PUBLIC DEBT MANAGEMENT
DEPARTMENT – MINISTRY OF FINANCE

Report on operational risk monitoring framework

Include progress made during the technical assistance and recommendations going forward

September 2017

Contents

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]. In other words, operational risk includes everything except market, liquidity and credit risks.

Since the inception report of the technical assistance was submitted to the Armenian authorities in March 2016, significant progress has been made to monitor and mitigate operational risks in the Public Debt Management Department (PDMD).

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.

However, the PDMD is still exposed to major operational risks. 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 and to name officially a "champion" of operational risk in charge of coordinating operational risk monitoring with all the units of the PDMD and reporting to the Director.

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.

1. Progress made since the inception report

Documented procedures have been developed for the main debt management activities. The procedures include (i) negotiation of external loans, (ii) issuance of bonds in the international capital markets, (iii) loans disbursements, (iv) debt data recording and validation, (v) external debt servicing, (vi) domestic debt servicing, (vii) access control to the debt management system. The section 3 of this document discusses the procedures.

The PDMD had no formal framework to manage operational risks. In other words, the staff had no guidance for assessing risk exposures from incidents or events that can impact critical activities of the department and, then, manage these risks. Under this technical

[1] Basel II, 2004, Bank for International Settlements.

assistance, an ORM framework was presented to the PDMD in line with the World Bank guidelines for government debt management.

The PDMD has already completed the following steps for establishing this operational risk management framework:

- Critical business processes, staff and systems have been identified and documented.
- A first identification of operational risks associated with the critical processes was done.
- A first business impact analysis has been performed.
- A first list of mitigation strategies has been proposed. Several mitigation strategies were already implemented in the PDMD.
- Following these activities, a first draft of the Business Continuity and Disaster Recovery plan has been written.

The section 4 of this document discusses the ORM framework and suggests a provisional structure to manage operational risks, while the section 5 discusses the Business Continuity Plan (BCP) which is a separate document prepared by the PDMD during this technical assistance.

The PDMD also completed a first draft of the code of ethics specific to the department, including conflict of interest guidelines.

2. Improving DeMPA scores from 2014

Although PDMD made substantial progress in the management of operational risk, there are still many gaps to close. For instance, Debt data security is still a challenge and the PDMD would only get slightly better votes, in case another DeMPA assessment would be performed by the World Bank, compared to the ones obtained in 2014.

The following paragraphs are discussing DeMPA scores for the Debt Performance Indicator (DPI) number 12, dedicated to Debt Administration and Data Security, and what is needed to improve it. In 2014, the PDMD scored D in each dimension of this indicator. Scores rank from A to D, where the score D means that the minimum requirements are not met.

DPI-12 Debt Administration and Data Security

Dimension	Score
1. Availability and quality of documented procedures for the processing of debt service.	D
2. Availability and quality of documented procedures for debt data recording and validation, as well as storage of agreements and debt administration records.	D
3. Availability and quality of documented procedures for controlling access to the central government's debt data recording and management system.	D
4. Frequency and off-site, secure storage of debt recording and management system backups.	D

Dimension 1

In order to score C in the first Dimension of the DPI-12, the PDMD must have written procedures for debt servicing. Now, this is the case.

To score B, payment orders must be prepared electronically and written procedures for debt servicing must be reviewed at least once every two years.

To score A, payment orders must be done through a Straight-Through-Processing (STP) payment system and written procedures for debt servicing must be reviewed at least once a year.

Currently, the PDMD prepares most payment orders electronically, but some orders are still processed manually, which would lead to a vote C for this dimension.

Dimension 2

In order to score C in the second Dimension of the DPI-12, the PDMD must have written procedures for debt recording and validating and the storage of debt administration records must be done in lockers with keys in a fire and flood proof room.

To score B, written procedures for debt recording and validating have to be reviewed at least once every two years.

To score A, a complete confirmation of data recorded with the Creditors and major domestic investors must be performed once a year and written procedures for debt recording and validating have to be reviewed at least once a year.

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, which are currently stored in the lockers of the Back-Office unit (BO), which are not fire and flood proof. Thus, the score would probably stay D for this dimension.

Dimension 3

In order to score C in the third Dimension of the DPI-12, the PDMD must have written procedures for controlling access to the central government's debt management system. Access to the system through a unique username and password for each user is mandatory.

To score B, written procedures for controlling access to the debt management system have to be reviewed at least once every two years.

To score A, the debt management system must produce an audit trail showing all the activities done by the user in the system and written procedures for controlling access to the debt management system have to be reviewed at least once a year.

Currently, the PDMD has written procedures for controlling access to the debt management system. DMFAS is the system used by the PDMD to record debt (UNCTAD is the system provider). Each DMFAS user need a unique username and password to enter the system which can track all the activities done by the user. However, domestic debt data are only recorded in Excel spreadsheets – not yet in the DMFAS system – which means the DMFAS database is incomplete. Consequently, the score would probably stay D for this dimension.

Dimension 4

In order to score C in the fourth Dimension of the DPI-12, the PDMD must backup the Debt database on a monthly basis. These database backups must be stored in a separate and secure location where they are protected from incidents such as theft, fire, flood (and others) that can damage backups.

To score B, the PDMD must backup the Debt database on a weekly basis.

To score A the PDMD must backup the Debt database on a daily basis and backups must be stored in a secure filing system before they are moved to the separate and secure location weekly.

Currently, the PDMD performs regular backups of the Debt database. But, these backups are not stored in a separate and secure location, they are only stored on external drives in the PDMD building. Consequently, the score would probably stay D for this dimension.

3. Procedures

The purpose of this section of the document is not to describe the procedures of the PDMD. This was done elsewhere. Indeed, each procedure has its own procedure document. This section discusses challenges, regarding operational risks these PDMD's procedures are still facing.

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.

3.1 Front Office

The procedure to negotiate external loans is now documented. Recently, the MoF made an important change to the negotiation process by requiring the presence of a debt specialist of the PDMD earlier in the process at the pre-consultation stage. This is an important decision allowing the PDMD to be informed earlier of the new loans in the pipeline. This will also help the PDMD to raise other participants awareness of the medium-term debt management strategy (MTDS).

The procedure to issue bonds in the international capital markets (Eurobonds) has also been documented. The MoF already issued two Eurobonds since 2012 and this process starts to be 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, but this problem seems to be solved now.

Auctions

Auctions of the Treasury Bills and Bonds is one of the most critical activity of any debt management office.

For primary auctions and buybacks, market participants 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, both also through the Ministry's VPN.

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. Additionally, when the winning bids are selected, the FO Officer must input manually the allocated amount and the cut-off yield in the Genium I Net 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.

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.

3.2 Middle Office

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

However, 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, IMF international trainings and other courses. The MO should pay particular attention to training and coaching of new staff when preparing the training plan.

3.3 Back Office

The procedures to record debt data in the database (loans agreements, disbursements, 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 in the DMFAS system (debt management system) is not complete. For external debt, some historical data for disbursements are not recorded yet. Indeed, when PDMD installed the system, the choice was made to record all the disbursements transactions since 31 December 2009, that is the cut-off date of the system (before that date only aggregate balance are available). This is a lot of individual entries to record in the system and the staff will need time before completing this task. Until this task is not completed, the BO officers will always need to use Excel Spreadsheets to check if payment notice are correct or loan outstanding amounts are up-to-date.

Furthermore, domestic debt transactions are not recorded in the DMFAS database, but in Excel spreadsheets. Thus, there is no possibility to track which officer has recorded a domestic debt operation and the integrity of domestic debt data is at risk in Excel spreadsheets.

Consequently, the PDMD does not have an integrated debt database and, every time the BO needs to prepare any projection schedule, it will need to work manually on many different Excel spreadsheets, therefore, increasing the risk of human errors and time response. 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.

The Excel debt database is stored in the local computer of the BO Officer. In case of problem with this computer, the database can be recovered from the folder of the Head of FO in the Intranet of the MoF or from other backup copies (in USB keys).

The procedure to control access to the DMFAS system is now documented. The PDMD did not have a person to fulfill the position of debt database administrator for the DMFAS. Thus, the BO and the IT Department have now agreed to separate the functions of this position between them. Basically, the Head of BO will be responsible to create users' profiles and

access codes, 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 still needs UNCTAD to provide them a DMFAS database administrator training, while PDMD users will need functional trainings. Apparently, DMFAS trainings should be organized on-site under the framework of the new ADB technical assistance program.

Debt payments

The procedures to prepare and execute debt payments are also documented. Usually debt payments are done through electronic payments orders, but in several cases, it can be done through manual payments orders.

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.

3.4 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 saving bonds. 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 system "Bankmail": an interface to electronic payment system of the banking sector managed by the Central Bank.
3. The Treasury Direct website, with administrator access. In this website, individuals can purchase online saving bonds and other government securities.

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 third 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.

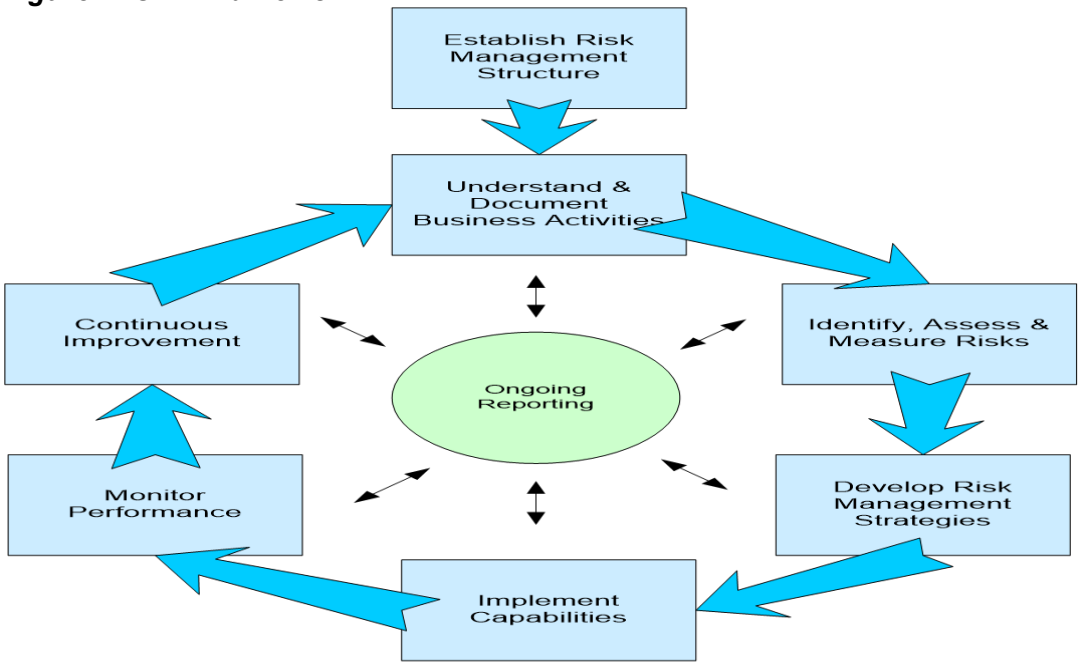
Main risks

- 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 hold by individual investors. Here, a backup solution could be implemented, in case of technology failure, to allow exceptionally using the old paper-based process.

4. Suggested structure to manage operational risk

With the support of the EU experts, 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 or twice a year, a formal ORM report to the risk management committee of the MoF.

Considering PDMD 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 an ORM "champion" based in the MO. Reporting should be kept to the simplest expression (a simple word page, for example) and the "champion" should be responsible for coordinating with the other units and filing units' messages.

The "champion" should organize regular meetings on risk management with the heads of the other units and the Director – once a month to start – and monitor if the decisions taken during these meetings are implemented. If some topics require it, they should be submitted to the Vice-minister decision.

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 "champion" 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.

5. Business Continuity

The PDMD has completed a draft of the Business Continuity Plan (BCP). 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.

5.1 Current IT situation

The servers 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.

However, the Ministry does not have an alternate data center with physical backup servers. IT Department is planning to set up such data center in Dilijan in the future. To this end, Ministry will need to go through a tender process to select the IT solution provider. IT Department is expecting to implement this center in Dilijan in 2018.

The MoF does not have an alternate operational site to relocate critical staff and ensure business continuity after a major incident.

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. Thus, PDMD can use the network of the Ministry to do backups of the databases and store them (NAS, network attached storage).

However, 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.

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.

It must be said that Ministry's network is not accessible remotely (from outside of the Ministry buildings). For example, PDMD staff cannot access their official e-mail accounts from home, or anywhere outside of the MoF buildings.

5.2 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

- IT policy guidance to save and store electronic files. The MoF has a shared drive where the users can save their files, but there are no written guidelines on when and

how to use it. Therefore, each staff, or each Head of unit, decides if she/he wants to use it, at which frequency and the types of documents she/he wants to store there.
- 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.

Key staff risk

- There is generally no handover period between the staff leaving the PDMD and the newcomer.

Failure to follow or adhere to administrative practices

- The PDMD does not report to managerial level when others Ministry's departments are sending macro-fiscal forecasts or other necessary information too late.
- There is no independent control unit at the level of the Ministry to monitor departments' delays in delivering products/services.

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.
- There is no appraisal meeting between staff and their manager in order to evaluate staff performance and manager performance (could be done on a semi-annual or annual basis).

However, there is a low staff turnover and head of units are experimented. Most of them are working in the MoF since several years.

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.

Intranet/Internet failures

- Only one communication outside of the building of the PDMD. One single line for phones, Internet and Ministry's network.

Infrastructure and Document storage deficiencies

- Debt administration documents (i.e. withdrawals applications, Eurobonds issuance supporting documents) are stored in closed lockers, but not in a secured fireproofed room.
- There is no clear policy defining who must acknowledge the reception of debt administration documents, the date of reception of the documents 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.

6. Recommendations

The IT Department of the MoF is currently looking to establish an alternative data center outside Yerevan, in Dilijan. It is also considering using this center 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.

Meanwhile, the PDMD should take additional measures to ensure business continuity:

1. 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.

2. 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.

3. The IT Department could consider giving a securitized remote access to the Ministry's network for the critical staff of the PDMD. Critical staff could use this remote access in case of contingencies, but also to access their e-mail accounts and work from home afterhours.

4. Debt database backups should be performed automatically on a daily basis. An agreement was found between the IT Department and the PDMD leaving the responsibility of DMFAS database backups to the IT Department. But, IT staff should ensure backups are performed daily.

5. PDMD should contact the UNCTAD (provider of the DMFAS system) to organize a database administrator training for the IT Department and a DMFAS users training for the PDMD staff.

6. Debt database could be integrated in a single database. Currently, domestic debt is recorded in Excel spreadsheets, rather than in the DMFAS system. Recording everything in the DMFAS system will improve the integrity of domestic debt data and allow audit trails to be performed (which officer has recorded the operation). Furthermore, it will also speed up debt reporting and reduce manual tasks and, therefore, potential human errors.

7. PDMD could consider choosing a more recent cut-off date for the DMFAS Debt database. Currently, historical records are still incomplete because it requires a lot of work from PDMD staff to record all the historical transactions since 2009. Choosing a more recent date would facilitate the task of BO officers, allowing the PDMD to enjoy a complete database sooner.

8. 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.

9. 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.

10. An alternate electricity generator and UPS batteries should be available in the PDMD building in the case where regular electricity power source fails.

11. PDMD should consider using fireproof lockers to store debt administration documents, like this is the case for original loan agreements in the Ministry of Foreign Affairs.

12. Semi-annual appraisal meetings could be organized between staff and their respective head of units to discuss staff performance and individual training and development plan.

13. PDMD should better segregate the functions of the Treasury Direct Unit by appointing a person to register customers' securities purchases, while the Head of the Unit will confirm the transaction and administrate the website.

14. PDMD should designate an ORM "champion" to monitor and store information received from each unit on incidents, suggested improvements, and new risks identified. Regular ORM meetings could be organized with the Director and the heads of units (i.e. once a month) to handle the problems identified.

15. ORM "champion" could prepare, once a year, 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.