****

Technical Assistance Consultant’s Report

Project Number: TA-9332 ARM

August 2018

Armenia: Strengthening Operational Risk Management Framework for Public Debt Management

Draft Report

Prepared by: Arindam Roy

Date: August 29, 2018

For: Asian Development Bank

This consultant’s report does not necessarily reflect the views of ADB or the Government concerned, and ADB and the Government cannot be held liable for its contents. (For project preparatory technical assistance: All the views expressed herein may not be incorporated into the proposed project’s design.

**CURRENCY EQUIVALENTS**

(as of December 2017)

Currency Unit – Dram (AMD)

AMD1.00 = 0.002 $

$1.00 = 484.10 AMD

**ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| ADB | – | Asian Development Bank |
| AMD | - | Armenian Dram |
| CBA | – | Central Bank of Armenia |
| DMFAS | – | Debt Management and Financial Accounting System |
| EU | - | European Union |
| G-Sec | - | Government Securities |
| ICD | - | International Cooperation Department |
| PDMD | - | Public Debt Management Department |
| MoF | – | Ministry of Finance |
| NASDAQ OMX | – | NASDAQ Stock Exchange Armenia |
| MTDS | – | Medium-Term Debt Management Strategy |
| TA | – | Technical Assistance |
| T-bills | – | Treasury Bills |
| T-bonds | – | Treasury Bonds |
|  |  |  |

**NOTE**

In this report, $ refers to US Dollars

Contents

[1. Introduction 3](#_Toc523327582)

[1. Procedures Influencing Operational Risk 3](#_Toc523327583)

[1.1 Front Office 4](#_Toc523327584)

[1.2 Middle Office 5](#_Toc523327585)

[1.3 Back Office 6](#_Toc523327586)

[1.4 Treasury Direct 8](#_Toc523327587)

[2. Operational Risk Management Framework 9](#_Toc523327588)

[3. Business Continuity 11](#_Toc523327589)

[3.1 Current IT situation 15](#_Toc523327590)

[3.2 Missing mitigation measures in the current BCP 16](#_Toc523327591)

[4. Summary Recommendations 18](#_Toc523327592)

# Introduction

Operational risk touches a wide range of traditional activities of a public debt management office. It is often defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”[[1]](#footnote-1). In other words, operational risk includes everything except market, liquidity and credit risks.

This report draws extensively from an earlier report prepared as part of a European Union (EU) technical assistance. Most of the recommendations made in the EU report remains relevant and therefore serves as the main basis for this report. Some of the issues related to operational risk have also been highlighted in the World Bank’s Debt Management Performance Assessment (DeMPA) report. In addition, the report recommends the Business Continuity Plan for PDMD based on a related report prepared by the EU project.

The EU report takes note of significant progress made by the Public Debt Management Department (PDMD) to monitor and mitigate operational risks. In particular, PDMD procedures are now documented. Furthermore, PDMD staff has identified, for the first time, the main operational risks and has drafted a document to handle business continuity. Additionally, the staff identified several measures to mitigate several operational risks and already implemented these measures. The PDMD also completed a first draft of the code of ethics specific to the department, including conflict of interest guidelines.

However, the PDMD is still exposed to major operational risks without any Business Continuity Plan to deal with major disruptions. Above all, any event preventing the access to the PDMD building, or any prolonged failure in the Ministry’s network or power supply, would leave the staff in great difficulty to ensure the continuity of PDMD’s critical activities.

In some cases, solutions must be found at the level of the Ministry of Finance (MoF), rather than the PDMD alone. For instance, the MoF should have a suitable alternate data center outside of the capital, with servers to back-up the ones in the main building.

Additionally, there is still a need to formalize the operational risk management (ORM) structure in the PDMD with an reporting arrangement on any incidents and monitoring of operational risks within PDMD which needs to be coordinated by the middle office in PDMD.

Developing a fully-fledged ORM framework that covers the wide range of risks considered “operational” is a long process which requires building up experience along the years. Consequently, PDMD should continue to focus on handling major operational risks and broaden regularly the spectrum of operational risks to be managed. But, considering the lack of staff which could be designated to execute these tasks, PDMD should keep reasonable expectations and avoid too ambitious targets.

# Procedures Influencing Operational Risk

This section discusses challenges arising from the operational procedures within PDMD with respect to operational risks, Operational risks which are not specific to one procedure, like technology failure or loss of data, are discussed in the section 5 of this document.

## Front Office

The documented procedure to negotiate and finalize external loans is now under the process of finalization as a Ministerial Order. The draft Order specifies the respective role of the PDMD along with other relevant departments like the Budget Process Management Department and the Department of Obligations to the State Budget within the overall coordination mechanism framework by the International Cooperation Department. This should set out the specific responsibilities of the various departments in MoF. This is an important decision allowing the PDMD to be informed earlier of the new loans in the pipeline and advising on its appropriateness with relation to its medium-term debt management strategy (MTDS) priorities. This will also help the PDMD to raise other participants awareness of the MTDS.

The procedure to issue bonds in the international capital markets (Eurobonds) has also been documented. The MoF already issued two Eurobonds since 2013 including buyback operations and this process is now well known by the PDMD staff. In this process, many risks are carried by the selected Lead Manager. Some difficulties happened when the MoF changed the electronic mailbox which caused the loss of some e-mails with the syndication team of the issuance in 2013, but this problem seems to be solved now. Nonetheless, since PDMD staff prevalently use the web-based corporate email instead of the Outlook configured corporate email, the data loss related to such emails occurred. To avoid any future occurrence, it is recommended that there is a clear policy guidance from the IT Department on the use of emails, preferably towards Outlook configured emails which can be stored in the local computer.

***Auctions***

Auctions of the Treasury Bills and Bonds is one of the most critical activity of any debt management office. For primary market auctions and buybacks, primary dealers connect to the auction platform managed by Nasdaq-OMX. The PDMD connects to this Nasdaq-OMX platform, called “Genium I Net”, through the Ministry’s Virtual Private Network (VPN) which requires a username and password. During the auction, the FO officer also needs to connect to the Central Bank network (CBAnet) and Internet.

In case of major disruption of the Ministry’s network, the FO staff responsible for the auction and the Head of FO can always move to the Nasdaq-OMX building, a couple of blocks away, to work from a computer prepared by the Nasdaq-OMX for this type of contingencies. The same applies for the access to the CBAnet in the Central Bank premises located close-by.

After the Primary Dealers have submitted their bids, the FO staff must submit them to the Head of the FO and the Director in order to decide the auction cut-off yield. This process is still quite manual and exposed to human error. For instance, the FO Officer must copy and paste participants bids in an Excel template. Furthermore, the Genium I Net system does not calculate the weighted average yield and the FO Officer must do it aside in an Excel template. This exposes FO to operational risk from human error. Going forward, it would be useful for the Genium I Net system or other middleware connected to the system to generate such reports within an electronic format whereby the FO can analyze and decide on the allocations within the system to avoid any manual inputs.

Additionally, when the bids are submitted, the Genium I Net system produces the cut-off yield based on the bid selected (in ascending order of yields) by the FO official and the total amount of bids received as the allocation amount. The FO Officer must then overwrite manually the desired allocated amount (when it is less than the total bid amount). However, in such instance, the system does not produce any computation that validates consistency between the cut-off yield and the desired allocated amount. It therefore has the possibility to allocate a wrong amount if the FO officer has incorrectly analyzed the total desired allocation amount. This constitutes another source of operational risk. The functionality in Genium I Net system should be amended accordingly whereby it should have an in-built facility to show the desired allocated amount and the relevant cut-off yield as a validation measure. This validation output within the system would be essential based on which the FO can review and decide on the final allocation within the system.

To reduce the risk of human error, the Head of the FO (or another authorized person) verifies the FO Officer inputs. In this particular case, the Head of FO is present when the officer inputs auction results.

In the event of any technological disruptions that could impact the submission and processing of electronic bids, currently there is no alternative back up plan for the PDMD which could lead to serious cash flow problems for the government. To deal with such eventuality, the PDMD in partnership with the NASDAQ-OMX have in place an alternative back up plan where such auctions could be conducted through a combination of electronic (for example, submission of bids through email) and manual process (for example, processing and allocation of the bids). Such process was undertaken during the upgradation process of the auction system in NASDAQ-OMX (Stockholm).

Publication of the auction results are done in the MoF website, but also in the Nasdaq-OMX website and through the CBAnet to mitigate the risk in case the MoF website goes down.

## Middle Office

The Middle Office procedures do not entail specific operational risks that the Front Office or Back Office would usually carry. These operational risks linked to systems access, critical files backups or human errors are discussed in the section 5.

Given that all the analytical work on MTDS and cash flow forecasting performed by the MO is undertaken in Excel spreadsheet based on inputs provided by other units within PDMD and other Departments within MoF, it remains exposed to human risk in its work process. To minimize the potential for such risks, it would be useful for MO to put in place a process whereby a different official is responsible to cross-check the accuracy in the use of input received from other units / Departments; as also the analytical work and the results.

The MO is also tasked with monitoring the compliance of strategic target indicators on a monthly basis based on the outturn of the government debt portfolio. Given that the information is received from BO maintained in Excel template, it would be useful for the MO to cross-check the accuracy of the data in its monitoring functions.

The design of the MTDS require good risk management knowledge (financial risks), and forecasting cashflows requires good treasury management knowledge. Thus, the MO staff must be trained adequately through specialized seminars, trainings and other courses. The MO should pay particular attention to training and coaching of new staff when preparing the training plan.

## Back Office

**Debt Data Records and Documentation**

Currently, the PDMD has got written procedures for debt recording and validating and original loan agreements are stored adequately in the Ministry of Foreign Affairs. However, debt administration records include supporting documents on loans disbursements, Eurobonds issuances and debt service payments, which are currently stored in the lockers of the Back-Office unit (BO), which are not fire and flood proof.

The data recorded on external loans are cross-checked with the creditor statements on a semi-annual basis before the time of making debt service payments for any reconciliation Data on Treasury Bills and Bonds are also periodically validated with the central depositories data maintained by the CBA before making debt service payments on them. s such, debt data maintained by PDMD is of good quality and validated as part of the debt service payments process at least on an annual basis.

**Debt Management System and Debt Database**

The procedures to record debt data in the database (loans agreements, disbursements, debt service payments etc.) are now documented. Debt data are recorded in the database by the BO Officer and then verified and validated by the Head of the BO.

Currently, the debt database is maintained in excel spreadsheet in PDMD. In parallel, the use of the DMFAS system within PDMD for recording external loans is continuing. The main part of external loans had been recorded with cut-off date as of end 2007. The DMFAS system currently records all information related to loan terms and disbursements transactions. The system is being used for obtaining information on disbursements, especially for multi-currency loans which is difficult to compute manually. The authorities have recently started the process of building external debt data in the DMFAS system starting from the signing date of loan agreement.

Maintaining all debt recording data within an excel spreadsheet is another potential source of operational risk with the possibility of human error or tampering, intended or otherwise. This situation exposes the PDMD to an important data integrity risk, considering Excel files can be easily damaged and user activities cannot be tracked like in a debt management system.

It would be essential to migrate and update and validate all external debt data records in the DMFAS system, with a phased approach whereby external debt database could be developed in the first instance on a loan-by-loan basis including records of debt service payments. Subsequently, domestic debt data on an instrument basis (not bid basis) could be recorded in the DMFAS system by developing an electronic interface between the central depository system and DMFAS system. This will ensure an integrated debt database in DMFAS. The MoF is in the process of developing a new IFMIS system wherein, a Debt Module is also planned to be developed as part of the new system which would serve as the debt management system for PDMD. Depending on the timing of completion of its development, PDMD can also consider developing its integrated debt database in the new Debt Module system instead of DMFAS.

Access to the system through a unique username and password for each user should be mandatory for the use of the system. The procedure to control access to the DMFAS system is now documented. The BO and the IT Department have now agreed to separate the functions of database administrator between them. The Head of BO will be responsible to create users’ profiles and access codes, activation/dis-activation of system’ modules and functions, while the IT Department will be responsible for all the IT system part and the backups of the database.

Notwithstanding this arrangement, the IT Department and Head of BO still needs UNCTAD to provide them a DMFAS database administrator training, while PDMD users will need functional trainings on the compilation of debt database. DMFAS trainings are currently planned under the framework of the ADB technical assistance program.

While developing its debt database in DMFAS, it will be imperative for the PDMD to review the existing written procedures for controlling access to the debt management system. This should be reviewed before the use of the system is activated and the review should be continued on an annual basis.

The debt management system should also produce an audit trail showing all the activities done by the user in the system. Information from such audit trail which should be used in the monitoring of ORM and through internal and external audits.

The Excel debt database is stored in the local computers of the BO Officer. In case of problem with this computer, the database can be recovered from other backup copies (in USB keys). To avoid the risk of data loss in PDMD premises due to any hazards, it is recommended that the database be stored in a secured filing system in a separate location, in the MoF server. For this purpose, PDMD needs to coordinate with the IT Department to provide them with a dedicated facility for storing public debt database.

Currently, the PDMD performs monthly backups of the debt database. This is in view of the long time taken to perform backups on debt database. To minimize the risk of data loss, it is recommended that PDMD perform a weekly back up of the database. Once the IT system is improved further, the frequency of backups could be enhanced to a daily process.

The debt database backups are currently not stored in a separate and secure location, they are only stored on external drives in the PDMD building and on USB keys. To enable retrieval of data in case of any event, it is recommended that monthly back up of the debt database is undertaken in the MoF server. . This process should start with the existing excel databases which would need to be eventually complemented / replaced by the DMFAS database once it is established. The backup location should ensure that the database is protected from incidents such as theft, fire, flood (and others) that can damage backups.

***Debt payments***

The procedures to prepare and execute debt payments are well documented. PDMD prepares a monthly schedule of all debt service payments and shares it with the Treasury Department and CBA. In the case of any discrepancies, PDMD will liaise with the respective Department to reconcile the projected debt service payments.

Debt service payments are initiated by the PDMD for external loans and Eurobonds, through payment orders, which is transmitted through the Treasury Department and CBA for externalization of payments in foreign currencies. The “four eyes” principle is being followed by PDMD for effecting det service payments after due cross-checking with their records and creditor statements.

Under the existing arrangement, for debt service payments on Treasury Bills and Bonds, the CBA makes automatic debit of the government account in the TSA maintained. Notwithstanding this arrangement, the PDMD prepares debt service instructions on government securities for the Treasury Department to facilitate its accounting of interest and principal payments on such debt obligations based on the budget codes.

Currently, the PDMD prepares most payment orders on external debt electronically, but some orders are still processed manually. The manual process related to payments for Eurobonds is undertaken through their fiscal agent after the manual payment order provided by PDMD to the CBA is confirmed with the fiscal agent following which the CBA effects the payments to the fiscal agent on an aggregate basis. Manual process for payments also include some specific creditor days which use next business day payment principle. To minimize risks related to timely payment of debt service payments, it will be important for PDMD to undertake all payments electronically.

The BO uses the Treasury Payment System (TPS) to process the payments. The Company Lsoft is the provider of the TPS system which is located in the servers based in the main building of the MoF. The main user of the TPS and the department responsible to monitor the system is the Operational Department. But, other departments of the Ministry are using it, especially the PDMD where all the units do use it.

If the BO Officer is not available, another BO Officer or the Head of the BO can execute the procedure and the relevant payment documents will be validated by the Head of BO or the Director of PDMD. The “four eyes” principle must always be respected to process the payment.

If the TPS is not working, the payment orders can be written manually in the appropriate paper form and brought to the CBA physically. Such arrangement is useful to avoid any risk of missed payments due to technological problems.

As a long-term measure for further strengthening risk management, payment orders could be processed through a Straight-Through-Processing (STP) payment system and written procedures for debt servicing reviewed annually.

## Treasury Direct

Treasury Direct refers to the retail debt program allowing individuals to purchase directly government securities, mainly saving bonds, in five selling point centers of Yerevan. It is also the name of a unit of the PDMD responsible for monitoring the retail debt program.

Recently, the PDMD also implemented an internet platform for Treasury Direct where citizens can register and buy Government securities. The internet platform is managed by Nasdaq-OMX.

For Treasury Direct, PDMD is using mainly 3 systems:

1. The system “Depend”: an interface to the Central Depositary system owned by the Nasdaq-OMX Stock Exchange for the registering of securities in Armenia.
2. The Treasury Direct website, with administrator access. In this website, individuals can purchase online saving bonds and other government securities.
3. The system “Bankmail”: an interface to electronic payment system of the banking sector managed by the Central Bank.

For the first two systems, interfaces are installed only in one computer in the Treasury Direct Unit of the PDMD. For both, software is located in a server in the main building of the MoF. The access to these systems is done through the Ministry’s VPN network. Access is also possible from the Treasury Direct selling point centers.

In case of major disruption, the Head of the Treasury Direct Unit has also the possibility to access directly to the system “Depend” at the Stock Exchange, and to the system “Bankmail” at the Central Bank.

For the Treasury Direct system, the Head of the Treasury Direct Unit has an administrator access with password which is linked to the IP address of her computer and two other computers in the PDMD.

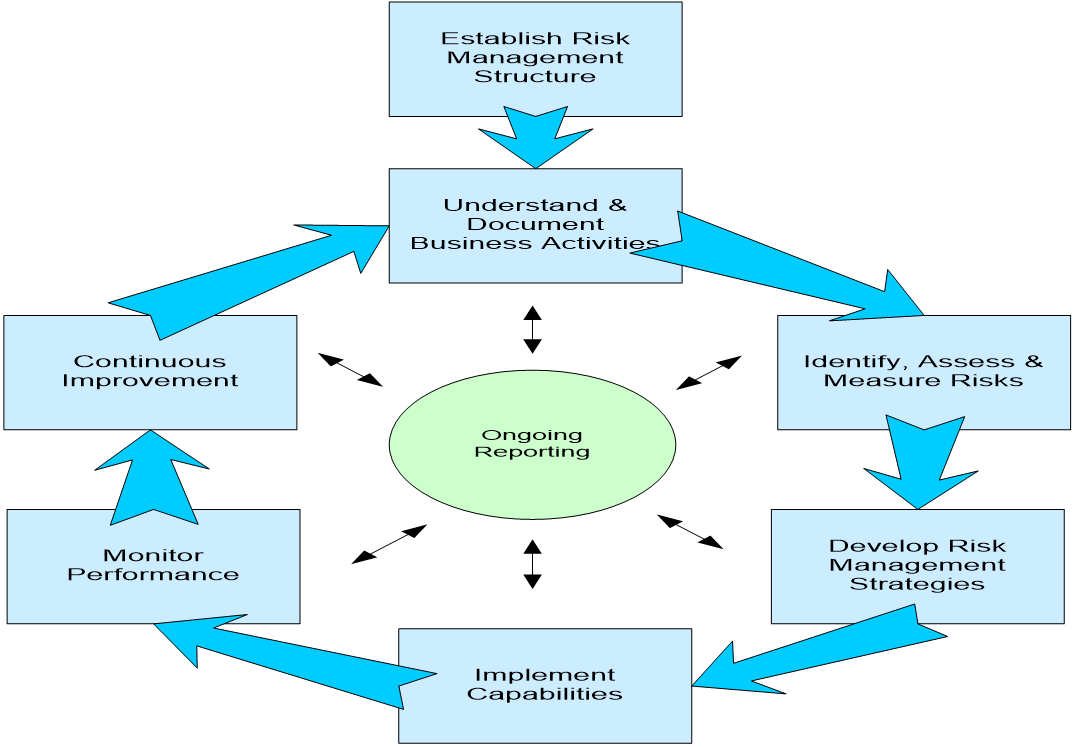
***Main risks***

* For practical reasons, the Treasury Direct Unit has not been divided into Front, Middle, Back Office areas. This is perfectly understandable due to the modest volumes transacted in the retail debt program. But, this is also a source of operational risks resulting from the weak segregation of functions. Indeed, the same person is performing front and back office tasks. For example, the Head of the Treasury Direct Unit is the administrator of the website, registers customers’ securities purchases and, then, confirms the transactions.
* The system “Depend” does not produce reliable reports figures. Thus, the Head of the Treasury Direct Unit has to recalculate the figures in an Excel spreadsheet, increasing human error risks.
* The creation of the internet platform and associated software has reduced the manual workload of the Treasury Direct Unit, which is a positive development. But, at the same time, it has increased the Unit dependence on technology and, therefore, augmented exposure to technology failures. For example, if the Head of the Treasury Direct Unit cannot access her administrator “window”, it is impossible to register securities purchases and update outstanding amounts held by individual investors. A backup solution could be implemented, in case of technology failure, to allow exceptionally using the old paper-based process.

# Operational Risk Management Framework

With the support of the EU TA assistance, the PDMD started to implement an ORM framework similar to the one developed by the World Bank and summarized in the figure below:

***Figure 1. ORM framework***



*Source: Six-Steps ORM Framework - Guidance for ORM in Government Debt Management, World Bank, 2010*

The staff worked on understanding and documenting main business activities (step 1), identifying, assessing and measuring operational risks (step 2) and developing several risk management strategies to prevent, reduce or sustain risks (step 3).

Some risk management strategies are even starting to be implemented (step 4), like the separation of the debt database administrator functions between the IT department and the Head of the BO. Monitoring the performance of each unit (step 5) and improving continuously operational risk management (step 6), as well as PDMD reporting on ORM, are steps not undertaken yet.

But, above all, the PDMD still needs to establish a formal operational risk management structure, which is the foundation of the ORM framework. Usually, the structure to manage operational risks includes a first level monitoring, where all the units are monitoring the operational risks associated with their own activities and reporting continuously incidents, improvements, new risks identified to the second level.

This second level is the team responsible for ORM and control, usually located in the Middle Office (MO). Then, the second level would report directly to senior management and prepare, once a year, a formal ORM report to the risk management committee of the MoF.

Considering PDMD has limited number of staff who could be dedicated to ORM, this structure should be simplified and tasks reduced to the most essential ones. Therefore, each unit will monitor its own operational risks and report continuously to the unit Head and MO Head directly of any incidents experienced.. Reporting should be based on a standardized template with any additional information provided being kept to the simplest expression (a simple word page, for example). The MO will be responsible for responsible for coordinating with the other units and filing units’ messages.

The MO should organize regular meetings on risk management with the heads of the other units and the Director – once a quarter – and monitor if the decisions taken during these meetings are implemented. If some topics require it, they should be submitted for decision by the Deputy-minister. The meeting will discuss the reasons and sources for occurrence of key incidents; its impact on the government’s reputational risk, liabilities and budget; and the solution for risk control and mitigation. A reporting template will be required to be prepared by PDMD based on which designated officials in individual units will report to the unit Head and MO Head simultaneously as and when the occurrence of such incidents takes place. For this purpose, the MO will need to consolidate information on key incidents on a monthly basis and monitor all types of operational risks across PDMD.

Once a year, the MO will be responsible for gathering other units’ inputs to update the BCP document. MO should also prepare a short ORM report focusing on (i) main new exposure to operational risk, (ii) suggested mitigation measures, (iii) actions to be undertaken by other units or the IT department to implement these measures.

If necessary, the MO could develop new operational risk management policies and procedures. But, considering this position will not be a full-time one, these tasks should not be too ambitious and overload the person responsible for ORM.

It must be clear that if the PDMD wants to implement a more sophisticated ORM structure, it will need to name one, or more, full-time staff for operational risk management.

Separately, the MO will report on overall operational risks and compliance on the Business Continuity Plan to the Director PDMD through an annual report, whereby any existing risks of major or significant category will be required to be flagged to the Deputy Minister for suitable action and resolution. Based on the availability of resources within PDMD, such reporting could be subsequently extended to quarterly reports,

# Business Continuity

A Business Continuity Plan (BCP) is part of operational risk management. It serves as an action plan during incidents and to recover critical activities afterwards. It allows sustaining the objectives and the strategy of the entity in the face of disruptive events. A disruptive event is any event (fire, systems failure, natural disasters, etc.) that interrupts the essential activities of the entity and could eventually prevent critical products and services to be delivered to clients.

It is important to understand that risks addressed by the BCP are only a portion of all the operational risks faced by a debt management office, explicitly the risks associated to business continuity. For example, inadequate recruitment policies or inefficient procedures can affect the performance of the PDMD, but not necessarily the continuity of its critical activities, and therefore are not handled in the BCP.

The PDMD has completed a draft of the Business Continuity Plan (BCP) with support from EU TA project. This BCP document is covering only the PDMD. The MoF does not have any BCP document. Notwithstanding progress made in this area, the PDMD is still vulnerable to any negative event that would hit the Ministry and prevent staff from working at their workplace. PDMD would hardly be in the capacity to ensure quickly the continuation of its critical activities.

All the units of the PDMD should be involved in maintaining and improving this BCP, but the Middle Office is responsible for collecting information and updating the document on a regular basis. Indeed, the plan is an essential part of operational risk management and, therefore, the risk unit takes the lead in the design and implementation of the BCP.

The BCP is designed to improve PDMD capacity to recover from disruptions and to reduce the impact of disruptions on PDMD critical activities. To this end, the PDMD implements measures to mitigate operational risks, if feasible. The operational risks are identified and classified according to their:

* Probability of occurrence: Very high / high / medium / low
* Severity of impact: Important / Significant / medium / low

Consequently, the BCP contains (i) a list of the operational risks identified by the PDMD (Table 1), (ii) a general description of critical processes, staff and systems, (iii) an assessment of potential impact of operational risks on PDMD critical activities, the Business Impact Analysis, (iv) a review of measures implemented to mitigate operational risks, and (v) a plan to resume critical activities following a major incident, the Disaster Recovery Plan. These five components must be reviewed annually.

***Table 1. Categories of operational risks***

|  |  |  |
| --- | --- | --- |
| Infrastructure and Technology Failure | | |
| 1. Hardware failure | 2. Software failure | 3. Internal Network Failure |
| 4. Failure of Communication lines of Ministry | 5. Data Corruption and Data Security | 6. Building and materials deficiencies |
| 7. Power Failure | 8. Poor maintenance |  |
| Incidents where access to premises is denied | | |
| 9. Building Fire or Flooding | 10. Gas Explosion | 11. Civil Disturbances |
| 12. Chemical Incident | 13. Sabotage |  |
| Personal, Management and Other Human Failure | | |
| 14. Key staff risk | 15. Human Error | 16. Poor training or inadequate supervision |
| 17. Lack of policy guidance | 18. Poorly specified delegations | 19. Failure to follow or adhere to administrative practices |
| 20. Fraud, Corruption or non-respect of code of conduct |  |  |
| Key services providers or Groups Dependencies | | |
| 21. Failure of key service providers (telephone, internet, banking, etc.) | 22. Third party providers (Central Bank and other outsourced operations) | 23. Incident on critical groups (Pandemic, travel, food poisoning, etc.) |
| Natural Disasters | | |
| 24. Earthquakes | 25. Landslides | 26. Severe Flooding |

PDMD will evaluate the impact on its critical business operations of each category of risk identified against the following criteria to determine the severity of the impact (Table 2):

* Impact to the reputation of the PDMD or the MoF
* Impact to resources needed to handle the problem and reporting
* Impact to the business of the PDMD

***Table 2. Criteria for the assessment of impact of risks***

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment of** | **Reputational** | **Financial Loss** | **Impact on Outputs** |
| **Impact** | **Impact** | **Impact** | **or Budget Variance** |
| **Very-High** | Loss of stakeholder confidence | Reported in government’s financial statements | Significant delay in achieving outputs |
| Loss of market confidence | Significant amount of time spent dealing with issue (i.e. greater than 30 person-days) | Significant debt service budget variance |
| Loss of trust, e.g. from primary dealers |  | (i.e. greater than 10%) |
| Extensive media coverage |  |  |
| High-level ministerial enquiry [or resignation] |  |  |
| **High** | Strained stakeholder relationships | Reported to minister | Large delay in achieving outputs |
| Temporary loss of market confidence | Large amount of time spent dealing with issue | Large debt service budget variance |
| Moderate media coverage | (i.e. between 20 and 30 person-days) | (i.e. between 5% and 10%) |
| Ministerial enquiry |  |  |
| **Medium** | Increased stakeholder attention | Reported to the entity responsible for monitoring the DMU | Moderate delay in achieving outputs |
| Market confidence not affected | Moderate amount of time spent dealing with issue (i.e. between 10 and 20 person-days) | Moderate debt service budget variance |
| Minor, if any, media attention |  | (i.e. between 3% and 5%) |
| Major attention within ministry/DMU |  |  |
| **Low** | Stakeholder and market relationships intact | Included in internal monthly reports | Little or no delay in achieving outputs |
| No media coverage | Minimal amount of time spent dealing with issue | Little or no debt service budget variance |
| Internal ministry/DMU enquiry | (i.e. less than 10 person-days) | (i.e. less than 3%) |

For each critical process and systems, staff must associate to each category of risks identified a probability of occurrence of the risk and a severity level of impact if this risk were to materialize. By representing the probability of occurrence against the severity level, a risk matrix can be obtained in order to complete the Business Impact Analysis. The person responsible for the BCP maintenance will update annually the risk matrix, based on information provided by each unit.

Following the draft BCP plan developed through support from EU TA project, this mission reviewed the risk matrix in consultation with MO in PDMD (Table 3).

*Table 3. Risk Matrix*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Low | Medium Impact | High | Very High Impact |
|  | Impact | Impact |
| Very High Probability |  | 4 | 3 | 7 |
| High Probability |  |  | 2, 5, 17 |  |
| Moderate Probability |  | 6, 8, 11, 14, 16, 18, 23 | 1, 19 | 5, 9, 20, 21, 22, 24 |
| Low Probability | 25 |  | 13, 26 | 10, 12 |

Based on this risk assessment, PDMD will be required to investigate and determine mitigation measures in priority for the category of risks included in the red cells of the matrix. In other words, high priority will be accorded to the category of risks having the most severe impact on PDMD business activities and the highest probability to occur.

The PDMD should select the most effective and suitable treatment of operational risks associated with each critical activity. It means making a choice between the following possible approaches:

* **Prevent or avoid** the risk, by taking measures to reduce or eliminate the probability of occurrence of an event.
* **Transfer** the risk, by outsourcing it or taking an insurance with a third party.
* **Contain** the risk, by using controls or other techniques to limit the severity of consequences of the risk materialization.
* **Accept** the risk and recover from the disruption by resuming critical activities as successfully and rapidly as possible.

## Current IT situation

The server room of the Ministry of Finance (securitized room) is located in the main building of the MoF (Melik Adamyan). The servers are running applications used by the PDMD, notably the Treasury Payment System (TPS), DMFAS, the Treasury Direct system, and the CBAnet. These servers also ensure the functioning of the Ministry VPN network.

The PDMD office is situated in another building close-by (Tigran Mets). PDMD computers are connecting to the Ministry’s network through the only communication line between the Tigran Mets building and the Melik Adamyan building. This line is also connecting telephones and Internet access.

The IT Department is backing up applications, at the end of the day, on virtual servers. Virtual servers are used by IT engineers to convert one physical server into multiple virtual servers which are independent. In doing so, hardware costs are reduced without preventing backups to be performed on different physical machines (servers). Currently, the IT Department runs 37 applications on virtual server, including DMFAS.

The Ministry have recently established an alternate data center in Dilijan with physical backup servers. The alternative data center in Dilijan is a mirror server of the MoF server in Yerevan,

The MoF does not have an alternate operational site to relocate critical staff and ensure business continuity after a major incident. The MoF is also considering using the alternative data center in Dilijan as an operational recovery site where the PDMD staff could work in the event of a major disruption in the main building.

This is an indispensable step to reduce current risk exposure to potential systems failures and events preventing staff from working in the MoF premises. This is important for the PDMD and the whole MoF.

***Storage***

To allow PDMD units backing up their files, the IT Department has dedicated a capacity of 2 Terabytes of storage on the virtual server. The virtual server in the MoF is used for day-to-day work of the MoF and not designed to store debt database. Thus, PDMD can use the network of the Ministry to do backups of the databases and store them (NAS, network attached storage) through a dedicated server in the MoF which can also be backed up in the alternative data center in Dilijan.

Currently the IT Department does not provide any staff to perform backups and storage tasks. This must be done by the staff of the PDMD, otherwise there will be no backups. This kind of tasks can be quite time-consuming, especially if PDMD staff wants to perform it daily. Going forward, IT staff should ensure backups are performed regularly.

***Disruption***

If a major disruption occurs and prevents PDMD staff to access their computers, it would be very difficult to ensure business continuity because PDMD does not have any prepared computers in others Ministry’s buildings. Although, theoretically, PDMD staff could connect to the Ministry’s network and run their activities from another building of the Ministry, in practice it would be very difficult.

The PDMD should request the IT Department to organize a room in the main building of the Ministry (Melik Adamyan) to relocate staff in case of events preventing access to the PDMD’s building (Tigran Mets). This room should be equipped with 2 or 3 computers reserved for PDMD staff, with full access to the Ministry’s network and containing the necessary applications to perform critical processes of the PDMD. These applications have been listed in the BCP in the table of critical systems.

The Ministry’s network is not accessible remotely (from outside of the Ministry buildings). Although PDMD staff can access their official e-mail accounts from home, or anywhere outside of the MoF buildings, they cannot access Ministry’s network for access to PDMD documents remotely.

The IT Department could consider giving a securitized remote access to the Ministry’s network for PDMD documents as a “read-only” facility to all staff of the PDMD. PDMD staff could use this remote access in case of contingencies and work from home afterhours.

## Missing mitigation measures in the current BCP

PDMD has put in place a series of operational risk mitigation measures in recent years and during the technical assistance provided by the EU. However, additional mitigation measures could be implemented. This section lists missing standard mitigation measures for the following risk category:

**Lack of policy guidance**

* Policy guidance to save and store electronic files within PDMD in the MoF server. The MoF has a shared drive where the users can save their files, but there are no written guidelines for PDMD on when and how to use it in terms of the documents stored as well as who could have access to them.
* IT Department did not provide any written policy for the security of the shared drive of the Ministry. Such policy could explain the frequency of backups, which folders are backed up, who has restricted access to which folders, etc.
* There is no report on the performance of the staff, because there are no clear indicators to measure staff performance. For instance, one could implement an indicator showing if staff are recording on time debt operations in the database.
* PDMD and IT Department could coordinate to prepare written guidelines to save electronic documents, use properly the shared drive of the Ministry and ensure files security. IT Department could organize a training on this topic for the employees of the MoF.

**Key staff risk**

* There is generally no handover period between the staff leaving the PDMD and the newcomer.
* However, there is a low staff turnover and head of units are experienced. Most of them are working in the MoF since several years.

**Absence of training or inadequate supervision**

* Lack of individual training plans and personal development plans
* Head of units are not participating to any training on managing resources.
* Based on the existing semi-annual appraisal taking place in PDMD, an annual training and development plan can be prepared for each staff in consultation with them.

**Data Corruption and inadequate data security**

* Ministry does not allow a cloud backup solution
* IT Department does not train staff to use the shared drive

**Hardware/Software failures**

* No alternate data center for servers
* No registry of incidents. If the staff calls IT department, the incident is not logged, there is no number associated with the incident to monitor it.
* There is no IT helpdesk to answer Ministry’s staff requests.
* IT Department could consider establishing an IT help desk to register and follow up all the incidents of the Ministry of Finance. This would improve IT Department time of response and the prioritization of intervention.

**Telecommunication failures**

* Only one communication outside of the building of the PDMD. One single line for phones, Internet and Ministry’s network.
* A second communication line (backup line) could be installed between the Tigran Mets building and the Melik Adamyan building. This line allows connection to the Ministry’s network, telephones and Internet access. However, in the long run, the MoF will need to implement a double redundancy by having a second line directly connected to an alternate data center, and close the triangle with a connection between the alternate data center and the main building.

**Infrastructure and Document storage deficiencies**

* Debt administration documents (i.e. withdrawals applications, Eurobonds issuance and debt service supporting documents) are stored in closed lockers, but not in a secured fireproofed room. There is a need to store these documents in a fireproof and secured lockers and also retain scanned copies of them in electronic format.
* There is no clear policy defining who must acknowledge the receipt of debt administration documents, recording of the date of receipt and who is responsible to scan documents before sending them to the other units.
* No uninterruptible power supply (UPS) battery in the case where regular electricity power source fails.
* No alternate electricity generator for the PDMD building in the case where regular electricity power source fails.
* An alternate electricity generator and UPS batteries should be available in the PDMD building in the case where electricity power source fails is not uncommon.

# Summary Recommendations

This section summarizes the key recommendations for strengthening operational risk management and implementing a business continuity plan. The recommendations have been prioritized as short, medium and long-term deliverables based on their criticality and lead time required for implementation.

|  |  |  |
| --- | --- | --- |
| Recommended Action Plan to Strengthen ORM and BCP | | |
| Debt Management Process/Dimesnions | Recommendation | Implementation Time |
| Front Office Procedures: | | |
| External Loan Negotiation | Ministerial Order to negotiate and finalize external loans that specifies the respective role of the PDMD along with other relevant departments | December 2018 |
| Auction of Government Securities | iGenium I Net system in NASDAQ-OMX or other middleware connected to the system to generate reports within an electronic format whereby the FO can analyze and decide on the allocations within the system to avoid any manual inputs. | December 2019 |
| The functionality in Genium I Net system should be amended to have an in-built facility to show the desired allocated amount and the relevant cut-off yield as a validation measure, before the FO can review and decide on the final allocation within the system. | December 2019 |
|  | Apply the “four eyes” principle by assigning separate responsibilities to officials within FO between undertaking the analysis on bid allocation and recording the final confirmation validating the allocation advice through the Genium I Net system. | December 2018 |
| Middle Office Procedures: | | |
| Risk Analysis | To minimize the potential for human risks on analysis undertaken in Excel spreadsheet , MO should put in place a process whereby a different official is responsible to cross-check the accuracy in the use of input received from other units / Departments; as also the analytical work and the results. | December 2018 |
| Risk Monitoring | MO to cross-check the accuracy of the data received from BO maintained in Excel template, for monitoring its debt target compliance functions. | December 2018 |
| Back Office Procedures: | | |
| Debt Data Records and Documentation | Store debt administration records including supporting documents on debt in lockers within PDMD which are fire and flood proof. | December 2019 |
| Maintain scanned documents of existing debt records in electronic format and store it with regular back ups. | December 2019 |
| Debt Management System and Debt Database | Update and validate all external debt data records in the DMFAS system, with a phased approach on a loan-by-loan basis including records of debt service payments. | December 2019 |
| Develop an electronic interface between the central depository system and DMFAS system or the Debt Module within the planned IFMIS. This will ensure an integrated debt database. | December 2019 |
| Provide secured access to DMFAS system through a unique username and password for each user within PDMD. Review the existing written procedures for controlling access to the debt management system. | December 2018 |
| Provide training on DMFAS database administrator training to IT department, while PDMD users will need functional trainings on the compilation of debt database | December 2018 |
| Produce an audit trail from DMFAS which should be used in the monitoring of ORM and through internal and external audits. | December 2020 |
| To avoid the risk of data loss, debt database should be stored in a secured filing system in a separate location, in the MoF server as a dedicated facility for storing public debt database. | December 2018 |
|  | PDMD performs a weekly back up of the database. Once the IT system is improved further, the frequency of backups could be enhanced to a daily process. | December 2018 |
|  | To enable retrieval of data in case of any event, it is recommended that monthly back up of the debt database is undertaken in the MoF server. The backup location should ensure that the database is protected from incidents such as theft, fire, flood (and others) that can damage backups. | December 2019 |
| Debt Payments | Prepare all debt payment orders electronically. | December 2018 |
| As a long-term, process payment orders through a Straight-Through-Processing (STP) payment system. | December 2020 |
| Review annually written procedures for debt servicing. | December 2018 |
| Treasury Direct | Separate the back (confirm the transaction and administrate the website) and front (register the securities) office functions on retail debt program within Treasury Direct. | December 2018 |
|  | Produce reliable reports within “Depend” system to avoid Treasury Direct Unit to recalculate the figures in an Excel spreadsheet. | December 2018 |
|  | Establish a backup solution using the old paper-based process to register securities purchases and update outstanding amounts of individual holdings, in case of technology failure, to allow exceptionally. | December 2018 |
| ORM Framework | PDMD establishes a formal operational risk management structure, which is the foundation of the ORM framework. This should include: 1) understanding and documenting main business activities; identifying, assessing and measuring operational risks; 3) developing several risk management strategies to prevent, reduce or sustain risks; 4) implementation of risk management strategies; 5) monitor the performance of each unit; 6) continuously improving ORM; and 7) reporting on ORM. | December 2018 |
|  | Monitor the performance of each unit within PDMD through a first level monitoring, where each unit will monitor its own operational risks and report continuously on incidents, improvements, new risks identified to the unit Head and MO Head directly of any incidents experienced. Reporting should be based on a standardized template. The MO will be responsible for responsible for coordinating with the other units and filing units’ messages.  . | December 2018 |
|  | Organize regular meetings on risk management with the heads of the other units and the Director – once a quarter – and monitor if the decisions taken during these meetings are implemented. | December 2018 |
|  | Through a second level, the MO within PDMD would report directly to senior management and prepare annually a formal ORM report to the risk management committee of the MoF | December 2019 |
|  | Consolidate information on and monitor all types of operational risks across PDMD and report on major risks to the Deputy Minister for suitable action and resolution | December 2019 |
|  | MO will report on overall operational risks and compliance on the Business Continuity Plan to the Director PDMD through an annual report, whereby any existing risks of major or significant category will be required to be flagged to the Deputy Minister for suitable action and resolution. Based on the availability of resources within PDMD, such reporting could be subsequently extended to quarterly reports,  . | December 2019 |
| Information Technology, Infrastructural and Human Resource Issues: | | |
| Disruption | Establish operational recovery site outside Yerevan where the PDMD staff could work in the event of a major disruption in the main building. | December 2019 |
|  | The IT Department should organize a room in the main building of the MoF (Melik Adamyan) to relocate staff of PDMD in case of events preventing access to the PDMD’s building (Tigran Mets). | December 2018 |
|  | The IT Department could consider giving a securitized remote access to the Ministry’s network for PDMD documents as a “read-only” facility to all staff of the PDMD. PDMD staff could use this remote access in case of contingencies and work from home afterhours. | December 2018 |
| Telecommunications | Install a second communication line (backup line) between the Tigran Mets building and the Melik Adamyan building. This line allows connection to the Ministry’s network, telephones and Internet access. | December 2018 |
| In the long run, the MoF implements a double redundancy by having the second line directly connected to an alternate data center. | December 2019 |
| Power | An alternate electricity generator and UPS batteries should be available in the PDMD building in the case where electricity power source fails is not uncommon. | December 2018 |
| Storage | IT staff should ensure backups of PDMD database are performed regularly. | December 2019 |
| PDMD can use the network of the Ministry to do backups of the debt database and store them through a dedicated server in the MoF which can also be backed up in the alternative data center in Dilijan. | December 2018 |
| Training and Supervision | Based on semi-annual appraisal process within PDMD, a training and development plan can be prepared for each staff in consultation with them.. | December 2019 |
| Hardware / Software Failures | IT Department could establish an IT help desk to register and follow up all the incidents of the Ministry of Finance. | December 2019 |
| IT Policy Guidance | A clear policy guidance from the IT Department on the use of emails, preferably towards Outlook configured emails which can be stored in the local computer. | December 2018 |
|  | PDMD and IT Department could coordinate to prepare written guidelines to save electronic documents, use properly the shared drive of the Ministry and ensure files security. | December 2019 |

1. Basel II, 2004, Bank for International Settlements. [↑](#footnote-ref-1)