay and delivery restrictions applied and which means of payment are accepted. It appears that these two conditions are not explicitly reflected in the legislation of Belarus.

A consumer protection cooperation agreement is set up with the CIS, but not with EU Member States. Within the CIS, a national authority in a country where consumer interests are harmed can call on their counterpart in the country where the trader is located and ask for action to stop the infringement.

[27] Law No. 225-3 of the Republic of Belarus of 10 May 2007 "On advertisement"

National legislation clearly defines the mechanisms of dispute settlement in case of disagreement between a provider and a recipient of the services. In the area of eCommerce they are determined by the Resolution No. 31 "On the rules of trade by samples"[28] for a case when the trader receives a prepayment for the goods or the delivery of services. There is a graded system of dispute settlement with indication of the consumer rights for exaction of a fine at certain steps of such dispute settlement. Mechanisms of dispute resolution between consumers and electronic services providers are defined by the Resolution No. 1055 "On the rules of rendering electronic services"[29].

According to Law No. 300-3 "On public and legal entities appeals"[30], citizens, legal entities and individual businessmen have a right to appeal to organisations by submitting electronic applications as well (art. 3). However, there is no online dispute resolution platform through which parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions.

The Law No. 225-3 "On advertisements" protects the right of consumer to unsubscribe from advertisement delivered by any means, but the technical realisation of un-subscription from the unsolicited commercial communications is left to advertiser. The current legal framework of Belarus allows the sending of unsolicited commercial communications by e-mail. It defines the requirements applied to information service providers and describes the rights of consumers. The requirements ensure that such communication is clearly and unambiguously identifiable, and that service providers respect the opt-out registration.

Competition

In compliance with the Directive 2000/31/EC on electronic commerce Article 3, the country's legislation does not restrict the freedom to provide eCommerce services by a lawful service provider established in another country. For cloud services provided to legal, natural entities and

[28] Resolution No. 31 of the Council of Ministers of the Republic of Belarus of 15 January 2009 "On the rules of trade by samples"

[29] Resolution No. 1055 of the Council of Ministers of the Republic of Belarus of 17 August 2006 "On the rules of rendering electronic services"

[30] Law No. 300-3 of the Republic of Belarus of 18.07.2011 "On public and legal entities appeals"

government organisations, the legislation imposes some requirements regarding place of storage of some type of data.

In relation to possible eCommerce applications, Decree No. 450 of the President “On Licensing of Certain Activities” regulates that the several electronic communications services of general use are subject to licensing. Resolution No. 649 “On Registration of Online Shops in the Trade Register” stipulates that from 1 July 2010 legal bodies and individual entrepreneurs perform their retail trade activities via online shops registered in the Trade Register of the Republic of Belarus. Information confirming the registration of an online shop in the Trade Register of the Republic of Belarus is submitted to a licensing authority. In general, the legislation of Belarus is compliant with the Directive 2000/31/EC on electronic commerce Article 4 which defines the principle excluding prior authorisation to pursuit the activity of an information society service provider, excluding for activities covered by other legislations.

ePayment

The explicit regulations on the fees for the use of certain means of payment (such as credit or debit cards, electronic valets) that prohibit traders from charging consumers excessive fees in respect of the use of a given means of payment could not have been found within this study. The legal framework of Belarus in the area of eCommerce payments is well defined. However, the rules on the fees for the use of means of payment are not explicitly stated.

Resolution No. 202 of 7 March 2014 defines the rules on creation of shipping and commercial invoices as electronic documents, as well as providing information about them[31]. Consignments and invoices as electronic documents (electronic invoices) are considered established if they are signed by a digital signature of participants. The national legislation assures equal treatment between paper and electronic invoices. There is no single national semantic data model and a common eInvoicing format facilitating interoperability and ensuring technology neutrality to facilitate the uptake of eInvoicing for eCommerce transactions for SMEs.

[31] Resolution No. 202 of the Council of Ministers of the Republic of Belarus of 7 March 2014 "On creation of shipping and commercial invoices as electronic documents, as well as providing information about them and making additions to the resolution of the Council of Ministers dated October 31, 2001 № 1585 and February 17, 2012 № 156 "

eLogistics

In compliance with the Directive 2000/31/EC on electronic commerce Articles 9-11 defining the fundamental principles of equal validity of electronic contracting and contract concluded offline, the national legislation establishes the equal validity of electronic contracting and contract concluded offline. Electronic signature is the only eligible means to electronic document validity. The online trader is not requested by legislation to provide the consumer with the technical means allowing identifying and correcting input errors prior to the placing of the order. Also, the legislation does not define the full scope of specific requirements to electronic contract.

Law No. 90-3 "On Protection of the Rights of Consumers"[32] defines the conditions for losses incurred by the consumer that shall be reimbursed in full above the penalty established by the law or contract. In addition, the Law provides for reimbursement of the damage caused in the result of defects of the goods (works, services) and compensation for emotional damage. The national legislation is compliant with the Directive 2011/83/EC on Consumer Rights. However, the legislation does not explicitly specify the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved.

Terms for delivery of goods are not stipulated by law on a special basis but are rather defined by contract. The seller must inform the buyer of delivery terms by providing such information via the website. The services provision period is regulated only by trade rules for domestic services. In case the seller violates the terms for transfer of pre-paid goods, the Law No. 90-3 "On Protection of the Rights of Consumers" defines the requirements. However, the legislation does not specify the time of delivery when the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay.

HDM roadmap

Internet security and privacy

Allowance to process user traffic data by the provider of an electronic communication service - assure to users their rights to manage online privacy. Amend the national legislation by explicit provisions about the processing of user traffic data. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a service

[32] Law No. 90-3 of the Republic of Belarus of 9 January 2002 "On Protection of the Rights of Consumers"

may need to process the data to the extent and for the duration necessary for such services or marketing. This should be conditioned by the requirement for the subscriber or user to whom the data relate to give his/her consent. Users or subscribers should be given the possibility to withdraw their consent for the processing of traffic data. This allowance can also concern processing of traffic data necessary for the purposes of subscriber billing and interconnection payments. The legislation should indicate if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

Specific liability regime for intermediary service providers - increase the transparency of rules for provision of cross border eCommerce services by SMEs. Amend the legislation by defining the specific liability regime for three categories of essential services assuring the provision of eCommerce online services. These are the conditions for mere conduit operators (transmission in a communication network), caching providers (temporary storage of information) and hosting services.

Consumer rights

Online trustmarks for retail websites - Reassure consumers on the reliability of accredited online service providers, especially across borders. For the development of eCommerce, there is a definitive usefulness and benefits of the country-wide trustmark schemes that help to reassure consumers on the reliability of accredited online traders and service providers. The next step would be harmonisation of national trustmarks schemes with EU Member States. Article 23 of the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) prescribes by 1 July 2015 to provide specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Cooperate with the Region for development of self-regulation and eCommerce positioning.

Minimum general information to be provided by information society service provider. Reinforce the legislation by an additional requirement to the service providers to indicate their electronic e-mail address. In accordance with the Article 5 (Directive 2000/31/EC on electronic commerce), it is required from the online service provider to establish an effective direct communication channel with its customers. It imposes the obligation on the service provider to render easily, directly and permanently accessible to both recipients of services and the competent authorities, the details of the service provider, including its electronic e-mail address, which allow it to be

contacted rapidly and communicated with in a direct and effective manner.

Consumer protection international cooperation mechanisms - Create a mechanism for international user protection between the Region and the EU. Belarus should study possibilities to cooperate with the Consumer Protection Cooperation (CPC) Network that brings together the public authorities in all the EU Member States (and other EEA countries) who are responsible for the enforcement of EU consumer protection laws. It also can make feasibility studies for development of a national segment of an information system for collection, storage and exchange of information on consumer protection infringements. This system could be later exchange information with the CPC-System, the common IT-tool used by the authorities of the EEA countries. It is an electronic database maintained by the European Commission and designed to provide a secure system for the exchange of information between competent authorities for the performance of their mutual assistance obligation under the Consumer Protection Cooperation Regulation.

Online dispute resolution system for consumers for eCommerce transactions - Provide reassurance to service providers and consumers, and build trust in eCommerce transactions. Set up of an online dispute resolution platform (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions. Through this website, parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions without going through traditional court legal procedures that are time and resources consuming. National entities responsible for settling alternative disputes receive the complaint electronically through the online platform and seek to resolve the dispute through existing legal alternative dispute resolution mechanisms.

ePayment

Legal framework in the area of eCommerce payments and rules on the fees for the use of means of payment - Make payments online more attractive to consumers and increase the competitiveness of SMEs. Define the rules on the fees for the use of certain means of payment and prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean.

Equal treatment between paper and electronic invoices - Reduce costs and delays of international eCommerce transactions. Implement mechanisms for mutual recognition of electronic digital signatures between countries, both within the EEU and the EU. Provide natural

and legal persons with simpler tools for conclusion of electronic contracts with smaller amounts than required for EDS, which nowadays is owned by few natural persons, because it is too expensive and difficult to acquire it for one-time transactions. These tools should be prescribed by the legislation, which would give them legal force and make them mandatory for acceptance by tax authorities. Develop a common national semantic data model for eInvoicing. Develop national standards for filling in electronic forms. Ensure legal certainty and promote the development of interoperable eInvoicing solutions based on international standards and mutual recognition of eInvoices between Belarus and the EU Member States.

eLogistics

Equal validity of electronic and offline contracts - Extend possibilities of cross-border trade by facilitating conclusion of contracts. Amend the legislation with requires that online traders provide the consumer with specific information prior to the order being placed. This should include information on steps to follow to conclude an electronic contract, the filing of the contract by the service provider, the technical means for identifying and correcting input errors prior to the placing of the order, the languages offered for the conclusion of the contract, availability of any relevant codes of conduct. Amend the legislation with requirements regarding placing of orders for electronic contracts. The online contract has to be concluded through an "order" placed by the consumer, followed by an electronic "acknowledgment" of the online trader without undue delay. The "order" and the "acknowledgement" are deemed to be received when the involved contracting parties are able to access them. Trader also has to provide the consumer with the technical means allowing him/her to identify and correct input errors prior to the placing of the order.

Rights on delivery of goods - Assure the conditions for the physical delivery of goods. The legislation should define the time of delivery when the trader shall deliver the goods (a defined maximum number of days from the conclusion of the contract) by transferring the physical possession or control of the goods to the consumer. Clearly define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

2.4.8 Georgia

State of play and gap analysis

Although Georgia is ranked 9th (of 185 countries) in the World Bank's ease-of doing business survey, there is potential and opportunity to reduce costs of doing business in the country through smarter government-to-business interaction. This potential is also stressed by the 2012 UN e-Government Survey and the country's online service availability score (i.e. supply). Still the level of e-Services use (i.e. demand and take-up) remains relatively low.

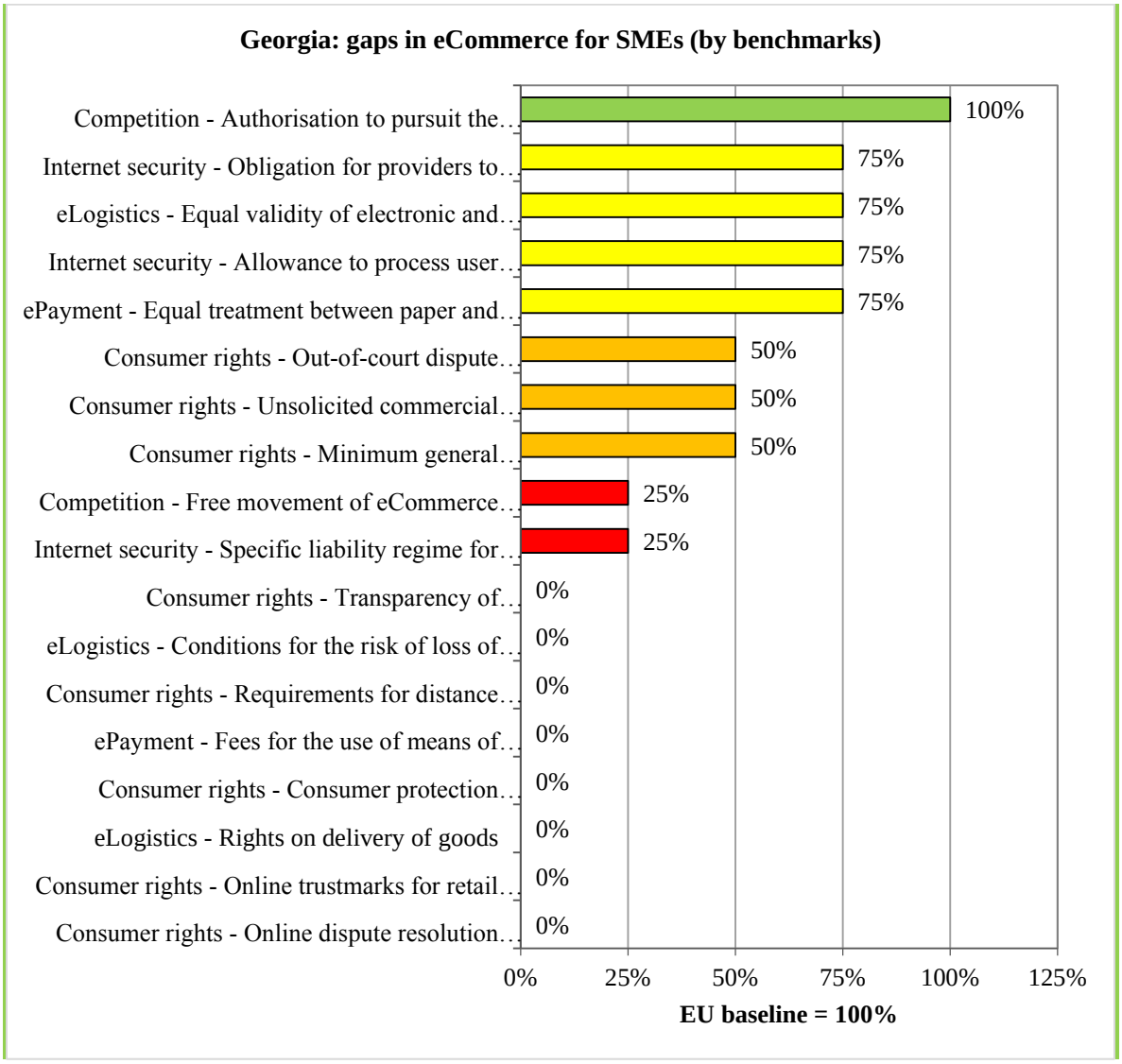

Exhibit 40- Georgia: state of play and gap analysis in eCommerce

Internet security and privacy

The Law on Protection of Personal Data prohibits retention of user specific personal data. Implementation of the law is monitored by the Personal Data Protection Inspector's office. Decree of Georgian National Communications Commission of March 16, 2006 on protection of consumers' rights in the field of electronic communications obliges communication service providers to retain data for certain period for billing and interconnection purposes. Such data shall be possessed by an operator for the period defined by the Georgian National Communications Commission. Retention of any data beyond time and purpose limits, including metadata is prohibited. Being precise on personal data, the national legislation does not explicitly define the rules of processing of user traffic data by providers of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

The current legal framework[33] does not define categories of online services and therefore any graded system of responsibilities. The national legislation does not define specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

National Legislation does not specify any obligation of information service providers to monitor transmitted information. The only obligation set in the consumer's rights protection decree by GNCC puts an obligation to the providers of hosting and registrars on the provisioning of legal content i.e. the provider of such services shall monitor the content and take it down in case it violates the law incl. Copyrights[34]. This general regulation on hosting and web-service providers to monitor legality of the content placed has not been yet applied and is considered to be amended.

Consumer rights

The country has not established any country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of

[33] Law on Protection of Personal Data; Statute on the Activities of and Procedure for Discharge of Powers by the Personal Data Protection Inspector; Decree of Georgian National Communications Commission of March 16, 2006 on protection of consumers right in the field of electronic communications

[34] One of ISPs, namely Silknet, has appealed to GNCC to rule against competitors placing illegal content (movies and other media) on the sites hosted and registered by competitors

qualified eCommerce service providers.

The national legislation related to advertisements on the Internet is not in place. There is no explicit requirement that advertisements on the Internet should indicate natural or legal person responsible for commercial communication and any conditions attached to the offers. It does not define explicit requirements to assure the transparency of commercial communications information to be provided.

For distance contracts (concluded online or by electronic means) or off-premises contracts, the national legislation does not require that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms.

The country has not established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce. The Association Agreement with the EU contains the set of eCommerce issues, including international cooperation issues.

The national legislation does not explicitly allow the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services (except for telecommunications), including by appropriate electronic means. This area can be however covered by the general regulations on arbitration. Georgia does not have an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.

The Personal Data Protection law gives a general definition that any provider – sender of commercial – marketing information message shall also provide means to unsubscribe from such notifications. Such regulation has only been implemented in case of SMS marketing services. The regulation shall further be extended to eCommerce area. The law defines overall requirement, but the national regulations do not define the requirements applied to sending of unsolicited commercial communications by e-mail.

Competition

The national legislation does not explicitly restrict the freedom to provide eCommerce services compliant to the national laws by a lawful service provider established in another country. However, for the entities providing service on the territory of Georgia an authorization is required. Regulations about eCommerce activities are not in place.

There is no legislation on eCommerce services. Any explicit requirements for a prior authorisation to pursuit the activity of eCommerce service provider are not stipulated.

ePayment

The national legislation does not define the requirements for eCommerce payments and does not define the rules on the fees for the use of means of electronic payment.

eInvoicing in common data format has been introduced by the Revenue Service of the Ministry of Finance[35] in 2010. It has a common format and has equal treatment to paper invoices. Georgia has developed and implemented an entire public finance management information structure, which is shared between different government entities. eInvoicing is active part of this system has been established from 2010 and is fully implemented both in public and private sectors. The national legislation assures equal treatment between paper and electronic invoices and defines the framework of a common national data model of e-invoicing format.

eLogistics

The law on electronic signatures and electronic documents specifies the equal validity of electronic and offline contracts. Planned amendments will bring current law into full compliance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The national regulations do not define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved, and does not define the requirements for time of delivery of goods purchased through eCommerce transaction.

HDM roadmap

Internet security and privacy

Allowance to process user traffic data - Assure to users their rights to manage online privacy. Amend the national legislation with the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications

[35] www.rs.ge

services or for the provision of value added services. The legislation should indicate if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

Specific liability regime for intermediary service providers - Increase the transparency of rules for provision of cross border eCommerce services by SMEs. Amend the national legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers. The legislation should be amended to define the degree of liability of the service provider for the information transmitted in a communication network of information provided by a recipient of the service. The liability of service provider should be defined for the automatic, intermediate and temporary storage of that information, performed for making more efficient the information's onward transmission to other recipients of the service upon their request. Liability of the hosting service providers should be defined for the information stored at the request of a recipient of the service, with some clearly defined liability exceptions (does not have actual knowledge of illegal activity or information, and others).

Consumer rights

Online trustmarks for retail websites - Reassure consumers on the reliability of accredited online service providers, especially across borders. Establish country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers. Encourage the establishment of price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services. Harmonise the development of the national trustmarks schemes with EU Member States. The Commission is in process to elaborate different policy options for EU-wide trust mark schemes and the effectiveness of cooperation platforms in the governance of such trust mark systems.

Transparency of commercial communications information to be provided - Assure transparency of commercial communications. Amend the legislation by requirements that advertisements on the Internet indicates natural or legal person responsible for commercial communication and any conditions attached to the offers.

Minimum pre-contractual information required for distance contracts. Assess the compliance of the current legal requirements for minimum pre-contractual information required for distance

contracts and off-premises contracts. Amend the legislation with requirements for the trader to provide the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms.

Consumer protection international cooperation mechanisms - Create a mechanism for international user protection between the Region and the EU. Establish consumer protection cooperation with the public authorities in the Region and the EU who are responsible for the enforcement of consumer protection laws, in priority, with neighbouring countries, countries with main trading volumes, EU Member States. Conduct feasibility studies for development of a national segment of an information system for collection, storage and exchange of information on consumer protection infringements.

Possibility for out-of-court dispute settlement - Facilitate dispute resolution for cross-border purchases. Amend the national legislation allowing the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

Online dispute resolution system for consumers for eCommerce transactions - Provide reassurance to service providers and consumers, and build trust in eCommerce transactions. Develop an online dispute resolution service (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions. Through this service, parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions without going through traditional court legal procedures that are time and resources consuming. National entities responsible for settling alternative disputes receive the complaint electronically through the online platform, process and seek to resolve the dispute through existing legal alternative dispute resolution mechanisms.

Requirements for sending of unsolicited commercial communication (spam) - Improve the effectiveness of promotion of products and services assuring consumer rights. Develop the relative regulations by defining requirements applied to unsolicited commercial communication send by e-mail. It must notably ensure that such communication is clearly and unambiguously identifiable.

ePayment

Legal framework in the area of eCommerce payments and rules on the fees for the use of

means of payment - Make payments online more attractive to consumers and increase the competitiveness of SMEs. Develop the regulations on the fees for the use of certain means of payment and prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean.

eLogistics

Conditions for the risk of loss of or damage to the goods - Reassure consumers and increase the attractiveness of cross-border eCommerce services. Amend legislation to define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. Stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

Rights on delivery of goods - Assure the conditions for the physical delivery of goods. Amend the legislation to define the time of delivery when the trader shall deliver the goods (a defined maximum number of days from the conclusion of the contract) by transferring the physical possession or control of the goods to the consumer. Define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

2.4.9 Moldova

State of play and gap analysis

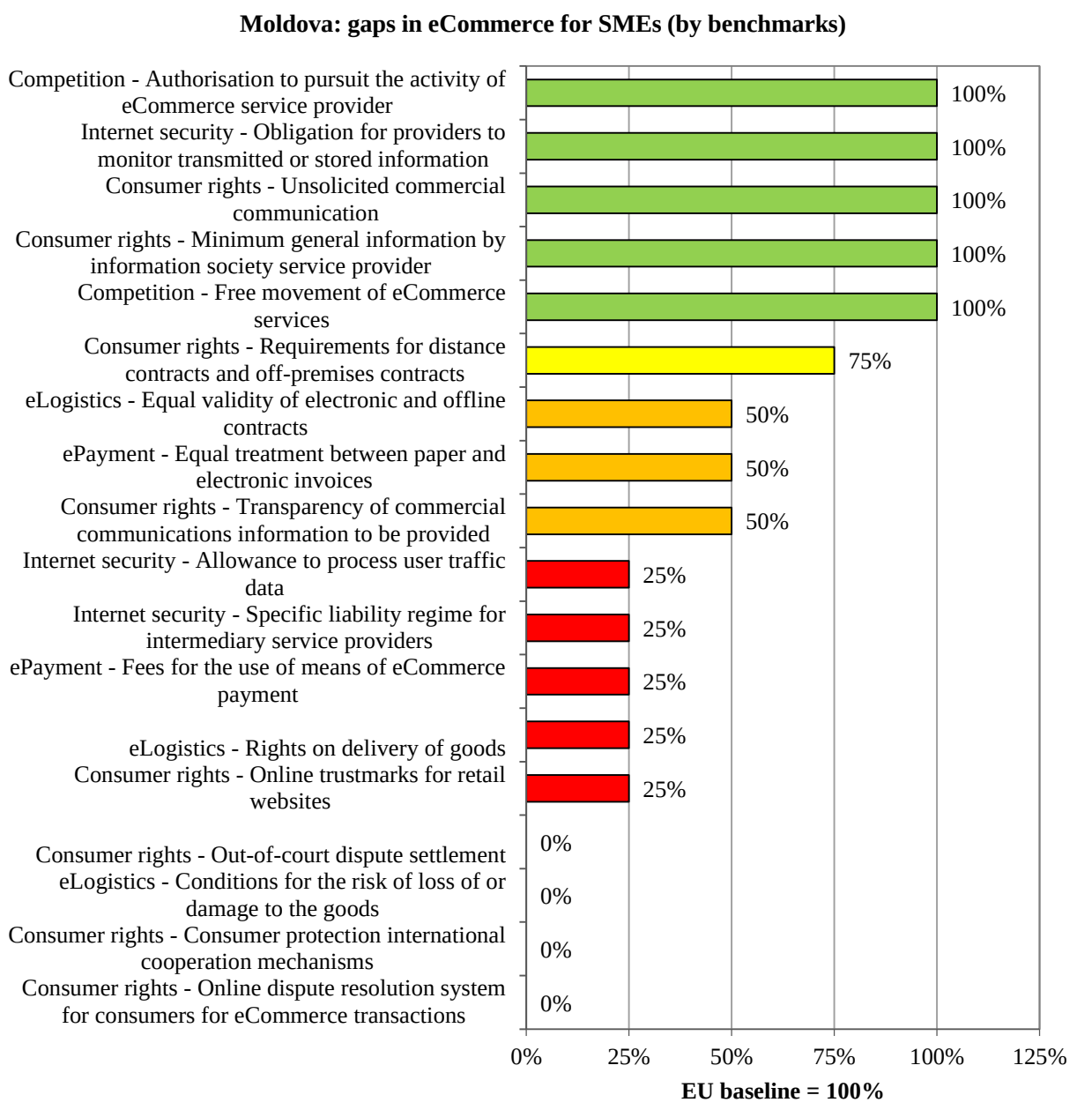

Exhibit 41- Moldova: state of play and gap analysis in eCommerce

Internet security and privacy

The national legislation (neither the Law “On electronic communications” nor the “On electronic

commerce") does not explicitly define the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services. The Action Plan for the implementation of the Association Agreement between the European Union and the Republic of Moldova stipulates that the provisions of the Directive 2002/58/EC will be implemented by June 16, 2017.

The current national legislation (Law No.241 "On electronic communications") does not define the overall degree of liability of the eCommerce intermediary service providers for the information transmitted in a communication network of information provided by a recipient of the service. It does not explicitly define specific liability regimes for three categories of online service providers. The approximation of the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce will be conducted by June 2017.

Intermediary service providers in eCommerce are not required to monitor and verify the accuracy of the transmitted, received and stored electronic documents and e-mails, as well as their compliance with the law, unless otherwise provided by the contract concluded with the participants of eCommerce, or the law (Art 12, Law No.284 of 22.07.2004 "On electronic commerce"). This is in accordance with the Directive 2000/31/EC on electronic commerce Article 15.

Consumer rights

The country has not established country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers. Currently, some eCommerce websites established on the territory of the Republic of Moldova use online seals and SSL protection provided by foreign providers. The Certification Authority (Special Telecommunications Centre, a Public Key Certification Authority) is delegated to issue SSL certificates from Unizeto and Symantec that are recognised by the most of browsers and insure high level of security[36].

eCommerce service providers are obliged to provide to other subjects of eCommerce interaction, as well as to state control bodies, appropriate access to reliable information about themselves in

[36] https://pki.cts.md/en/services/servers-certificates.html

electronic form in the Moldovan language, and if necessary, in other languages (Law No.284 of 22.07.2004 “On electronic commerce”, Art 11).

The Law N1227 “On advertisement” does not specify any requirements to the advertisement on the Internet. The Law No.284 of 22.07.2004 “On electronic commerce” Art 11(2) defines requirements for outgoing advertisement from the eCommerce service provider about clear information about goods, works or services, prices and tariffs and their conditions of sale, execution or provision. The requirements emphasising the need for transparency when advertisements are displayed on the Internet are generally provisioned in the legislation. However, the legislation is not explicit about the specific requirements to the different types of commercial communications on the Internet such as promotional offers, premiums, promotional competitions or games.

The Law No.284 of 22.07.2004 “On electronic commerce” chapter IV defines the general requirements applied to distance contract and minimum of legally defined pre-contractual information. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the law indicates that the trader shall be required to make the consumer aware in a clear and prominent manner, and directly before the consumer places his order. These requirements are compliant with the provisions of the Directive 2011/83/EC on Consumer Rights. Directive 2000/31/EC will be approximated by 2016.

The country has not yet established any international cooperation mechanisms between the national public authorities and the authorities of other countries that are responsible for enforcement of consumer protection laws, including the legal framework on eCommerce.

The country’s legislation does not define the mechanisms of dispute resolution, in the event of disagreement between an information society service provider and the recipient of the service (Law N241 “On electronic communication”, law No.284 of 22.07.2004 “On electronic commerce”). The legislation does not include prerequisites for the use of out-of-court schemes for dispute settlement. Directive 2000/31/EC will be approximated by June 2016. The country has not yet deployed an online dispute resolution platform through which parties can initiate alternative dispute resolution in relation to disputes concerning online transactions.

The national legislation clearly defines the requirements applied to sending of unsolicited commercial communications by e-mail. Sending commercial messages by e-mail (unsolicited commercial communication) is prohibited, except in cases where the recipient previously agreed

to receive such communications (Law N284 “On electronic commerce” Art 17). Any person has the right to opt out of receiving commercial messages. This ensure that communication is clearly and unambiguously identifiable, legal or natural person sending unsolicited commercial communication is clearly indicated, conditions of promotions and discounts are described.

Competition

The subjects of eCommerce can be physical and legal entities, including foreign ones, regardless of the type of ownership and organisational - legal form, as well as the state as a legal entity. Participation in e-commerce, unless otherwise provided by contract or by law, cannot serve as a basis for establishing additional requirements, procedures or restrictions on entrepreneurial activity (Law N284 “On electronic commerce” Art 7). By this, the country’s legislation does not restrict the freedom to provide eCommerce services by a provider from another country.

The right to carry out eCommerce activities arises from the date of state registration of the legal entity or individual entrepreneur, except in cases provided by the Law on regulation of entrepreneurial activity by licensing. If the items for sale, works or services must obtain a license or permit, eCommerce can be carried out after obtaining a license or authorisation to engage in the relevant activity (Law N284 “On electronic commerce” Art 9). The legal framework of the country ensure that the taking up and pursuit of the activity of an information society service provider, including eCommerce activities, may not be made subject to prior authorisation or any other requirement having equivalent effect. The legislation restricts starting of eCommerce activities by a condition of getting prior authorisation in some particular sectors or for some products. This complies with the Directive 2000/31/EC on electronic commerce Article 4.

ePayment

The national legislation does not define the requirements for eCommerce payments, the rules on the fees for the use of means of electronic payment. Directive 2000/31/EC will be approximated by June 2017.

The national legal framework stipulates that the handwritten signature is equivalent with the electronic one. However, there is no mechanism in place to verify that the invoice was signed by authorised person. The legal framework requires on certain occasions to apply the stamp, even if documents are signed electronically they have to be printed put and stamped. Infrastructure is

required to be implemented. The secondary acts (including the technical provisions) to implement the Law no.91 of 29.05.2014 on eSignature and eDocument will be elaborated and adopted in 2015. It is not clear who has the mandate to monitor and verify application of the electronic signature. Launched on February 11, 2014, the eInvoice service[37] represents a software solution designed for the economic agents from Moldova in terms of bills and invoices' development and electronic circulation. For eInvoice service, the user must be in possession of a digital (mobile) signature issued by an accredited certification centre. There is no defined framework of a common national data model of eInvoicing format.

eLogistics

The legal force of an electronic contract is equivalent to a contract drawn up in writing and signed by the parties, including those certified by the seal of the parties. An electronic contract has the probative value equivalent to a written contract. The legislation explicitly describes the cases when a contract cannot be signed in electronic format. Also, the provisions indicates requirements which are compulsory to include in electronic contract activity (Law N284 "On electronic commerce" Art 20). Nevertheless, the provisions of this legislative act are planned to be revised. There are at least three centres in the country, which offer the electronic signature, so most of the persons have to use at least three different types of electronic signatures depending of the document that is signed. The legal framework requires application of a timestamp and it needs to be revised. Currently, it is not possible to submit contracts concluded online to some authorities. Mechanisms to verify transactions also need to be revised, as it is not duly finalised.

The national legislation does not define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the parties involved. The missing provisions also concern the standardisation of the remedies available to consumers for damaged or faulty goods. Consumers should be entitled to replacement or repair in the first instance and a refund or discount only where specific circumstances apply.

The current legislation only stipulates that electronic contract must contain the following prerequisites: conditions of declining the transaction, the procedure and terms of performance

[37] http://egov.md/index.php/en/for-business/e-invoice#.VRE4lTSsVQc

(Law N284 “On electronic commerce” Art 20). The legislation does not define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract. The national legislation does not define the requirements for time of delivery of goods purchased through eCommerce transactions and should be aligned with Directive 2011/83/EC on Consumer Rights.

HDM roadmap

The following sections present the aspects where progress on HDM can be made, the objectives and individual follow-up actions of the country for harmonisation in the priority area:

Internet security and privacy

Allowance to process user traffic data - Assure to users their rights to manage online privacy. Amend the national legislation with the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

Specific liability regime for intermediary service providers - Increase the transparency of rules for provision of cross border eCommerce services by SMEs. Amend the national legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers.

Consumer rights

Online trustmarks for retail websites. Align the legislation with the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions. Establish country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers. The next step would be harmonisation of national trustmarks schemes with EU Member States. The Commission is in process to elaborate different policy options for EU-wide trustmark schemes and the effectiveness of cooperation platforms in the governance of such trustmark systems.

Transparency of commercial communications information to be provided. Amend the legislation with the requirements emphasising the need for transparency when advertisements are displayed on the Internet for the types of the online commercial communications such as promotional offers, discounts, premiums, promotional competitions or games.

Minimum pre-contractual information required for distance contracts. Assess the compliance of the current legal requirements for minimum pre-contractual information required for distance contracts and off-premises contracts on: 1) delivery restrictions applied, and 2) which means of payment are accepted

Consumer protection international cooperation mechanisms - create a mechanism for international user protection between the Region and the EU. Establish consumer protection cooperation with the public authorities in different countries who are responsible for the enforcement of consumer protection laws, in priority, with neighbouring countries, countries with main trading volumes, EU Member States. Especially for consumer protection in eCommerce field, the authorities can establish an information system for efficient exchange of information between competent authorities of different countries for action to stop infringements.

Possibility for out-of-court dispute settlement - facilitate dispute resolution for cross-border purchases. Amend the national legislation allowing the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

Online dispute resolution system for consumers for eCommerce transactions - provide reassurance to service providers and consumers, and build trust in eCommerce transactions. Set up an online dispute resolution platform (an interactive website free of charge) facilitates and speeds up resolution of disputes related to eCommerce transactions. Through this website, parties can initiate alternative dispute resolution procedure in relation to disputes concerning online transactions without going through traditional court legal procedures that are time and resources consuming. National entities responsible for settling alternative disputes receive the complaint electronically through the online platform and seek to resolve the dispute through existing legal alternative dispute resolution mechanisms.

ePayment

Legal framework in the area of eCommerce payments and rules on the fees for the use of means of payment - make payments online more attractive to consumers and increase the competitiveness of SMEs. A comprehensive national legislation for eCommerce payments by credit or debit card, on Internet, on phone, using mobile and other electronic payments will present a substantial benefit for eCommerce development and market integration in this field with the EU. Amend the legislation by including the rules on the fees for the use of certain

means of payment (e.g. online, mobile, credit or debit cards, electronic valets) and prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean.

Equal treatment between paper and electronic invoices - reduce costs and delays of international eCommerce transactions. Define national technical standards by promoting the development of interoperable e-invoicing solutions based on common with the EU standards, paying particular attention to the needs of small and medium-sized enterprises. Define a single and clear semantic data model and a common eInvoicing format compatible with the EU best practices to facilitate semantic interoperability, ensure technology neutrality, facilitate the uptake of e-invoicing for eCommerce transactions for SMEs.

Equal validity of electronic and offline contracts -extend possibilities of cross-border trade by facilitating conclusion of contracts. The legal framework requires application of timestamp and it needs to be revised in order to enforce its implementation. Currently, it is not possible to submit contracts concluded online to some authorities (for example, the fiscal inspectorate requires stamped and signed documents).

Conditions for the risk of loss of or damage to the goods - reassure consumers and increase the attractiveness of cross-border eCommerce services. Amend legislation to define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a third party indicated by the consumer, or the carrier. Stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

Rights on delivery of goods - ensure the conditions for the physical delivery of goods. Amend the legislation to define the time of delivery when the trader shall deliver the goods (a defined maximum number of days from the conclusion of the contract) by transferring the physical possession or control of the goods to the consumer. Define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

2.4.10 Ukraine

eCommerce is one of the top fastest growing economic sectors in the country. There are at least 7,000 online stores. The top 300 of them control 80% of the market. Only platform prom.ua hosts eShops of 481,771 companies with the total catalogue of 21,950,835 products and services. The average annual turnover of the country in eCommerce increases by 45% per year.

State of play and gap analysis

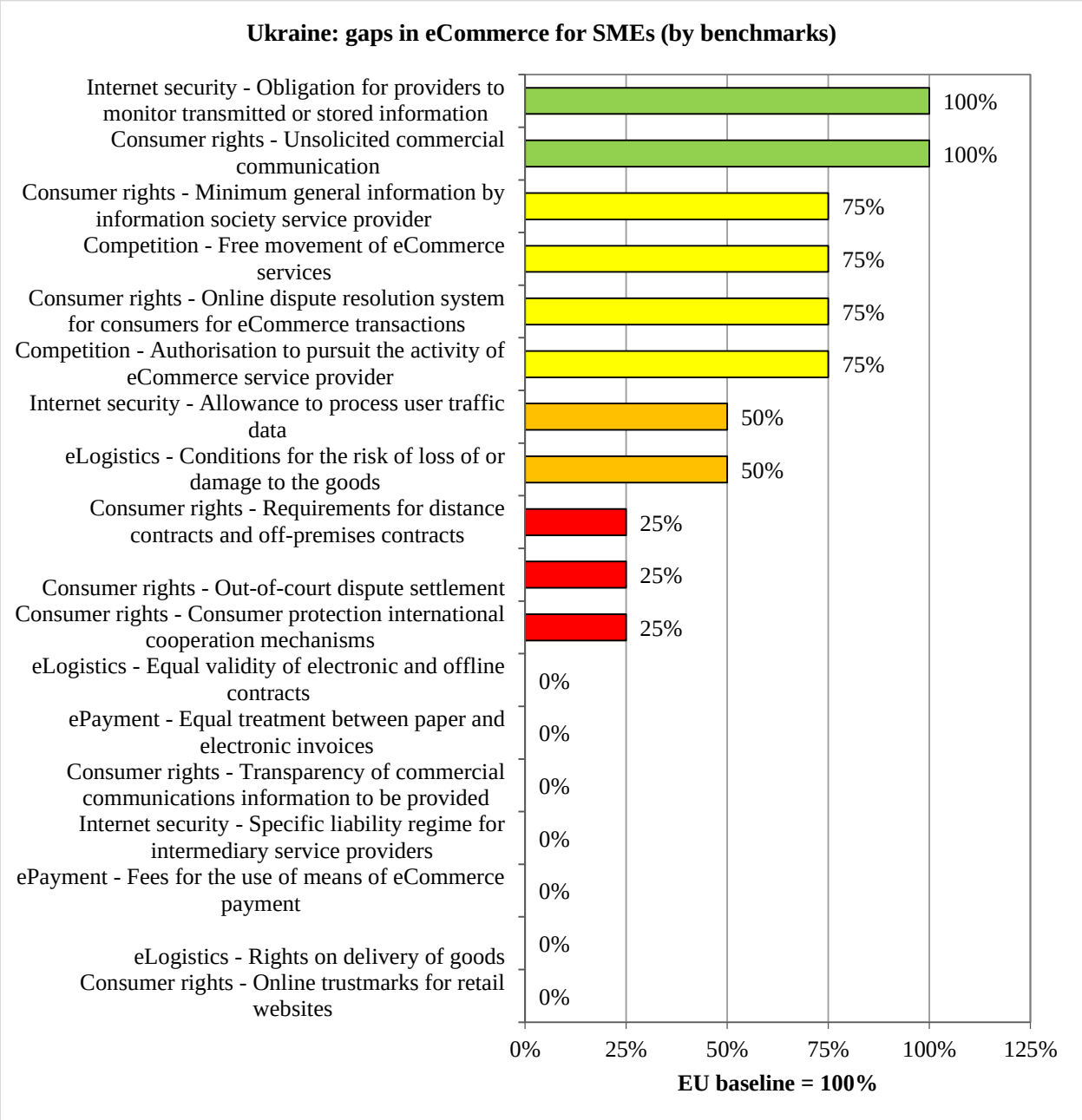

Exhibit 42- Ukraine: state of play and gap analysis in eCommerce

Internet security and privacy

The Law "On Personal Data Protection" regulates legal relations related to the protection and processing of personal data, including the right to privacy in connection with the processing of personal data. According to the Law, the subscriber gives their perpetual consent for processing of their personal data. This is confirmed by the subscriber in their agreement, as well consignment about transfer of information from a special database containing personal data to third parties in accordance with applicable law. The national legislation defines the general principles of data protection, but it does not explicitly define the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services.

The current national legislation does not provide the specific liability regime for transmission conduit operators, caching providers and hosting services providers. Ukraine's Parliament will consider in the second reading the draft law "On Electronic Commerce". The draft law describes the basic principles of the market regulation, the rights and obligations of the online vendors and their customers, differentiates responsibilities of good's sellers, service providers of intermediate character such as internet access, hosting, and domain name registrars.

The Security Service of Ukraine (SSU) has the right to monitor transmitted or stored information. All providers and operators are required to provide lawful interception and link up to the SSU's systems. The national legislation defines the requirements on information services providers to monitor information transmitted in order to detect illegal activities and to inform the competent public authorities. This is compliant with the general provisions of the Directive 2000/31/EC on electronic commerce Article 15.

Consumer rights

The country has not established country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers. Without trustmark for electronic identification and trust services for electronic transactions, customers can not be assured in the trustfulness of qualified of eCommerce service providers.

The Law "On advertising" regulates the requirements on minimum general information to be indicated by information society service provider. This is compliant with the requirements of the

Directive 2000/31/EC on electronic commerce Article 5.

The national legislation (Law “On advertising”) does not impose that advertisements on the Internet indicate natural (for legal persons there is a legal requirement) responsible for commercial communication and any conditions attached to the offers.

The law “On Consumer Protection” regulates relations between consumers of goods and services, and manufacturers and sellers. However, the national legislation does not explicitly require that the trader provides the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms in case of distance or off-premises contract.

Consumer protection aspects are covered by the EU-Ukraine Association agreement. The Action plan of consumer rights protection to meet the EU Decrees requirements has been developed by the Ministry of Economy with the execution deadline up to the 2nd half 2016. Ukraine has not yet established international cooperation mechanisms between the national public authorities and the authorities of other countries who are responsible for enforcement of consumer protection laws, including for eCommerce.

The national legislation currently does not define the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means. Some basic principles will be reflected in the draft of the Law on eCommerce.

The Government Resolution № 295 ”On rules providing telecom services” includes an obligation about dispute resolution (art.40) and obligations of the service providers in case of low quality of their services to deal through the court system. The country has an online application service for dispute resolution through which parties can initiate dispute resolution in relation to disputes concerning online transactions.

The national legislation prohibits the sending of unsolicited commercial communications by e-mail (Government Resolution № 295”On rules providing telecom services”). The EU best practice in this domain preserves the possibility to either prohibit or allow the sending of unsolicited commercials by e-mail. Compliant with the requirements of the Directive 2000/31/EC on electronic commerce Article 7.

Competition

The national legislation does not explicitly restrict the freedom to provide eCommerce services

compliant to the national laws by a lawful service provider established in another country.

Ukraine's legislation does not explicitly define the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. The regulation of authorisations for eCommerce activities falls under the overall legal framework. This principle does not prejudice the authorisation schemes of Ukraine; neither does it specifically and exclusively target at information society services, or areas which are covered by another legislation. This is partially compliant with the EC Directive on electronic commerce that defines the principle excluding prior authorisation to pursuit the activity of an information society service provider (Directive 2000/31/EC on electronic commerce Article 4).

ePayment

The national legislation does not yet define the rules on the fees for the use of means of electronic payment. A comprehensive national legislation for eCommerce payments by credit or debit card, on Internet, on phone, using mobile and other electronic payments presents a substantial benefit for eCommerce development and market integration in this field at European level.

There is no legislation basis at the moment, though some documents can be circulated in electronic form (Tax Vouchers, limited Acts of Acceptance). The legislation of Ukraine does not explicitly assure equal treatment between paper and electronic invoices. This does not comply with the situation in the EU where the EC has identified a set of actions to support the uptake of eInvoicing by ensuring legal certainty and promoting the development of interoperable eInvoicing solutions based on a common standard, paying particular attention to the needs of small and medium-sized enterprises.

eLogistics

The national legislation does not explicitly establish the equal validity of electronic contracting and contract concluded offline together with defining the specific requirements to electronic contracts. The EC Directive on electronic commerce (Directive 2000/31/EC on electronic commerce Articles 9-11) requires the fundamental principles of equal validity of electronic contracting and contract concluded offline, and not only for eCommerce.

The national legislation does not explicitly define the conditions for the risk of loss of or damage to the goods purchased within eCommerce transaction and responsibilities of the trader, the

consumer, a third party indicated by the consumer, or the carrier. It also does not stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply. However, the law of Ukraine “On Consumer Protection” regulates relations between consumers of goods and services, and manufacturers and sellers.

The national legislation does not define the requirements for time of delivery of goods purchased through eCommerce. The harmonisation would increase international opportunities for hosting service providers and Cloud computing services providers.

HDM roadmap

The following sections present the aspects where progress on HDM can be made, the objectives and individual follow-up actions of the country for harmonisation in the priority area:

Internet security and privacy

Allowance to process user traffic data - assure to users their rights to manage online privacy. Amend the national legislation with the rules of processing of user traffic data by the provider of an electronic communication service for the purposes of marketing electronic communications services or for the provision of value added services. The legislation should indicate if the service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing.

Specific liability regime for intermediary service providers - increase the transparency of rules for provision of cross border eCommerce services by SMEs. Amend the national legislation with provisions about the specific liability regimes for three categories of online service providers: transmission conduit operators, caching providers and hosting services providers. The legislation should be amended to define the degree of liability of the service provider for the information transmitted in a communication network of information provided by a recipient of the service. The liability of service provider should be defined for the automatic, intermediate and temporary storage of that information, performed for making more efficient the information’s onward transmission to other recipients of the service upon their request. Liability of the hosting service providers should be defined for the information stored at the request of a recipient of the service, with some clearly defined liability exceptions (does not have actual knowledge of illegal activity or information, and others).

Consumer rights

Reassure consumers on the reliability of accredited online service providers, especially across borders. Establish country-wide trustmark scheme(s) for electronic identification and trust services for electronic transactions which assure the trustfulness of qualified eCommerce service providers. Encourage the establishment of price-comparison websites. Such certified sites will help consumers to make informed decisions when using online retail services. Harmonise the development of the national trustmarks schemes with EU Member States. The Commission is in process to elaborate different policy options for EU-wide trust mark schemes and the effectiveness of cooperation platforms in the governance of such trust mark systems.

Transparency of commercial communications information to be provided - assure transparency of commercial communications. Amend the legislation by requirements that advertisements on the Internet indicates natural person responsible for commercial communication and any conditions attached to the offers.

Minimum pre-contractual information required for distance contracts. Assess the compliance of the current legal requirements for minimum pre-contractual information required for distance contracts and off-premises contracts. If required, amend the legislation with requirements for the trader to provide the consumer with a minimum of legally defined pre-contractual information and comprehensive explanation of contractual terms.

Consumer protection international cooperation mechanisms - create a mechanism for international user protection between the Region and the EU. Establish consumer protection cooperation with the public authorities in the Region and the EU who are responsible for the enforcement of consumer protection laws, in priority, with neighbouring countries, countries with main trading volumes, EU Member States. Conduct feasibility studies for development of a national segment of an information system for collection, storage and exchange of information on consumer protection infringements.

Possibility for out-of-court dispute settlement -facilitate dispute resolution for cross-border purchases. Amend the national legislation allowing the use of out-of-court schemes for dispute settlement regarding provision of eCommerce services, including by appropriate electronic means.

ePayment

Legal framework in the area of eCommerce payments and rules on the fees for the use of means of payment. Make online payments more attractive to consumers and increase the competitiveness of SMEs. Define the rules on the fees for the use of certain means of payment and prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such mean.

Equal treatment between paper and electronic invoices -reduce costs and delays of international eCommerce transactions. Amend the national legislation assuring equal treatment between paper and electronic invoices. Define national technical standards by promoting the development of interoperable e-invoicing solutions based on common with the EU standards, paying particular attention to the needs of small and medium-sized enterprises. Define a single and clear semantic data model and a common eInvoicing format compatible with the EU best practices to facilitate semantic interoperability, ensure technology neutrality and facilitate the uptake of e-invoicing for eCommerce transactions for SMEs.

eLogistics

Equal validity of electronic and offline contracts -extend possibilities of cross-border trade by facilitating conclusion of contracts. Amended the national legislation to assure the same validity of the contracts concluded by electronic means and contracts concluded offline by "traditional" means. Amend the legislation with requires that online traders provide the consumer with specific information prior to the order being placed. This should include information on steps to follow to conclude an electronic contract, the filing of the contract by the service provider, the technical means for identifying and correcting input errors prior to the placing of the order, the languages offered for the conclusion of the contract, availability of any relevant codes of conduct. Amend the legislation with requirements regarding placing of orders for electronic contracts. The online contract has to be concluded through an "order" placed by the consumer, followed by an electronic "acknowledgment" of the online trader without undue delay. The "order" and the "acknowledgement" are deemed to be received when the involved contracting parties are able to access them. Trader also has to provide the consumer with the technical means allowing him/her to identify and correct input errors prior to the placing of the order.

Conditions for the risk of loss of or damage to the goods -reassure consumers and increase the attractiveness of cross-border eCommerce services. Amend legislation to define the conditions for the risk of loss of or damage to the goods and responsibilities of the trader, the consumer, a

third party indicated by the consumer, or the carrier. Stipulate the remedies available to consumers for damaged or faulty goods, entitlement of consumers to replacement or repair of goods, a refund or discount where specific circumstances apply.

Rights on delivery of goods -assure the conditions for the physical delivery of goods. Amend the legislation by defining the time of delivery when the trader shall deliver the goods (a defined maximum number of days from the conclusion of the contract) by transferring the physical possession or control of the goods to the consumer. Define the conditions when the trader fails to fulfil his obligations to deliver the goods at the time agreed, additional period of time and the right of the consumer to terminate the contract and get reimbursement of all sums paid under the contract.

2.5 Digital Skills

2.5.1 EU baseline

The EU Baseline for "Digital Skills" consists of a number of benchmarks derived from the legal and regulatory framework for electronic communications. The key documents in that framework are;

Digital Single Market

The European Union President has renewed the EU's strategy on the basis of an Agenda for Growth, Fairness and Democratic Change; an agenda that concentrates on areas where the European Union is able to make a real change. Creating a connected digital single market is one of the ten priorities. Its completion could generate significant additional growth for 2014-2019. This includes:

- Making Europe a world leader in ICT to succeed in the global digital economy and society by creating a connected digital single market, and thereby creating hundreds of thousands of new jobs, notably for young job-seekers, and a vibrant knowledge based society.
- Reinforcing digital skills and learning across society, with a view to empowering Europe's workforce and consumers for the digital era.

Digital Agenda for Europe containing references to Digital Skills and Jobs

The Digital Agenda for Europe aims to help Europe's citizens and businesses to get the most out of digital technologies. It is one of the flagship initiatives under Europe 2020, the EU's strategy to deliver smart sustainable and inclusive growth. Pillar IV of the Digital Agenda for Europe defines "*Enhanced digital literacy, skills and inclusion"*. In a Review of Digital Priorities in December 2012[38], one of the 7 key areas for further efforts to stimulate the conditions to create growth and jobs was *"Launch Grand Coalition on Digital Jobs".* The role of information and communications technology (ICT) in raising productivity and living standards is critical. The largest obstacle to harnessing the power of ICT is the shortage of digital skills. While demand

[38] See ec.europa.eu/digital-agenda/en/news/digital-do-list-new-digital-priorities-2013-2014

for ICT practitioners is growing by around 3% a year, the number of fresh ICT graduates and skilled ICT workers is not keeping up. By 2020, Europe might face a shortage of almost 825,000 ICT professionals. Meanwhile, about 25 million Europeans are currently unemployed. This is what is termed the "*digital skills gap"*.

Grand Coalition for Digital Jobs

In March 2013 the Commission launched the *Grand Coalition for Digital Jobs*: a multi-stakeholder partnership that aims to facilitate collaboration among business and education providers, public and private actors to take action attracting young people into ICT education, and to retrain unemployed people. The goal is to increase the supply of ICT practitioners by 2015, so as to ensure a sufficient number of them in Europe in the near future.

The Grand Coalition for Digital Jobs delivers concrete actions, which can be implemented in the short-term and have high local impact. It builds on on-going programmes and best practices that could be scaled-up, for example training and matching for digital jobs, certification to improve recognition, innovative learning and teaching, mobility and awareness raising.

National Coalitions for Digital Jobs

National Coalitions (NCs) and Local Coalitions (LCs) are multi-stakeholder partnerships which aim to promote and implement the objectives of the Grand Coalition for Digital Jobs in each EU Member State by means of concrete action plans. Any actions that can contribute to helping bridge the gap between people looking for jobs in the ICT market and industry (all sectors) can be considered. NCs and LCs can focus on those actions most appropriate to their local circumstances.

The Communication on Opening Up Education and the Research and Innovation Programme

Both these programmes aim at enabling opportunities for better learning through use of modern devices, wider connectivity and interoperability, non-discriminatory access to quality content and innovative teaching methodologies which are responsive to learner's individual needs.

The Communication on Opening Up Education sets out a European agenda for stimulating high-quality, innovative ways of learning and teaching through new technologies and digital content. 'Opening up Education' proposes actions towards more open learning environments to deliver education of higher quality and efficacy and thus contributing to the Europe 2020 goals of boosting EU competitiveness and growth through better skilled workforce and more employment.

It contributes to the EU headline targets for reducing early school leaving and increasing tertiary or equivalent attainment and builds on the recent initiatives 'Rethinking Education', 'European Higher Education in the World' as well as the flagship initiative Digital Agenda. It proposes actions at EU and national levels, notably:

- helping learning institutions, teachers and learners to acquire digital skills and learning methods;

- supporting development and availability of open educational resources;

- connecting classrooms and deploying digital devices and content;

- mobilising all stakeholders (teachers, learners, families, economic and social partners) to change the role of digital technologies at education institutions.

Initiatives linked to Opening up Education will be funded with support from Erasmus+, the new EU programme for education, training, youth and sport, and Horizon 2020, the new research and innovation programme, as well as the EU structural funds.

Connected Continent legislative package delivering sustainable jobs

The legislative package for a "Connected Continent: Building a Telecoms Single Market", contains key objectives to enable sustainable digital jobs and industries.

The single telecoms market can enable growth in jobs by:

- Making the digital sector, which has a very young workforce, a job priority - this would be a way to address youth unemployment in Europe;
- Helping “start-ups” grow by giving them the world’s biggest market to sell to from Day 1;
- Supporting labour force changes in telecoms companies which have not adapted to new digital, data-driven business models
- Working with companies in the Grand Coalition for Digital Skills and Jobs, to train individuals and to improve the overall digital ecosystem.

Employment package of 2012

The Employment package is a set of policy documents looking into how EU employment policies intersect with a number of other policy areas in support of smart, sustainable and inclusive growth. It identifies the EU's biggest job potential areas and the most effective ways for EU countries to create more jobs. Measures are proposed in supporting job creation, restoring the dynamics of labour markets (including investing in Digital Skills) and improving EU governance.

Policy, leadership and resources

The benchmarks derived from the EU baseline regarding policy, leadership and resources include

Measuring the digital skills gap

The EU has undertaken regular studies of digital skills gaps[39]. The goal has been to monitor the supply and demand of digital skills across Europe, benchmarking national policy initiatives and multi-stakeholder partnerships in the European Union. This provides a basis for understanding the impact of initiatives launched at EU and national level, proposing remedies where necessary and identifying efficient methods of fostering multi-stakeholder partnerships so as to reduce e-skills shortages, gaps and mismatches. Some components of the EU skills gap are;

- Lack of ICT practitioners
- Lack of e-Leaders
- Decline of computer science graduates
- Lack of soft skills
- Lack of social skills
- Lack of ICT skills needed in performing various types of jobs (other than ICT)
- High youth unemployment
- Long-term unemployed people do not have sufficient ICT skills to find a new job
- Low number of women employed in the ICT sector

[39] For the latest (2104) report see http://eskills-monitor2013.eu/fileadmin/monitor2013/documents/Country_Reports/Brochure/e-Skills_Monitor_Broschuere.pdf

- Multi-cultural and international broader view missing -> low number of ICT entrepreneurs
- Lack of teachers ICT training/professional development (e.g. to teach coding)

The European Commission has just launched a new survey on digital skills in the workforce. Its purpose is to collect information on the digital skills required by enterprises across the European Union. The preliminary results of this study will be published at around September 2015.

Policy context

Digital technology is changing the way we work, learn and live. Therefore, we need to make sure that we deliver the right skills to our kids, students, workers and citizens. The European Commission is promoting various initiatives aimed at increasing training in digital skills for the workforce and for consumers; modernising education across the EU; harnessing digital technologies for learning and for the recognition and validation of skills; and anticipating and analysing skills needs. A strong digital economy is vital for innovation, growth, jobs and European competitiveness. The spread of digital is having a massive impact on the labour market and the type of skills needed in the economy and in the society:

- Firstly, it is changing the structure of employment, leading to the automation of "routine" tasks and to the creation of new and different types of jobs.
- Secondly, it is leading to the need for more skilled ICT professionals in all sectors of the economy. It is estimated that across the EU there will be 825,000 unfilled vacancies for ICT professionals by 2020.
- Thirdly, it is leading to the need for digital skills for nearly all jobs where ICT complements existing tasks. In the near future 90% of jobs - in careers such as engineering, accountancy, nursing, medicine, art, architecture, and many more - will require some level of digital skills.
- Fourthly, it changes the way we learn by fostering online communities, by enabling personalised learning experiences, by supporting the development of soft skills such as problem solving, collaboration and creativity, and by making learning fun.
- Finally, it is leading to the need for every citizen to have at least basic digital skills in order to live, work, learn and participate in the modern society.

Digital Skills requires a co-ordinated policy approach, within the context of national policies for uptake of ICT for competitiveness, growth, employment, education, lifelong training and social inclusion. Digital Skills must be elevated to have an important place in long-term national policy. Each country should take a central role in developing these national policies and actions, within which a long-term Digital Skills agenda is launched, to improve cooperation and mobilisation of all stakeholders and to adopt best strategies and practices in order to better face global competitive challenges. Countries should therefore ensure that they develop, with national and local stakeholders, clear long-term Digital Skills policies. Within the national policy, the key components of action should be defined – long term co-operation, human resources investment, making science, maths and ICT attractive, developing digital literacy for employability and e-inclusion and lifelong acquisition of Digital Skills.

Leadership and awareness raising

The Grand Coalition for Digital Jobs encourages stakeholders to "pledge" concrete actions. Pledges are concrete commitments by companies, universities, and other stakeholders to address the digital skills gap[40]. Actions such as industry-led training, encouraging cross-border mobility for ICT workers, certifying skills, modernising school and university curricula and raising awareness need the active engagement of all stakeholders at national level.

Some countries are forming National Coalitions for Digital Jobs. These are partnerships that bring together the government (e.g. education and employment ministries) with ICT and ICT-using businesses, education and training providers, public and private employment services, associations, NGOs, social partners

Resources

The European Commission encourages Member States to use available funding (e.g. from ESF, Youth Employment Initiative, Horison 2020, Erasmus+, etc.) to fund activities of national coalitions aimed to digital skills development. Although The Grand Coalition does not have a specific budget line to support its activities, there are several funding sources at European and national level to support projects boosting digital skills. A website[41] gives a number of funding

[40] See: http://ec.europa.eu/digital-agenda/en/make-pledge

[41] https://ec.europa.eu/digital-agenda/en/potential-funding

instruments that are available to stakeholders as well as the non-financial support that can be obtained. Each country could ensure that it creates, or has access to, sufficient funding to drive the activities of national and local coalitions and promote Digital Skills development. Examples of committed resources for national coalitions are pledges by coalition partners for training, awareness raising events, job fairs, and incubator initiatives; sponsorships and private funding, government funding.

Open Educational Resources (OER), ensures that educational materials produced with public funding are available to all, so that learning can happen anytime, anywhere. Massive Open Online Courses (MOOCs) allow students, practitioners and educational institutions to share free-to-use course material and the EU-funded Open Education Europa portal provides access to the many resources available. In addition, large scale pilot projects such as Open Discovery Space, co-funded by the European Commission, are working with teachers to create and make better use of OER.

Initiatives linked to the Opening up Education will be funded with support from Erasmus+, the new EU programme for education, training, youth and sport, and Horizon 2020, which is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness.

Best practice, initiatives and implementation

The benchmarks derived from the EU baseline on best practice, digital skills initiatives and implementation include;

Best practices

The European Commission has provided a platform for exchange of best practices, promoting a regular dialogue on Digital Skills, and has produced a Toolkit for National and Local Coalitions. The EU has also developed a European e-Competence Framework (e-CF) which provides a reference of 40 competences as required at the ICT workplace, using a common language for competences, skills and proficiency levels that can be understood across Europe.

Initiatives to create growth and jobs in Europe

The **Grand Coalition for Digital Jobs** is the largest collaborative effort in Europe to date to address the digital skills shortage. So far 80 stakeholders, representing large and smaller companies, education providers and NGOs have made pledges, i.e. concrete commitments to act to reduce digital skills gaps. Likewise, national coalitions for digital jobs aimed to facilitate high-impact actions at local level have already been (see below and examples in Annex B).

National Coalitions have the following key objectives: Innovative learning and teaching, Increase the number of ICT specialists, Fostering digital entrepreneurship, Certification of digital skills, Improved digital literacy, Awareness raising. Broadly speaking, the goals of national coalitions are same as of the Grand Coalition.

So far 8 national coalitions have been launched (in Bulgaria, Greece, Italy, Malta, Latvia, Lithuania, Poland, Romania) and many more are under formation (see also Annex B).

There are also some **Local Coalitions**, which either focus on a specific geographical region or have particular objectives, e.g.: Italy: multi-sector network on educational robotics (ER) WGGD Greece: equal employment opportunities for women in ICT, attract more girls to Science, Technology, Engineering and Mathematics (see also Annex C).

Coding has become the focus of a specific work stream under the Grand Coalition aimed to encourage coding and computer science across Europe, both within schools and beyond. Europe is promoting coding through various initiatives, such as the EU code Week and the European Coding Initiative and through pilot projects on digital learning in schools.

In January 2013, the Commission adopted the **Entrepreneurship 2020 Action Plan** to unleash Europe's entrepreneurial potential. This Action Plan includes a set of actions, such as a Start-up Europe Partnership, to unlock expertise, mentoring, technology and services; work with European investors in order to increase the flow of venture capital and crowd-funding (in particular for web start-ups); and stimulate the emergence of Massive Online Open Courses (MOOCs) and the setting up of platforms for mentoring, and skill building.

The **Web Entrepreneurs Leaders Club** brings together world-class web entrepreneurs to strengthen the web entrepreneurial culture in Europe as well as a European network of web business accelerators.

ICT for better education

A learner-centred pedagogy using ICT and interdisciplinary research makes personalised and adaptive learning possible. For instance, learning analytics tools support teachers' work by providing individual feedback and recommendations to students and educational games are powerful tools to engage kids (and students of all ages) in learning. Fostering of online teachers' communities across Europe empowers them to use and co-create the wealth of educational repositories.

United Kingdom - "Tech Partnership"

The Tech Partnership is a growing network of employers, collaborating to create the skills to accelerate the growth of the digital economy. Its leadership includes the CEOs of major companies in the tech industry, heads of technology from companies across the economy, and small company representation. www.thetechpartnership.com

The Partnership's strategy. Its strategy is to:

-Inspire new talent: inspiring young people, particularly girls, about technology education and careers

-Create new jobs: accelerating the flow of talented people from all backgrounds into technology careers, with a particular focus on apprentices and graduates

-Develop new skills: making it easier for employers to develop strategic digital skills, for example cyber security, big data, mobile, e-commerce and the Internet of Things

-Raise standards: setting industry standards, accrediting and promoting education and training that meets them.

The Partnership's aims. Its aims are that, by 2020:

-There will be a 50:50 gender balance in young people entering tech careers, expanding the pool of talent coming into the sector

-Digital careers will be in the top quartile of desirable jobs in the view of 16-21 year olds

-The number of tech apprenticeships will be doubled, giving the nation a new pipeline of home grown talent to support the growth of the digital economy

Local Coalition – UK (Scotland)

Scottish Local Coalition was launched in March 2014 which aims to review future skills and employment demands, in order to help the sector respond to and embrace the ICT skills challenges that exist in a dynamic and rapidly evolving sector.

The Scottish Government is committed to Scotland being a world class digital nation by 2020. Digital Skills are critical to achieving this vision which is why Scotland's First Minister personally

launched Scotland's industry guided Skills Investment Plan (SIP) for the ICT and Digital Technologies sector and announced additional funding of £6.6 million for digital skills.

Partnership is central to this approach - The Digital Scotland – Business Excellence Partnership was created to ensure a strategic and co-ordinated approach between our public agencies and with industry.

2.5.2 Overview of the state of play and gap analysis for the Region

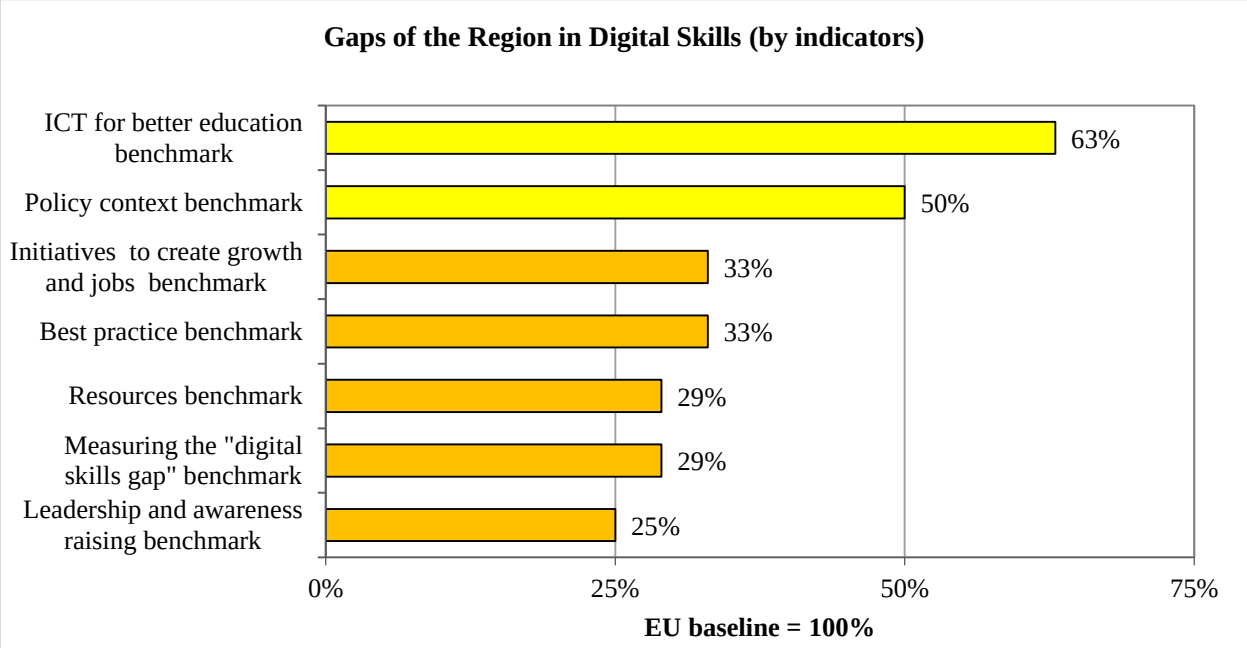

Exhibit 43 - State of play and gaps of the Region in Digital Skills

2.5.3 Overview of common actions for the Region

The main finding is that there is no systematic measurement and monitoring of the "Digital Skills Gap) in the Region, so awareness of the skills shortages is not at a sufficient level to bring about coordinated initiatives to promote Digital Skills and to create jobs and growth.

Initiatives could be commenced immediately to measure and monitor the skills gaps, to raise awareness and to form national and local coalitions in coordination with Europe's Grand Coalition for Digital Jobs.

The co-ordination of digital skills initiatives, awareness raising and best practice adoption would be greatly leveraged by welcoming the Region into Europe's Grand Coalition for Digital Jobs.

2.5.4 Benefits for and readiness analysis of the Region

For Digital Skills, the earliest need is the systematic measurement and monitoring of the skills gap. Without this measurement, awareness of the need to match demand and supply is missing and the beneficial coordination of initiatives and sharing of best practices with the EU is not currently in place.

2.5.5 Armenia

State of play and gap analysis

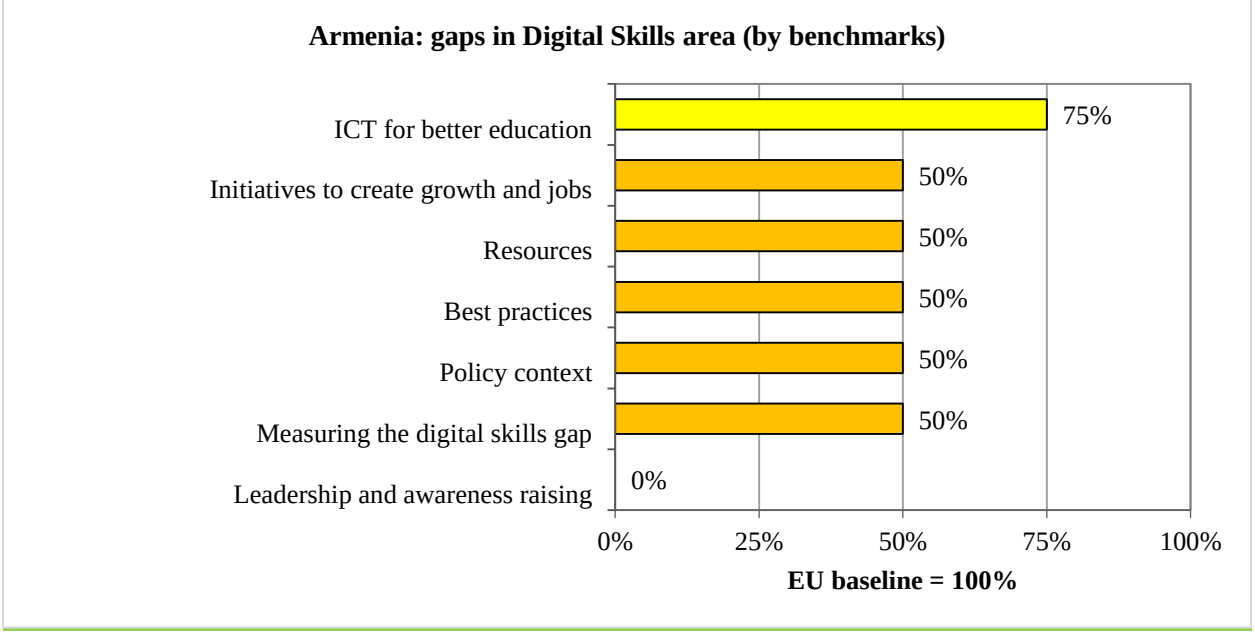

Exhibit 44 - Armenia: state of play and gap analysis in Digital Skills

The National Centre of Educational Technologies (NCED) implements and publishes a Survey on the Application of IT Technologies in the Educational Institutions on an annual basis. In addition, the Enterprise Incubator Foundation published a report on the IT Skills Gap in 2014. No other dedicated and periodical surveys are done in the area of digital skills in general.

Though the Government has announced that IT sector is a priority sector for the country's economic development and for the creation of knowledge based economy, the strategies for the development of digital skills should be unified and enhanced to pursue this goal. Separate

initiatives undertaken in this area are the E-society development strategy 2009-2010, a number of programs for the development of IT user skills for targeted groups (teachers, students, youth, etc.), offline and online academies operated by IT companies. However, there is a need for a single initiative and a single approach. There are a number of international programs and funds available in Armenia. Initiatives are implemented under these programs. However no special funds are available for the development of digital skills.

The responsibilities for the development of digital skills are distributed among a number of institutions – notably NCED (in education), National Quality Assurance Organisation and the Ministry of Economy. Development of IT skills has been in the focus in Armenia mainly led by the initiatives of the private sector, professional organisations and NGOs. Coding, informatics and engineering has been actively taken into the schools' agenda. However, these initiatives are not part of a special national agenda rather separate uncoordinated actions.

There is a proxy to the eCompetence Framework on the national level developed by the Ministry of Social Protection. However this framework includes only high-level competences and no dedicated digital competences are defined.

All schools are connected to the internet and have computer labs. About 18,000 computers are distributed in 1400 schools of Armenia. Now, the state actions are addressed to the upgrade of the generation of the computers and the improvement of the internet connection. In 2016 the NCED will launch 2 workshops for the repair of the computers and parts of computers at the schools.

HDM roadmap

An in-depth analysis of the skills gap in the digital area is a priority. Only based on such research an effective IT and Digital skills policy can be developed. Although the IT sector is announced to be a priority sector for Armenia, the government has not shown any dedicated support and the lack of a comprehensive assessment of the digital skills is an evidence of this. An important area to cover by such research is the demand for the digital and IT skills outside the IT sector.

A thorough assessment of the gap in digital skills and policy development based on it will help to adjust the curriculum in the educational institutions to provide necessary skills to the students

and to serve the market needs. The availability of such framework has a high significance given the globalisation trends and the need for high workforce mobility.

The only obstacle is the low availability of the financial resources.

Conditions for harmonisation

There are possible benefits for harmonising with the EU in the area of digital skills. The ICT sector has been recognised as a priority for the Russian Federation but they have not proposed any system for the promotion of digital skills and jobs.

The highest potential for harmonisation is within the area of leadership and awareness raising. All other areas have gaps, but most progress has already been made in the area of ICT for better education.

Pilot Projects

It is recommended that Armenia joins a Regional initiative to measure the Digital Skills gap, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap.

The pilot project can be undertaken within the scope of a proposed “National Coalition for Digital Jobs” to be created in Armenia in conjunction with the EU’s “Grand Coalition”.

2.5.6 Azerbaijan

State of play and gap analysis

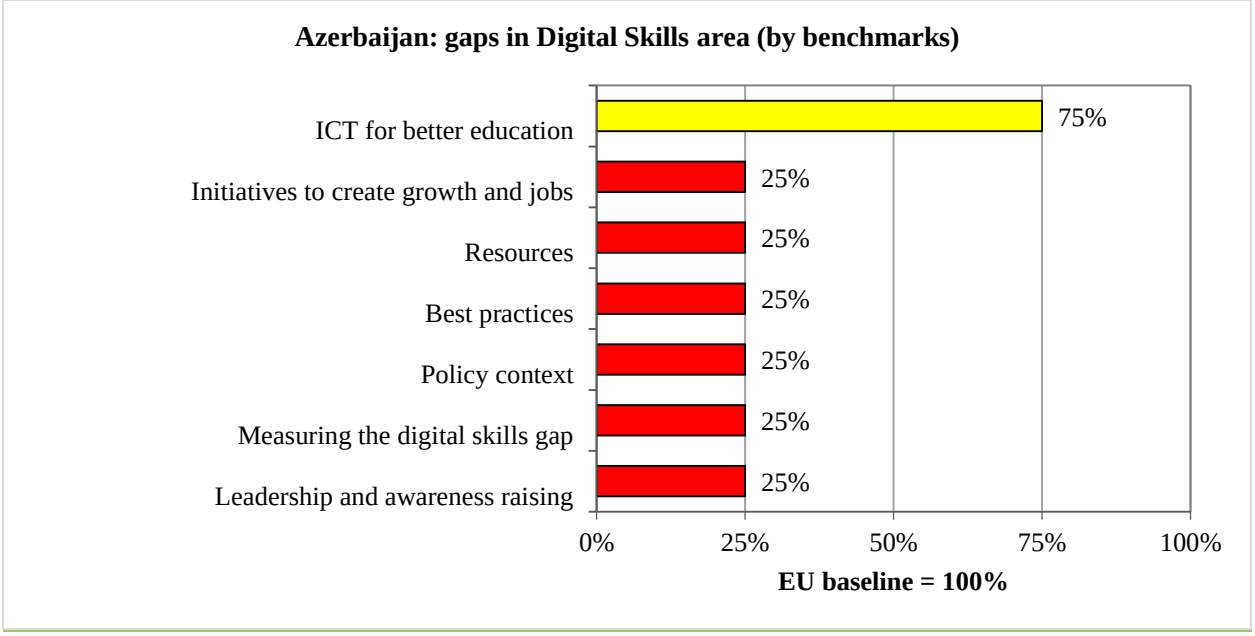

Exhibit 45 - Azerbaijan: state of play and gap analysis in Digital Skills

The Ministry of Education is the central executive body responsible for formation, execution and regulation of state policy on education process, as well as for performing methodical guidance to education process in Azerbaijan. The Ministry is also responsible for the development of digital skills.

There are a number of web based e-education resources of the Ministry, such as education portal, e-textbook and curriculum portal.

As for e-services rendered by the Ministry they are divided into Interactive and Informative services.

The Interactive Services include:

- e-application
- Submission of applications and documents for recruitment of teachers to secondary schools
- State Program for study of Azeri youth abroad in the years 2007-2015
- Provision of information on current academic achievements of pupils
- Submission of applications and documents for admission to initial vocational education

institutions

- Online-check of recognition of foreign higher education qualifications and definition of their equivalence
- Nostrification procedure.

The Informative Services include:

- Contact with senior officials of the Ministry of Education
- Education institutions
- Admission procedure to education institutions
- Current achievements of pupils (System for parental control)
- Assessments of pupil achievement
- Rules for changing education institutions
- Deinstitutionalisation and children protection
- Notification
- Ethical standards model

As there are no Coalitions for Digital Jobs in Azerbaijan, there is no funding considered for these activities. This topic is new to Azerbaijan and almost no work has been implemented.

The main purpose of the "Xalq kompüteri" (People Computer) project is to create the conditions for obtaining on favourable terms modern computers and licensed software by different social groups, to increase digital skills by expanding ICT implementation in the regions, to support the activity of Azerbaijani government in development of information society and e-Government. This project was jointly implemented by the Ministry of Communication and High Technologies, the Ministry of Education, Hewlett Packard, Microsoft and Bestcomp Group,

During the first phase of the project, secondary school teachers and schoolchildren, university teachers and students were involved. In the near future, all the citizens will have the opportunity to join the project. Up to now 25,300 people obtained computers from the project. At the same

time in order to prepare highly-qualified specialists in ICT within the universities, Microsoft and CISCO academies have been established by private companies.

No actions have been undertaken to promote the growth in digital jobs. However, a number of projects together with UNDP and other stakeholders are being implemented to develop the skills of local specialists.

The first state program on “Provision of Educational Establishments in the Republic of Azerbaijan with Information and Communication Technologies in 2005-2007” was approved by a presidential decree at the end of 2004. This particular program was mostly focused on the provision of computer equipment to schools and the Ministry of Education was responsible for its administration. Furthermore, the “State Program on Informatisation of Educational System 2008-2012” emerged, and the program covered all aspects of ICT integration. The second state program aimed to improve the quality and accessibility of education opportunities through the efficient application of modern information and communication technologies in all grades levels as well as to establish shared space for the exchange of information and experiences. Successful integration of ICT into education had also been prioritised in the “State Strategy for the Development of Education” which was approved by a Presidential decree in 2013.

The latest data shows that 82% of secondary schools, 45% of technical-professional schools, 91% of state vocational schools, and all higher education facilities in Azerbaijan have been provided with computer equipment and fast internet connectivity. Around 70% of the pedagogical personnel participated in special training courses on integration of ICT into the classroom activities. Another important issue besides the provision of ICT training for the pedagogical personnel is the improvement of the education management skills.

The Data and Resource Centre was established as the core of the technical infrastructure of Azerbaijan Educational Network aiming at gathering education resources and providing educational institutions with access to local and international educational content. To protect students’ psychology, as well as, limit their usage of harmful information the Websense program is applied in the frame of the Azerbaijan Education Network. This program automatically filters all websites and bans access to internet resources which are not allowed. This technology limits searching harmful information through more than 60 categories in different languages. It enables providing maximum protection of children from harmful content.

Furthermore, different initiatives in the field of distance education were introduced, websites for the educational establishments were created and an educational portal was started. Throughout the country a pilot project “E-school” was initiated in 50 schools, among which 15 were also included in “One Student - One Computer” pilot project.

Additionally, for the purposes of storing all existing resources in one centre, the portal – e-resurs.edu.az has been created. By means of this portal, users are presented with the ability to access e-lessons, video lessons, competitions, e-tasks, various educational games and resources.

Another useful portal, created by the Ministry of Education, is www.e-test.edu.az which includes over 30,000 questions and helps interested students improve their knowledge and skills in Mathematics and Azerbaijani language subjects. In addition to this, www.video.edu.az is home to over 100 videos covering the topics of chemistry, physics, literature, language and biology. Also, e-textbooks for the second, third, sixth and seventh grades were placed in the portal - www.e-derslik.edu.az, which covers large user base. According to the current statistics, the portal counts well over 25,000 registered users.

Furthermore, different international e-resources were adapted to complement our educational system. As a result, 200 e-resources were translated from different languages into Azerbaijani and placed under “Foreign e-resources” category in the portal for public use.

On the official web page of the Ministry of Education a segment called “e-services” has been introduced, which includes 5 fully operational electronic services offered by the Ministry. Those being:

- Submission of applications and documents for recruitment of teachers to secondary schools;
- State Program aimed at supporting Azerbaijani youth to study abroad in the years 2007-2015;
- Provision of access to information on academic achievements of pupils;
- Submission of applications and documents for admission to initial vocational education institutions;
- Online check of recognition of higher education qualifications and definition of their

equivalence.

- A new electronic system was very recently created for the admission of the children to the first grade of secondary schools, lyceums and gymnasiums of Baku. The new electronic system is expected to increase the efficiency of the admission process in the country.

HDM roadmap

A comprehensive survey on “Digital Skills gap” is definitely required to measure the needs and opportunities for digital skills. It would be advantageous to use the experience of the EU in conducting a survey on the “digital skills gap”. Azerbaijan needs to follow best practices in to develop policy and coordinate initiatives. There is a general lack of experience and a lack of information on best practices.

Azerbaijan needs to take actions for forming of National Coalitions for Digital Jobs to address the digital skills gap, but again there is a lack of information and experience and there could be unwillingness of local stakeholders to form the national or local coalitions. Azerbaijan needs to study the experience of EU countries in forming coalitions and establish links with Europe’s “Grand Coalition for Digital Jobs”. Then it needs to attract local stakeholders for forming national coalitions.

The development of digital jobs in Azerbaijan will have clear technological and economic benefits. Azerbaijan lacks a clear vision for development of a digital jobs market and has first to study best practices and prepare a platform for exchange of best practices, promoting a regular dialogue on Digital Skills, and to develop an e-Competence Framework.

A wide range of opportunities exist for development of infrastructure in this area. Organisation of experience sharing visits, training, manuals to study the best practices, increased use of modern technologies in the sectors of economy, cooperation with EU countries in the sphere of digital skills, establishing a basis for forming of National Coalitions on Digital Jobs.

The proposal is to organise experience sharing programs and training on available funding to promote Digital Skills initiatives. This needs access to sufficient funding to drive the activities of national and local coalitions and promote Digital Skills development. Another proposal is to establish a Web Entrepreneurs Leaders’ Club and to organise training on how to measure digital skills gap

Conditions for harmonisation

As the notion of “Digital Skills” is new to Azerbaijan, the country has barely started to implement measures for the development of digital skills, relevant resources are just being developed and a survey to measure the “Digital Skills gap” in Azerbaijan needs to be undertaken as an essential initial step to raise awareness of the problem.

The main legislative act regulating education activities is the Law “On Education”. A number of measures are stipulated in the “State Strategy for the development of education in the Republic of Azerbaijan” (covering 2015-2023) approved by Presidential Decree. There are not any international agreements on Digital Skills.

Pilot Projects

It is recommended that Azerbaijan joins a Regional initiative to measure the Digital Skills gap, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap.

The pilot project can be undertaken within the scope of a proposed “National Coalition for Digital Jobs” to be created in Azerbaijan in conjunction with the EU’s “Grand Coalition”.

2.5.7 Belarus

State of play and gap analysis

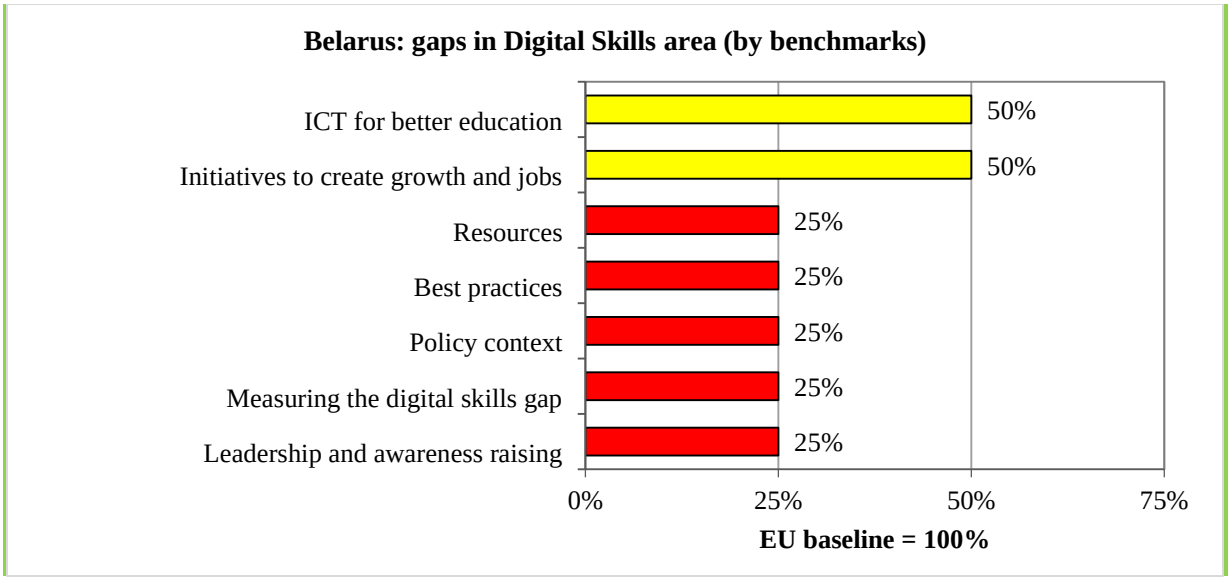

Exhibit 46 - Belarus: state of play and gap analysis in Digital Skills

The IT sector in Belarus is considered to be the largest IT cluster in the Central and Eastern Europe (CEEOA 2010). Due to the limited domestic demand especially from industrial enterprises, it is rather well integrated into the world market, delivering outsourcing services to major IT vendors of the world (like HP, IBM, Microsoft, Oracle, SAP, 1C), but also possessing a developed network of constant smaller foreign partners.

Because there is only a small domestic market for IT products (it is mainly represented by state institutions, financial enterprises, banks, and corporate customers, with a rather small share of industrial enterprises), Belarusian companies mainly target at Western customers' orders. The niche on the world IT market of Belarusian companies can be described as an offshore IT service provider (software development, outsourcing) for clients who expect the involvement of highly skilled technology resources at low costs.

Though the problems with ICT education are widely known by the private ICT sector and the regulators, there has been no thorough survey to measure the “Digital Skills gap”. There is no single body governing and regulating the ICT sector. The Ministry for Communications and Informatisation regulates the telecommunications sector and radio spectrum; the Operation and Analytical Centre deals with information security (electronic identification, cryptography, critically important objects of infrastructure); the Ministry of Trade handles eCommerce; the Ministry of Economy regulates pricing and antimonopoly policy; the Ministry for Taxation is responsible for electronic invoices; the State Customs Committee handles eCustoms issues; the Ministry for

Information regulates content on the Internet. On the one hand, this means that managing informatisation processes is deeply integrated into functions of bodies of every industry. On the other hand, there is no single body that would have a general view of the problems in informatisation of the country and develop and realise the holistic national ICT strategy, embracing the industrial sector.

Neither Ministry of Education nor the Ministry for Labour have a department in their structure that would be responsible for IT education and digital skills in general.

There is no platform for exchange of best practices, or for promoting a regular dialogue on Digital Skills. Instead of the European e-Competence Framework (e-CF) which provides a reference of 40 competences as required at the ICT workplace, in Belarus a National Classifier of the Republic of Belarus 006-2009 OKRB "Professions of workers and office employees" is used. The most widespread (in Belarusian industry) IT professions were added to this recently, but there is still work to be done to continue updating the Classifier with the most recent professions.

Linkages of the academic sector and IT companies in the educational process include the following basic forms of interaction[42];

- the establishment of joint training labs;
- participation of enterprises in the correction of the nomenclature of specialties and curriculum content;
- organisation of students' practice in enterprises, training of trainers in enterprises;
- delegation of employees of enterprises to universities as teachers;
- financing by companies of training activities of universities, and other forms of linkages.

The main purpose of this interaction is proactive involvement of IT enterprises in the training of IT professionals who will not require retraining after employment.

[42] Pobol, A. Export-oriented IT companies developing their resource base and institutional environment. Working paper. Minsk: 2014. – 14 p.

The Sectoral program of informatisation of education in 2014-2015[43] sets the following priority areas of ICT in education;

- creation of a unified information environment, including the national system of electronic educational resources, network infrastructure and access services to national and international educational resources;
- extensive use of ICT in teaching activities, introduction of new methods and forms of education using ICT, as well as improving the system of training in ICT;
- creation of information-analytical systems, databases and data banks to automate management processes in education.

HDM roadmap

The challenges to be addressed within the HDM initiative are the following;

- insufficient involvement in ICT of such groups as young people and women due to a list of reasons such as different entrance barriers, lack of career guidance, a long list of myths and misunderstandings about the possibilities of IT-career for "ordinary" people and so on;
- absence or poor development of the system of career guidance and re-training for unemployed or inefficiently employed to increase their involvement in ICT industry;
- low efficiency of ICT skills training caused, on the one hand, by the gap between educational and real ICT-related job requirements and, on the other hand, by the different training goals and content standards in different parts of Europe and the countries of the Eastern Partnership. This increases the time lag between finishing the study and efficient job placement, so as limits the opportunities for outsourcing based on comparative advantages of different regions and countries, labour force migration and effective cooperation;
- high cost of ICT skills training resulted from such system problems as (1) shortage of ICT trainers resulted from the general shortage of the ICT specialists and their high wages, (2) necessity to update educational curricula much more often in comparison

[43] http://giac.unibel.by/ru/main.aspx?guid=16991

with the other spheres of education , and maybe the most important (3) absence of the unified approach, curricula and content standards within Europe and the countries of the Eastern Partnership (so every country and even every educational institution solves the first two problems itself).

- fear and unwillingness to use digital technologies caused by the low level of Digital Skills literacy result in slowing the implementation of information technologies, lower competitiveness, higher costs and decrease of the economic growth in general;
- manual and paper based procedures make harmful influence on the environment in a long term perspective.

The actions required include the following;

- develop a unified approach, curriculum and educational content standards for ICT skills based on the European e-Competence Framework;
- create the system of user-generated electronic content to be used for distance learning including the unified assessment approaches and methodologies;
- develop a unified curriculum for Train the Trainers sessions within Europe and the Region, carry out these sessions;
- carry out promotional activities within Europe and the Region to decrease the influence of myths and to increase the popularity of ICT skills and the advantages of a unified approach. The low level of digital infrastructure literacy (common Digital Skills for eCommerce, eCustoms, eInvoicing and other digital market procedures) result in lower efficiency of these procedures and necessity to duplicate digital procedures with manual ones;
- create a Europe-wide and Regional structured database (cloud project) framework of Digital Skills related to the digital infrastructure (including but not limited to eCommerce, eCustoms, eInvoicing);
- develop simple instructions and educational instruments to develop Digital Skills for the effective digital infrastructure including educational materials, Train the Trainers sessions, assessment procedures;

- analyse (based on the results of the other priority topics projects of the HDM initiative) the possibilities to improve and simplify the required Digital Skills for the effective digital infrastructure (this might be a part of the other HDM priorities projects as one of the possible outcomes).

For digital start-ups, there is almost no knowledge on how to create an international digital business, except for software outsourcing scheme (when large international vendors like Oracle or Microsoft subcontract software development to Belarus). Very little knowledge is available about software development under a trademark and its international marketing; about cloud computing business models and about public-private partnership as a business (this knowledge is also needed critically by governmental bodies).

Recently, in the EU, the list of 23 IT professions were described from the viewpoint of competencies needed. Belarus would benefit from assistance in preparation (education of these IT specialists according to standards). However, preparation of final IT specialists (individual fellowships and internships) would not be productive because the prepared staff would immediately be absorbed by industry, because the gap between supply and demand with advanced IT skills is huge in the country. What is needed is to train the trainers who could multiply the skills by educating further specialists in mass.

Conditions for harmonisation

Belarus lacks the educational programmes of the high quality for the new IT professions; educational materials; qualified trainers and educational (electronic) courses for these professions, as well as the system of knowledge assessment according to international (EU) standards, that will allow issuing the internationally acknowledgeable certificates.

In Belarus, there 118 regions; at least one trainer should be available for each regional centre. In larger cities, more trainers per region are needed, so we need a total of about 300 trainers in new IT professions. To provide that 300 trainers continue training activities, we need to have 600 trainers prepared. The methodologies and materials should be prepared to such extent that the person with an average level of preparation would be able to study himself. They should allow that the trainer serves as a communicator and a guide in self-learning, not as a best

expert in the subject. This will allow trainers with average skills to prepare many students with much better knowledge that that of a trainer.

There is a strong need to bring Belarus into Europe's Grand Coalition for Digital Jobs to share experience on how to involve stakeholders in new creative models for increasing digital skills. Unless this is done, Belarus will tend to rely on the more traditional "Train the Trainers" model for increasing digital skills.

Pilot Projects

It is recommended that Belarus joins a Regional initiative to measure the Digital Skills gap, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap.

The pilot project can be undertaken within the scope of a proposed "National Coalition for Digital Jobs" to be created in Belarus in conjunction with the EU's "Grand Coalition".

2.5.8 Georgia

State of play and gap analysis

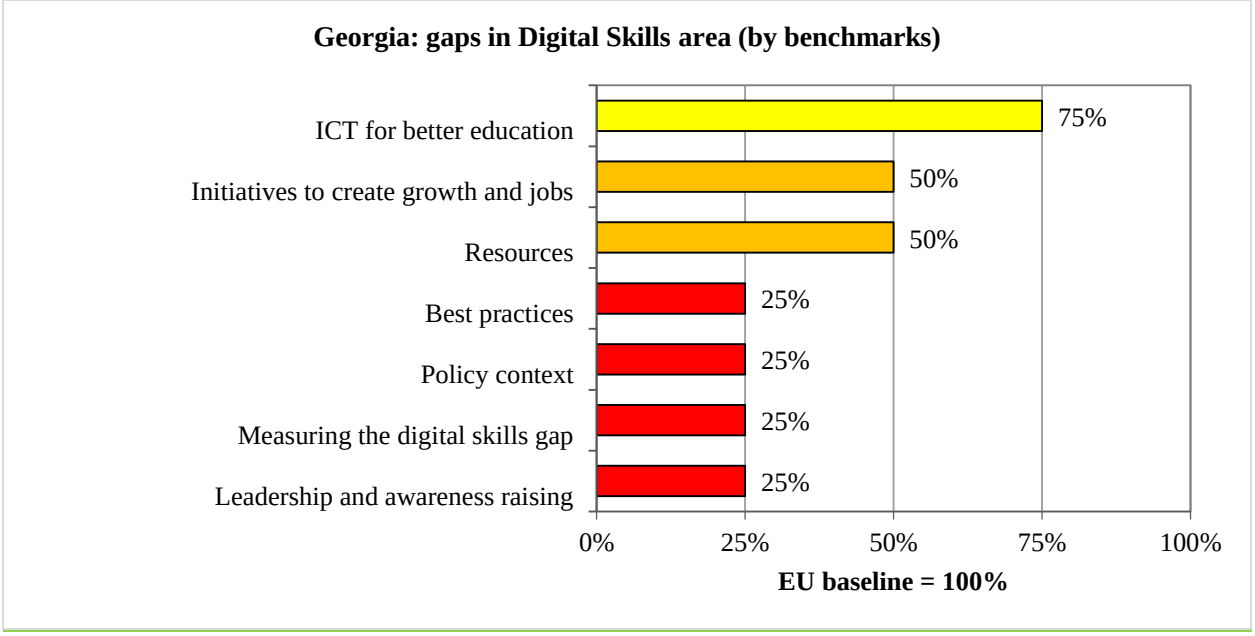

Exhibit 47 - Georgia: state of play and gap analysis in Digital Skills

Georgia has not carried out a thorough survey to measure the "Digital Skills gap" and published the results. The Government has declared a commitment to the development of digital economy. Various initiatives have been launched but there is no clear long-term Digital Skills policy.

The overall understanding and declaration of the importance of digital economy is in place, as well as, recognition of importance of digital skills at different levels but distinctive policy has not been adopted on the issue. The government has initiatives to promote innovation and technology, including state coordination committee. A technological park that will be opened in Georgia in 2015, is a further basis for developing of ICT skills.

The presence of legislation on E-Commerce, E-signature, ICT in schools, plus the creation of Georgian Innovation and Technology Agency, has resulted in some initiatives already being launched.

The E-Georgia initiative is not yet adopted. This includes e-inclusion and ICT skills development policies[44].

A memorandum was signed between Silknet and the Georgian Technical University that would enable graduates of the University to undertake internships with future possibilities to be employed at Silknet.

No best practice sharing instruments in the format of national coalitions have been developed. No "pledges" are present, though particular cooperation initiatives are underway.

"Buki" – a netbook for all first grade pupils was launched as a project in 2010. In the pilot phase 3,000 pupils from Tbilisi, Batumi, Kutaisi, Zugdidi, Mestia and Tserovani, and 150 class tutors received a netbook. In 2011, all first grade 60,000 pupils received netbooks and also 3,300 class tutors the same netbooks (with special software to control pupils' netbooks). Since 2011, every year the first graders receive netbooks, now notebooks, therefore now all primary school pupils have one per household.

HDM roadmap

[44] http://www.dea.gov.ge/uploads/eGeorgia%20Strategy.pdf

The Ministry of Education is getting funding from the state budget or international donor funding. In case additional frameworks are formed, the same budget or donor planning shall be applied. The Georgian Innovation and Technology Agency has already started ICT initiatives with centrally organised funding.

As a first step, a “Digital Skills gap” survey is required to bring an understanding of the problem that responsible authorities are faced with. There needs to be a co-ordinated focus on digital skills development and ICT market simulation within an open international IT skills market.

Conditions for harmonisation

An institutional framework is not in place and the importance of such a policy and cooperation framework is underestimated by the stakeholders. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. There is a lack of understanding of the EU baseline for Digital Skills. Cooperation between Government and the private sector on these issues, would increase trust and would have long term benefit.

Over-formalisation of the process could lead to creation of more barriers for the cooperative projects in Digital Jobs creation. This is because the EU baseline may be seen as over-bureaucratic and burdensome on businesses. In the case where the EU baseline and framework is too conservative and bureaucratic, it would be difficult to be implemented.

Pilot Projects

It is recommended that Georgia joins a Regional initiative to measure the Digital Skills gap, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap.

The pilot project can be undertaken within the scope of a proposed “National Coalition for Digital Jobs” to be created in Georgia in conjunction with the EU’s “Grand Coalition”.

2.5.9 Moldova

State of play and gap analysis

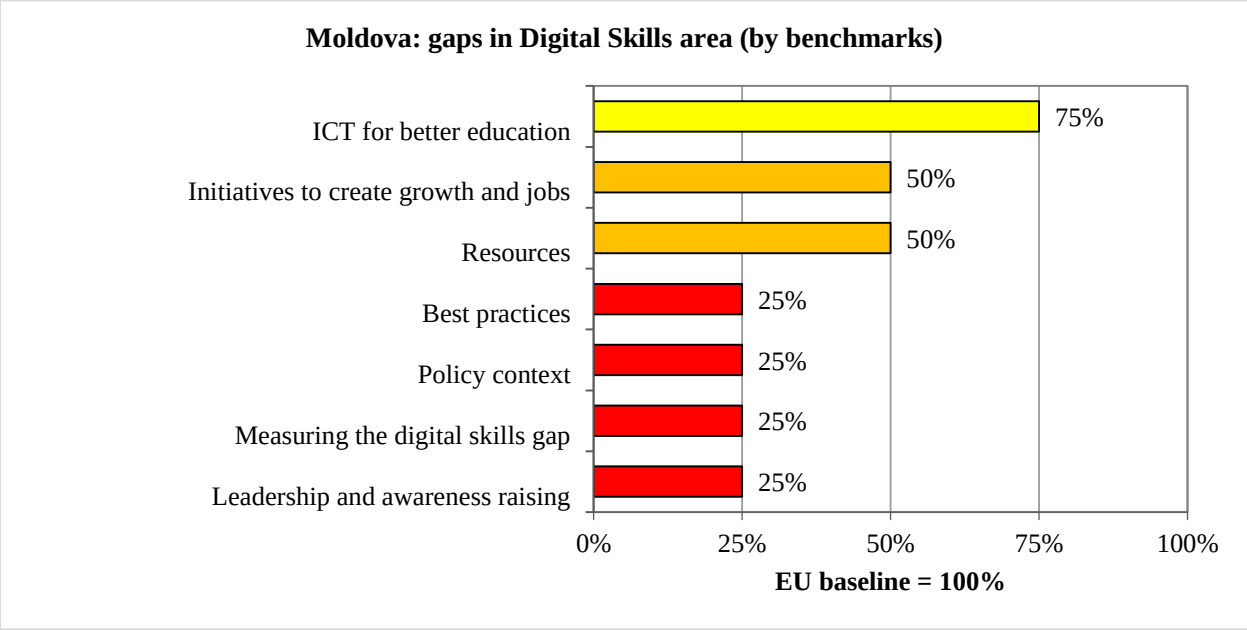

Exhibit 48 - Moldova: state of play and gap analysis in Digital Skills

There is no complete study of the overview of the situation on Digital Skills in Moldova. There are separate papers related to ICT Industry Competitiveness Skills requirements (developed in 2012 with the support of USAID and the National Association of ICT Companies), and a separate strategy stating the necessity of developing digital skills (Digital Moldova 2020). There is also an Education Strategy 2020[45]. A complete and holistic overview is lacking in the country, pieces of it can be identified in a variety of separate documents. The Ministry of Labour who is responsible of job needs analysis, doesn't have an overall approach to determine the needs and skills to match the jobs with education.

Although there is a clear understanding of the recognition that a strong digital economy is vital for innovation, growth, jobs and competitiveness, there is no long term clear vision and policies on how exactly to develop digital skills on a nationwide basis. No clear action plan is defined.

[45] ICT industry Training needs report, Moldova Digitala 2020: http://edu.gov.md/ro/strategia-educa-ie-2020/

Only selected references are included in other policy documents, however they are not supported by concrete projects and actions. Some of the project are related to introducing STEM education and developing entrepreneurship skills, but they are mainly either in pilot phases or mainly supported by donors (for e.g. Intel Teach programs, 1 to 1 Computing pilot program, piloting of new curricula for Informatics, Robotics). All the initiatives have a budgetary constraint in being rolled out in education.

Some of the projects are present in Moldova, but there is a low experience in understanding the various EU initiatives, besides there is low level of openness from the side of various educational stakeholders. For example, moves to introduce of MOOCs have took place in 2013, but the Universities from Moldova opposed the process. There is not sufficient cooperation towards joint application with European Countries to various projects. In close cooperation with the educational institutions, insufficient interest and application capacity has been observed over the past 4 years.

No best practice sharing frameworks have been developed and adopted. Entrepreneurship support takes part mainly through private initiatives and donor driven projects. There are exceptions related to schools equipment, but the majority are under the European level of equipping the schools with computers. Only a few schools participate in such pilots as Smart Classroom, Digital Classrooms, School Hubs funded by various donors have the access to Connected Classrooms.

HDM roadmap

As a first step, a “Digital Skills gap” survey is required to bring an understanding of the problem that responsible authorities are faced with. There needs to be a co-ordinated focus on digital skills development and ICT market simulation within an open international IT skills market.

Conditions for the harmonisation

There is strong harmonisation potential across all areas, and some progress has already been made in preparing the policy context. An institutional framework is not in place but the importance of such a policy and cooperation framework is underestimated by the stakeholders. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. There is a lack of understanding of the EU baseline for Digital Skills.

Cooperation between Government and the private sector on these issues, would increase trust and would have long term benefit.

Pilot Projects

It is recommended that Moldova joins a Regional initiative to measure the Digital Skills gap, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap.

The pilot project can be undertaken within the scope of a proposed "National Coalition for Digital Jobs" to be created in Moldova in conjunction with the EU's "Grand Coalition".

2.5.10 Ukraine

State of play and gap analysis

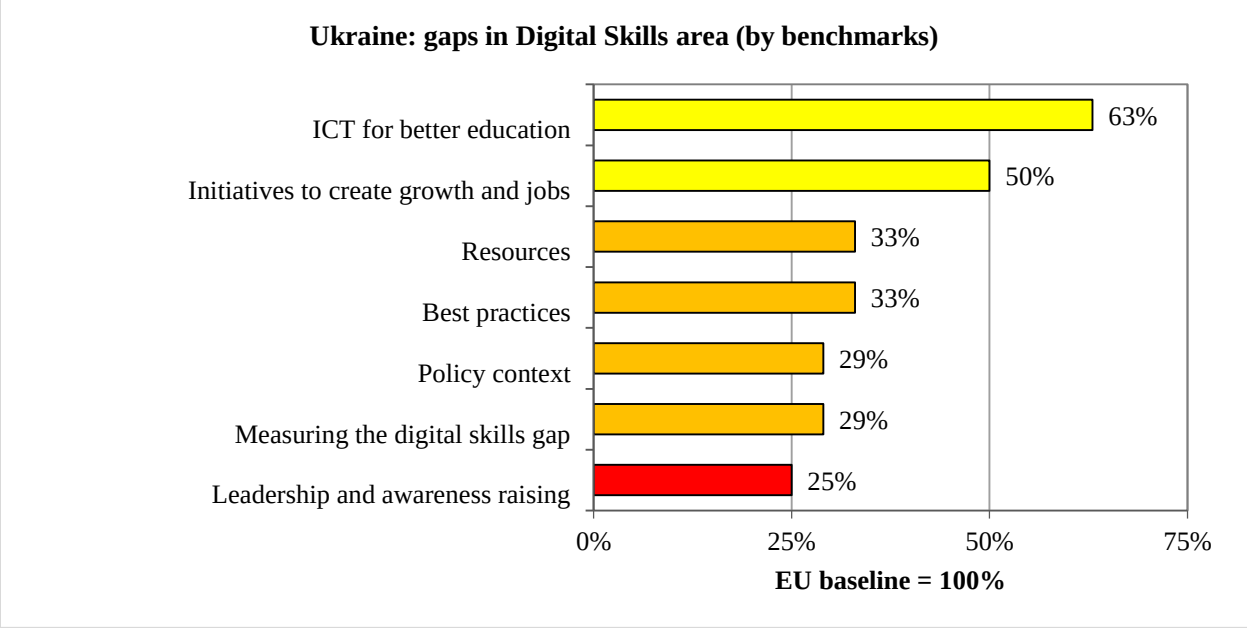

Exhibit 49 - Ukraine: state of play and gap analysis in Digital Skills

There has been no national survey to measure the "Digital Skills gap". There is research concerning the effectiveness of IT Education, the effectiveness of IT graduates training conducted by non-profit organisations and consulting companies. Only partial surveys have been carried out. The Ministry of Economy calculates professional demands forecasts by

industry (IT skills are not highlighted separately), the Ministry of Education provides summary for university graduates, including generalised IT focus. IT skills at state bodies are periodically measured by e-readiness surveys. The IT education/IT skills reports at the current stage are generated primarily by Non-Government Organisations (for example the IT Association) and periodically by international IT companies

The Ministry of Economic Development and Trade in Ukraine (Department of Digital Economy) are working on this issue. Although Ukraine is an active participant of Horizon 2020 and Erasmus+ programs, there is no particular focus on Digital Skills initiatives

There are no Digital Jobs coalitions, only NGOs and independent formations.

Work is in the process of creating a “Digital Agenda for Ukraine”. The initiative is provided by the Ministry of Economic Development and Trade. There are no program/initiatives available on the governmental level. Some selected focuses can be traced through industry programs (for example the Action Plan to Support Programming Products for the software industry – currently under the last stages of review by Ministries. This includes provisions for;

- school IT programs development for 5-11 grades
- demand analysis for selected IT professions graduates
- also, NGOs are running programs for practitioners in limited formats – for testers, outsourcing etc.

Ukraine has low digitally equipped schools and the limited access to the broadband internet. Since 2012 several programs were run to focus on schools digital equipment.

As of 2015, Kiev and large cities have the following:

1) The program “100%” launched by Ministry of Education to promote IT educational programs, ensure availability of computerised equipment and schools access to Internet. The program was planned for 2011-2012, extended and then stopped.

2) The program “Openworld” was launched by the Investment Agency of Ukraine since 2011 aiming at creation of single base of electronic schoolbooks and provision of notebook to each student and electronic boards and equipment to selected schools - as of 2013, 54 schools covered within stage 1, at stage 2 the project was paused.

HDM roadmap

The carrying out of a “Skills Gap” a survey will bring an understanding of the problem that responsible authorities are faced with. But there is a lack of a single identified stream with assigned responsibility defined. Responsibilities are split and coordinated between the Ministry of Social Development, the Ministry of Economics and the Ministry of Education.

There needs to be a co-ordinated focus on digital skills development, IT market simulation, an open international IT skills market, technology boost due to IT skills simulation, but there is no political will, no current action steps are developed with clear political support/ownership.

The IT market would benefit from stimulation, to become an open international market with development of local markets to boost skills and technology due to IT skills simulation. The political benefits would include better satisfaction and trust by citizens due to the social and economic boost.

The obstacles are the lack of a centralised programme with no political will and support. There is a lack of financing for initiatives, lack of internet access in village schools. This needs strong political will (prioritisation) and support.

Conditions for harmonisation

Recently the Ministry of economic development and trade in Ukraine has created the Department of Digital Economy that would be responsible for;

- implementation of a program for the development of broadband internet access;
- standardisation, security and trust to the digital services;
- information society formation;
- e-government and e-administration services - optimising functions of state structures and their full and maximum automation with the use of ICT technologies;
- enhancing of digital skills and setting new learning goals for civil servants.
- program support and development of investment in innovation and start-ups;
- development of e-commerce and online payment methods and procurement;

- development of ICT in different sectors: smart city, health sector etc.

There are clear opportunities to join the EU's "Grand Coalition for Digital Jobs". The rationale is there but not on government initiative – it will come from professional unions, NGOs and IT companies. The likely participants are;

1) IT laboratories in the Universities by CisCO, SAP Ukraine;

2) IT hackathons and competitions for schools/universities/IT specialists

3) IT open universities (http://brainacad.com/ and other)

4) NGOs and companies participation in school and university IT programs review

The Digital Agenda highlights were announced on April, 2 2015 at the new Department presentation – the detailed plan is currently being developed.

There is strong harmonisation potential across all areas, building on the progress already made in the areas of policy, leadership and ICT for better education.

Pilot Projects

It is recommended that Ukraine joins a Regional initiative to measure the Digital Skills gap, using a pilot framework for the initial measurement and working together with the other countries and the EU to finalise a common methodology for further measurement and monitoring of the national Digital Skills gap.

The pilot project can be undertaken within the scope of a proposed "National Coalition for Digital Jobs" to be created in Ukraine in conjunction with the EU's "Grand Coalition".

2.6 Telecom Rules

2.6.1 EU baseline

The EU Baseline for "Telecoms Rules" consists of a number of benchmarks derived from the legal and regulatory framework for electronic communications. The key documents in that framework are;

Framework Directive (based on 2002/21/EC and the Better Regulation Directive 2009/140/EC)

- Regulator independence and structure - separation of policy, regulatory and operational functions, operation of the regulator – transparency of decisions, adequate financial and human resources, clear procedures for public consultation for new regulatory measures and mechanisms to appeal regulatory decisions.
- Clear procedures for the identification, definition and analysis of relevant markets that are subject to ex-ante regulation in order to determine SMP;
- Rights of way: simple, efficient, transparent procedures, applied without discrimination or delay

Authorisation Directive (based on 2002/20/EC and the Better Regulation Directive 2009/140/EC)

- A general authorisation procedure with simple notification for market participants and restricting the need for individual licences to specific, objectively justified cases

Access Directive (based on 2002/19/EC and the Better Regulation Directive 2009/140/EC)

- For operators found to have SMP under the market analysis procedures carried out in accordance with the framework directive, the regulator shall impose proportionate regulatory obligations with regard to:
    - access to, and use of, specific network facilities
    - price controls on access and interconnection charges, including obligations for cost orientation
    - transparency, non-discrimination and accounting separation

Universal Service Directive (based 2002/22/EC and the Citizens' Rights Directive 2009/136/EC)

- A defined policy and clear regulation on universal service obligations, including the establishment of mechanisms for costing and financing
- Mechanisms for ensuring users' interests and rights, in particular by introducing number portability and the single European Emergency Call number 112
- Effective measures for ensuring quality of service in a broadband environment.

Directive on Privacy and Electronic Communications (based on 2002/58/EC, the Amending Directive 2006/24/EC and the Citizens' Rights Directive 2009/136/EC)

- Implemented regulation to ensure protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and for free movement of electronic communication equipment and services

Radio Spectrum Decision 676/2002/EC46 and the 2012 Radio Spectrum Policy Programme

- Adopt a policy and regulations ensuring the harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources

Commission recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment (9/2013)

- Adopt measures to increase effectiveness of broadband competition and for enhancing investment in infrastructure for high speed broadband services.

Leadership, policy, strategy and resources

The benchmarks derived from the EU baseline legal framework include

- Separation of policy, regulatory and operational functions in the electronic communications sector
- Requirement for transparency and public consultation before introducing new policy or regulatory measures
- Clear, competitively neutral policy for the provision of a defined set of services to any person requesting it, including internet access at affordable prices
- Commission Recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment: Clear policy towards increased effectiveness of broadband competition and for enhancing investment in infrastructure for high speed broadband services
- Radio Spectrum Policy Programme: Clear policy and regulations ensuring the

[46] DECISION No 676/2002/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0676&from=EN

harmonised availability and efficient use of spectrum, taking account of the market needs and the optimal use of scarce resources

- Clear mandate for the regulator to protect users' rights and freedoms
- Clear procedures for the identification, definition and analysis of relevant markets that are subject to ex-ante regulation in order to determine SMP
- Rights of way: simple, efficient, transparent procedures, applied without discrimination or delay
- A general authorisation procedure with simple notification for market participants and restricting the need for individual licences to specific, objectively justified cases
- Adequate human and financial resources to carry out effective independent regulatory function
- Commission Recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment: To encourage access by investors to sources of capital for investment in broadband infrastructure

Implementation and Infrastructures

The benchmarks derived from the EU baseline legal framework include

- Clear mechanisms to appeal regulatory decisions
- For operators found to have SMP under the market analysis procedures carried out in accordance with the Framework Directive, the regulator shall impose proportionate regulatory obligations with regard to:
    - access to, and use of, specific network facilities
    - price controls on access and interconnection charges, including obligations for cost orientation
    - transparency, non-discrimination and accounting separation
- Introduction of number portability and the single European Emergency Call number 112
- Effective measures for ensuring quality of service in a broadband environment.
- Commission Recommendation on the Regulatory Treatment of Fixed and Mobile

Termination Rates in the EU.

- Commission recommendation on Broadband Investment: Clear date for adoption into legal and regulatory framework
- "Digital Agenda" targets: Clearly defined targets for achievement of universal fast broadband access and take-up

Services

The benchmarks derived from the EU baseline legal framework include

- Penetration (take-up) of fixed broadband services: Actual achievement (latest results)
- Penetration (take-up) of mobile broadband services: Actual achievement (latest results)

Best practice example

Broadband acceleration in Slovenia[47]

Slovenia became a member state of the EU in 2004 and. The EU's "Digital Agenda" sets a target of 100% access to high-speed broadband by 2020.

The Slovenia government recognised the importance of broadband in the "*Resolution on National Development Projects for the Period 2007-2023"* adopted in 2006. The resolution contained a national broadband plan for Slovenia. Although broadband penetration was relatively high (67% in 2011) and DSL coverage in terms of households was not far behind the EU average (90% nationally against an average of 96% across the EU), rural penetration was only 60% compared with 78% across the EU. The plan involved accelerated construction of broadband networks in less developed areas particularly in rural areas, connecting these areas to a national backbone and upgrading the existing fixed broadband network with fixed or wireless broadband networks, depending on economic justification.

The Slovenian broadband goals included:

[47] From EC 2010 report "The socio-economic impact of bandwidth" http://ec.europa.eu/digital-agenda/en/news/study-socio-economic-impact-bandwidth-smart-20100033

- Sustainable increase in the wellbeing and quality of life of all people
- Increased global competitiveness by promoting innovation and entrepreneurship, expending the use of information and communication s technology and efficient upgrading and investment in learning, education, training, research and development
- Faster development for all regions and a “closing the gap” for the least developed regions

Municipalities play an important role in broadband development in Slovenia. They identify local needs, encourage citizens to engage with the technology, balance interests and ensure that local development programmes are aligned with regional and national development plans.

Slovenia allocated EUR 82 million of public funding (including monies from European Structural Funds, The Republic of Slovenia and public private sector partnerships) to accelerate the deployment of broadband networks access across the country.

2.6.2 Overview of the state of play and gap analysis for the Region

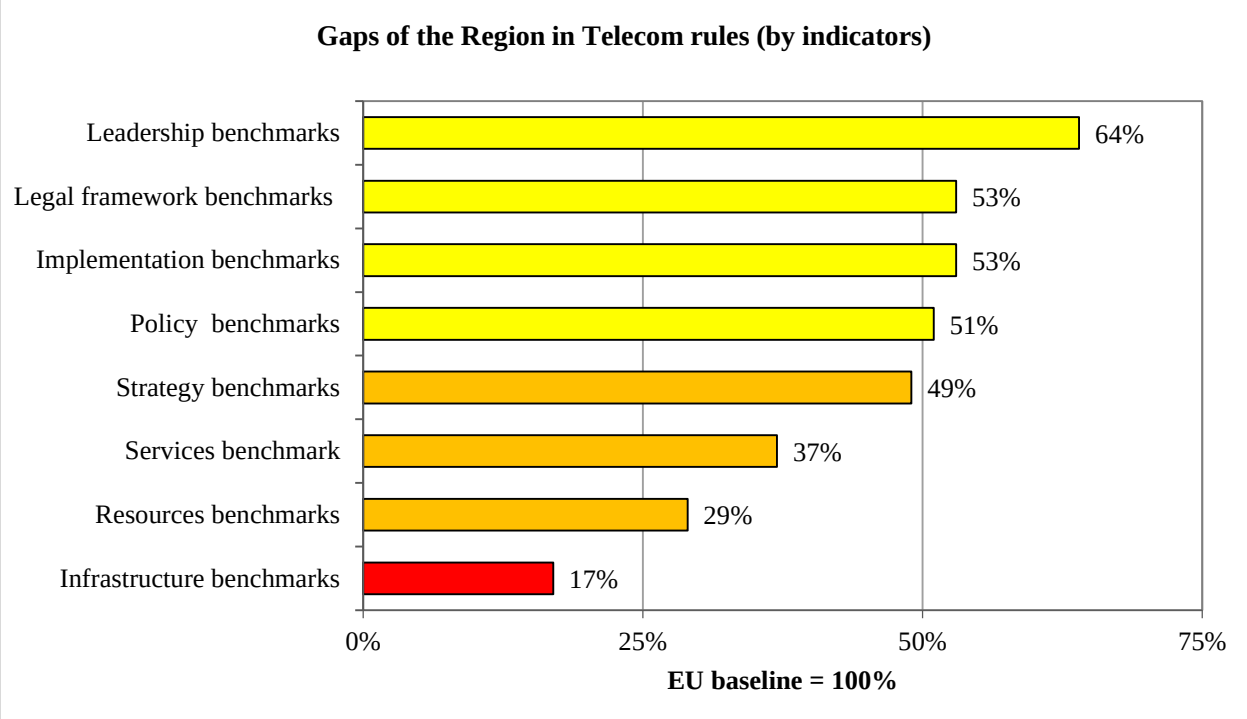

Exhibit 50 - State of play and gaps of the Region in Telecom rules (by indicators)

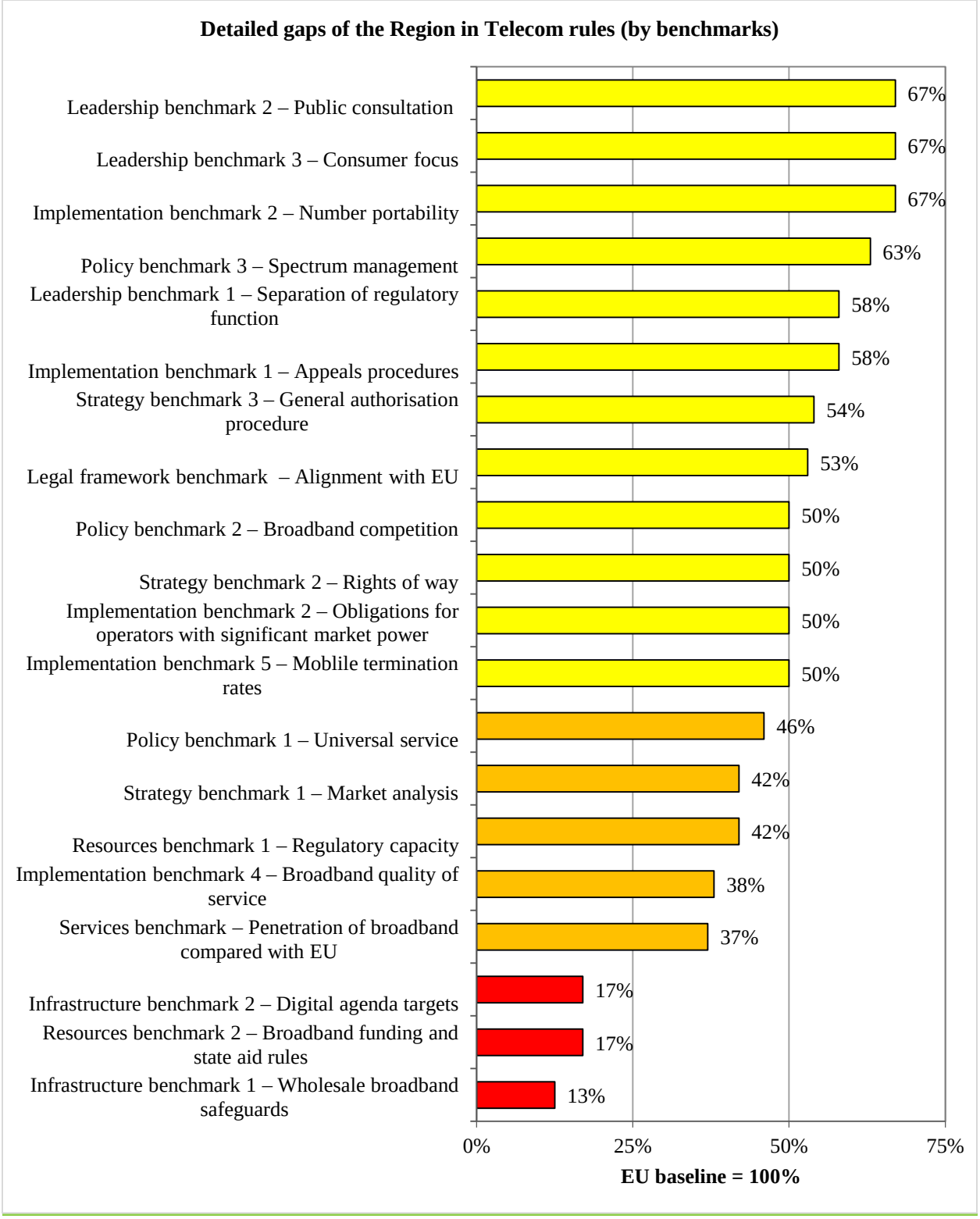

Exhibit 51-State of play and detailed gaps of the Region in Telecom rules (by benchmarks)

2.6.3 Overview of common actions for the Region

For Telecom Rules, the main finding is that there are significant gaps in access and take up of broadband services between the Region and the EU, particularly in rural areas. There is no consistent policy for universal access to high speed broadband across the Region. By harmonising with a "Digital Agenda" policy for universal access to high-speed broadband (>30 Mbps), the Region could benefit from an accelerated removal of the large digital divide between the urban and rural areas.

There are currently widely different approaches to infrastructure investment across the region. In Azerbaijan and Belarus this investment is largely state-funded, and there remain significant barriers to alternative investment, limiting the roll-out of competitive broadband services. In the other countries where investments are left largely to the competitive market, there is insufficient high-speed broadband infrastructure in rural areas. By harmonising the policy and regulatory frameworks for Telecom Rules with the EU, these significant gaps could be closed faster, enabling much greater access and take up broadband services. Faster investment in infrastructure across the Region, giving better access to high-speed broadband, is an essential pre-requisite for the overall harmonisation of digital markets.

At the moment the major challenge is extending next generation networks and high-speed broadband access out to rural areas. Although there are clear benefits to this modern technology investment, the full impact is not being realised for two reasons. The first is that in the countries with no state-aid funding in place to accelerate investment, it not yet clear whether private operators will be sufficiently incentivised to expand their networks. The second is that in the countries where investment is state-led, there are insufficient competitive safeguards to promote alternative investments. This is the case in Azerbaijan and Belarus, where good progress has been made in bringing broadband infrastructure to rural areas, but there are no state-aid rules to ensure open wholesale access to these networks guaranteeing competition and consumer choice at the retail level.

There is currently no clear policy in Armenia, Georgia, Moldova or Ukraine for state participation in the sector to accelerate infrastructure investment out to rural areas. If such an approach was

taken with state ownership or operational control over networks, then there would need to be strong regulation, for example to ensure that a wholesale-only open access network model was used, which would safeguard competition in the retail broadband market. The necessary requirements of the EU baseline with respect to broadband infrastructure investments are largely missing from all countries.

The benefits of the EU baseline approach would be a more cost effective (shared infrastructure) model for retail operators, reducing their costs and risks. The networks could therefore be extended faster and to more rural areas, giving access to many more of the Region's citizens to the information society in the future. The non-discrimination and other obligations for access to next generation networks need to be defined based on the EU baseline, which specifies an "equivalence of inputs" principle, tests of technical replicability of the new retail offer, development of BU LRIC+ costing models for access services and monitoring requirements for service level agreements between the wholesale provider and the access seeker. There is a risk that any new regulations for the next generation access era will not be effectively implemented by the incumbent operator, based on the experience from the regulation of access for legacy technologies.

Spectrum management policy should also emphasise an economic and social approach with regard to the allocation and use of spectrum with particular focus on ensuring greater spectrum efficiency, better frequency planning and safeguards against anti-competitive behaviour plus the creation of opportunities for innovation and employment creation, economic growth and social integration.

Other specific aspects that should be included in spectrum policy are the need for international coordination in particular with regard to the reduction of international roaming charges. Under the EU baseline, regulators should be explicitly allowed to take appropriate ex-ante or ex-post regulatory measures such as;

- action to amend existing rights, to prohibit certain acquisitions of rights of use of spectrum, to impose conditions on spectrum hoarding
- to limit the amount of spectrum available for each undertaking, or to avoid excessive accumulation of rights of use of spectrum
- to avoid distortions of competition in line with the principles for public pan-European cellular digital land-based mobile communications

There may still be obstacles to alternative operators when applying for rights of way to install networks on public and private property. At minimum this causes unnecessary delay and at worst, it is discriminatory behaviour and favours the incumbent in a competitive market. The procedures must be simplified and made transparent.

2.6.4 Benefits for and readiness analysis of the Region

For Telecom Rules, the largest gap is in the lack of policies and regulatory enablers for investment in infrastructure for universal access to high-speed broadband access. The investment gap is particularly large in rural areas, prolonging a significant digital divide. This is the single most pressing barrier to the harmonisation of digital markets.

For Telecoms Rules, the policy and regulatory framework for the promotion of investment in high-speed broadband infrastructure using the EU baseline is already being initiated in Georgia and could be commenced elsewhere. First and foremost, an adoption of a Regional policy for universal high-speed broadband access within a defined timescale should be achievable. The divergent policy approaches currently being used across the Region, could be aligned in a universal model, using the experience from the EU baseline, where both private and state-aided investments already play a vital role in achieving universal high-speed broadband access. At the policy level, this could be commenced immediately, together with the necessary detailed work on the alignment of telecom rules within national legal and regulatory frameworks.

A large benefit to the Region could be achieved by closing the significant gap in access to high-speed broadband services. In 2013, the average take up of fixed broadband services in the Region was 12.7 per 100 population, compared to EU average penetration of 30 per 100 population. For mobile broadband the gap is even wider, at 20.6 per 100 population in the Region compared to 61 per 100 population in the EU. Accelerated investments are required to close this “broadband gap”. By adopting harmonised policy and regulatory enablers to investment, the region could close the gap over a 5 to 10 year period. Using established empirical evidence[48], the potential for macro-economic gain from increased broadband take-up

[48] Sources: Katz 2010; Analysys Mason 2010; McKinsey 2010; Qiang & Rossotto 2009; and Czernich et al. 2009. See also ITU publication “The Impact of Broadband on the Economy: Research to Date and

across the region could be between €4.3Bn and €6.4Bn per annum. Further economic benefits could be achieved by adopting a harmonised approach to spectrum exploitation, particularly in the use of the "digital dividend" spectrum for broadband services.

2.6.5 Armenia

State of play and gap analysis

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – "Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572."

The Law on Electronic communications was adopted in 2005. The 2003 EU regulatory framework was taken into account during the preparation of Law of Armenia "On Electronic Communications" and in other legislation. In certain aspects, it meets the criteria set out by the EU regulatory frameworks, although in many cases only partially. Such is the case of interconnection and access regime, tariff regulation, market analysis, consumer protection, spectrum management, interconnection disputes etc.

Commission (PSRC) is the regulatory agency. No changes to the legislation on this aspect are expected after Armenia's integration to Eurasian Economic Union. MTC conducts public consultations with PSRC and with other state agencies and stakeholders from the business domain.. The invitations and drafts to the board members are sent a week prior to the voting and information about draft regulation is placed on PSRCS's website. Media representatives are invited to the voting as well. The decrees issued by the regulator PSRC carry legal enforcement. Any new regulations are adopted by the voting of the PSRC board. However, the PSRC as an institution is not defined in the Constitution. The Law on PSRC defines the procedure to file for a review to PSRC, which have to be answered within one month. After this the decision of the regulator can be appealed at the court. However, appeals against the tariff rates for public services may not be accepted by the courts.

Policy Issues April 2012" https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf

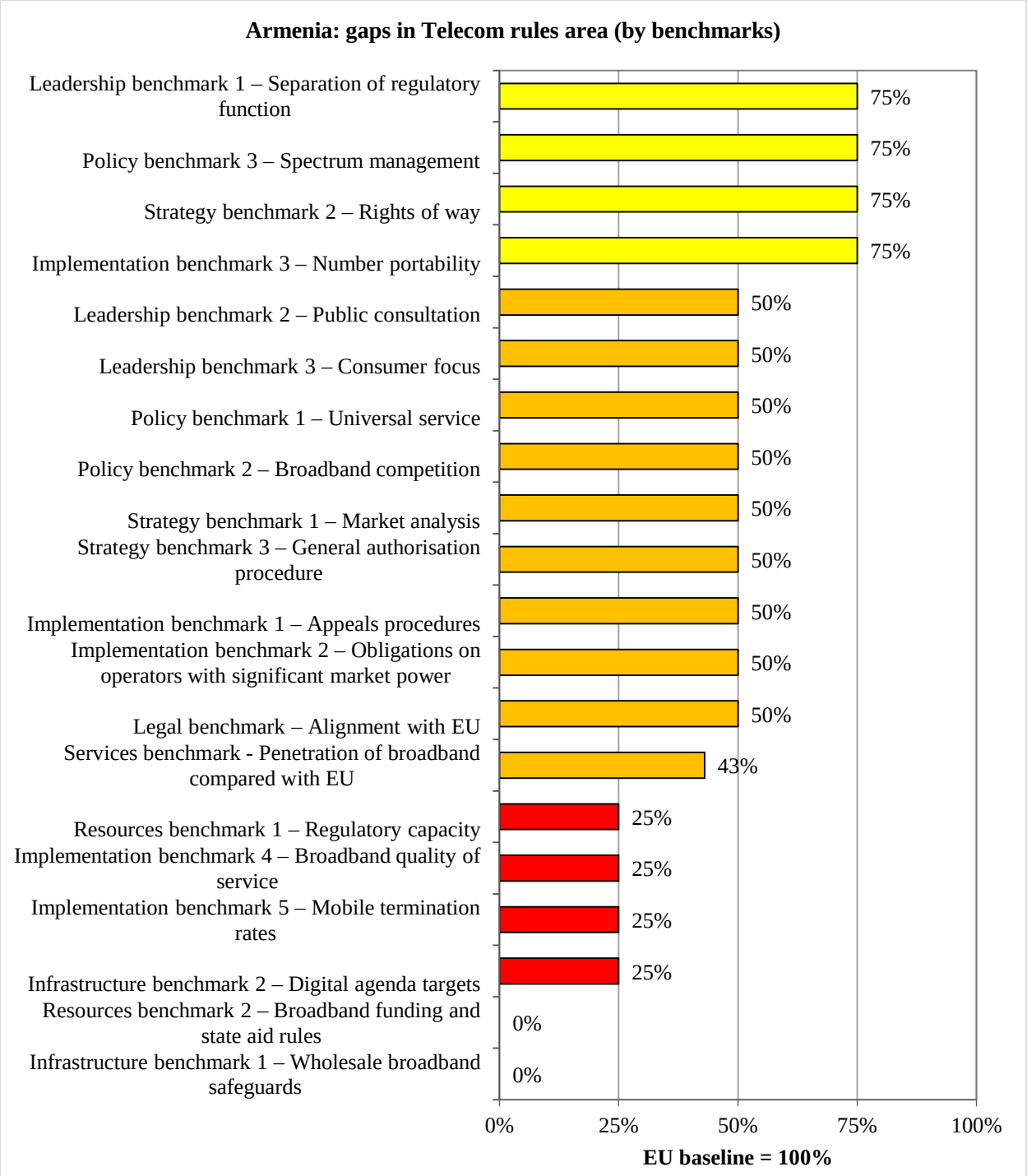

Exhibit 52- Armenia: state of play and gap analysis in Telecom rules

The functions in the telecom sector are clearly defined by the Law. The Ministry of Transport and Communication (MTC) is the policy making and the Public Services Regulatory

The Law on Electronic Communications defines the scope of consumer rights in the sector. It includes the right of access to electronic communications, the right to receive clear information and the right to a contract with all specifications regarding the service provided. Emergency services numbers are accessible free of charge. Public access to services is ensured by internet access points in postal offices throughout the country. A few minor initiatives are undertaken to enable access for disabled users, however this area is underdeveloped.

Fixed line penetration remains low (19 per 100 population) and the main operator has a number of service provision obligations defined in its licence. However, it is claimed that in current market, there is no need in a universal service operator. There do not appear to be any provisions implemented for disabled persons or for basic internet access.

There is no dedicated policy for the attraction and promotion of investments into the sector with any established formats of support, only a few local initiatives for separate areas of ICT. The mobile broadband sector is well developed in Armenia with 99% of coverage of 3G, but fixed broadband currently has low penetration. At the moment, the market is not seen to have enough potential to justify additional broadband investment.

The methodology and main principles of the spectrum management are defined in the Law on Electronic Communications, in a Decree by the Minister of the Transport and Communication, and by the Law on Television and Radio. The spectrum distribution table is based on ITU methodology. The distribution is done based on the market needs and following national priorities.

The PSRC is responsible for ex-ante regulation however the Commission for the Protection of Competition (SCPEC) defines how to identify relevant markets. For the electronic communications sector market regulation, PSRC has a list and definitions of the markets to be regulated which is broadly consistent with the EU baseline. In identification of significant market power, PSRC consults with SCPEC. The procedures to analyse markets are based on simple market share and not on the full set of criteria defined in the EU baseline. Full market reviews of all listed markets have not been carried out and public consultations are rarely initiated through the PSRC website. The Regulator has all necessary provisions to impose obligations on operators with significant market power, but the full requirements for transparency, non-discrimination and cost orientation that are defined in the EU baseline ore not in place.

The legal framework for the rights of the way is in place and operating. In some cases the procedures may be problematic or inefficient in regard to the required time, however, the requests are fulfilled most of the time. The rights of way are defined and enforced by different laws, regulations, decrees by the Office of the Mayor, Ministry of Culture and others. There appear to be no common procedures or “one stop shop” approaches.

If an operator wants to build a network it is required to apply for a complex licence, which has to be issued by PSRC and so a decision is still required by the regulator before market entry, unlike in the EU baseline. Numbering and spectrum resources are available upon allowance by the Regulator. PSRC. Service delivery in the electronic communications sector is no longer licensed. There is a simple notification procedure defined for the new entrants in the market, if they do not require spectrum or numbering ability.

The public services regulator PSRC receives funding via the state, which collects fees only from defined entities from across 18 public sector activities, including one telecommunications company. The mechanisms of funding of the PSRC are transparent and defined clearly. The budget of PSRC is subject to the same restrictions and conditions as other state entities. The regulatory unit for the electronic communications is a small unit within PSRC, whose resources are not matched to the sector as a whole. In comparison to the equivalent organisations required to regulate the EU baseline, the PSRC telecommunications division is significantly understaffed.

There are no formal structures or institutional programs to support investment into broadband infrastructure and no state-aid rules.

Mobile number portability is in place, but it is not actively promoted by the regulator and there are discriminatory provisions on customers regarding the number of portings that can be made. The portability fixed phone numbers is not available with no timescale defined for its implementation.

The single European emergency number has been introduced. According to a PSRC decree, an operator is obliged to publish any limitations of the connection on its website. A government decree on internet management refers to the regulation in the area of net-neutrality. However, the Ministry of Transport and Communication has not initiated legislative change based on the decree and there are no regulations or decrees applied by PSRC in this area.

The price for wholesale mobile call termination is set by the regulator PSRC in co-operation with the mobile operators. No calculations are done by the LRIC methodology as required in the EU baseline. Instead it has been done mainly by a benchmarking in comparison with Europe, Georgia and Moldova.

HDM roadmap

There remain significant differences at a detailed level with the EU acquis, especially in the areas of sufficiency of regulatory resources, complete transparency and user orientation. The ex-ante approach to improving competitive markets and consumer choice of services is not aligned at the detailed level, nor are the removal of entry and investment barriers and the implementation of competitive market safeguards for investors. Many of the specific enablers to broadband infrastructure investment are absent, including transparency and cost-orientation of equivalent wholesale offerings to alternative operators, infrastructure sharing and co-ordination of civil works across public infrastructure sectors, rights of way and access to building infrastructures. There are no state-aid rules in place to accelerate broadband investments, make high-speed broadband available in rural areas and to ensure competition for those services.

Spectrum policies and management, although implementing effective services, are not fully aligned with the more liberalised market mechanisms employed in the EU.

The various regulations adopted by the sector regulator and elsewhere regarding the electronic communications sector will require a thorough examination to determine consistency with the EU legal and regulatory framework for the sector. More promotion of competitive market choices is required by the regulator, particularly in presenting clear information to consumers to assist them in making more informed and independent choices between different services and providers in terms of geographical availability, quality and price. Of particular value would be a review of the regulations that relate to consumer rights and freedoms, and also of those regulations dealing with the removal of investment barriers and the provision of competitive market safeguards.

Conditions for harmonisation

There is a clear perception that the promotion of competition and investment in broadband is not necessary at the current stage of market development. The Ministry of Transport and

Communication has a strategy in the sector of electronic communications overall, however no special targets are determined for the broadband sector separately. The strategy is to leave the sector to market forces.

The EU baseline recognises that market forces alone will not achieve universal high-speed broadband access within the desired timescale, as set by the “Digital Agenda 2020” target for universal access to high-speed (>30Mbps) broadband everywhere by 2020. The EU Baseline therefore defines specific enablers to Next Generation investments and competition which are absent in Armenia.

There are no targets defined and there is the opinion that there is no need to set and pursue targets in this particular stage of development for Armenia’s broadband sector. The achievement of universal broadband access is not therefore a target. It is expected that full market coverage will be reached by the competitive market acting without special high-speed broadband policies and targets. However, fixed and mobile broadband penetration are currently well below the EU averages.

The reported penetration of broadband services for 2013 was;

Armenia fixed broadband penetration	7.88 per 100 population (EU 30 per 100)
Armenia mobile broadband penetration	31.1 per 100 population (EU 61 per 100)

For Armenia, this represents an added potential of +22 per 100 population if Armenia reached the existing EU average level. Under this hypothetical situation, the added GDP potential to the Armenian economy is between €175m and €260m per annum. This takes into account only fixed broadband penetration. Harmonisation of spectrum exploitation would bring further economic benefits.

Pilot Projects

It is recommended that Armenia joins a Regional initiative to harmonise policy with the EU on universal high-speed broadband access. The objective is to install a firm policy commitment for the region and within each country for universal high-speed broadband access. This policy

should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, Armenia should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

2.6.6 Azerbaijan

State of play and gap analysis

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – "Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572."

The Electronic communication law was introduced in 2005. The 2003 EU regulatory framework was partly considered in the regulatory legislation. Under the current ongoing State Programme on alignment of Azerbaijani legislation with EU legislation, certain normative acts are being reconsidered while taking into account the EU regulatory framework. The ministry (MCHT) executes the policy making and regulatory functions for the sector. The Department of Regulation created within the Ministry functions with 10 people, financed from the centralised budget of MCHT.

At the moment there are no ex-ante market review procedures in place that align to the EU baseline. All operators function in the market is on the basis of licence, excluding internet service providers. However, no restriction exists for obtaining the licence and the procedures have been simplified. One-off and annual fees are applied for allocation of scarce resources.

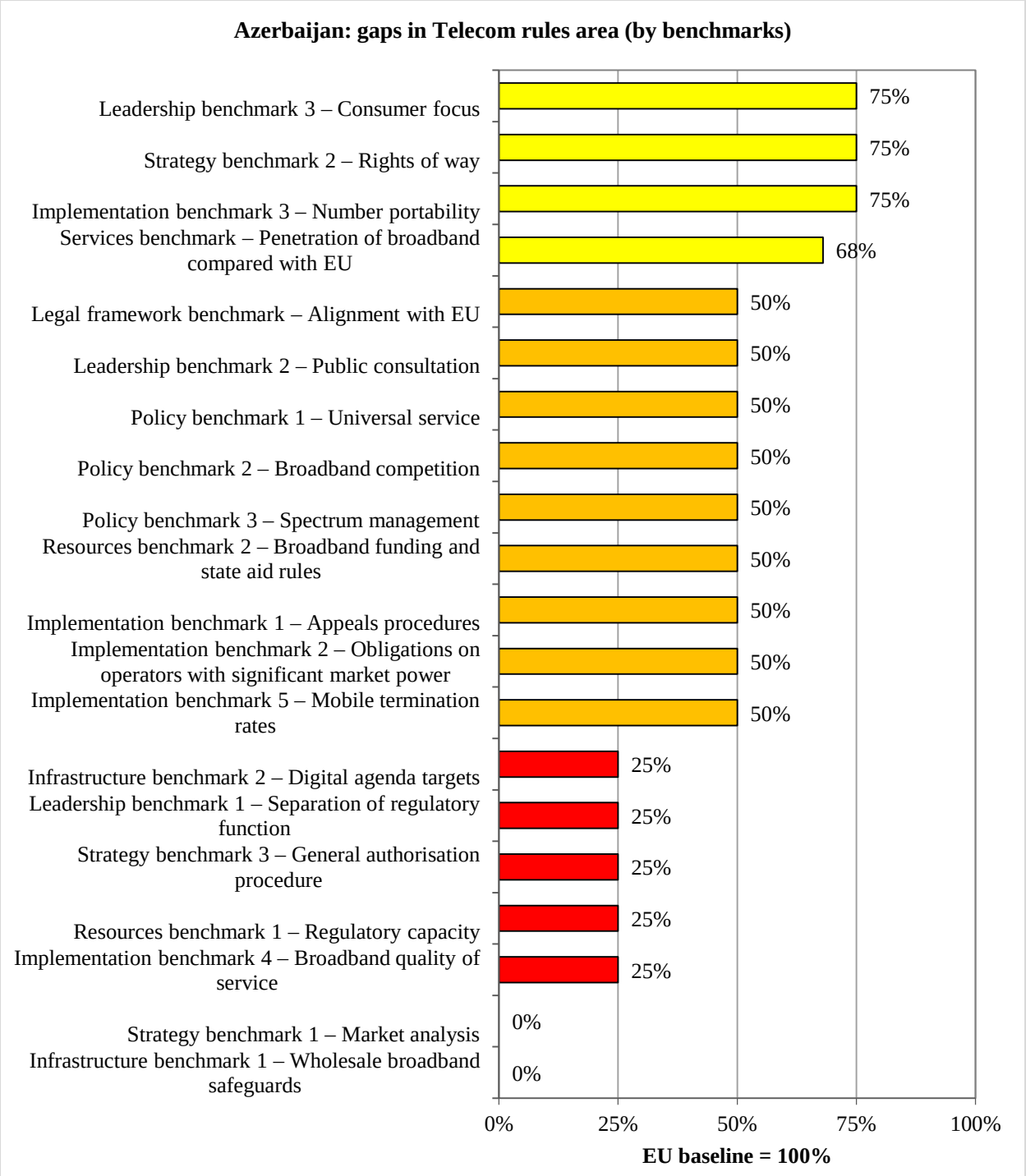

Exhibit 53- Azerbaijan: state of play and gap analysis in Telecom rules

Access to public or private property to build and operate the telecom infrastructure is carried out on the basis of agreement between two parties. The timeframe for obtaining right-of-way permit from private and public property owners is one month.

The State itself invests in the development of broadband infrastructure. The State Fund for Development of Information Technologies was established under the MCHT. The Fund's activities are:

- Term investments with the acquisition of equity participation and shares in the authorised capital of legal entities operating in the ICT field;
- Financing of business entities operating in the field of ICT by granting low-interest loans through authorised banks and non-bank credit institutions;
- Grant financing of innovative and applied scientific and technical projects (start-ups)

The "Fibre to Home" project, seeks to provide high-speed and high-quality broadband internet services in 2013-2015 and in subsequent years. The project includes various aspects of telecommunications networks, including the laying of fibre lines to out-settlements and telephone cabinets in the backbone network, to upgrade switching and transmission facilities, installation of telephones in residential areas that have no telephones, many-storied buildings, settlements partly provided with telephones with the introduction of cutting-edge technologies, implementing structural and tariff reforms and improving the regulatory issues.

Within the framework of the project by 2015 and in future period, Baku residents are to be provided with broadband access at speeds of 100 Mbps. In other major cities and district centres the figure is 30 Mbps, in settlements and rural areas - 10 Mbps. In 2013, the State Oil Fund allocated AZN 103.6m (€115m) for financing the first phase of the project.

Although this project provides fibre to the home infrastructure, it does not appear to give competitive retail broadband services. Operators are generally unwilling to give access to their network elements and infrastructure and there are not any open access regulations implemented to ensure competition.

The national frequency plan and the assignment of radio frequencies are set by the State Commission on Radiofrequencies of the Republic of Azerbaijan. In general, frequency assignment is implemented on a “first come first serve” basis.

Besides the law “On Telecommunications”, the interrelations between operators/ service providers are regulated by the Rules “On usage of public communication networks”, the Laws “On Anti-Monopoly” and “On Unfair Competition” that envisage an equal access to and use of public networks and facilities. The operators independently set the prices and charges. However in case of rise of dispute on this matter, the Ministry may intervene.

Mobile number portability has been provided since 2014. Porting takes typically 10 days, significantly longer than the EU baseline requirement of 1 day. Emergency call number 112 is available nationwide but it covers only the Ministry of Emergency Situations.

Internet service providers are not required to have a licence to operate in the market. At the same time the quality of service standard is implied through the “Obligations on organisation and provision of universal telecommunication services”, but this makes no specific references to the added complexities involved in regulating broadband quality of service.

Measures have been adopted to impose price control and cost-accounting for wholesale voice call termination both for fixed and mobile services. These measures require the use of “best practice methodology”. In practice, charges are not based on LRIC models defined in the EU baseline.

HDM roadmap

The Ministry of Communication and High Technology (MCHT) is preparing draft amendments to the existing Law “On telecommunications” with the aim of aligning it with the 2009 EU regulatory framework. More specifically, the areas of market analysis, spectrum management, universal service, consumer protection and clear division of policy making and regulatory issues should be undergoing the alignment process. Laws with regards to other EU regulatory frameworks (such as on e-commerce, e-signature, data protection etc.) are already adopted and applied.

A “National Programme on legal approximation of the legislation of the Republic of Azerbaijan with the EU Acquis” it is stated that the Law “On Telecommunications” 2005 must be supplemented and amended for the purposes of implementation of the following provisions:

- Liberalisation of communication services;

- The abolition of all special or exclusive rights or licenses granted to operators for the importation, marketing, connection, bringing into service of telecommunication terminal equipment and/or marketing of such equipment already granted to public or private bodies;
- Determination of the rights of all economic operators to import, market, connect, bring into service and maintain terminal equipment;
- The guarantee of an easy access to terminal points and publication of their physical, commercial and economic conditions and characteristics;
- The regulations pertaining to all technical specifications and type-approval procedures used for terminal equipment must be easily accessible;
- To define SMP in specific telecommunication markets using the market share basis or the operator's control of market behaviour;
- To encourage competition through stimulating the development of communication services and networks as well as by means of consultation authorities, auditions, regulatory powers and competition surveys of the NRA.
- Provide for competitive offering of Internet services and not restrict the free movement of conditional access devices;
- Provide for a competitive, open, objective, non-discriminatory and transparent legal framework to ensure the conditions for the effective use and availability of the radio spectrum;
- Provide that licenses for provision of mobile services grant a set of rights and obligations to operators and the obligations of incumbents to share site, antenna and cable with new operators in the market;
- Protect health against radio frequency, along with safety and security of transmissions;
- Provide competitive bidding procedures for third generation services (UMTS) and allocation of radio and wireless communication frequencies.
- To ensure equal opportunities for new operators providing services to the consumers to access telecommunication market;

- Adoption of rules on Standard Conditions of Interconnection and Use of Networks;
- To enable the National Regulatory Authorities (NRA) to act, among other things, by imposing special obligations on operators, who retain a Significant Market Power (SMP);
- To enhance transparency in relation to interconnection and/or access;
- To enforce a series of obligations:
    - of non-discrimination to ensure that operators apply equivalent conditions in equivalent circumstances to undertakings providing equivalent services,
    - regarding unbundling local loop,
    - of accounting separation in relation to specified activities concerning interconnection and/or access,
    - of access to, and use of, specific network facilities,
    - relating to cost recovery and price controls,
    - for cost orientation of prices,
    - concerning cost accounting systems;
- To ensure that no minimum requirement on interconnection points can be established, nor discrimination in interconnection charges between facility-based operators and simple resellers.
- Measures regarding state-aid and competition.
- Provide that licenses for provision of mobile services grant a set of rights and obligations to operators and the obligations of incumbents to share site, antenna and cable with new operators in the market;
- Protect health against radio frequency, along with safety and security of transmissions;
- Provide competitive bidding procedures for third generation services (Universal Mobile Telecommunication System- UMTS) and allocation of radio and wireless communication frequencies.
- Provisions regarding the directory enquiry services and directories;
- The accessibility of pay phones to disabled users or the quality of services;

- Special measures for disabled users;
- Determination of the price or tariff caps or common tariffs for services provided by undertakings having universal service obligations throughout the territory of the republic;
- determination of the economic indicators for telecommunication operators and providers carrying out universal service obligations and control over their observing such indicators;
- Establishment of the compensation mechanisms for costs incurred by operators in provision of universal service obligations;
- Establishment of a mechanism for compensation from governmental and non-governmental funds and/or a mechanism for sharing costs between providers of electronic communication networks and services (obligatory payment of telecommunication operators and providers to universal telecommunication services (fund));
- Separate accountings of such services need to be introduced.

The National Programme document also states that, for the specific assessment on reform, the legal review should include protection of privacy and consumer protection, provision of easy access by service providers, consumers and other interested parties to any information regarding rights, conditions, procedures, charges, fees and decisions concerning the market. The Programme also defines sector-specific regulations need to be enacted in the relevant fields of Telecommunications legislation, including;

- An Independent Privacy Authority needs to be established in order to determine the principles and obligations for the use of data and protection of confidentiality of communications.
- The Law of the Republic of Azerbaijan “On Telecommunications” No 927-IIQ of 14 June 2005 needs to be supplemented with more specific provisions regarding data retrieval and use of consumers’ information, including obligations of the specific operators as regards processing of data, authorisation requirements, storage of information, etc.
- Introduction of the specific provisions prohibiting listening, tapping and storage of

communications by persons other than users without their respective consents.

- Specific provisions discouraging unsolicited electronic messages ("spamming") and cookies (hidden information exchanged between an Internet user and a web server and stored in a file of the user's hard disk). This also applies to SMS and MMS services, as well as other electronic messages received on any fixed or mobile terminal.

The various regulations adopted by the sector regulator and elsewhere regarding the electronic communications sector will require a thorough examination to determine consistency with the EU legal and regulatory framework for the sector. More promotion of competitive market choices is required by the regulator, particularly in presenting clear information to consumers to assist them in making more informed and independent choices between different services and providers in terms of geographical availability, quality and price. Of particular value would be a review of the regulations that relate to market analysis, determination of significant market power and obligations for non-discriminatory and cost-oriented access to network elements and infrastructure. New regulations will be required to promote broadband competition and investment.

Conditions for harmonisation

The "National Programme on legal approximation of the legislation of the Republic of Azerbaijan with the EU Acquis" includes telecommunications and one of the fields to be covered for legal approximation. This document was approved by the Decree of the President of the Republic of Azerbaijan in 2007. However, many of the provisions in the telecommunications area have not yet been aligned and no clear date has been set for completion of the legal approximation work. There should be amendments to the main normative documents for the gradual establishment of a National Regulatory Authority (NRA) politically and budgetary independent from the political power.

These amendments, when implemented will align regulations to the EU baseline. The need to adopt more market oriented spectrum management procedures will become a priority as the usage of frequency spectrum, particularly with broadband services will grow significantly over the coming years.

Regulation of electronic communications markets continues to be carried out by a small department within the MCIT, which has overall responsibility for the sector. The focus of the regulation has been traditionally towards retail price maintenance, basic universal services and interconnection rules.

At present the Ministry of Communications and High Technologies (MCHT) holds the functions of policy making and regulation in the telecommunication sector. It has now been decided to establish an independent regulatory body. For this purpose the Department of Regulation has been created in the Ministry as a first step towards the establishing of separate agency.

Aztelekom and Baktelekom, two state-owned telecom operators are currently on the process of privatisation, but no clear timescale has been set.

The National Strategy for “Development of Information Society in Azerbaijan for 2014-2020” defines some general targets:

- Development of high-quality broadband infrastructure;
- Adding of broadband internet to the list of universal services
- All schools to be connected to broadband internet

These targets are not specific in the coverage, specification and timing of universal high-speed broadband access.

The reported penetration of broadband services for 2013 was

- Azerbaijan fixed broadband penetration - 17.0 per 100 population (EU 30 per 100)
- Azerbaijan mobile broadband penetration - 45.1 per 100 population (EU 61 per 100)

For Azerbaijan, this represents an added potential of +13 per 100 population if Azerbaijan reached the existing EU average level. Under this hypothetical situation, the added GDP potential to the Azerbaijan economy is between €780m and €1,170m per annum. This takes into account only fixed broadband penetration. Harmonisation of spectrum exploitation would bring further economic benefits

Pilot Projects

It is recommended that Azerbaijan joins a Regional initiative to harmonise policy with the EU on universal high-speed broadband access. The objective is to install a firm policy commitment for the region and within each country for universal high-speed broadband access. This policy should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, Azerbaijan should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

2.6.7 Belarus

State of play and gap analysis

A detailed description of the legal and regulatory framework and its implementation is contained in the February 2015 report – "Benchmarking Electronic Communications Markets in EaP countries ENPI / 2012 / 307-572."

Belarus has achieved the highest level of penetration of broadband services - fixed broadband stands at 28.3 per 100 population and mobile broadband at 54 per 100. This gives the highest broadband penetration in the Region, with a small gap under the EU average. These levels of service penetration have only been achieved in part through private investment and the competitive market still has restrictions. The results have been achieved primarily through applying state policy and state investment in the sector.

The Ministry of Communication and Informatisation (MCI) is the body responsible for policy and regulation. Another regulatory body The Operational and Analytical Centre (OAC) determines policy for ICT development. Both bodies are financed fully from the state budget.

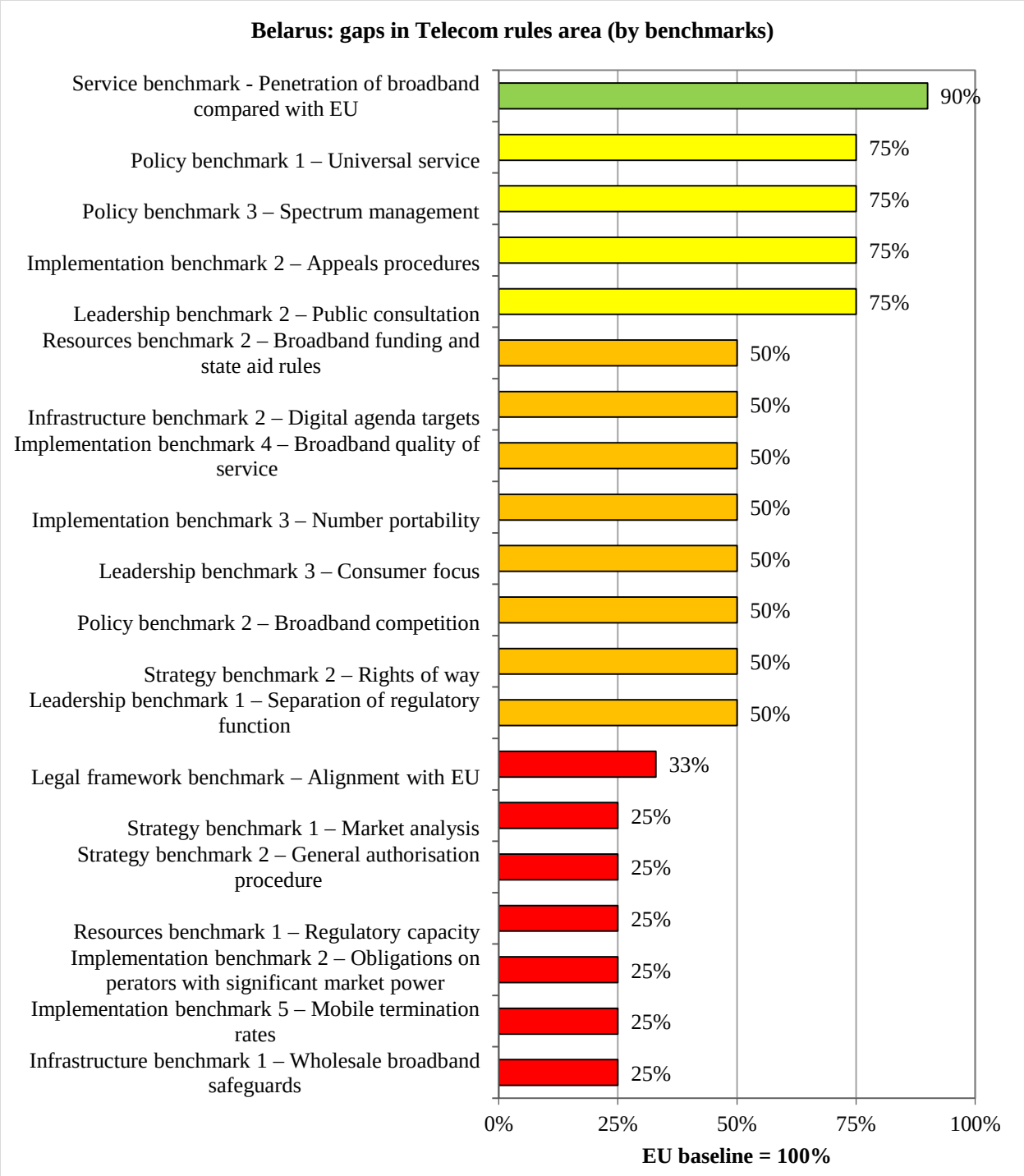

Exhibit 54- Belarus: state of play and gap analysis in Telecom rules

There is a “National program of accelerated development of services in the field of information and communication technologies for the period 2011 – 2015”. The development of ICT is

intended to promote an information society based on innovation and increased quality in the interaction of information between citizens, business and government. This is also supported by the creation of the state system of provision of electronic services.

The State Commission for Radio Frequencies is the sole authority responsible for frequency allocation. The preparation and approval of the national frequency plan is performed in cooperation with MCI and frequency assignment is carried out by the State Inspectorate for Telecommunications within MCI.

A Directive of the President requires discussion of draft acts of legislation that may have a significant impact on the business environment, through the establishment of public consultative and (or) expert councils with representatives of business entities and their associations (unions, associations). Proposals also have to be published on the official websites of government agencies and in the mass media.

The Constitution guarantees human right to access to the information and right of freedom of the expression of opinions. The applicable legislation contains provisions determining necessity to protect personal data. The Law “On electronic communication” stipulates that an electronic communications operator is obliged to ensure high quality, privacy and timely provision of information to consumers on the terms and conditions of service. An operator cannot deny the subscriber access to the Internet if there is technical capability to provide service. This is strengthened by a citizen’s right to appeal. Users are entitled to information on tariffs, types of electronic communications services, service delivery time, work shifts of electronic communications operators, as well as to the information necessary to use electronic communications services.

The scope of the universal service obligation includes local calls, payphone services and internet connection at points of public usage. The funding is covered from a special state budget fund for universal service. There is a national quality of service standard that must be adhered to, but there is no regulation of minimum or maximum data rates that must be provided for internet services. The universal service provider, selected by tender, is RUP "Beltelekom", which also has the defined status as the national multi-purpose electronic services operator with exclusive rights to international traffic.

Investment activity is governed by the “National program of accelerated development of services in the field of information and communication technologies for years 2011 – 2015”, which defines the following investments:

1. Construction of multiservice network of electronic communication: Development of local networks of electronic communication with connection to points of access to the data transfer network for satisfaction of demand for multimedia services (State budget)
2. Modernisation and development of networks of fixed broadband access to the Internet: Construction of fibre-to-the home.
3. Modernisation of intra-zone transport data transfer networks between each district centre

The total investment funding 2011 – 2015 is €28m from the special innovation fund, €5m from the universal service fund, €194m from the state fund.

For years 2013-14 in Belarus there was completed the forming of the regulatory framework of use of radio-frequency spectrum. In regulations it is expressly stated that the main aim is to harmonise the use of spectrum with international distribution, including the European one. Belarus is a member of Regional Commonwealth in the Field of Communications and coordinates its policy of use of radio-frequency spectrum in the framework of the Commonwealth with other countries, including all its neighbours, of that Lithuania and Latvia has observer status. Belarus is also a member of the European Conference of Postal and Telecommunications Administrations (CEPT) and focuses on the decisions made in the framework of CEPT. The radio network is developed in Belarus in accordance with general principles approved worldwide and in Europe.

Belarus relies on the regulation of designated “natural monopolies” which differs significantly from the ex-ante market analysis procedure in the EU baseline. The main differences are in the identification and definition of relevant markets subject to ex-ante regulation. In the EU these are all wholesale markets, in Belarus the approach appears to apply only to retail markets. The determination of significant market power in the EU baseline is based on a number of demand and supply side substitution criteria, as well as on the likely behaviour of the entities within the market. In Belarus the determination is almost entirely done by calculating the retail market share, regardless of many other relevant factors.

In the EU baseline, the market remedies are mainly to promote competition by obliging an operator with significant market power to provide alternative operators transparent and non-discriminatory access to its network, at cost oriented wholesale charges. By doing this the alternative operators can offer competitive services to customers without the need to overcome significant investment barriers. In Belarus the obligations on dominant or natural monopoly entities almost exclusively involve retail price fixing. In the EU baseline there is no definition of natural monopolies. The objective of ex-ante regulation in the EU baseline is to make markets progressively more competitive if they are not already. The objectives of the Belarusian method appear to be to accept that natural monopolies exist and to control end prices to consumers.

For rights of way, there is a multi-stop, multi-stage process requiring a great deal of data to be submitted and special restrictions may apply (including the need for the operator to integrate with the single unitary digital network ERSPD).

In Belarus providing electronic communications services is subject to licensing. The possibility to abolish individual licences (as in the EU baseline) has been discussed, but it will be a structural decision involving many sectors, when the market is ready for it. General licensing requirements and conditions, placed on a licensee include compliance with the requirements and conditions, set by laws and regulations, including technical laws and regulations, regulating licensing activity, presence in the staff of at least one specialist, having corresponding to the area of rendered services professional preparation and qualification, confirmed by the document, approving getting necessary education, availability of a decision of an authorised organisation for the right of using the radio-frequency spectrum, and compliance with the terms launching of services specified.

The MCI is funded by the state. As regulatory body, it has sufficient financial resources. There are no additional sources of financing payable by operators. Financing is not enough for major projects, including fibre optic infrastructure. Qualified human resources are lacking both in the area of management and in the area of implementation of telecommunication development projects.

Facilities of universal service fund (described above in paragraph 4.1) are entirely used for capital investment associated with multi-purpose electric communication service.

The procedures for funding of broadband acceleration are not aligned with the EU baseline in the important aspects of technological neutrality, advancement of competition and adherence to state-aid rules which define the criteria for state subsidies.

In Belarus, the consumer has the right to issue a claim to the provider of the telecommunication service. In practice, operators settle disputes among themselves, but precedents of appealing to MCI exist. The OAC can also settle defined disputes. The Supreme Economic Court and the President serve as a last instance for appeals. Any decision of government authorities can be appealed in Court, claims and recommendations on the part of parties concerned, including citizens, can be accepted.

Mobile number portability has been introduced. The service then commences with the new operator within 24 hours. A number cannot then be ported again within 90 days. Fixed number portability has not been implemented and nor has the single European emergency number and no dates are yet set.

The detailed quality parameters for internet services are published in tabular form and apply to all services that include internet access. They are very detailed and define quality suitable for efficient internet access, which is a requirement of the EU baseline only for universal service involving access at a fixed location. The above approach differs from the EU baseline in the sense that regulatory intervention is only required in the EU if consumers do not have sufficient competitive choices such that, if there is a quality issue with one broadband provider, the consumer can switch easily to another provider. In this competitive market situation prevailing in the EU, regulatory intervention is only relevant as a basic safety net within universal service obligations. In Belarus the broadband quality parameters apply to all operators in the market.

The wholesale rate for mobile voice call termination is not based on long run incremental costs.

Although a detailed legal gap analysis between the Belarusian and EU legal and regulatory frameworks for electronic communications, it is clear that there are fundamental differences in many aspects of regulatory independence, selection of markets for ex-ante regulation and determination of significant market power, access and interconnection, licensing and authorisation, spectrum liberalisation, the overall stimulation of market competitiveness and investment in broadband infrastructure.

The MCI is currently developing a document on separate accounting of costs for operators.

The development of separated accounting will assist in only part of fulfilling the requirements defined in the EU baseline for the promotion of broadband competition and investment in the era of next generation access networks.

The Strategy for the Development of Information Society is being developed as a plan up to 2022, and its first revision is currently submitted for discussion. Providing infrastructure for broadband fixed and mobile access is one of the main directions of development in the strategy.

HDM roadmap

Last year the project to build the Single (United) Republican Network of Data Transfer (ERSPD) was finished, according proposing common usage of modern infrastructure in the country. ERSPD is designed to provide various convergent services and is created in accordance with Presidential “On some measures of evolution of the data transfer network”. The procedure and the conditions of electronic communications networks connection to the electronic communications network of general use, including the ERSPD. Interconnection to networks is regulated by a 2014 OAC Resolution. Under this framework, all state and non-state organisations and individual entrepreneurs are provided with equal access to ERSPD. The tariffs for interconnection are defined in a separate Order issued by OAC.

Data transfer networks, designed for provision of national security, defence and law enforcement, will not be the part of ERSPD.

There is a limitation that the operators who laid down their own fibre optic lines to users cannot provide the possibility to use such for other operators. Fibre optic technology has emerged relatively recently, and regulators haven’t developed the legal framework, regulating relationships between the operators in this sector and requiring operators to share their infrastructure yet.

In the standard for the networks construction there is a provision, stipulating several levels of division, i.e. operators shall in practice come to the mutual agreement. But today the market doesn’t use this possibility, and the operators still prefer constructing their own networks. This problem will be solved with substitution of old technologies and spreading of fibre optics. We’d appreciate this legislation to be developed in a harmonised way with other regulations at the international level.

Apart from communications lines, cable ducts are used, that are also used by alternative operators. If in some places there is no possibility to lay a cable, necessary parts are completed by an operator. Therefore, there is no structural problem from the point of view of impossibility to use the available infrastructure by operators.

From the above analysis it is not clear if the operator of the ERSPD will run the network as a wholesale only business with no retail service offerings, or a vertically integrated wholesale-retail business. If the later, then, under the EU baseline there is a need to ensure that the wholesale inputs used by the vertically integrated operator can be used in a non-discriminatory way by other operators seeking access to the same wholesale inputs to offer replicable services of their own at the retail level. The EU baseline also contains safeguards to both access seeker and infrastructure operator in the form of relevant costing methodologies for access charging. Finally, the EU baseline contains definitions of the regulatory approach to service level agreements between operators, with relevant monitoring requirements.

According to the MCI, currently each operator covers from 37% to 46% of the territory using 3G technology. Currently the Ministry of Communications is working to provide spectrum to enable the operators to cover the whole territory, including under populated rural areas where it is economically unattractive.

Conditions for harmonisation

The National Strategy for Intensive Development of ICT Services for 2011-2015 stipulates the following tasks: “Updating and development of technical regulatory acts, guidelines, instructions and other documents on the basic processes of construction, maintenance of communication facilities, equipment installation and other works”; amendments to the Law “On Electric Communications" in terms of de-monopolisation of the market of international electric communication services; amendments to the Law “On Natural Monopolies” in terms of excluding electric communication services from the sphere of natural monopolies.

It is planned to harmonise the legislation in accordance with other countries of the EEU. Detailed focused analysis for bringing the legislation to conformity with the EU legislation has not been conducted.

In 2014 there were discussions on a public/ private partnership to facilitate ICT projects giving the possibility of entering into investment contracts between investors and the Republic of

Belarus. These partnerships will benefit from benefits including customs and tax advantages and investment guarantees.

The main point is that these investments, although accelerating broadband infrastructure, do not promote a competitive market, as required in the EU baseline. In the past, operators used available networks to render broadband services. For example, ADSL-access was developing on the basis of the existing copper cables so that operators didn't necessarily have to build their own additional infrastructure. 3-5 years ago the peak of subscribers was related to this type of access. Now higher-speed broadband demand has provided an incentive for alternative operators themselves build their own optical fibre networks.

More promotion of competitive market choices is required by the regulator, particularly in presenting clear information to consumers to assist them in making more informed and independent choices between different services and providers in terms of geographical availability, quality and price. Of particular value would be a review of the regulations that relate to market analysis, determination of significant market power and obligations for non-discriminatory and cost-oriented access to network elements and infrastructure. New regulations will be required to promote broadband competition and investment.

In the use of radio-frequency spectrum Belarus has inherited certain specific problems from the USSR that are not present in Western countries. In the bands where historically general-use communication has developed, in Belarus other consumers operate ("special users", military sector). Currently in Belarus, the required arrangements are carried out to ensure co-existence of two systems within one spectrum. In Belarus the issue of conversion has been very thoroughly worked out – the legislation has been developed, and it is actually complied with, which constitutes a very progressive achievement in the post-Soviet space.

The reported penetration of broadband services for 2014 was:

- Belarus fixed broadband penetration - 28.3 per 100 population (EU 30 per 100);
- Belarus mobile broadband penetration - 54.0 per 100 population (EU 61 per 100)

For Belarus, with fixed broadband penetration of 28.3 per 100 population, this represents an added potential of only +2 per 100 population if Belarus reached the existing EU average level of 30 per 100 population. Under this hypothetical situation, the added GDP potential to the Belarus economy is between €90m and €140m per annum. This takes into account only fixed

broadband penetration. Harmonisation of spectrum exploitation would bring further economic benefits.

Pilot Projects

It is recommended that Belarus joins a Regional initiative to harmonise policy with the EU on universal high-speed broadband access. The objective is to install a firm policy commitment for the region and within each country for universal high-speed broadband access. This policy should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, Belarus should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

2.6.8 Georgia

State of play and gap analysis

Georgian National Communications Commission (GNCC) was established. Later the state-owned incumbent operator was privatised. The Law on Electronic Communications and the Law on Broadcasting clearly sets the boundaries and define the roles. GNCC is an independent regulatory authority funded by a regulatory fee collected from the telecommunications and broadcasting sector operators. Spectrum fee contributions, licence and other fees are paid directly to the state budget. GNCC has adequate financial and human resources to carry its functions, maintain independence and high quality of work. The regulator has adequate resources to attract and hire qualified personnel.

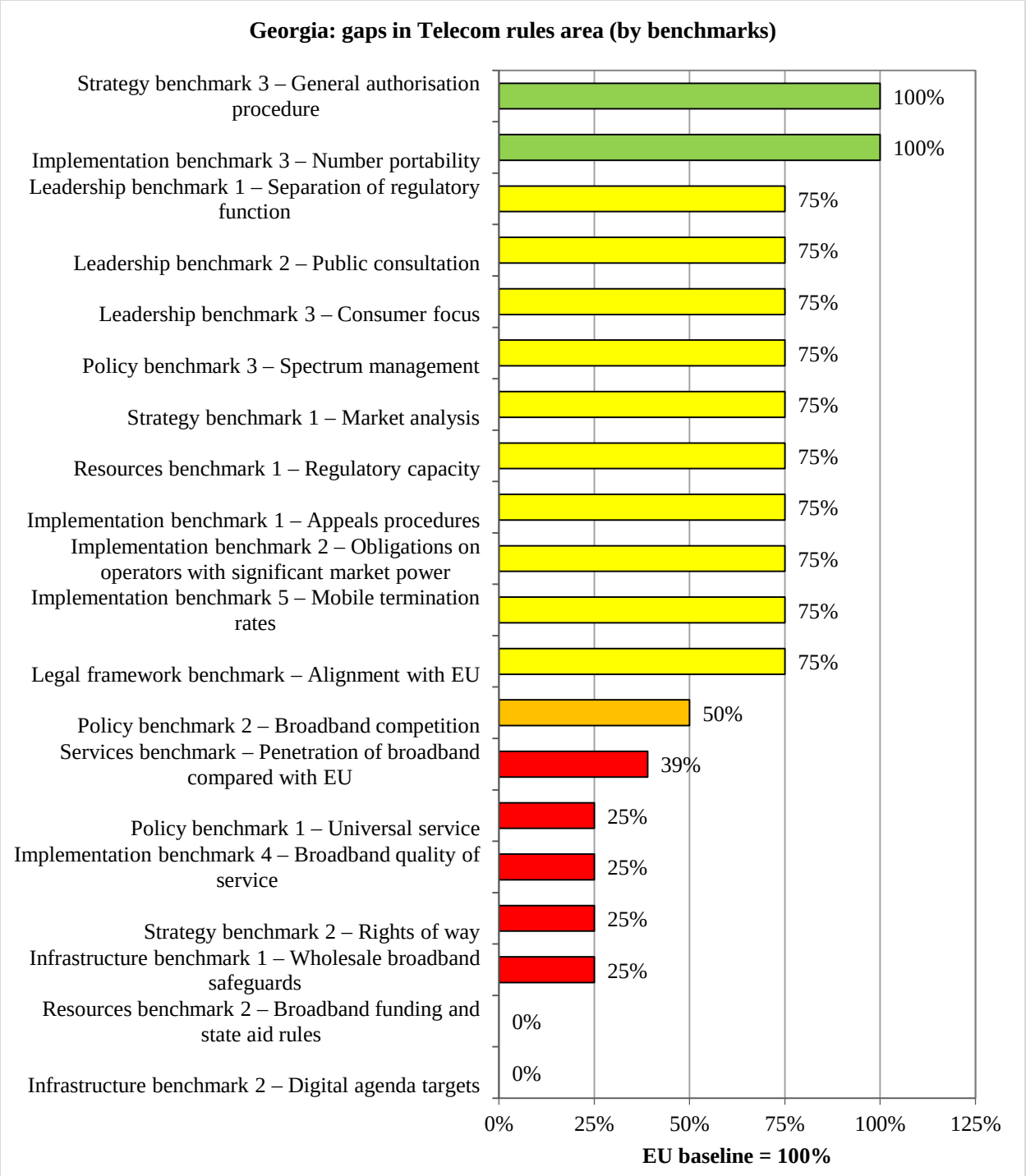

Exhibit 55- Georgia: state of play and gap analysis in Telecom rules

Clear separation of policy making, regulatory and operational functions was established in 2000, when the converged sector regulator for telecommunications, broadcasting and internet, the

Consultations are held on major issues and there are procedures for public hearings at GNCC and the Ministry of Economy and Sustainable Development (MESD), though not all decisions are subject to such procedures. The consultation is performed with the timing that is relevant to the issue and urgency of matter discussed allows, as decided by GNCC and MESD.

Georgia has not yet adopted clear written policy with regards to consumer rights, though these issues are fragmentally reflected in various documents and policies. The EU baseline is not yet fully reflected in such regulations. GNCC has established an independent consumer rights protection office where information is available and complaint procedures are addressed. A Consumers' Defender represents consumers in disputes with service providers. Legal assistance of an Ombudsman Institution is free of charge.

Universal Service policy has not been adopted and is not reflected in any regulatory, legal or institutional forms, though the government is planning to implement broadband development project in rural areas in 2015-2020.

Competition policy as reflected in legislation guaranteeing free access to the market, technological neutrality and access of elements of network facilities are implemented. Competition facilitation and promotion is a declared strategy at GNCC. Market entities with significant market power are regulated to give equal access to operators to their regulated infrastructure and services. No additional measures were undertaken to promote infrastructure sharing.

The latest EU baseline definition of the relevant market for wholesale access to infrastructure for to broadband development has yet to be analysed. Physical infrastructure definitions have to be introduced, as well as, relevant regulations to promote cost sharing, co-operation on civil works and cost reduction of broadband networks (as per directive 61/2014 of EC).

General regulations and rules of allocation of frequency resources are in place and described in the laws of Electronic Communication and Broadcasting. Frequency auctions and allocations are performed in a transparent manner. A long term frequency development allocation policy is not available. Spectrum regulations are in place, though for the achievement of EU baseline, additional amendments and changes are planned as per the Association Agreement implementation plan. Transparency of allocations and auctions are provided.

There is a sector-specific regulation on identification of operators with significant market power in relevant markets adopted by the regulator GNCC. The rules for identification of relevant markets are not clearly set. Therefore identification of these markets has been initiated by operators or GNCC itself and approved by the GMCC. Significant market power has been identified on the relevant markets of voice call termination, access to ducts, access to local loop/copper pairs, wholesale broadband access and backbone capacities.

Rights of way are provided by non-sector specific legislation and deal with the right of way of linear infrastructure (mainly utilities). The rules are not uniform across private and public sectors. Moreover, state entities have different rules and procedures for granting respective rights. The approach to granting rights of way is not unilateral even across all governmental agencies. Some agencies regulate the procedure and timing, whereas others, such as local governments are free to decide. Therefore the issue has become of greater concern for private companies recently.

This is an area not specifically identified in the Georgia/ EU Association Agreement, but it could benefit new investment in broadband infrastructure, especially in rural areas if the rights of way procedures were standardised and included in a “one-stop-shop” application process.

A general authorisation procedure is established and start of operation in electronic communication sector requires only a simple registration procedure unless it concerns scarce resources where additional authorisations are requested for the services. A special tax is imposed on mobile communication, collected and paid to the state budget. This additional tax is not allowed under the EU baseline.

There are no provisions in policy or regulations for state funding, either through universal service mechanisms or state-aid mechanisms.

Decisions of the regulator GNCC may be appealed in Court. All decisions of the regulator include a statement that such decision can be appealed at court by a defined deadline. The procedures of appeal are well defined in legislation. In its 15 years of existence, there have been cases when GNCC’s decisions were overturned by the court.

Access obligations are defined and imposed, in accordance with the EU baseline. The procedures and conditions are clearly set in the law.

Full fixed and mobile number portability are in place and the single European emergency number-112 is implemented.

Broadband quality of service is not regulated. Where broadband networks are already in place, mainly in towns and cities, consumers already have sufficient competitive choices to switch between broadband operators and find better quality of service. This is not the case in many rural areas and, because there are no universal service provisions in Georgia, there are no safety net provisions for effective internet access.

As part of ex-ante regulation, accounting separation was imposed on several operators. Even with such practice in place, the methodology was not in line with the EU baseline. LRIC models are not yet in place, but as announced recently, the regulator GNCC is planning to engage consultants to develop dynamic Long Run Incremental Cost (LRIC) model for mobile and fixed line call termination. In accordance with the EC Recommendation 2009/396/EC. The work shall be concluded by the end of 2015.

HDM roadmap

Recent moves by the MESD have identified the extent of the significant rural infrastructure gap, where investment is needed if high-speed broadband is to be extended beyond the main population centres. This is a resource area that should be aligned with the EU baseline in the important aspects of technological neutrality, advancement of competition and adherence to state-aid rules which should be put in place to define the criteria for future state subsidies. Such policy or regulations are not in place. Recent moves by the MESD to assess the extent of the “broadband infrastructure gap” in rural areas have not yet produced any clear policy towards universal high-speed broadband access. In order to ensure Georgian population with high speed internet MESD has recently introduced a project on construction of broadband infrastructure and delivery of services based on open access principle. Under the project the Georgian Government intends to award a winning bidder the construction of fibre optic network across the country to deliver broadband high-speed internet to rural areas.

Conditions for the harmonisation

The Georgia/ EU Association agreement Annex XV-B, “Rules applicable to telecommunications services” defines the specific topics and timescales (3-5 years) for harmonisation of the Georgian and EU legal and regulatory frameworks for electronic communications.

The spectrum policy adopted by GNCC has already taken account of some liberalising steps required in the EU baseline.

Spectrum trading is already allowed and Georgia is open to further regulation promoting easy access to spectrum and innovative types of authorisation such as collective use of spectrum. Georgia could be a very good early participant in the proposed Single Digital Market drive for more effective spectrum coordination, and common EU-wide criteria for spectrum assignment at national level; creating incentives for investment in high-speed broadband.

The various regulations adopted by GNCC and elsewhere regarding the electronic communications sector will require a thorough examination to determine consistency with the EU legal and regulatory framework for the sector. More promotion of competitive market choices is required by the GNCC, particularly in presenting clear information to consumers to assist them in making more informed and independent choices between different services and providers in terms of geographical availability, quality and price.

Of particular value would be a review of the regulations that relate to cost-oriented access to next generation network elements and infrastructure and the requirement for wholesale service to enable an access seeker to have equivalence of output retail service with the retail offerings of a vertically integrated wholesale and retail operator. New regulations will be required to promote broadband competition and investment, especially in the areas of cost efficiency by infrastructure sharing, joint use and the coordination of civil works. Rights of access to in-building infrastructures for high-speed broadband services will also require new regulations.

Generally, technological neutrality and non-discrimination obligations are part of the laws and regulations, though separate regulation for broadband competition and investment promotion is not in place.

The reported penetration of broadband services for 2013 was;

- Georgia fixed broadband penetration - 12.0 per 100 population (EU 30 per 100)
- Georgia mobile broadband penetration - 23.6per 100 population (EU 61 per 100)

For Georgia, with fixed broadband penetration of 12.0 per 100 population, this represents an added potential 18 per 100 population if Georgia reached the existing EU average level of 30 per 100 population. Under this hypothetical situation, the added GDP potential to the Georgia economy is between €220m and €330m per annum. This takes into account only fixed broadband penetration. Harmonisation of spectrum exploitation would bring further economic benefits.

Pilot Projects

It is recommended that Georgia joins a Regional initiative to harmonise policy with the EU on universal high-speed broadband access. The objective is to install a firm policy commitment for the region and within each country for universal high-speed broadband access. This policy should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, Georgia should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

2.6.9 Moldova

State of play and gap analysis

The process of separation of policy-making, regulation and operator activities was completed in 2000. There are remaining difficulties with implementing reforms, and from the government's political influence arising from the remaining state shareholding in the sector and also its interest as a promoter of general social interest. Public officials still act as members of the boards of operators, representing the state's interest.

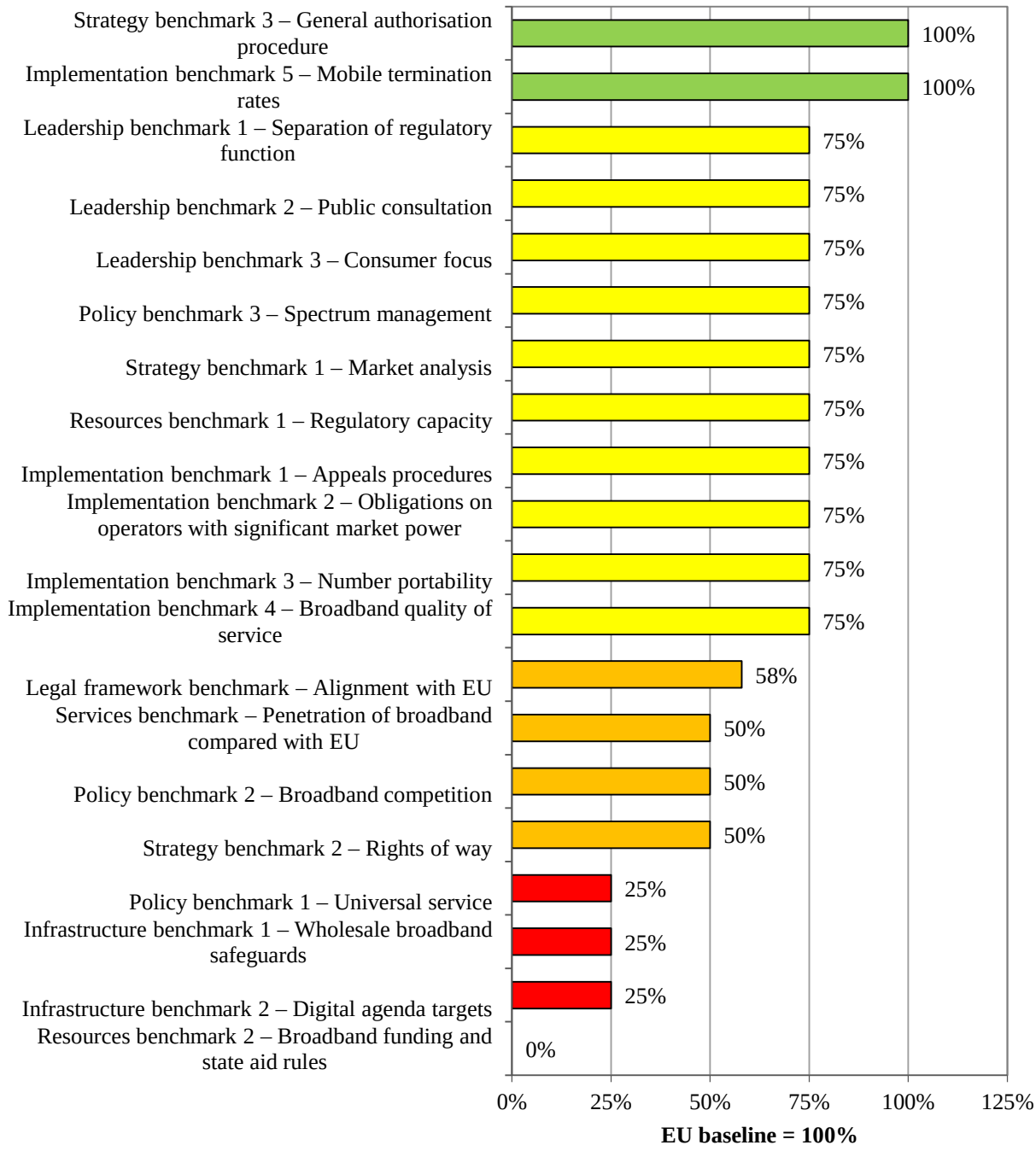

Exhibit 56- Moldova: state of play and gap analysis in Telecom rules

Under the law, the policy and regulatory functions are separated. In practice, the regulator is not fully independent. Firstly, its management is appointed by the Government (management of

other regulatory bodies is appointed by the Parliament. Generally, the Ministry on Information Technology and Communications (MITC) has clear powers to set forward policy for the electronic communications sector. It retains also some regulatory functions within spectrum management.

All public authorities to conduct their decision-making activities in a transparent manner and to publish for consultation any draft regulations. ANRCETI consults all draft decisions of public interest. The term of public consultation cannot be shorter than 14 days and the results of the consultation must be published. Usually, the authorities publish a synthesis of recommendations, including the reasons for accepting or rejecting them. However, decisions to accept or reject recommendations are not always well substantiated. Draft laws and regulations, which are not initiated by the telecommunications authorities, but have a bearing on the telecom sector, are occasionally not consulted, e.g. legislative proposal to consolidate the legal framework for fighting cybercrime, made by the Ministry of Interior. Policies of major impact, in particular those that require major investments, need to be announced well in advance to allow companies to plan.

ANRCETI has approved relevant regulations intended to protect users in the context of the electronic communications services that are provided by operators: These include users' rights relating to networks and services, unfair commercial practices and unfair contract provisions, procedures for dispute resolution, confidentiality and personal data protection. A consultation for the transposition of the legislation on consumer rights is underway.

Operators are required to measure and publish quality parameters. ANRCETI sets mandatory or recommended parameter values. Access for disabled users (with visual or hearing impairment) to equivalent services as for other users is not generally provided.

The right to privacy and confidentiality of electronic communications is not well protected. The EU e-Commerce, e-Privacy and Data Retention Directives have not been (fully) transposed. The National Centre for Personal Data Protection supervises the observance of information protection, in particular the right to information, access, correction, appeal or removal of data. Free movement of electronic communications equipment and services across national boundaries is ensured to some extent. The sharing of billing platforms installed abroad is prohibited, transfer of personal data abroad is restricted and subject to approval from the data protection authority.

The law “On electronic communications” provides that every citizen has the right to access a minimum list of services that form the Universal service basket, including access to the public telephone network, at a fixed location, access to directory enquiry service and to directories of subscribers, access to public pay-phones, including free access to emergency services. The funding mechanism for universal service via contributions from operators has not been commenced.

Sufficient spectrum has been granted to mobile operators for traditional and broadband services. Further spectrum is available and the spectrum management plan provides for their auctioning. Technological neutrality is implemented. There is wide voluntary passive infrastructure sharing between mobile operators.

In fixed networks, the obligations imposed on the fixed incumbent are the normal wholesale access types including local loop unbundling, bitstream access and access to poles and ducts. These obligations require open access, transparency, non-discrimination and price control. In practice, the alternative operators do not always have easy access to these network elements, or if they are granted access, it is provided under non-competitive conditions. As a result, alternative operators have largely built their own networks, which are not economically sustainable beyond the urban areas. Obligations for next generation access networks are not fully imposed yet according to the EU baseline.

The programme provides for caps on spectrum that can be acquired by an operator in various bands in an auction. Also, the law provides for the automatic withdrawal of a spectrum licence if none of the frequencies granted is used for 12 consecutive months. Technological neutrality is implemented. Spectrum can be assigned in specific blocks. The program did not necessarily ensure efficient allocation and use of spectrum.

ANRCETI has implemented the regulatory regime based on ex-ante regulation according to the EU baseline. For the next generation access era, the EU baseline non-discrimination and costing methodology recommendation has not yet been implemented.

The Law “On electronic communications” provides the right of way of the operators, but no specific procedure exists, so the process of obtaining access can be difficult and lengthy. Passive infrastructure sharing between the mobile operators is widely used.

The general authorisation regime was implemented in 2008. Any person can start an activity of providing electronic networks and services by simply notifying ANRCETI. The information required is the minimum necessary to allow the regulator to hold a registry. A license for the use of numbering resources is issued by ANRCETI in no more than 7 days after the request.

The rights of use of the spectrum, for which the number of licences is limited, are issued by ANRCETI using transparent public contests (auctions or beauty contests). For bands with an unspecified number of licenses, the licenses are issued on a first-come-first-served basis. In the view of the operators, the spectrum licence fees are excessive and are not based on the European baseline requirement for transparent administrative costs and objective justification of any additional market pricing. The spectrum policy adopted by ANRCETI has already taken account of some liberalising steps required in the EU baseline. For mobile broadband spectrum, more spectrum is available, and the spectrum management plan provides for their auctioning. The auction format is not yet established. Technological neutrality is implemented. Concerns exist regarding the possible proposals by Ministry of Health to restrict the placing of mobile base stations.

The budget of ANRCETI consists from regulatory fees levied proportionally on the operators and from annual numbering fees. ANRCETI has a fully autonomous budget, using the maximum allowed rate of 0.3% levy on operator revenues.

Any affected person may appeal against the decisions taken by the authorities. After the person requests the issuing authority to revoke or change the decision and does not obtain a favourable answer, there is a 3-step appeal system to the Court of Appeal and Supreme Court of Justice.

The obligations imposed on the fixed incumbent on local loop unbundling, bitstream access and access to poles and ducts, including access, transparency, non-discrimination and cost orientation. From 2014, wholesale termination rates are pure LRIC based. Obligations are still in place to reduce to the same level the termination rates for incoming international calls by July 2018.

ANRCETI introduced fixed and mobile portability in 2013. It takes up to 5 working days to port a mobile or fixed number, unless the user requests a longer term (but not more than 30 days). The porting is made with no cost for the user. The single European emergency call number 112 has not yet been implemented, pending the approval of the enabling regulations.

Operators are required to publish quality parameters for their services on their web-sites. There is difficulty in checking the figures and there is a low user awareness. There are legal provisions prohibiting false advertising. Minimum or recommended parameters are established in the regulations for spectrum licence conditions. Operators are required to include some of these minimum service quality levels in their consumer contracts. Operators have obligations to offer users the possibility to measure online their broadband quality. Net-neutrality provisions have not been adopted yet. In practice, competitive pressures ensure that access to specific applications is not generally impaired, blocked or charged additionally.

In the specific area of telecoms rules, much of the focus of policy and regulatory implementation in the EU is towards the enabling conditions for meeting the “Digital Agenda” targets for universal high speed broadband access.

HDM roadmap

Moldova has set specific policy “Digital Agenda” type objectives and targets for the electronic communications sector and has commitment to a competitive market and to harmonise the legal and regulatory framework with the EU. The incumbent operator is still state-owned. A clear policy needs to be developed to define the government role and set clear targets for achieving universal access to high-speed broadband services (>30 Mbps) together with clearly defined investments and an implementation plan to achieve the targets. There is an “investment gap” in broadband infrastructure serving rural areas. This gap could be filled by coordinated investments involving the private sector, digital broadcasting networks and government. State-aid rules need to be defined to ensure that any accelerating subsidies used by the state (of deployed from universal service funding) preserves a competitive market.

There is no adopted strategy promoting high-speed broadband infrastructure investment. The Government Decision in 2013 on “Digital Moldova 2020” and The Government Decision in 2014 on the “Roadmap to improving the competitiveness of Republic of Moldova” stipulate that the MICT is responsible for the development of a 2014-2020 program on development of fixed broadband networks (with the aim to ensuring access to all citizens to a minimum of 30 Mbps speed). A draft law on the use of associated infrastructure (aimed at ensuring the access of the operators to alternative infrastructures) is currently under public consultation. The MICT programme has not yet been published.

The actions, responsibilities and timeframes for the implementation of the universal service are part of a draft National Program for Universal Service Implementation, drafted by the sector ministry, but so far it has not been approved.

There is no state aid or state funding for investment in the broadband networks in Moldova. There is low financial capacity of the Government and local authorities and rural areas suffer from underdeveloped broadband networks.

A public consultation on draft state-aid rules for broadband was put on hold at the request of operators.

Conditions for the harmonisation

The Parliament has approved the Association agreement between Republic of Moldova and the European Union (law no.112 of 02.07.2014). The Association agreement contains the obligations of the Republic of Moldova to introduce reforms to allow approximation of the national legislation and by-laws to the EU framework, including the relevant European framework for electronic communications and radio spectrum. The timeframe for implementing the aquis varies from 1,5 to 3 years for different EU Directives and Decisions.

The Moldovan legislation is generally aligned with the 2003 EU regulatory framework, except for e-privacy directive, and partially with the 2009 telecom package.

The last policy paper for broadband development was for period 2010-2013. Partially the need in public policy is covered by the national program of management of radio spectrum for 2013-2020. It addresses issues of allocating sufficient radio spectrum for mobile broadband networks.

Overall, Moldova has developed a competitive market for traditional services and introduced most of the key features of the EU legal and regulatory framework. The state has full ownership of the incumbent operator, and there is still the possibility of a resulting political influence over the sector regulator ANRCETI. For example, if the regulator removed the fixed line market from the list of services subject to ex-ante regulation, then retail pricing controls would be removed on this basic service. The government would object to any raising of the tariff for a fixed line, citing political, rather than market efficiency arguments.

ANRCETI and the responsible ministry need now to ensure that the policies and regulation are extended to the next generation of networks and services in the broadband era. Both fixed and mobile broadband penetration lag significantly behind the EU averages and there is a need to

promote infrastructure investment out to rural areas where broadband penetration is still very low.

There are no state-aid rules for broadband investments and not yet any policy defining the government's role in achieving universal broadband access in the same way that the "Digital Agenda" benefits the EU.

The overall macro-economic, social and business benefits of high-speed broadband have been acknowledged and there are targets for the achievement of universal high-speed broadband access. The ministry has not yet published an implementation plan to achieve these targets. This plan must define clearly the role of the state and the private sector, the state-aid rules applying to any subsidies, the ownership and operation and investment models to be used and the regulations that will need to be put in place to ensure open wholesale access and to preserve competition for broadband services at retail level.

Clearly, a co-ordinated approach is necessary to achieve the full benefits of universal high-speed broadband access. The right elements are in place to make significant further progress - the commitment to harmonisation with the EU legal and regulatory framework, ANRCETI's awareness of the regulatory issues and its database of existing infrastructure, the operator's own investment plans and the new move by the ministry to fill the policy gap. These elements should be co-ordinated together to produce a clear national broadband policy and plan, supported by private investors and using central funding within a clear state-aid framework.

A policy for encouraging a broadband investment has not been approved yet. Also, the development of broadband networks relies only on investments of the operators, but with no funding from the state.

The Spectrum management program for 2013-2020 is approved by Government. The policy is oriented to a harmonised use of the spectrum with the last EU developments.

There is no policy or legal act in place that would promote the re-use of the existing infrastructure by the operators or joint construction. The only regulations relevant to this are the obligations on operators with significant market power in the relevant market to grant access to its infrastructures. A draft new law on access to public and private property, is pending approval by the Parliament.

The various regulations adopted by ANRCETI and elsewhere regarding the electronic communications sector will require a thorough examination to determine consistency with the EU legal and regulatory framework for the sector.

Of particular value would be a review of the regulations that relate to cost-oriented access to next generation network elements and infrastructure and the requirement for wholesale service to enable an access seeker to have equivalence of output retail service with the retail offerings of a vertically integrated wholesale and retail operator. New regulations will be required to promote broadband competition and investment, especially in the areas of cost efficiency by infrastructure sharing, joint use and the coordination of civil works. Rights of access to in-building infrastructures for high-speed broadband services will also require new regulations.

The reported penetration of broadband services for 2013 was;

- Moldova fixed broadband penetration - 14.0 per 100 population (EU 30 per 100)
- Moldova mobile broadband penetration - 31.3 per 100 population (EU 61 per 100)

For Moldova, with fixed broadband penetration of 14 per 100 population, this represents an added potential 16 per 100 population if Moldova reached the existing EU average level of 30 per 100 population. Under this hypothetical situation, the added GDP potential to the Moldova economy is between €100m and €140m per annum. This takes into account only fixed broadband penetration.

Pilot Projects

It is recommended that Moldova joins a Regional initiative to harmonise policy with the EU on universal high-speed broadband access. The objective is to install a firm policy commitment for the region and within each country for universal high-speed broadband access. This policy should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, Moldova should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment

schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

2.6.10 Ukraine

State of play and gap analysis

The law on Telecommunications dates back to 2004. In 2008 the National Commission for the State Regulation of Communications and Informatisation (NCCIR) was formed in 2008 to regulate the sector.

Parliament is responsible for policy making and the Cabinet of Ministers is responsible for policy enforcement. NCCIR is responsible for regulation and the State Service for Special Communication and Information Protection of Ukraine has a set of overlapping responsibilities for preparing policy proposals, technical issues and policy enforcement. The Antimonopoly committee of Ukraine is responsible for competition regulation. NCCIR is wholly financed from a reserved section of the state budget. The number of NCCIR staff has to be approved by the President of Ukraine. NCCIR's staff list has to be agreed with the Ministry of Finance.

The State enterprise Ukrainian Centre of Radiofrequencies (UCRF, under NCCIR governance) is responsible for radiofrequency monitoring and the issuance of radio-electronic devices permits. The NCCIR activities are under Cabinet of Ministers influence, not legally, but in fact. At the same time NCCIR is not defined as central executive government body according to current legislation. UCRF, as a self-supporting state enterprise performs functions of state bodies. The Antimonopoly committee and NCCIR have powers which overlap in the sector of electronic communications.

The Law "On Telecommunications" states that the Cabinet of Ministers and not NCCIR adopts rules for telecommunication services provision. For example the Law "On Radiofrequencies Resource of Ukraine" prescribes that spectrum tender procedures should be adopted by NCCIR, but the last procedure (for 3G mobile services) had to be approved by Cabinet of Ministers. UCRF being business entity under NCCIR governance issues according to the Law on

Radiofrequencies Resources of Ukraine permits which are compulsory for operators of radio-electronic devices.

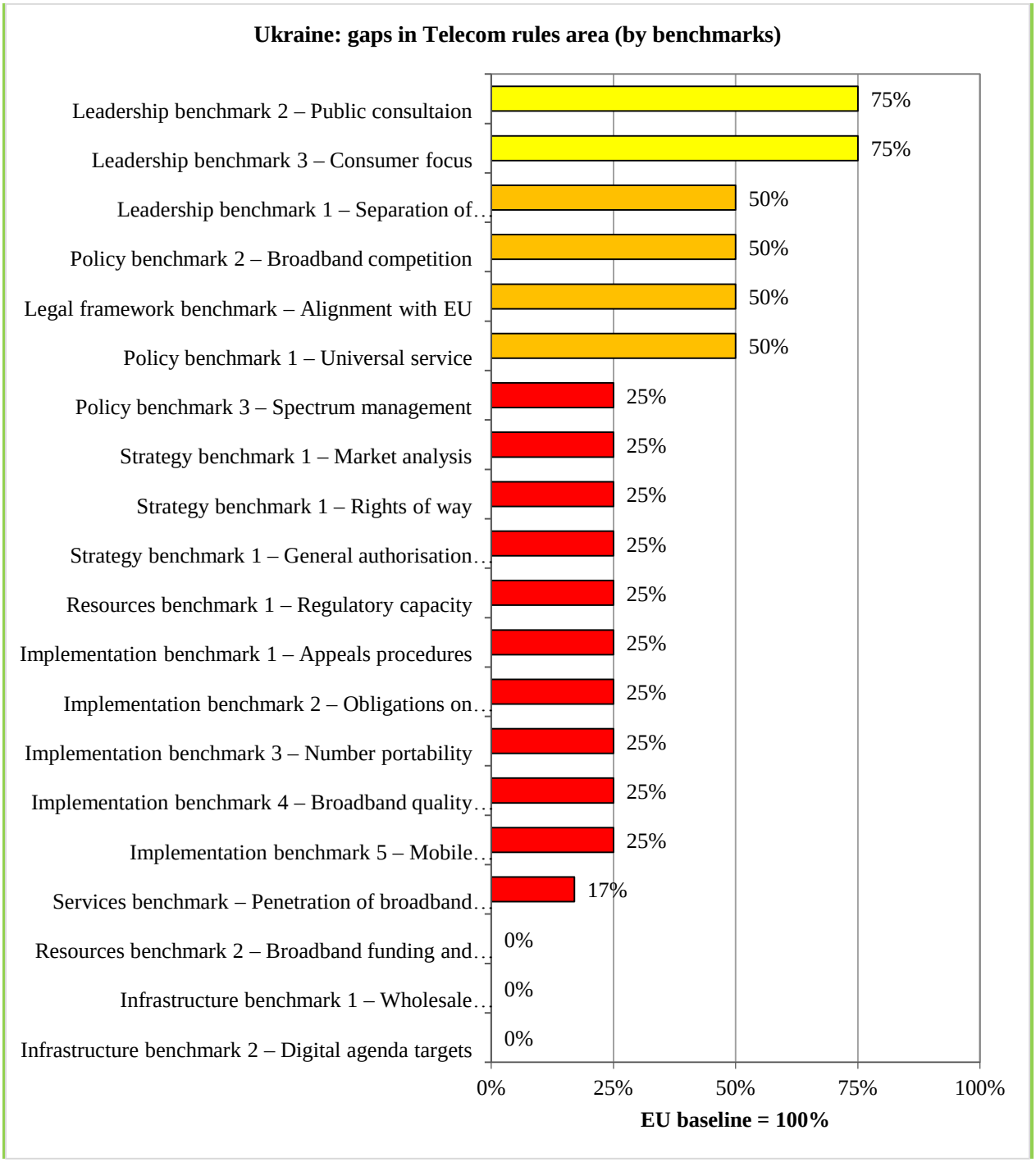

Exhibit 57- Ukraine: state of play and gap analysis in Telecom rules

According to the Law “On Telecommunications”, regulatory measures regarding the wholesale market can be applied both to operators with significant market power defined by NCCIR and Antimonopoly Committee. The existence of a number of different entities that can impact the market makes it difficult to understand how sector regulation can be independent, as defined in the EU baseline.

Proposed new policies and new regulations are published in a draft form, allowing a reasonable period (no less than one calendar month) for public comment and discussion by any party. After public discussion, NCCIR sends the draft document to competent state bodies like Antimonopoly Committee, Ministry of Economic Development and Trade of Ukraine for approval and to Ministry of Justice for evaluation on legal compliance and registrations as a legal act. Any person or business entity can appeal against it to competent bodies and ask for disapproval. If the Ministry of Justice concludes the draft policy or regulation act is not in line with legislation, this document will be rejected for registration as a legal act.

There is a requirement in the Law to carry out the publication of draft legal acts. At the same time, in the case of legislative initiative of People's Deputies, the advance publication procedure and discussion is formal and often not implemented. The requirements in the EU baseline for the publication of the results of public consultation are not met. Only the final approved version of the legal act is published. No reasons of why certain comments have been accepted or rejected are provided. All decisions adopted by any state authority including the regulator NCCIR may be appealed in the Administrative court by a private person or legal entity within 6 months. Proposed new policies and new regulations are published by NCCIR in draft form, allowing a reasonable period (not less than one calendar month) for public comment and discussion by any party. Any person or business entity can appeal. If the Ministry of Justice evaluates the draft policy or regulation act as non-compliance to legislation, this document will be rejected for registration as legal act. If telecommunications operators fail to agree on the conclusion, modification or termination of a contract, the interested party may refer the dispute to the NCCIR. If their decision does not satisfy one of the parties, then the disaffected party may apply to the court.

The Laws “On Telecommunications”, “On Protection of Consumers’ Rights”, “On Protection of the Personal Data” contain many of the requirements of the EU baseline requirements. The rights of consumers are foreseen and protected by national legislation. The laws only define the

principles and mechanisms for the protection of consumers' rights under the Constitution, the Law "On Telecommunications", all practical protection mechanisms have not been established.

According to the Law on Telecommunications, basic (universal) services include access to the public switched network, local fixed calls, emergency services, pay-stations and access to reference information. Access to the internet is not included. Obligations to provide the universal services are imposed on the incumbent operator. There is no provision in the regulations for defining the costs or compensation mechanisms for universal service.

NCCIR issues radio-frequency licences according to application (fees are approved by the Cabinet of Ministers) or through a contest with fair, open and non-discriminating conditions, decided by NCCIR.

The preparation of the plan of radio-frequency resource usage is primarily the responsibility of State Service of Special Communication and Information Protection (SSSC). The Plan consists of two parts - first is a list of existing radio-technologies, users and frequency bands; second is a list of prospective technologies and approximate implementation dates. The Plan has not yet taken into account the latest technologies available. Spectrum distribution has not necessarily been equal, leading to distortions in competitive markets.

There is no specific regulation on operators' access to public and private property for the purposes of building and operating electronic communications infrastructure. Therefore, all cases relevant to the granting of permission to install and maintain electronic communications facilities on public or private property are different from case to case. All disputes between parties have to be resolved in courts. In practice, the mechanisms exist for rights of way and payment although using the procedures is complicated.

Entrance to the markets of fixed, mobile communication services, telecommunication and broadcast networks and services require licences. Internet service providers can freely enter the market. Access to other operator's infrastructure except cable duct is not regulated. The incumbent operator as a monopolist, has to provide the access to its cable ducting. NCCIR has no power to analyse markets other than mobile termination and so there are no operators designated with significant market power in infrastructure markets and no imposed market remedies. Cost-sharing agreements are not promoted.

Numbering resource use also requires a special permit. Spectrum use is also licensed. There is no general authorisation procedure. There is a special tax fee for mobile operator services in addition to sales tax, which is reserved for the State Pension fund (7.5%). Fees for the right to use numbering, licensing and annual fees for the right to use frequencies go straight to the state budget. NCCIR is a legal entity and their property belongs to state.

Under the EU baseline, methods and of regulatory funding must be transparent, and fess have to be objectively justified. The imposition of a special tax on mobile operators is discriminatory and distorts the investment potential of the market, which is not allowed under the EU baseline.

No state aid is provided and there is no universal service fund implemented. Universal services are defined, with obligations to provide the universal services imposed on the incumbent operator. Access to the internet is not included into the list of universal services. NCCIR has a right to impose remedies on financing universal services on operators with significant market power and fixed line operators. Broadband services are not available on the whole territory of Ukraine.

Number Portability is not implemented, nor is the European emergency number service 112. Operators transfer all calls on number 112 to other emergency numbers or use a system which helps subscribers to call needed numbers.

Broadband services price and quality are not regulated, operators have an obligation to submit their quality measurement results to NCCIR for publishing. The list of measurements is different for fixed, mobile and internet operators. All requirements are common, there are no specific requirements for broadband services. There are no regulations for net neutrality.

There is no plan for promoting broadband competition and investment and no regulations regarding non-discrimination and costing methodology for next generation access networks.

Although a “Digital Agenda” target has been announced for universal high speed (>30Mbps) broadband, there is no state aid available to accelerate investments and no specific state-aid rules or investment regulations to ensure cost effectiveness in high-speed broadband infrastructure and the promotion of competition.

Price control for wholesale voice call termination on individual public telephone networks is based on benchmarks and not using long run incremental costs according to the EU baseline.

HDM roadmap

Of particular value would be a review of the regulations that relate to ex-ante regulation including the selection of relevant markets, market definition, analysis and determination of significant market power in each relevant market. Also needed are regulations to enforce non-discriminatory cost-oriented access to next generation network elements and infrastructure and the requirement for the next generation network wholesale service provider to allow an access seeker to have equivalence of output retail service with the retail offerings of a vertically integrated wholesale and retail operator. New regulations will be required to promote broadband competition and investment, especially in the areas of cost efficiency by infrastructure sharing, joint use and the coordination of civil works. Rights of access to in-building infrastructures for high-speed broadband services will also require new regulations. Operators' access to public and private property is based on provisions of the "Civil Code of Ukraine" and agreements between parties. Nevertheless, NCCIR is working on a specific document to implement common procedures for use in the electronic communications sector. The document has already been publicly commented and discussed; all interested operators gave their proposals.

NCCIR is not authorised to regulate access to infrastructure and network elements; no SMP definition procedure and no right to impose remedies. The respective changes are introduced into the Law, NRA develops and approves the clear procedures for the identification, definition and analysis of relevant markets that are subject to ex-ante regulation, the respective authorities approves the procedure, NRA conducts the analysis and imposes remedies on operators with SMP. Such a procedure will reduce barriers to fair competition on the market.

Under the requirements of the Ukraine/ EU Association Agreement, when respective changes are introduced into the Law, NCCIR could develop clear procedures for the identification, definition and analysis of relevant markets that are subject to ex-ante regulation. Then, in full co-ordination with NCA, NCCIR could conducts the analysis and impose remedies on operators found to have significant market power in the defined relevant markets.

The procedure for ex-ante regulation of retail markets was developed though not approved by the respective authorities. First, the procedure has to be agreed by several authorities, which are likely to reject it. Second, changes into the Law "On Telecommunications" have to be introduced in order to empower NCCIR to regulate any new markets on an ex-ante basis. Finally, some discrepancies might be associated with the markets to be included into the list for analysis.

There remains the risk that markets will not be regulated. Consequently, operators with significant market power in relevant markets will continue to enjoy their market position and abuse alternative operators and customers through setting unjustified charges. The respective procedure exists for the wholesale call interconnection market only. On the remaining markets recommended in the EU baseline, operators with significant market power are not regulated on an ex-ante basis.

Number portability is foreseen in the Ukraine/ EU Association Agreement and by the Law “On Telecommunications” as a right of a consumer and a correspondent duty of the operator since July 2010, but has not been launched in practice. The NCCIR has prepared a draft resolution of the Cabinet of Ministers of Ukraine "On Amendments to the Rules of giving and receiving telecommunications services”. There is also a draft decree on “Amendments to the Basic requirements for the contract to provide telecommunications services” and “On approval of the transfer of services to the subscriber number." In order to implement portability numbers for mobile and fixed numbers the "Ukrainian State Centre of Radio Frequencies" was designated as the organisation providing centralised technical management of personal numbers and ported subscriber database.

Existence of the single emergency call number 112 is foreseen by a special law. According to its provisions, State Enterprise “Emergency Centre 112” shall establish special centres to receive calls on number 112. However, these centres are not being established yet.

It may be difficult to implement improvements by means of secondary legislation, and in any case there is a risk of any NCCIR regulation being contradictory to the general civil law. There could be resistance from some state and local authorities to any changes in their procedures

Conditions for the harmonisation

Ukraine has set specific policy “Digital Agenda” type objectives and targets for the electronic communications sector and has commitment to a competitive market and to harmonise the legal and regulatory framework with the EU. The incumbent operator is still state-owed. A clear implementation plan needs to be developed to define the government role and establish specific projects for achieving universal access to high-speed broadband services (>30 Mbps) together with clearly defined investments. There is an “investment gap” in broadband infrastructure serving rural areas. This gap could be filled by coordinated investments involving the private sector, digital broadcasting networks and government. State-aid rules need to be defined to

ensure that any accelerating subsidies used by the state (of deployed from universal service funding) preserves a competitive market. No state aid is provided.

The current range of organisational units that have some responsibilities for policy making and regulation of the sector includes the sector regulator NCCIR, its technical arm that has technical and spectrum management responsibilities, the Antimonopoly Committee, the responsible ministry and the decision making roles of government and the Cabinet of Ministers. During public and legal consultations, there are many possibilities to block decisions. There needs to be a clearer definition and separation of the roles of policy and law making and the independent function of sector regulation. The clearer definition will lead to more transparency and certainty in planning and implementation for the sector and better use of time and human resources. It will also avoid duplication and reduce the scope for political interference in the proper functioning of market regulation

In 2014 the Cabinet of Ministers adopted general Plan on implementation for 2014-2017. According to the plan NCCIR is responsible for harmonisation aspects of electronic communications legal and regulatory frameworks under the Ukraine/ EU Association Agreement

NCCIR has no authorisation to limit the maximum amount of spectrum or amend existing licences in case of inefficient usage or Infrastructure

The various regulations adopted by NCCIR and elsewhere regarding the electronic communications sector will require a thorough examination to determine consistency with the EU legal and regulatory framework for the sector.

The reported penetration of broadband services for 2013 was:

- Ukraine fixed broadband penetration - 8.8 per 100 population (EU 30 per 100)
- Ukraine mobile broadband penetration - 6.7 per 100 population (EU 61 per 100)

For Ukraine, with fixed broadband penetration of 8.8 per 100 population, this represents an added potential 21.2 per 100 population if Ukraine reached the existing EU average level of 30 per 100 population. Under this hypothetical situation, the added GDP potential to the Ukraine economy is between €2.9Bnm and €4.3Bn per annum. This takes into account only fixed broadband penetration.

Pilot Projects

It is recommended that Ukraine joins a Regional initiative to harmonise policy with the EU on universal high-speed broadband access. The objective is to install a firm policy commitment for the region and within each country for universal high-speed broadband access. This policy should aim to be in harmony with the EU's Digital Agenda target that all citizens should have access to >30Mbps broadband service by 2020.

In parallel with this fundamental policy commitment, Ukraine should pilot rural broadband infrastructure investment projects to establish the best models of public/ private investment, municipal participation, service and technology requirements, ownership and governance, state aid and co-financing, operation and sustainability. The piloting of rural infrastructure investment schemes will inform future implementation decisions investment levels and timescales for national and Regional broadband universality.

CONCLUSIONS

Network, information and cyber security

All Partner Countries demonstrate strong political will to address the constantly evolving NIS-related challenges, including the willingness to cooperate with the EU and internationally. They share common problems and challenges that need to be addressed in order to create a level playing field with the EU to make stronger progress in NIS. The most typical findings include the following:

- The legal basis is minimally adequate but by and large (with some exceptions) is not compatible with the European Cyber security strategy. There is a need for similar national strategies to include, for example, the minimal level of requirements in relation to NIS, especially in the field of critical information infrastructure; at the moment it is usually a mix of (old) legacy and new laws/regulations that need to be streamlined and consolidated (assuming that having fewer good laws is better than having a fragmented legal basis consisting of many legal older acts and secondary regulations).
- Getting access to European resources and practices is not always easy, as there is no

cooperation mechanisms and channels of information exchange in the field of cybercrime (except bilateral activities and certain initiatives of the Council of Europe, which is most active in engaging the Region. The fact that almost all Partner Countries have signed the Cybercrime Convention and aligned accordingly their national legislation creates an important entry point for continuing and expanding cooperation. It is recommended to establish an intra-regional knowledge-sharing facility in the field of network, information and cyber-security to get on-demand access to good European practices and hands-on expertise. That would particularly concern CERT-EU and ENISA training and advisory services.

- Almost all Partner Countries have national or government CERTs which provide certain services. However, the scope and breadths of such services is rather limited. Many initiatives are ad-hoc and periodic rather than regular (e.g. cyber-attack simulations). Also, strategies for alert-platforms and hotlines seeking public feedback need to be reconsidered and improved. Defining critical information infrastructures, especially in the private sector, is a serious challenge. There is a need to build capacities of the CERTs so as they would be able to expand their services to wider audiences.
- One of the biggest gaps exists in the field of the transparent reporting on security risks, incidents and breaches when the disclosure of such information is the public interest. Establishing clarity about the criteria of public interest would be an important step forward towards best European practices.
- The protection of the confidentiality of personal data and online privacy is guaranteed by laws but their enforcement is weaker due to the fragmentation of existing legal basis. Passing a dedicated law on the protection on personal data is a progress from the point of view of European and international practice (some Partner Countries already have such laws; assistance in law drafting could be important).
- As governments procure new technologies and harness national capacities in information and cyber security, the issue of striking the right balance between internet safety and openness becomes critically important. It is essential that the European Cyber security strategy guides Partner Countries to ensure such balance.

Electronic identification and trust services

The main conclusion is that while the state of play varies among Partner Countries, the extent of such variation is not fundamental – the list of problems, challenges and obstacles and their nature are similar, although the EU Association Countries are more advanced in legal reform. On the other hand, the some countries might be closer to mutual recognition of eID/eTS services between themselves. Achieving the EU baseline lies in the national interest of the entire region. Therefore, it is reasonable to roll out cooperation support programmes for all the countries, with certain adequate fine-tuning to reflect upon specific country circumstances at the same time. Certain fast-track initiatives could also be developed for individual countries, for example, to join such EU large-scale pilots as the STORK 2.0 platform for cross-border eID exchanges.

Except Estonia, the experience and best practices of other EU Member States EU are less applied in Partner Countries. There must be much better knowledge sharing and solution adaptation mechanisms created in the region so as to expose the Region to the rich expertise of the EU. The access to the European knowledge in eID/eTS is still rather restricted. This is an important conclusion form the study judging from the interview results held with government officials. The most typical findings include the following:

- While the issue of electronic identification is well understood and in many cases advanced within national borders, not yet internationally (although there are such plans), the notion of trust services is less understood and somewhat ‘decoupled’ from eID issues.
- Electronic signature has served well business community but not ordinary citizens. In most cases, few citizens use it, which is a reflection of the lack of e-services that would require secure electronic identification and authentication (login pass codes are used instead). That undermines the security of important services that become increasingly sophisticated and transactional.
- While the legal basis at the moment is minimally adequate, it does not address future needs. There is a need to approximation national legislation with that of the EU (with eIDAS Regulation in the first place) if the Region to benefit from harmonisation with the EU Digital Single Market and online commerce.
- There is also a shortage of qualified specialists in the field.

- The issue of personal data and online privacy protection is growing in importance and EU support would help to consolidate and streamline present legal and regulatory frameworks.
- eProcurement has been among the key drivers of building relevant infrastructure and services closely linked with eCommerce. In some countries all public procure is implemented online (other countries plan to do it in the near future). However, as a rule, of digital signature is not integrated into e-procurement platforms which undermines its security and also puts limits to the full automation of award and post-award stages where strong identification is needed.
- Mobile eID technologies are becoming a reality in the Region and most likely it will become widespread in the near future.

eCustoms

The legal framework in eCustoms in the Partner Countries is the most advanced towards the harmonisation with the EU Member States. The overall legal framework and several major regulatory provisions related to eCustoms area (paperless environment for customs and trade, risk management framework, status of authorised economic operator) are in line with the EU baseline.

The weakest aspect is the information services. Several key information services have not yet been developed and implemented in the Partner Countries. The information exchange with the EU or even with other neighbouring countries is very limited. Belarus and Armenia already have automated information exchange is organised.

The biggest common gaps of the Partner Countries are in the implementation and use of information services such as a system for registration and identification of authorised economic operators. None of the Partner Countries has set up an anti-counterfeiting and anti-piracy system that allows right holders to submit online claims and ask the intervention of Customs in order to take measures against goods infringing certain IPR rights.

Recommendations

In eCustoms, priority actions have been identified in development of infrastructures and services, where the biggest common gaps for the DSM harmonisation have been identified.

These are the actions related to setting up Economic Operators Registration and Identification system interconnected with the EC TAXUD system, setting up a centralised Anti-Counterfeiting and Anti-Piracy System for the Partner Countries and it connection with the EU central COPIS system, automation of the exchange of data about Authorised Economic Operators with EU, and creation of the national segments of the Registered Exporters System.

The study has identified several aspects of mutual interest in the Region where it is possible to propose several multi-country projects for the Region;

- Exchange of summary electronic declaration for pre-arrival and pre-departure information
- Exchange of data on Authorised Economic Operators
- Uniform user management and the digital signatures framework
- System for exchange of electronic trade certificates
- Common Anti-Fraud Information System
- Systems interconnection for lodging preliminary and summary declarations
- Single Window – interconnected paperless environment for customs and trade

eCommerce

The legal framework of the most of the Partner Countries applies the principle excluding prior authorisation to pursuit the activity of eCommerce service provider. Another aspect in the state of play of the Partner Countries which well complies with the EU baseline is that eCommerce service providers shall render easily, directly and permanently accessible to the recipients of the service and competent authorities minimum general information that may be vital for customers claiming their rights. The Partner Countries do not restrict the freedom to provide information society and eCommerce services by service providers from another country.

The biggest common gaps of the Partner Countries are related to the legal provisions and frameworks assuring consumer rights (consumer protection international cooperation mechanisms, out of court dispute settlement mechanisms, transparency of commercial communications information to be provided by eCommerce traders). None of the Partner Countries has established an on-line dispute resolution system for customers of eCommerce transactions. This gap is linked to another important gap in harmonisation between the EU and

Partner Countries, which is a weak consumer protection international cooperation mechanisms in place in the Partner Countries.

The Region has achieved in average about a half of compliance towards the harmonisation of practices with the EU Member States in eCommerce. The Partner Countries have defined the legal frameworks, deployed basic infrastructures and services mainly for eCommerce operating inside the countries. The legal provisions and information services towards the international integration are missing.

These are the areas which help in creation of more accessible markets and facilitate a rapid boost in trade for SMEs. With proper financing, the development of information services is easier for the Partner Countries comparing to the long cycle of harmonisation of the legal and regulatory frameworks. Pilot projects in information services development would show immediate benefit for SMEs and customers that use these services.

Recommendations

In eCommerce, priority actions are: setting-up an eCommerce platform for SMEs, setting up online dispute resolution system for consumers for eCommerce transactions, common online trustmark scheme for eCommerce websites, harmonised semantic data model and format of electronic invoice and electronic contracts.

The Partner Countries would get significant benefits from establishing a common trustmark scheme for the Region. Another possibility is to join the work in progress on EU-wide trustmark schemes, which aims to reassure consumers on the reliability of accredited traders. This trustmarks will facilitate the promotion of Regional eCommerce platforms for SMEs. Such certified sites help consumers to make informed decisions when using online retail services.

Another important area for the common actions for the Partner Countries is the harmonisation of the legal frameworks across the Region. The following aspects have been identified as the most important: definition of common minimum general information to be provided by eCommerce service providers in the EaP countries, common transparency requirement of commercial communications, rules on the conditions for the risk of loss of or damage to the goods, harmonisation of rights on delivery of goods.

Digital skills

For Digital Skills, the main finding is that there is no systematic measurement of the digital skills gap across the Region. This measurement is required to increase awareness and to monitor the progress of digital skills development. Some initiatives have already started, particularly in the area of ICT deployment for better education.

Recommendations

The Region would particularly benefit from harmonising with the Grand Coalition for Digital Jobs, Europe's largest collaborative effort to address the digital skills shortage. By establishing national and local coalitions across the Region, awareness would be raised and better coordination with the EU would accelerate innovative learning and teaching, increase the number of ICT specialists, foster digital entrepreneurship, provide certification of digital skills and improved digital literacy.

Telecom rules

For Telecom Rules, the main finding is that there are significant gaps in access and take up of broadband services between the Region and the EU, particularly in rural areas. There is no consistent policy for universal access to high speed broadband across the Region. By harmonising with a "Digital Agenda" policy for universal access to high-speed broadband (>30 Mbps), the Region could benefit from an accelerated removal of the large digital divide between the urban and rural areas. There are currently widely different approaches to infrastructure investment across the region. In countries where this investment is largely state-funded, there remain significant barriers to alternative investment and the roll-out of competitive broadband services. In other countries where investments are left entirely to the competitive market, there is insufficient high-speed broadband infrastructure in rural areas.

Recommendations

By harmonising the policy and regulatory frameworks for telecom rules with the EU, these significant gaps could be closed faster, enabling much greater access and take up broadband services. Faster investment in infrastructure across the Region, giving better access to high-speed broadband, is an essential pre-requisite for the overall harmonisation of digital markets.

GLOSSARY

- **Eastern European Partnership** - is a joint initiative of the EU and its Eastern European partners: Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine. Launched in 2009 at the Prague Summit, it brings our Eastern European partners closer to the EU.
- **Partner Country** – one of the 6 Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine)
- **Region** - 6 Eastern Partnership countries collectively
- **Eurasian Economic Union**: The Eurasian Economic Union is an international organisation for regional economic integration and provides for free movement of goods, services, capital and labour, pursues coordinated, harmonised and single policy in the sectors determined by the Treaty and international agreements within the Union. The Member-States of the Eurasian Economic Union are the Republic of Armenia, the Republic of Belarus, the Republic of Kazakhstan and the Russian Federation.
- **Computer data** – any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function (Source: Directive of 2010 (COM (2010) 517 final) on attacks against information systems)
- **Computer emergency response team (CERT)** – Organisation formed to study internet security vulnerabilities, and to provide assistance to online sites that become victims of cracker or hacker attacks. Commonly, it offers a 24-hour emergency response service, shares information for improving cyber security, and coordinates responses to cyber-security threats (Source: ENISA).
- **Critical (information) infrastructure (CII)** – The systems, services, networks and infrastructures that form a vital part of a nation's economy and society, providing essential goods and services. Their disruption or destruction would have a serious impact on vital societal functions (Source: ENISA).
- **Cyber security/ information security** – There is no universally accepted nor straightforward definition of cyber security. When comparing it to 'information security'

some people regard it as overlapping. Or they may view information security as focused on protecting specific individual systems and the information within organisations, while Cyber Security is seen as being focused on protecting the infrastructure and networks of CIIs (Source: ENISA[49]).

- **Cyber-security** – The term commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of networks and infrastructures and the confidentiality of the information contained therein (Source: "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace").
- **Cybercrime** – The term commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware) (Source: "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace").
- **Developing a national Cyber Security Strategy** – specifying the scope, determining priorities and defining the principles and objectives of Cyber Security on a national level (according to ENISA).
- **Evaluating a national Cyber Security Strategy** – assessing the results of the activities using a set of objective performance metrics. Executing a national Cyber Security Strategy – Executing the national cyber-security strategy means specifying the action plan(s) and putting the strategy into practice through executing the activities (Source: ENISA).

[49] All references to ENISA as a source refer to ENISA guidebook 'Practical Guide on Development and Execution' for National Cyber Security Strategies (2012).

- **Risk** – Any circumstance or event having a potential adverse effect on security (Source: "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace").
- **Incident** – Any circumstance or event having an actual adverse effect on security (Source: "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace").
- **Incident handling** – All procedures supporting the analysis, containment and response to an incident (Source: "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace").
- **Information system** – any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance (Source: Directive of 2010 (COM (2010) 517 final) on attacks against information systems)
- **National Cyber Security centre (NCSC)** – A national Cyber Security centre is commonly tasked with protecting the national (critical) information infrastructures. The NCSC may have responsibilities concentrating on, for example, developing and offering expertise and advice, supporting and implementing responses to threats or incidents, and strengthening crisis management (Source: ENISA).
- **National Cyber Security Strategy** – a strategic framework for a nation's approach to cyber security. It is a tool to improve the security and resilience of national infrastructures and services. It is a high-level, top-down approach to Cyber Security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe (Source: ENISA).
- **Network and information system** – Any electronic communications network, any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance (Source: Proposal for a Directive of the European Parliament and the Council concerning measures to

ensure a high common level of network and information security across the Union (COM/2013/048 final)).

- **Network operating centre (NOC)** – commonly serves as a hub for coordinating the operational management of domestic incidents, as well as situational awareness. An NOC is a standing interagency organisation that operates on a 24/7 basis, fusing law enforcement, national intelligence, emergency response, and private-sector reporting. An NOC commonly facilitates national security information-sharing and operational coordination among (international) public and private sector partners (Source: ENISA).
- **Risk-based approach** – an approach to intelligence analysis that has as its objective the calculation of the risk attributable to a threat source or acts threatened by a threat source. It provides a means of providing strategic intelligence for planning and policymaking (ENISA).
- **Security** – The ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system (Source: “Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace”).
- **Security standard** – a set of security features to be provided by a system before it can be deemed to be suitable for use in a particular security processing mode, or in accordance with a generalised security policy (Source: ENISA).
- **Security baseline** – The measures that should be implemented to reach a specific minimum security level (Source: ENISA).
- **Trust service provider** – A natural or legal person who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals (Source: “Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace”).
- **eCustoms** initiative aims to replace paper format customs procedures with electronic ones, thus creating a more efficient and modern customs environment. For the purposes

of this study, eCustoms also comprises aspects of cross border trade, interaction between different government and non-government authorities involved in the procedures of issuing permits for external trade.

- **eCommerce for SMEs** is doing business electronically by SMEs. This includes the sharing of standardised unstructured or structured business information by any electronic means. It is trading in products or services by SMEs using computer networks, such as the Internet. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail.
- **eCommerce platform for SMEs** is typically defined as inter-organisational information system through which multiple buyers and sellers interact electronically to identify potential trading partners, select them and execute transactions. Such eCommerce platform performs the main tasks such as sourcing, automated purchasing, and processing to facilitate the sellers and buyers to do business transactions.
- **Information society service -** the basic definition is provided in the Directive 98/34/EC and covers any service normally provided, for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
- The concept of **"at a distance"** implies that the service is provided without the parties (i.e. the service provider and the recipient) being simultaneously present. Medical advice requiring the physical examination of a patient does not fall, for instance, within the definition of an "information society service". However, certain telemedicine services may be covered because they are by definition provided in situations where the healthcare professional and the patient (or two healthcare professionals) are not in the same location.
- The expression **"by electronic means"** is taken to mean that a service is sent initially and received at its destination using electronic equipment for the processing (including digital compression) and storage of data, and that it is entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means. The service must be conveyed from its point of departure to its point of arrival by means of electronic (processing and storage) equipment and by telecommunications means.

- **Service provider** - any natural or legal person providing an information society service
- **Established service provider** - a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.
- **The coordinated field** covers rules related to a wide range of activities such as online information, online advertising, online shopping and online contracting. Various national rules may also have consequences for to the taking up and pursuit of the activity of an information society service. The "coordinated field", however, does not cover requirements applicable to goods (e.g. safety standards, labelling and liability, classification for the purpose of protecting children) or conditions for the delivery or the transport of goods sold via the Internet, generally to the customer's home.
- **Distance contract** means any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;
- **Off-premises contract** means any contract between the trader and the consumer:

  (a) concluded in the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader;

  (b) for which an offer was made by the consumer in the same circumstances as referred to in point (a);

  (c) concluded on the business premises of the trader or through any means of distance communication immediately after the consumer was personally and individually addressed in a place which is not the business premises of the trader in the simultaneous physical presence of the trader and the consumer
- **Digital signature -** a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender
- **Common Communication Network (CCN)** - DG TAXUD’s gateway for all tax and

customs applications in the EU, supporting areas of taxation between member states, including VAT, excise duties, transit and import

- **Bitstream access** is a wholesale offering, typically from the incumbent telecommunications network provider, which allows an alternative service provider to offer fixed broadband services to end users by utilising the incumbent's digital network on a resale basis.
- **Digital Skills**: For the purposes of this study, Digital Skills are broadly defined[50] as ICT-related skills for the labour force, including ICT professionals, digital learners and citizens). Moreover, digital skills could be classified as follows: ICT user skills – required for effective application of ICT systems and services by the individual; ICT practitioner skills required for researching, developing and designing, managing, consulting, marketing and selling, integrating, installing and administrating, maintaining, supporting and servicing ICT systems; and E-business skills needed to exploit opportunities provided by ICT, notably the Internet, to ensure more efficient and effective performance of different types of organisations, to explore possibilities for new ways of conducting business and organisational processes, and to establish new businesses.
- **Telecom Rules**: The EU's policy, legal, regulatory and implementation framework for electronic communications is a series of rules which apply throughout the EU Member States. The rules encourage competition, improve the functioning of the market and guarantee basic user rights. The overall goal is for European consumers to be able to benefit from increased choice thanks to competitive prices, high quality and innovative services. The rules are flexible, technology-neutral and aim at deregulation in the longer term. The rules were updated in 2009 to take into account the developments in this area and are transposed into national legislation in all member states. The content carried over electronic communications networks is regulated by audio-visual media services rules.
- **Long Run Incremental Cost (LRIC)** – a costing methodology used mainly in setting

[50] See also http://eskills-monitor2013.eu/fileadmin/monitor2013/documents/MONITOR_Final_Report.pdfwww

wholesale interconnection and access rates between one network operator and another in order to ensure fair conditions for a competitive market. Under LRIC, the inter-operator charges are set with reference to a forward-looking (i.e. best technology) network. Other costs which do not vary, are specifically excluded from the calculation.

- **Universal Mobile Telecommunication System (UMTS)** - is a third generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP(3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing cdmaOne technology.
- **Eurasian Economic Community (EAEC or EurAsEC)** originated from the Commonwealth of Independent States (CIS) on 29 March 1996. The Eurasian Economic Community was terminated from 1 January 2015 in connection with the launch of the Eurasian Economic Union.
- **Customs Union (CU) / Eurasian Customs Union (EACU)** is a customs union which consists of all the member states of the Eurasian Economic Union.
- **Secure Sockets Layer(SSL)** is cryptographic protocol designed to provide communications security over a computer network.
- **Software as a service (SaaS)** is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software".

ABBREVIATIONS

AA – Association Agreement

ADR - Alternative Dispute Resolution

AEO – Authorised Economic Operator

CoE – Council of Europe

COPIS - EU centralised Anti-Counterfeiting and Anti-Piracy System

CCN - Common Communication Network

CERT – Computer Emergency Response Team

CII – Critical Information Infrastructure

CIIP – Critical Information Infrastructure Protection

CIP – Critical Infrastructure Protection

CIS – Commonwealth of Independent States

CSIRT – Computer Security Incident Response Team

CU - Customs Union (Eurasian Customs Union (EACU))

DDoS – Distributed Denial of Service

DSM – Digital Single Market

EAEC or EurAsEC - Eurasian Economic Community

EaP – Eastern Partnership

EEA – European Economic Area

EEU - Eurasian Economic Union

EDS - electronic digital signature

eID – Electronic Identification

ENISA – European Network and Information Security Agency

EORI -Economic Operators Registration and Identification number

eTS – Electronic Trust Services

EU – European Union

FIRST – Forum of Incident Response and Security Teams

HDM – Harmonisation of Digital Markets

IPM – Intellectual Property Management

ISP – Internet Service Provider

LEA – Law enforcement agency

LRIC - Long Run Incremental Cost

MOOCs - Massive Open Online Courses

MS – Member States

NCTS - New Computerised Transit System

NIS – Network, information and cyber security

ODR -Online Dispute Resolution

SaaS – software as a service

SSL – secure sockets layer

STEM – Science, Technology, Engineering and Maths

T3P – Trusted Third Party

UMTS - Universal Mobile Telecommunication System

Kantor Management Consultants

ibf INTERNATIONAL CONSULTING

ICMPD 20YEARS

eptisa

European Commission

DIRECTORATE-GENERAL FOR NEIGHBOURHOOD AND ENLARGEMENT NEGOTIATIONS–

Short term high quality studies to support activities under the Eastern Partnership

HiQSTEP PROJECT

HARMONISATION OF THE DIGITAL MARKETS IN THE EASTERN PARTNERSHIP

ANNEXES: TECHNICAL NOTES

First draft submitted: 20.4.2015

Final draft submitted: 8.6.2015

Final version submitted: