2020 Annual Operational Risk Report

Prepared by CRO's Office

Content

Introduction

2020 Annual Operational Risk Report describes all the identified Operational Risk events of the Pension Agency except for the activities of Investment Board and Investment Office. It also assesses financial and reputational impacts of those identified risk events and overviews CRO's recommendations that are proposed actions designed with the objective to reduce the impact and probability of occurrence of the identified risk events.

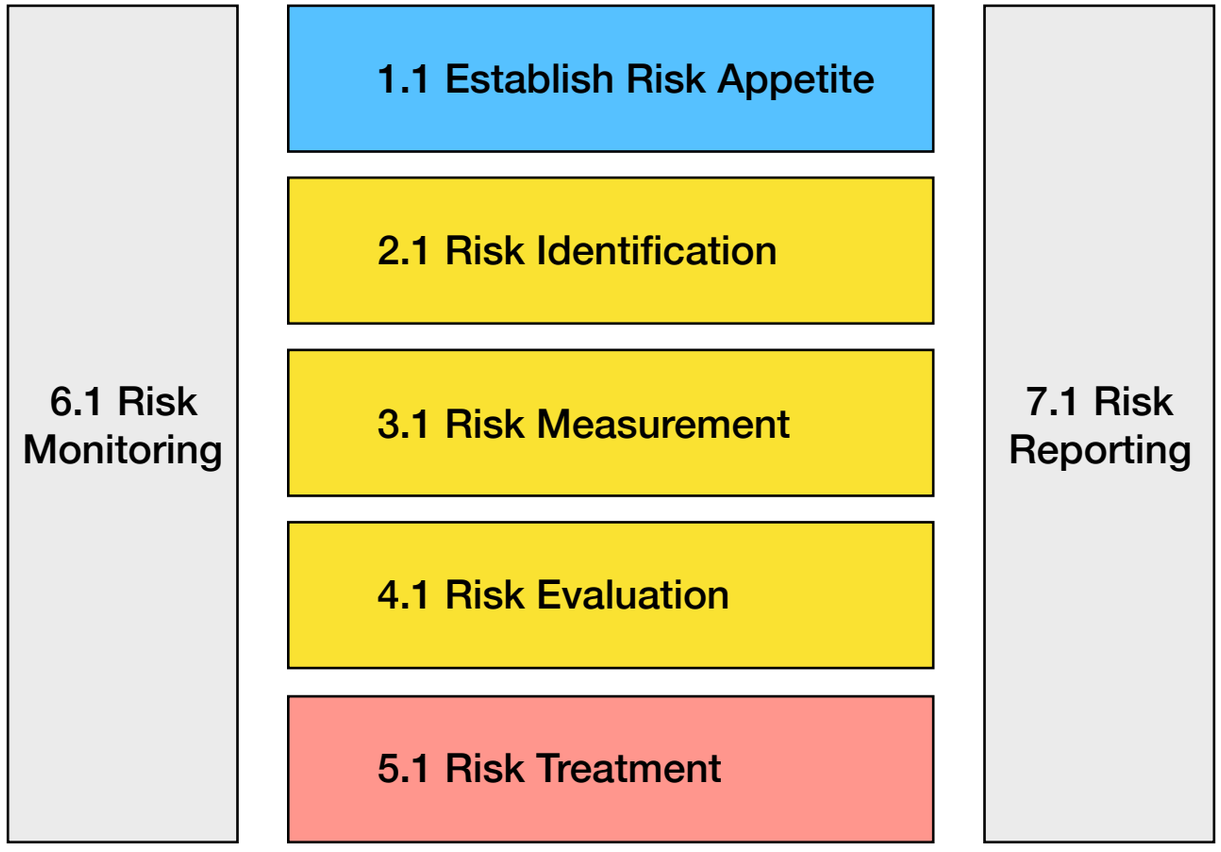
Due to the constraints in human resources and critical importance of the Electronic Pension Contribution Administration System, the CRO's office has decided to prioritize assessment of Pension Agency's activities only related to administration of the pension scheme, however by the end of Q1 of 2021, the Risk Control Department aims to also analyze the operational risk events that are related to the activities of Investment Board and Investment Office.

Introduction

2020 Annual Operational Risk Report in total includes 27 Operational Risk Events and corresponding CRO's 60 recommendations, however this presentation only highlights short descriptions of risks that materially affect investment activities and the Pension Fund and therefore, they need to be brought to the Investment Board's attention.

Introduction

The document is developed in accordance to **Operational Risk Management Framework** document that itself defines the operational risk management stages related to risk identification, measurement, assessment, treatment, monitoring and reporting.



PA's Operational Risk Management Framework is in compliance with foundational principles of ISO 31000

02 Risks Owned by Operations Department

Deficiencies in PA's Verification Procedures of Pension Contribution Payment Obligations by Private-Sector Employers

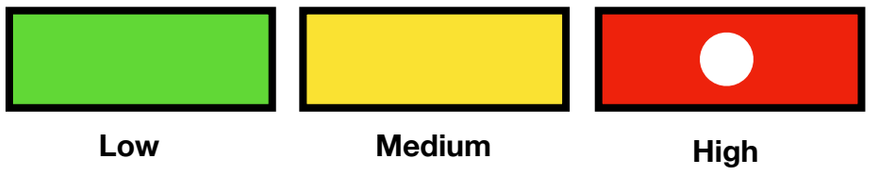
Risk Classification — Inadequate/Failed Operational Processes | External Fraud

Process Owner — Operations Department

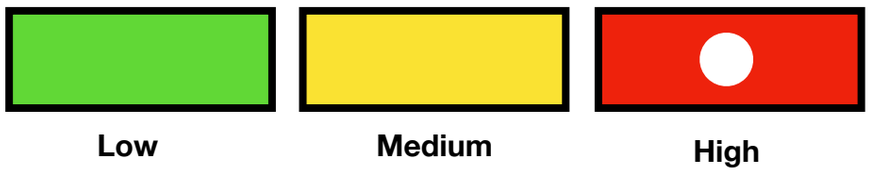
Risk Number — OP_001

In accordance to the Law, the Pension Agency must inspect the adequacy of performance of Employer and Employee contribution payment obligations and in case of partial or full failure to meet Employer's or Employee's payment obligation, the Agency then must send corresponding information by electronic means to the Employer, Employee and Revenue service, which based on the received information must take measures set by the Georgian legislation. The Pension Agency's controlling and verification procedures are conducted with the significant deficiencies and the estimated expected loss of Pension Fund due to non-fulfillment of pension payment obligation is around 40 million Georgian Lari as of December 31st, 2019.

Financial Risk:



Reputational Risk:



Operations Department

OP_001 Statistics

Table 2: Citizens that submitted Revenue Service Declarations as of December 2019, however they are not at all registered in Electronic Pension Contribution Administration System*

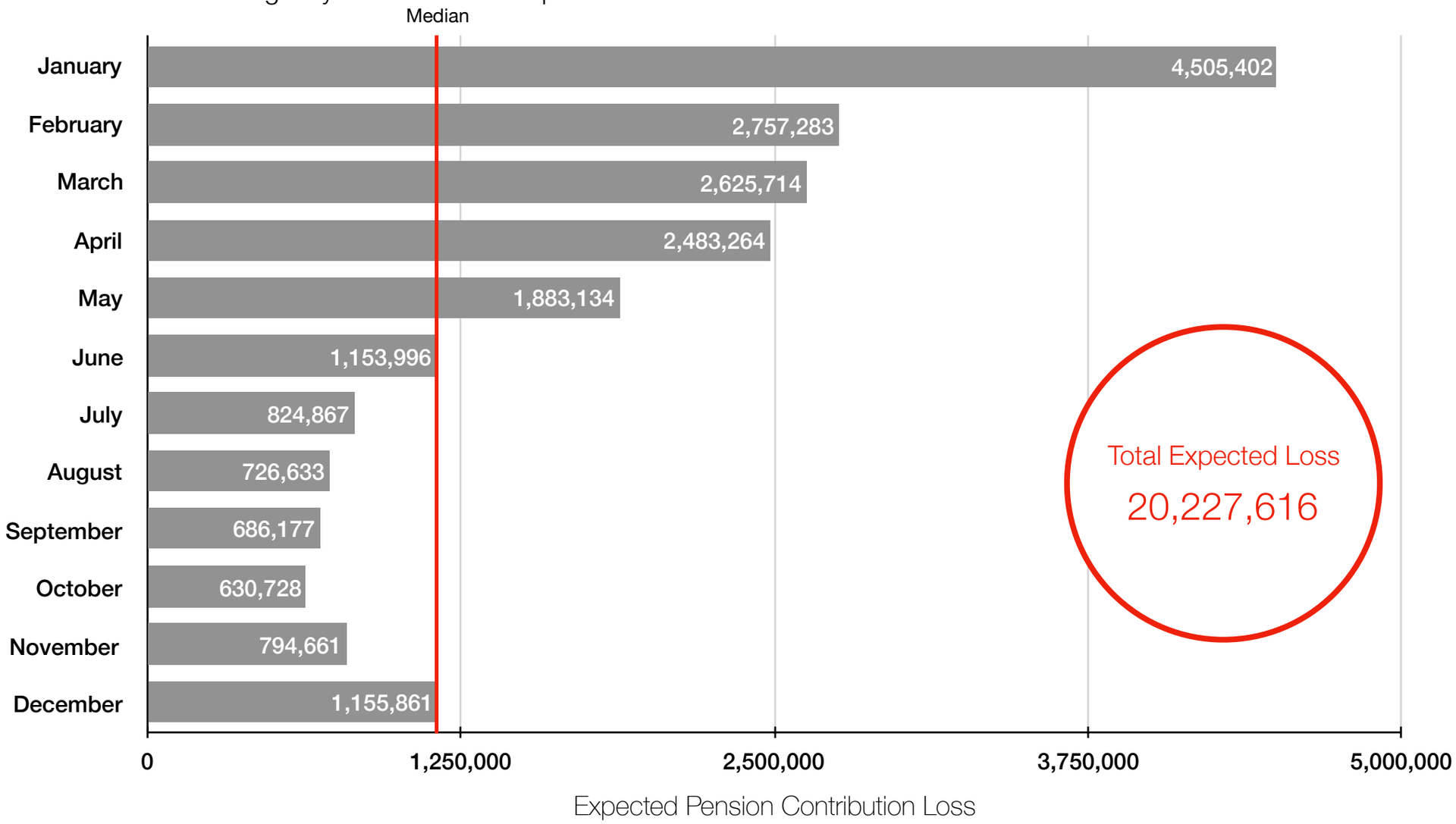
Revenue Service “Income Type”	Citizens	Total Declared Salary	Expected “Fund” Loss
Salary	39,457	236,073,945	14,164,437
Service Compensation	12,635	103,334,809	6,200,089
Other	46,742	109,430,638	6,565,838
Total (without “Other)	**52,092**	**339,408,754**	**20,364,525**
Total	**98,834**	**448,839,392**	**26,930,364**

*Calculated as a result of comparison between the Pension Agency’s and Revenue Service’s Databases.

Operations Department

OP_001 Statistics

Chart 1: Expected Pension Contribution Loss as of 2019 for Participants, who has less “Income” declared in Pension Agency Declarations compared to “Revenue Service” Declarations*

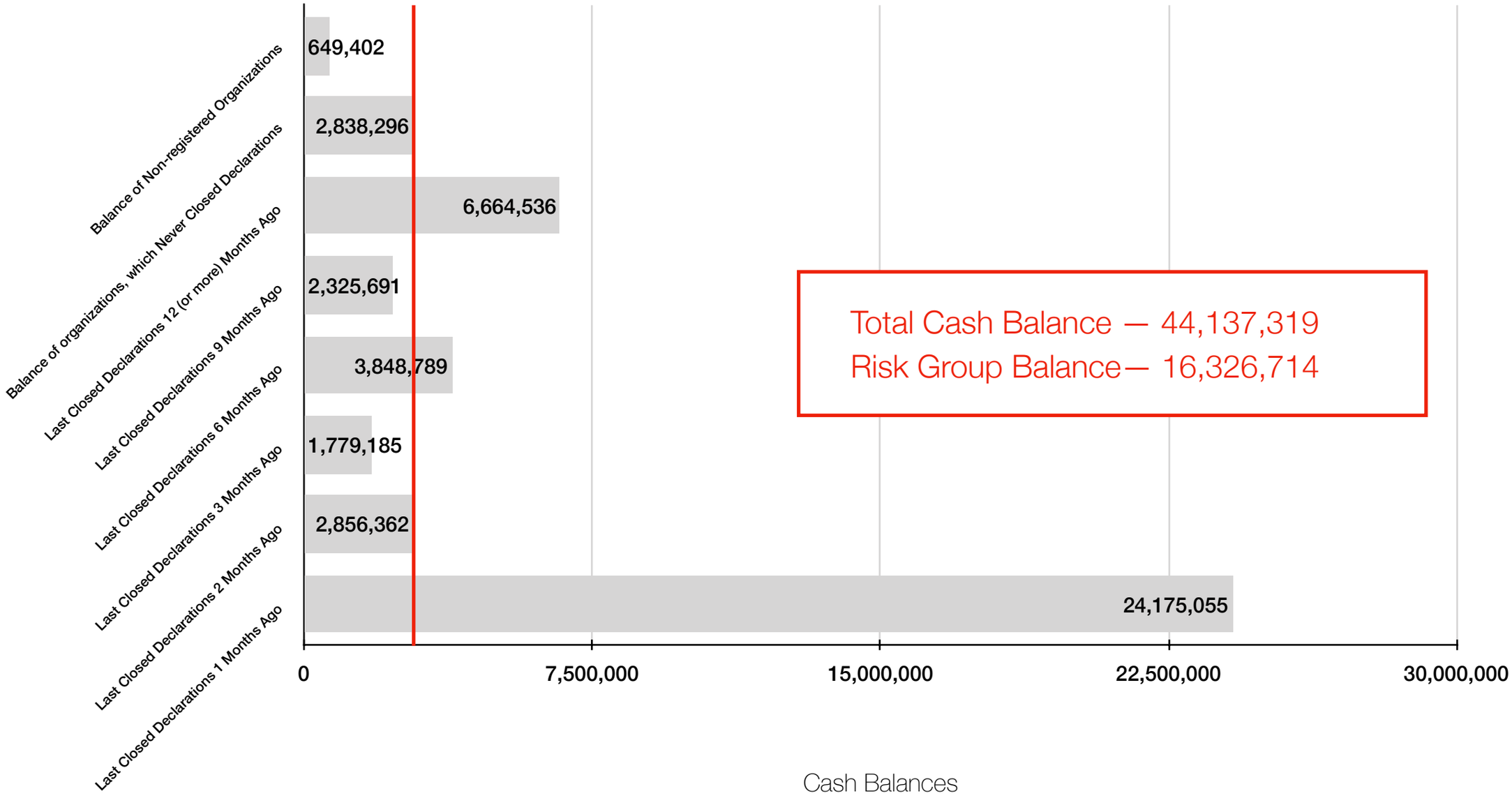


*Calculated as a result of comparison between the Pension Agency’s and Revenue Service’s Databases.

Operations Department

OP_001 Statistics

Chart 2: Pension Agency Outside the Fund (Pension Assets) Cash Balances as of December 31st 2020. There is high probability that organizations, which have never submitted Pension Declarations or they submitted more than 3 months ago are not adequately fulfilling their payment obligations.



Operations Department

Risk Number — OP_001

PA's Activities to treat OP Risk_001 — 2019 & 2020

2019	During 2019, PA has formally requested from Revenue Service to provide from its databases the information on the basis of which the PA could have examined the facts of the due fulfillment by employers and employees, however such information was not provided.
Quarter 1, 2020	PA has again formally requested from Revenue Service to provide from its databases the information on the basis of which the PA could have examined the facts of the due fulfillment by employers and employees and this time Revenue Service shared the information to the Agency
	As a result of comparison between the Pension Agency's and Revenue Service's databases, PA has detected the facts, when employer failed to fulfil or partially fulfill the payment contribution obligations and it has shared the respective results to Revenue Service, which should have taken enforcement measures provided for by the legislation of Georgia.
Quarter 3, 2020	Revenue Service has formally notified the PA that provided information and the PA's inspection procedures were not sufficient to take any further enforcement measures.
	PA and Revenue Service formed the MoU in accordance to which parties shall develop electronic service through which the information on the basis of which the PA must examine the facts of the due fulfillment by employers and employees will be automatically examined.
Quarter 4, 2020	PA initiated working meeting with Revenue Service in regards to the proper enforcement mechanisms after the facts of full of partially non-fulfillment of obligations will be detected, however parties could not agree on this matter. Revenue Service interpretation of the Law is that PA is responsible to conduct the full inspection procedures and the Revenue Service will issue fines on the basis of PA's inspection.

Operations Department

Risk Number — OP_001

Risk Treatment and Recommendations		Responsibility
Recommendation_001	Information Technology Department in accordance to the best International practice (“OWASP”) must ensure to implement live electronic information sharing mechanism with the Revenue Service. **status — ongoing**	**Information Technology Department**
Recommendation_002	Operations Department must ensure to establish the formal methodology document based on which the PA can control facts of the due fulfillment of pension contributions by employers and Participants.	**Operations Department**
Recommendation_003	The Director of PA in accordance to the Article 8, paragraph 3 must present to the Supervisory Board plan for the development and improvement of the funded pension scheme, where there will be assessed the possibility to unite the Revenue Service and PA’s declaration system with the objective to minimize the risk of discrepancies.	**Director**
Recommendation_004	The Director of the PA shall initiate and Supervisory Board shall lead the working group between the PA, Revenue Service and other government agencies with the objective to establish the roles and responsibilities in regards to enforcement measures.	**Director / Supervisory Board**
Recommendation_005	The Director of the PA shall initiate changes in PA’s declaration system, so that employers must also indicate the date of salary payment to its employees.	**Director**

Operations Department

Other Risks

Table 4: Short Summary of Identified Risk Factors in Operations Department

Risk ID	Risk Description	Financial Impact	Reputational Impact	Risk Treatment Short Description
OP_002	**Deficiencies in the PA's administration procedures of pension contributions made by the Government Sector as the employer.** In accordance to the Director's Decree №2 government organizations pay pension contributions and submit respective pension declarations through the consolidated Treasury Service. **Criteria 1** — there are cases, when actual submission of pension declarations and cash transfers are not the same day operations, which on its part means that during that time gap, Participant might loose expected accrued interests. In 2019, expected loss due to this event was 90,690 Georgian Lari, while in 2020, it was 10,137 Georgian Lari. **Criteria 2** — the Agency does not have the formal service agreement with Treasury Service, in addition, operational and IT procedures are not formalized, mapped and documented. **Criteria 3** - there were two cases, when Government Subsidy amounts were not enough on Treasury Accounts, so there were delays in pension contributions.	**Medium**	**Medium**	**Recommendation 006:** Establish service agreement with Treasury Service. **status — ongoing** **Recommendation 007 & 008:** Establish formilized and documented IT and Operational Processes. **Recommendation 005:** By the end of 2021 Formulate the Plan for Consolidation of Pension Agency's and Revenue Service's Declaration System
OP_005	**Deficiencies in the Correcting Declaration Processes by the Private Sector.** Based on today's practices, any private sector organization, at any time, can correct its submitted declaration and therefore, withdraw cash (contribution + accrued interest) from Pension Fund without any limitation. As of December 31st of 2020, total 4,298,902 Lari were withdrawn from the Pension Fund due to the corrections. There is risk of fraud in existing procedures: **Scenario 1** — the organization might correct declaration, receive initial pension contribution balance and plus accrued interest, then again re-submit the same declaration with the corresponding pension contribution, however without the accrued interest. **Scenario 2** — in stressed liquidity environment any organization at any time can correct declarations and receive the cash from Pension Fund.	**High**	**High**	**Recommendation 015:** Establish Internal Control Mechanisms based on the withdrawn amount, correction frequency and the time period after the initial declaration submission. **status — ongoing** **Recommendation 016:** Implement IT Web-Service with Revenue Service with the Automated Declaration Verification Check.

Operations Department

Other Risks

Table 4: Short Summary of Identified Risk Factors in Operational Department

Risk ID	Risk Description	Financial Risk	Reputational Risk	Risk Treatment Short Description
OP_003	**Deficiencies in the PA's administration procedures of pension contributions made by the Self-employed Participants.** The Agency as of December 31st of 2020 can not differentiate the Individual Entrepreneur as Employer, Individual Entrepreneur as the Self Employed and Individual Entrepreneur as Employee.	**Medium**	**Medium**	**Recommendation 009**: Corresponding adjustments in Director's Decree №2. **status — ongoing**
				Recommendation 010: Establish formilized and documented Operational Mapping for the PA's administration procedures of pension contributions made by Self-employed Participants.
				Recommendation 011: IT department must ensure to updated Electronic Pension Contribution web system process for Self-employed Participants. **status — ongoing**
OP_004	**Deficiencies in the PA's administration procedures of pension contributions made by Participants, who are not taxed at the source in accordance with the legislation.** Some of those employers (embassy, international organizations etc.) who are exempt from 'tax payment at the source' are not paying Employer's 2% of the Gross Wage and they claim that their employees must be treated as Self-Employees.	**Low**	**Medium**	**Recommendation 012:** Corresponding adjustments in Director's Decree №2. **status — ongoing**
				Recommendation 013: Adjustment in Declaration Filling Process in Electronic Pension Contribution System **status — ongoing**
				Recommendation 014: The Director of PA shall initiate the possible changes in the Law to clarify the obligations of those employees who are not taxed at the source.
OP_007	**Deficiencies in the PA's administration procedures for those Participants, who are eligible to Opt Out from the pension scheme in accordance to Article 22.** In accordance to the Directors Decree №2, after Participants leaves the pension scheme, the Pension Agency, first, transfers withdrawn amount to the Employer, who is responsible, then to transfer corresponding amounts to Participant. But, there are cases, when the Employers does not or partially fulfil their obligation.	**Low**	**Medium**	**Recommendation 019:** Adjustments in Director's Decree №1, so that Pension Agency transfers withdrawn amounts directly to Participant
				Recommendation 020: Complete Documentation Archivization Processes from Social Service Agency

Operations Department

Other Risks

Table 4: Short Summary of Identified Risk Factors in Operational Department

Risk ID	Risk Description	Financial Risk	Reputational Risk	Risk Treatment Short Description
OP_009	**Deficiencies in the PA's administration procedures of pensions payment at retirement age.** As of December 2020, the pension appointment procedures is manual process, in addition, "programed pension payment process" is not yet implemented and therefore, it is not available for Participants.	**Low**	**Low**	**Recommendation 022:** IT must implement automated pension payment system solutions status — ongoing
				Recommendation 023: The PA shall notify a Participant in writing of his or her impending Pension Age six month prior to Pension Age.
				Recommendation 024: Adjustments in Director's Decree №3 in regards to "programmed pension payment process" in collaboration with the Investment Office.
OP_008	**There is risk of fraud in case of payment of Pensions due to disability or due to permanently leaving the country.** The participant can obtain 3rd degree of disability status in accordance to the Law of Georgia on Medical and Social Examination and based on that h/she can withdraw the pension contributions. The same applies to Participants who can obtain permanent residence documents.	**Low**	**Medium**	**Recommendation 021:** The Director of PA shall initiate the possible changes in the Law to clarify the formal disability status.
OP_010	**Deficiencies in the Participation registration process in electronic system of pension contributions.** As of now, in order to register in electronic system participants must first obtain their "passwords" from their employers, which cause breaches in availability and /or confidentiality of Participants data. In addition, the inadequate registration process means less registered users (12% of Active Participants), which on its part weakens the controlling mechanisms.	**Medium**	**Medium**	**Recommendation 026:** Adjustments in Director's Decree №2
				Recommendation 027: Implement Electronic Identification System through e-ID Cards. status — ongoing

03 Risks Owned by Information Technology Department

Deficiencies in Pension Agency’s Information Technology Governance

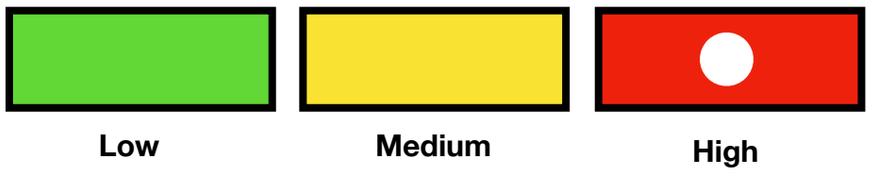
Risk Classification — Technology

Process Owner — Information Technology Department

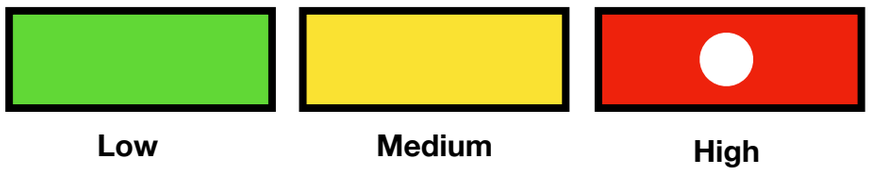
Risk Number — OP_016

The Agency’s Information Technology (IT) Governance* Framework is under-developed — the Agency does not have the formilized and documented processes to identify business IT requirements; the Agency does not have IT Committee to evaluate and monitor IT use in organization; the Agency does not have IT Strategic document and IT development is based on tactical not strategic decisions and objectives; IT human and financial resources are limited, there is no segregation of duties and there are only five full-time staff members, who oversee the System Administration, Network Administration, Software Development, Testing, Database Management and IT Support.

Financial Risk:



Reputational Risk:



*https://www.itgovernance.co.uk/it_governance

Temporary Software Licenses on Critical Information Technology Services

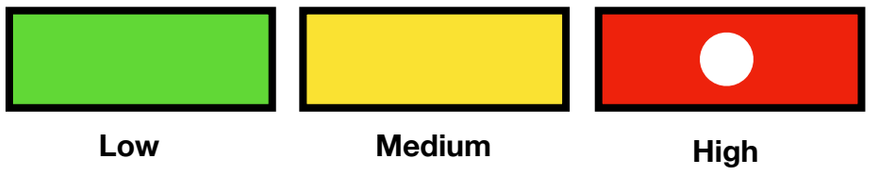
Risk Classification — Technology | Information Security Risk

Process Owner — Information Technology Department

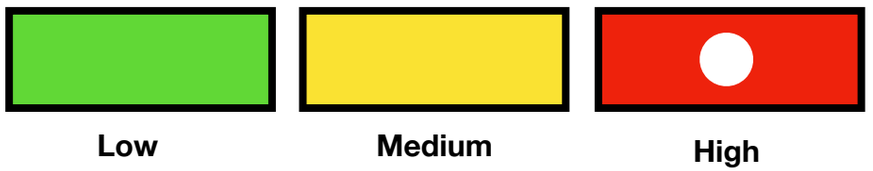
Risk Number — OP_021

There is no licenses for softwares running critical services, including MS SQL Server and Microsoft Hyper-V. The Agency is using trial versions for free and every time, at the expiration date it is renewing its trials, which causes following risk factors — there is high risk of service availability; also there is material risk of abrupt service breakdown without any adequate IT support from vendors; there is increased risks of cyber attacks due to delays or omissions of security patches. In 2020, there was the incident, when services were temporarily freeze due to trial updates.

Financial Risk:



Reputational Risk:



Failure in Procedures and Systems For Malware Protection

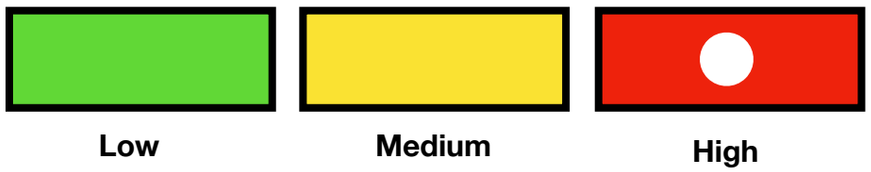
Risk Classification — Technology | Information Security Risk

Process Owner — Information Technology Department

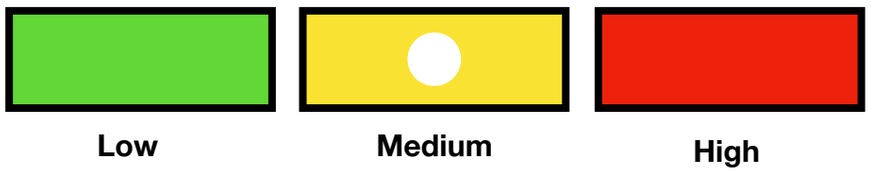
Risk Number — OP_022

There is not centralized approach for Malware Protection implementation, which must ensure protection of information assets and information processing facilities. This creates high risks of unauthorized access, damage or impediment of information and theft of information resources.

Financial Risk:



Reputational Risk:



Deficiencies in Pension Agency’s Vulnerability Management System

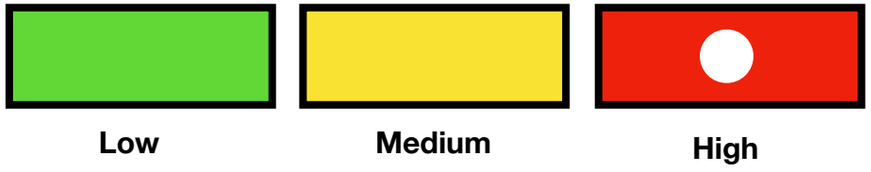
Risk Classification — Technology | Information Security Risk

Process Owner — Information Technology Department

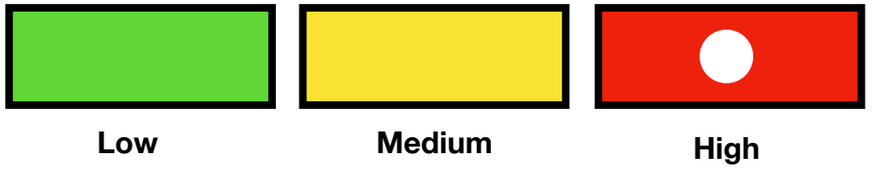
Risk Number — OP_018

The Agency has no Vulnerability Management Policy and corresponding technical instruments to periodically monitor, evaluate and report its vulnerabilities and to conduct the periodic Penetration Testing covering different scenarios and threats. The process is very important to uninterrupted operations of the Electronic Pension Contribution System, as the majority of security breaches and cyber-attacks are based on exploitation of known technical vulnerabilities. The importance of the above-mentioned process could be even more highlighted considering the fact that the Agency does not have documented Secure Development Policy that is in accordance with the best international standards (OWASP)*, while at the same time all the Agency’s critical services are in-house developed.

Financial Risk:



Reputational Risk:



For more details regarding the risk factors related to the Secure Development Policy is detailed in 2020 Annual Operation Risk Report with the Risk Number OP_025.

Deficiencies in Pension Agency's Access Management System

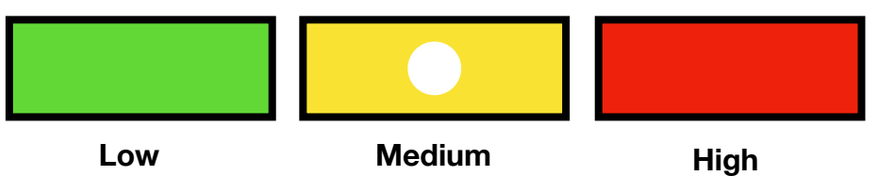
Risk Classification — Technology | Information Security Risk

Process Owner — Information Technology Department

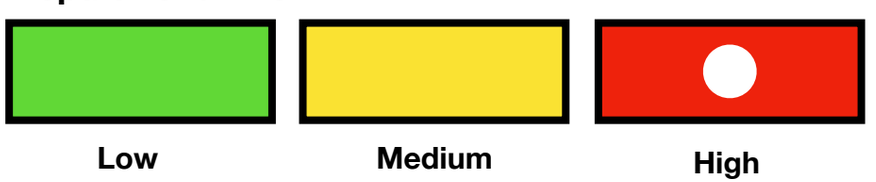
Risk Number — OP_017

The Agency does not have the centralized and formilized user access management system and there is not Access Control Policy to ensure user registration and de-registration, user access provisioning, management of privileged access rights, also revision of users access rights and removal or adjustments of access rights. In addition, there is no Remote Access Management formal procedures. As a result, there is high risks of the potential breach in confidentiality, which might cause damage or impediments of information or theft of information resources. In September 2020, Head of Information Technology Department identified the incident, when some of the Agency's ex-independent contractors had unauthorized access rights to the Agency's source codes, however the incident was immediately resolved and it did not cause any damage for the Agency.

Financial Risk:



Reputational Risk:



Deficiencies in Pension Agency’s Data Leakage Prevention Procedures

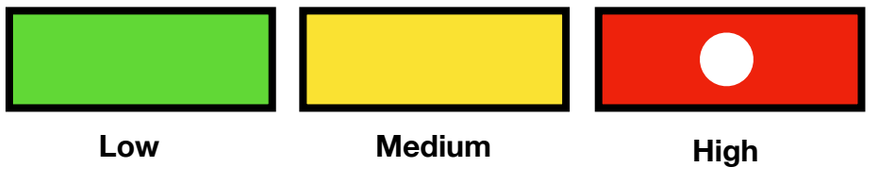
Risk Classification — Technology | Information Security Risk

Process Owner — Information Technology Department

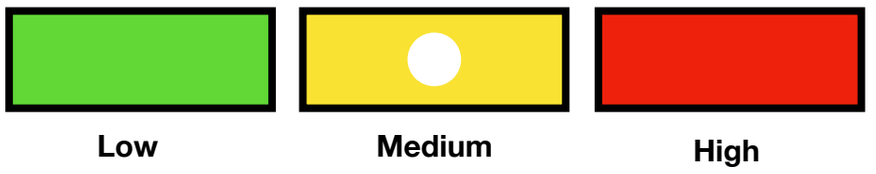
Risk Number — OP_026

In accordance to the PA’s Information Security Officer’s already developed Information Asset and Information Asset Risk Assessment Inventory, the high priority was assigned to the fact that the Agency does not have the set of technical tools and formal procedures to ensure that sensitive data (Personal Data, Professional Secret, Commercial Secret) is not lost, misused or accessed.

Financial Risk:



Reputational Risk:



Information Technology Department

Other IT Risks

Table 4: Short Summary of Identified Risk Factors in Information Technology Department.

Risk ID	Risk Description	Financial Risk	Reputational Risk
OP_020	**Deficiencies in Logging Procedures.** JSON files are sent by the external sources and received by the Agency 24/7 basis with the pre-agreed data structure, however the Agency does not have the Centralized Solution for Log Collection and corresponding log review procedures. In addition, there is deficiencies in error handling procedures, there is not system of clear and compact error messages communicating the problems and triggering immediate corrective actions.	**Medium**	**Medium**
OP_019	**Deficiencies in Network Connection and Monitoring Procedures.** The Agency does not have the communication security policy and network configuration monitoring tools and processes, therefore there is no formilized process to protect the data passed through the network links.	**Medium**	**Medium**
OP_024	**Deficiencies in PA's Database Back Up Procedures.** There is practice of regular backup of information asses, however there is no documented Backup Policy and policy for data classification.	**High**	**High**

*For detailed Risk Description, Classification and Risk Measurement criteria please see the full 2020 Operational Risk Report.

Information Technology Department

Short Summary of IT Risk Treatment*		Priority
OP 016—Deficiencies in IT Governance	**Recommendation 036:** Create IT Steering Committee, which will evaluate and monitor IT activities in organization	High
	Recommendation 037: Create medium-term IT Strategic Document, which will be in line with Pension Agency's overall corporate strategy and in line with national e-Governance Strategy status — ongoing	
	Recommendation 038: Increase IT Financial and Human Resources to ensure proper functioning of electronic pension contribution administration system and its business continuity.	
OP 021 —Temporary Software Licenses	**Recommendation 048:** All Software running critical services identified by the Agency's Information Security Committee must be fully licensed and regularly updated/patched (MS SQL Server, Microsoft Hyper V, Windows Server, Server Operating System, Office 365 etc) status — ongoing	High
OP 024 —Malware Protection	**Recommendation 049:** Appropriate detection, prevention and recovery technical solutions and formilized procedures must be implemented combined with increased activities in Employee Awareness status — ongoing	High
OP 018 — Vulnerability Management System	**Recommendation 041:** Develop Vulnerability Management Policy and corresponding formilized procedures	High
	Recommendation 042: Deploy Penetration Testing of the Agency's Information Systems, including scenarios covering insider threats.	
	Recommendation 043: Deploy Vulnerability Scanner (s) and corresponding monitoring tools	
OP 017 — Access Management	**Recommendation 039:** Develop Access Policy in compliance with ISO 27001 and Deploy corresponding IT solutions (Active Directory)	High
	Recommendation 040: Deploy Vulnerability Scanner (s) and corresponding monitoring tools Deploy Internal Control Mechanisms including Privileged Access Management (PAM) solutions and SIEM	High
OP 026 — Data Leakage Prevention	**Recommendation 054:** Deploy DLP solutions & Develop DLP formilized and Information Data Classification Procedures status — ongoing	High

*For detailed Risk Description, Classification and Risk Measurement criteria please see the full 2020 Operational Risk Report.

Operational Risk Report

OP_001

Short Summary of IT Risk Treatment*		Priority
OP 020—Logging Procedures	**Recommendation 046:** Elaborate Logging Requirements (Policy for Event Logging) and assure that log review procedures are done regularly.	**Medium**
	Recommendation 047: Deploy Security Information and Event Management (SIEM) system and elaborate error handling procedures. status — ongoing	
OP 019 —Netowork Monitoring	**Recommendation 044 & 045:** Implement Network Monitoring System, establish Network Communication Policy and corresponding configuration monitoring process and in addition, deploy Web Application Firewall. status — ongoing	**Medium**
OP 024 —Backup Policy and Data Classification	**Recommendation 051:** Develop Data Classification document and procedures and deploy Data Classification Tool status — ongoing	**Medium**
	Recommendation 052: Develop and implement backup policy to protect against the loss of data	

*For detailed Risk Description, Classification and Risk Measurement criteria please see the full 2020 Operational Risk Report.

04 Risks Owned by Other Administrative Units

Operational Risk Register

Table 4: Short Summary of Identified Risk Factors in PR, Participant Relations and Administrative Departments

Risk ID	Risk Description	Financial Risk	Reputational Risk	Risk Treatment Short Description
OP_011	**Deficiencies in Public Relations procedures.** The Pension Agency's Public Relations governance framework, which on its part includes financial and technical resources, PR strategy document, information campaigns and brand identity, requires the significant improvements. In addition, there is deficiencies in social media communication process and practices (for details see OP_012 in 2020 Annual Operational Risk Report).	**Medium**	**High**	**Recommendation 027 :** Approve Communication Policy already endorsed by IB minutes
				Recommendation 028: Create PR Strategy, brand identity documents and targeted information campaigns **status — ongoing**
				Recommendation 029: Increase PR Budget and Technical Resources
OP_013	**Deficiencies in Participant Service and Relationship processes.** The significant part of PA's services are delivered to Participants via regional Social Service Agencies, but the quality of services are very low and Participant Relationship Department do not have formilized and documented service quality monitoring procedures (for more details about deficiencies in monitoring process see OP_014 in 2020 Annual Operational Risk Report).	**Low**	**High**	**Recommendation 032:** Revise the Service Agreement with Social Service Agencies
				Recommendation 033: The Director of PA in accordance to the Article 8, paragraph 3 must present to the Supervisory Board plan for the development and improvement of the funded pension scheme, where there will be discussed accessibility and availability of participant services across all the administrative divisions of Georgia
OP_028	**Deficiencies in PA's tendering procedures.** There is not formalized market research procedures in the Agency, therefore there are incidents, when announced tenders are failed or when only the one bidder takes participation in the announced tenders.	**Medium**	**Medium**	**Recommendation 059 & 060:** Formilize and Document the Tendering, Market Research and Monitoring Procedures and define the proper roles and responsibilities **status — ongoing**

*For detailed Risk Description, Classification and Risk Measurement criteria please see the full 2020 Operational Risk Report.

Operational Risk Register

Table 4: Short Summary of Identified Risk Factors in PR, Participant Relations and Administrative Departments

Risk ID	Risk Description	Financial Risk	Reputational Risk	Risk Treatment Short Description
OP_011	**Deficiencies in Physical Asset Security and Safety.** The Agency does not have the full-time security guard, there is no entry identification system for non-employees, there should be formilized camera surveillance procedures, server security infrastructure requires improvement, office electrical system has to be re-orginized.	**Medium**	**Medium**	**Recommendation 055 & 056:** Hiring Security Guard and Electrician part-time employees **Recommendation 057:** Improvements the Technical Infrastructure (SNAPT, SNMP, Generators, etc.) **Recommendation 058:** Establish Formilized Physical & Security Protocols and policies including camera surveillance procedures

*For detailed Risk Description, Classification and Risk Measurement criteria please see the full 2020 Operational Risk Report.

Thank you