Guidance for Operational Risk Management in Government Debt Management

Tomas Magnusson, Abha Prasad and Ian Storkey

March 2010

Guidance for Operational Risk Management in Government Debt Management[1]

Tomas Magnusson, Abha Prasad and Ian Storkey

In government debt management (DeM), the categories of risk such as market risk (exchange rate and interest rate risk), credit risk, refinancing risk and liquidity risk are relatively well known; operational risk is however, less well known and an area that has not been given much attention to by government debt managers in developing a risk management framework. This paper introduces the concepts of operational risk as applied to government DeM and attempts to present a framework for debt managers to manage operational risks while undertaking public debt management operations. It draws on existing literature for operational risk management principles and practices that have been formulated by the Bank for International Settlements (BIS) Basel Committee on Banking Supervision and the Committee of Sponsoring Organizations (COSO). It provides guidance on developing a framework for assessing risk exposures from incidents or events that can adversely impact on reputation, financial cost, outputs and/or budget variance.

1. INTRODUCTION

Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel II, June 2004). In debt management operations, the categories of risks, such as market risk (exchange rate and interest rate risk), credit risk, refinancing risk and liquidity risk, are relatively well known; however operational risk is not. The area has not been given due attention to by government debt managers in developing a risk management framework. A similar conclusion on aspects pertaining to operational risk management is borne out from the early results of the World Bank's assessments using its government Debt Management Performance Assessment (DeMPA) tool.[2]

The results of the DeMPA exercise indicate significant deficiencies among countries on operational risk management. As at end-December 2009 from among the 27 finalized DeMPA reports, almost all of these countries had either weak or non-existent frameworks for operational risk management. Among the assessed countries, only one quarter of the countries met with the minimum effectiveness requirements[3] for "debt administration and data security" and only six percent of countries demonstrated effective practice for aspects relating to "segregation of duties, staff capacity and business continuity" (these are as covered by the DeMPA tool. The DeMPA indicators and a more detailed description of the assessment results are presented in Box 1 and Annex 1, respectively.

---

[1] This paper has benefitted from valuable comments and suggestions from Phillip Anderson, Sudarshan Gooptu, Mike Williams, Mats Filipsson and Leonardo F. Hernandez. Valuable suggestions given by Lars Jessen and Gregory Horman on an earlier draft are gratefully acknowledged. Authors are thankful to Signe Zeikate for her help with the DeMPA data. The findings, interpretations, and conclusions are the authors' own and should not be attributed to the World Bank, its Executive Board of Directors, or any of its member countries.

[2] The Debt Management Performance Assessment (DeMPA) indicator set is a sample of proficiencies of a Debt Management Unit. These results relate to 27 finalised assessments. (http://go.worldbank.org/5AHEF2KF70).

[3] DeMPA indicators are scored on a scale from A to D. Score C or higher indicates that the minimum requirements for effective debt management under the DeMPA have been met; while score D indicates the absence of the same.

This paper thus, introduces the concepts of operational risk as applied to government debt management (DeM)[4] and attempts to present a framework for debt managers to manage operational risks while undertaking public debt management operations. It draws on existing literature for operational risk management principles and practices that have been formulated by the Bank for International Settlements (BIS) Basel Committee on Banking Supervision, the Committee of Sponsoring Organizations (COSO) and the findings of the DeMPAs.

Box1: The DeMPA Performance Indicators

The DeMPA is a set of 15 indicators (and 35 dimensions) that cover six core functions of debt management (see table below): 1) governance and strategy development, 2) coordination with macroeconomic policies, 3) borrowing and related financing activities, 4) cash flow forecasting and cash balance management, 5) operational risk management, and 6) debt records and reporting. Operational risk management is covered by two debt performance indicators (DPI): DPI-12 Debt Administration and Data Security, and DPI-13 Segregation of Duties, Staff Capacity and Business Continuity.

	Governance and Strategy Development
DPI-1	Legal Framework
DPI-2	Managerial Structure
DPI-3	Debt Management Strategy
DPI-4	Evaluation of Debt Management Operations
DPI-5	Audit
	Coordination with Macroeconomic Policies
DPI-6	Coordination with Fiscal Policy
DPI-7	Coordination with Monetary Policy
	Borrowing and Related Financing Activities
DPI-8	Domestic Market Borrowing
DPI-9	External Borrowing
DPI-10	Loan Guarantees, On-Lending, and Derivatives
	Cash Flow Forecasting and Cash Balance Management
DPI-11	Cash Flow Forecasting and Cash Balance Management
	Operational Risk Management
DPI-12	Debt Administration and Data Security
DPI-13	Segregation of Duties, Staff Capacity, and Business Continuity
	Debt Records and Reporting
DPI-14	Debt Records
DPI-15	Debt Reporting

[4] Government debt management is the process of establishing and executing a strategy for managing the government's debt in order to raise the required amount of funding, achieve its risk and cost objectives, and to meet any other sovereign debt management goals the government may have set, such as developing and maintaining an efficient market for government securities.

2. Operational Risk for Government Debt Management

Government debt management units (DMUs) are responsible for managing the costs and risk of the government's debt portfolio, which is often the largest financial portfolio in the country. As such, it is very important that DMUs develop policies and procedures to manage the risks that they face, namely, market risk (exchange rate and interest rate risk), credit risk, refinancing risk, liquidity risk, and operational risk. This partly reflects the high value of the financial transactions involved and the consequences of substantial financial loss including on debt service costs. But there is potentially also severe reputational and political damage associated with operational error or failure.

There are many high profile examples of operational risk management failures in financial institutions such as Barings (1995), Daiwa Bank (1995), Kidder Peabody (1994), Salomon Inc (1994 and 1996), and Societe Generale (2008) which lost US$7 billion due to one trader and lax internal control. There are few high profile cases for governments that have been reported.

There are two examples affecting local governments that led to severe reputational and political damage for both governments. First, the Hammersmith and Fulham Council in the United Kingdom received a high court ruling in 1989 that they did not have the legal authority to enter into dozens of swap contracts totalling about US$9.5 billion. While the local government did not lose on the swaps (the court's decision cost British and foreign banks approximately US$1 billion in defaulted swap payments), the impact was significant for not only Hammersmith and Fulham but also the 77 other local governments as it effectively terminated any further activities in the financial markets. The failure to comply with legal requirements can be classified as an operational risk management failure.

Second, Orange County, a prosperous district in California, declared bankruptcy after suffering losses of around US$1.6 billion from derivatives trading in one of its principal investment pools. The pool was intended to be a conservative but profitable way of managing the county's cash-flows, and those of 241 associated local government entities. Instead, it triggered the largest financial failure of a local government in US history. While the loss was the result of the failure to control or limit market risk, operational risk management weaknesses were identified as a primary reason for this incident to occur.

Weak operational risk management can also lead to corruption, evidenced by the Anglo Leasing Affair in Kenya in 2004 that involved a supplier's credit with extremely bad conditions for Kenya. All payments by Kenya were transferred to Anglo Leasing & Finance Ltd's account with a small bank in Zurich, and in the end it was discovered that Anglo Leasing did not even exist. The scandal resulted in both the Permanent Secretary and the Head of the Debt Management Department having to resign. The official report by the new Financial Secretary concluded that over the years the institutional framework for contracting and managing external commercial loans had collapsed.

2.1. International Principles

Under Basel II (International Convergence of Capital Measurement and Capital Standards: A Revised Framework, June 2004), operational risk is defined as **"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external**

events." The definition explicitly includes legal risk, but excludes strategic and reputation risk.[5]

While this definition and sound practices established by the Basel Committee on Banking Supervision and COSO[6], and usefully elaborated by entities such as TransConstellation,[7] have been primarily designed for the banking and financial sector, the governing principles can appropriately be applied to government DeM operations. What is necessary is a framework for managing it that is appropriate to the range and nature of government DeM operations and the operating environment, particularly for low and middle income countries.[8]

Awareness of operational risk is low in many countries, or is perceived as something applicable only to the private sector. Moreover, it attracts little attention by senior management because it is not seen as important or a priority. The problem of course is that operational risk is a wide umbrella, often seen as covering everything except for market, credit, refinancing, and liquidity risks. Unlike market or credit risk, operational risk is mainly endogenous to a DMU. Apart from external events such as natural catastrophes, it is linked to the business environment, nature and complexity of the DMU's activities, the processes and systems in place, and the quality of the management and of the information flows.[9]

DMUs are increasingly using derivatives, collateral and netting arrangements to manage their exposure to market and credit risk. This may generate other forms of risk as these transactions are by their nature complex, which creates increased operational complexities and risks. More importantly, operational risks are more difficult to manage as the embedded risk cannot be captured and measured in the same way as market and credit risk. In addition, market or credit risks can be effectively managed by a relatively small number of debt managers in the DMU (normally in the front and middle office) whereas operational risks must be addressed at all levels across all of government DeM operations.

2.2. CATEGORIES OF OPERATIONAL RISKS FOR GOVERNMENT DEBT MANAGEMENT

The Basel II definition as quoted above includes legal risk but excludes strategic and reputation risk. The strategic and reputation risk, however, can be caused by both bad operational risk management and an unexpected consequence of an informed business decision. A poor strategic decision due to lack of adequate training of staff and lack of system support is an operational risk, while an informed strategic decision based on a reasonable cost/risk analysis that still resulted in a loss for the government is an ordinary business risk. Both can of course affect the reputation of the government. However, in the former case the

[5] This definition was adopted by the Basel Committee as part of its work in developing a minimum regulatory capital charge for operational risk.
[6] COSO has developed a management framework which is used in the TransConstellation tool.
[7] TransConstellation was established in December 2003 as a not-for-profit entity by industry leaders in the field of financial-transaction processing, all located in Belgium. The members include Euroclear, SWIFT, and The Bank of New York Mellon (Brussels office).
[8] A risk exposure is a product of two elements: the likelihood of a risk event, which in turn triggers a loss or other impact (e.g. reputational); and the size of that impact.
[9] Even if the DMU cannot control external events, it can mitigate the damage of these events by good operational risk management, e.g. by having in place a business continuity plan.

reputation will be more damaged as the government will be criticized for not knowing what it is doing, putting the taxpayer's money at risk.

The categories of operational risks that are relevant for government DeM including examples under each category are set out in the following table.

INFRASTRUCTURE AND TECHNOLOGY FAILURES		
Power failure	Hardware failure	Sabotage
Data corruption including viruses	LAN/WAN/Intranet/ Internet failure	Internal flood (sprinklers, pipes)
Voice network failure	Theft of equipment	Theft of data/information
Poor maintenance	Accidental damage	
INCIDENTS WHERE ACCESS TO PREMISES IS DENIED		
Flooding or a fire concern	Health and safety violation	Hazardous chemicals accident
Gas or chemical leak	Industrial action or riot	Bomb or terrorist threat
Building fire or explosion	Internal/external flood	Sabotage or terrorism
KEY SERVICE PROVIDERS OR RESOURCE FAILURES DEPENDENCIES		
Failure of key service providers (telephone, internet, banking etc)	Third party providers (Central Bank and other outsourced operations)	Impact of incident on critical teams or groups (travel, food poisoning, group incident)
STAFF, MANAGEMENT AND RELATED HUMAN FAILURES		
Human error (which may be due to poor training or inadequate supervision)	Poor training or inadequate supervision (which may lead to human error or execution of unauthorized transactions)	Failure to follow code of conduct or conflict of interest guidelines
Lack of policy guidance (which may lead to poor decisions or unauthorized activities)	Poor understanding of risk environment (which may lead to unnecessary or unknown risks)	Poorly specified delegations (which may lead to execution of unauthorized transactions)
Failure to follow or adhere to administrative practices (which may lead to processing errors)	Key person risk (which may lead to human error when key person is absent)	Fraudulent, corrupt or dishonest practices (which may lead to financial loss and political embarrassment)
FAILURE TO MEET STATUTORY, LEGAL, HUMAN RESOURCES AND OTHER OBLIGATIONS		
Legal/statutory obligations (e.g. compliance with loan agreements)	Management directives (e.g. internal policies and procedures)	Procedures manuals and delegated authorities
Reporting obligations (e.g. to higher authorities and international institutions)	Contractual obligations (e.g. debt service obligations)	Health and safety regulations (e.g. national workplace laws or regulations)
MAJOR NATURAL AND REGIONAL DISASTERS		
Earthquake	Severe flooding	Tsunami
Volcanic eruption	Severe fires	Civil disturbance or terrorism

Source: Authors' compilation

2.3. PRINCIPLES APPROPRIATE TO GOVERNMENT DEBT MANAGEMENT

It is useful to consider the principles for operational risk management within the context of the legal and managerial structure that shapes and directs the operations of the DMU. It includes the legislation that defines goals, authorities, and accountabilities. It also embodies the management framework, covering issues such as the formulation and implementation of a debt management strategy, operational procedures, quality assurance practices, and reporting responsibilities. The governance structure for operational risk management may be quite extensive with an operational risk committee, audit committee, a management committee, and an advisory or decision-making board.

An integral part of any framework will be the principles for operational risk management. The following sets out the principles that might apply to government DeM operations. These are based on principles developed for the banking sector set out as sound practice by the Basel Committee on Banking Supervision at the Bank for International Settlements (2003). The same, mutatis mutandis, are applicable for government debt management offices/units that also operate in the financial markets.

DEVELOPING AN APPROPRIATE RISK MANAGEMENT ENVIRONMENT

PRINCIPLE 1

The Head of the DMU and/or members of the decision-making board (if this exists) should be aware of the major aspects of debt management operational risks as a distinct risk category that should be managed, and the Head of the DMU (or the board) should approve and periodically review the operational risk management framework applicable to all government DeM operations. The framework should provide a definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

PRINCIPLE 2

The Head of the DMU and/or members of the decision-making board (if this exists) should ensure that the operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management (refer Principle 8).

PRINCIPLE 3

Senior management across all government DeM operations should have responsibility for implementing the operational risk management framework approved by the Head of the DMU and/or the decision-making board (if this exists). The framework should be consistently implemented throughout all DeM operations, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk across all DeM activities, processes and systems.

RISK MANAGEMENT: IDENTIFICATION, ASSESSMENT, MONITORING, AND MITIGATION / CONTROL

PRINCIPLE 4

The DMU should identify and assess operational risk exposures inherent in all activities, processes and systems.[10] The debt managers should also ensure that before new activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment and managed appropriately.

PRINCIPLE 5

The DMU should implement a process to regularly monitor operational risk profiles and material risk exposures. There should be regular reporting of pertinent information to the Head of the DMU, and members of the decision-making board (if this exists) that supports the proactive management of operational risk.

PRINCIPLE 6

The DMU should have policies, processes and procedures to control and/or mitigate material operational risks. The DMU should periodically review their operational risk profile and should adjust their risk limitation and control strategies in the context of the government's overall debt and risk management strategy.

PRINCIPLE 7

The DMU should have in place contingency and business continuity plans to ensure its ability to operate on an ongoing basis and limit losses in the event of any[11] business disruption.

ROLE OF INTERNAL AND EXTERNAL AUDITORS

PRINCIPLE 8

Internal and external auditors should independently examine and assess the DMU's framework for identifying, assessing, monitoring and controlling/mitigating material operational risks. External auditors should independently conduct, directly or indirectly, regular evaluation of DeM policies, procedures and practices related to operational risks.

ROLE OF DISCLOSURE

PRINCIPLE 9

The DMU should make sufficient public disclosure to allow the Minister of Finance and government as well as market participants to assess their approach to operational risk management. This should include a statement setting out the DMU's approach to managing operational risk and the publication of the external auditor's report on a review of operational risk management policies, procedures and practices.

---

[10] The focus should be on material or important activities, processes and systems without wasting too much time on unessential or less important activities, processes and systems.

[11] An uninterruptable power supply (UPS) may in practice be more relevant than a disaster recovery site, although countries really need both.

3. OPERATIONAL RISK MANAGEMENT FRAMEWORK

Developing an operational risk management framework can be an evolutionary process as it will take time and effort to not only identify and understand the risks but also the mitigation techniques in an environment that is constantly changing. There is no need to try to do everything perfectly from the outset. The framework can be developed and applied incrementally as techniques improve and DMU staff begin to understand the risks and mitigation techniques. For the framework to succeed, it is extremely important to develop a culture of risk awareness across the DMU and ensure that all staff are involved in developing and implementing the framework.

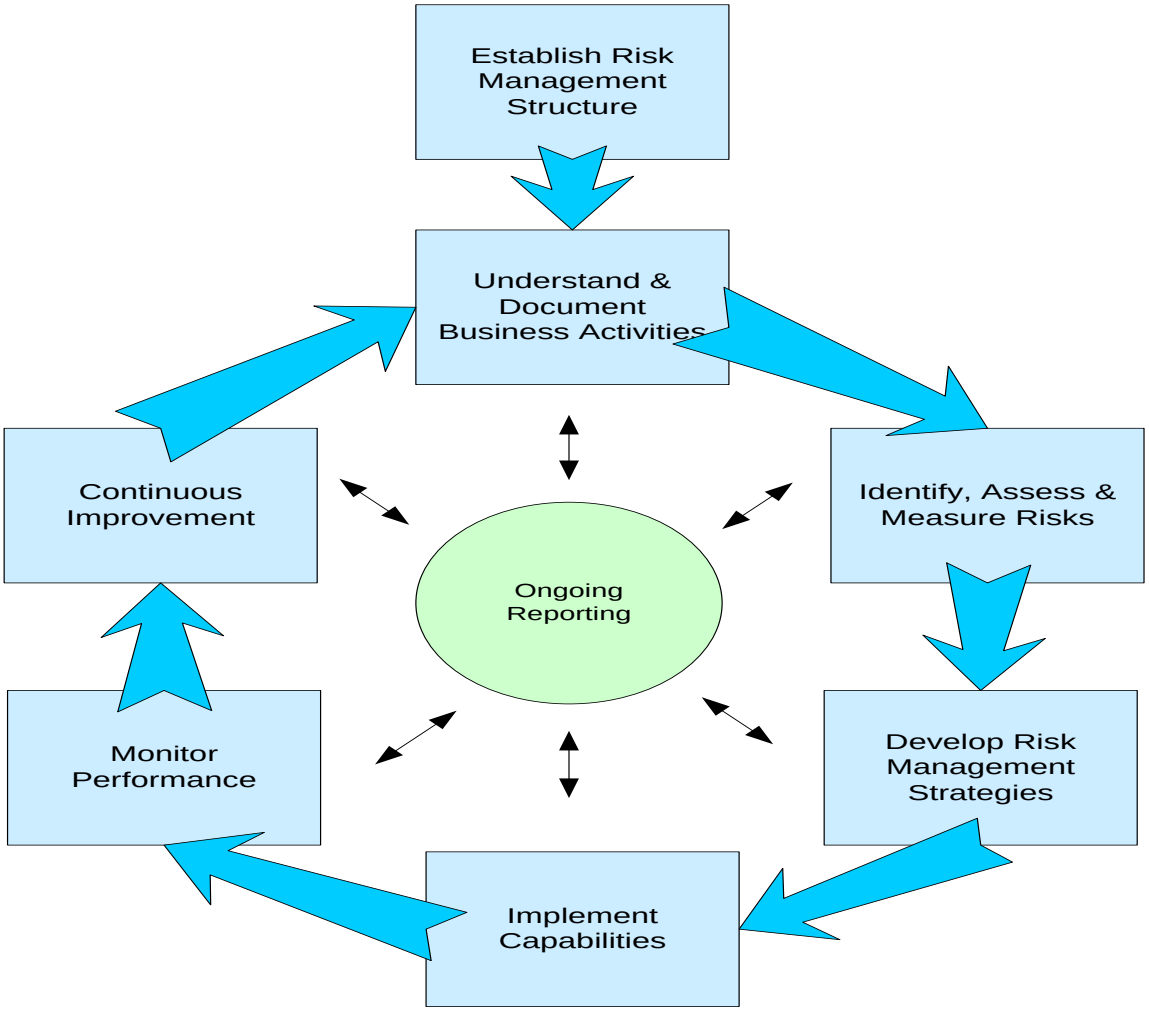
The first stage involves senior management understanding and signalling to all staff in the DMU the importance attached to operational risk management and the need for their participation and ongoing cooperation. The principles as outlined above that will be followed in the management of operational risk need to be made clear to all staff and embedded into day-to-day DeM operations. Each line manager needs to be made responsible for operational risk management in their own business area.

It is advisable that a "risk champion" from the middle office be appointed to take overall responsibility for operational risk management. The risk champion will lead and guide the process across the DMU, coordinate reporting to senior management, and develop the appropriate operational risk management policies and procedures and control environment. Ideally the risk champion would have relevant background or experience, although this will often not be possible. There are, however, opportunities for professional training in operational risk management and business continuity planning which could be considered.

Once the structure has been established, the development and maintenance of an operational risk management framework for a DMU should follow a six-step process:

1. Understand and document business activities
2. Identify, assess and measure risks
3. Develop risk management strategies
4. Implement capabilities
5. Monitor performance
6. Continuous improvement

The six-step process including ongoing reporting and continuous improvement is demonstrated in the following diagram.



3.1. UNDERSTAND AND DOCUMENT BUSINESS ACTIVITIES

The first step is to understand DeM operations by breaking down the main DeM functions into activities, processes or systems, each with a stated objective for each business area. This can be done by convening workshops and brainstorming sessions for each DeM function to fully understand the activities, processes and systems and identify the key risks that might impact on DeM operations. Process maps and process-flow analysis can be used along with existing procedure manuals to understand DeM operations. The risk champion should oversee this process to ensure a common understanding and consistency of approach and terminology. This should be at a level that will balance the amount of detail and usefulness to senior management and the overall process.

This can be brought together in documentation that sets out activities, processes and systems together with the risks faced by the DMU which is then used to design processes and control points that mitigate the assessed risks in steps 2 and 3, and the documentation that is prepared in step 4.

3.2. IDENTIFY, ASSESS AND MEASURE RISKS

For the second step, it is important to involve everyone responsible for DeM operations, including the more junior staff, as it helps to develop a risk understanding and a risk culture within the DMU. Again, this can be done by convening workshops and brainstorming sessions for each DeM function.

For each category of operational risk set out above, the DMU should assess the risk exposures in terms of reputation, financial loss and/or impact on outputs or budget variance as a result of an incident or event affecting their operations. This requires separately assessing the probability and the impact, for example using a combination of Very-High/High/Medium/Low Probability and Very-High/High/Medium/Low Impact from a reputation, financial cost and budget perspective as shown in the following table.

	Low Impact	**Medium Impact**	**High Impact**	**Very-High Impact**
Very-High Probability (almost certain)	VHpLi	VHpMi	VHpHi	VHpVHi
High Probability (probable)	HpLi	HpMi	HpHi	HpVHi
Medium Probability (possible)	MpLi	MpMi	MpHi	MpVHi
Low Probability (remote)	LpLi	LpMi	LpHi	LpVHi

Depending on its risk tolerance level, the DMU may wish to also include the Medium Probability/Medium Impact combinations and Low Probability/Very-High Impact assessment, where the impact could be extreme either in reputation, financial cost or budget terms.

Not all operational risks will be of equal importance for each DMU as this will be a country specific judgement. Therefore, the following practical guidelines are provided to assist in characterizing the impacts across the full range of DeM operations.

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

Source: Authors' compilation

The outcome of the assessment will be a high-level summary of risks that will be consistent across the full range of DeM operations, as a way of identifying priorities for senior management. The assessment technique can be flexible in that it can initially be undertaken in a broad brush way and improved over time as experience develops, particularly when there is a history of loss-event data.

3.3. Develop Risk Management Strategies

In step three, the DMU should develop operational risk management strategies that concentrate on improving resilience and ensuring mitigation techniques are put in place for those areas identified as having a combination of Very-High/High Probability and Very-High/High Impact. For these areas, the DMU should select the most cost effective and suitable risk treatment approach for each DeM function using one or more of the following:

- prevention or avoidance, where the probability of an event occurring is reduced or eliminated (e.g. install back-up power generators, use more than one telecom provider, train staff, or implement fraud prevention policies and procedures)
- transference, where risks are passed to third parties (e.g. insurance or outsourcing with risk management incorporated in service level agreements)
- containment, where the potential impact of an event occurring is limited in the early stages using controls or other techniques (e.g. implement fraud detection policies and procedures, put in place escalation procedures so that management can respond immediately should an event begin to escalate, or have more than one person to perform a particular task or activity)
- acceptance and recovery, where an event or disruption might well occur but DeM operations can be resumed successfully (e.g. have in place a disaster recovery plan that is regularly tested at a recovery location)

The risk champion should then report to senior management on the greatest exposures, the risk management techniques to mitigate, control, or limit the risks, the actions that are recommended to address the greatest exposures, and an estimate of costs. Senior management can then assess the cost-risk trade-off before making decisions or seeking approval from higher level (the decision-making board), if this exists. As an example, if the DMU is subject to frequent power outages, it may be deemed sufficient given the cost to install an uninterruptible power supply (UPS) rather than install a much more expensive back-up power generator.[12] However, if DeM operations become more active and continuity of business becomes more critical, it may be sufficient to justify the expense of an emergency generator given the potential impact from power outages. This is often the case in low or middle income countries where the Central Bank will have an emergency power generator whereas the Ministry of Finance will not.

The risk assessment and operational risk management strategy approved can be documented in the DeM operational risk management plan. A business continuity or disaster recovery plan can be incorporated in the plan or maintained as a separate document.

3.4. IMPLEMENT CAPABILITIES

The risk champion can oversee the implementation of measures approved by senior management and incorporate into the wider risk management monitoring and control policies and procedures for the DMU. This process may comprise, among others:

- training program for DeM line managers and staff to understand their roles and responsibilities in compliance with the operational risk management policies and procedures, and possibly introducing risk-reduction objectives for each member of the DMU
- raising awareness with external parties to cover all activities external to the DMU (e.g., IT department of the Ministry of Finance, Central Bank and other third party

[12] But a UPS will only last for a short time – so there is a trade off between the UPS and a backup generator which depends on the risk of a long rather than short outage (power cut).

providers) of the operational risk management framework and seek their cooperation in monitoring and reporting and, where possible, requiring these service providers to meet the same operational risk management standards as the DMU[13]

- introducing operational risk management into service level agreements or a memorandum of understanding with third party providers and contracts with external suppliers (explaining in practical terms the significance of such procedures)
- developing control tools that are documented in procedures, technical and other manuals and monitored by the DMU risk monitoring and compliance unit including the risk champion and/or internal audit
- developing reporting requirements, particularly to senior management, of significant incidents or exceptions and the process of review to ensure that these are not repeated
- developing, maintaining and annual testing of the business continuity and disaster recovery plan

3.5. MONITOR PERFORMANCE

The monitoring process assesses the presence and functioning of the operational risk management policies and procedures over time through a combination of ongoing monitoring activities and specific evaluations. Ongoing monitoring occurs in the normal course of DeM operations; it is the responsibility in the first instance of line managers, with coordinating responsibility assigned to the middle office/risk monitoring and compliance unit/risk champion.[14] The scope and frequency of specific evaluations depends on an assessment of risk and the effectiveness of ongoing monitoring procedures. The specific evaluations could be undertaken by external audit.

It is necessary to report regularly to senior management on the risk profile, identifying areas that are improving or deteriorating, and priorities for mitigating action. An important element of monitoring performance is reporting of incidents or exceptions to senior management, normally as part of a risk monitoring and compliance report. For serious incidents or events, it may be necessary to identify badly managed risks and the action needed to avoid repeating such incidents. Many incidents may often be the fault of management failing to develop an adequate control environment rather than the individuals that may be deemed directly responsible—indeed for this to work effectively a "no blame" culture is important.

One course of action is to identify which line manager has the lead responsibility for managing and controlling each of the identified risks, and then ask each line manager to report periodically on the risks for which they are responsible, whether these have increased or reduced, and whether and what action should be taken. In this way, the line managers are involved in the process which ensures "buy-in" of the business areas across all DeM operations. The middle office/risk monitoring and compliance unit/risk champion will be responsible for collecting the reports together with the preparation of exception/error reports,

[13] For example, in the UK, the Debt Management Office (DMO) requires the Bank of England's internal auditors to comment to the DMO on the Bank's internal control regime. Also, DMUs are beginning to develop service level agreements with the Ministry of Finance IT function, which include arrangements for handling specific events should they arise.

[14] It is common that the monitoring and compliance unit is part of the middle office.

and summarising the key points and main risk drivers. Changes in the risk profile since the last monitoring assessment should be noted. The report would go on to make recommendations for consideration by senior management.

3.6. CONTINUOUS IMPROVEMENT

As was noted earlier, operational risk management can be improved over time as experience develops, particularly when there is a history of incidents or events and their impact in terms of reputation, financial loss and budget. It may also be valuable to learn from other DMUs through ongoing monitoring and communication channels. The six-step process should be revisited on an annual basis, although the first step may just involve an update of the business activities, processes and systems reflecting changes from the previous assessment.

DMUs in countries such as Australia, Denmark, France, New Zealand, Sweden and the United Kingdom have set out their policies for managing operational risk on their websites and/or in their annual reports. Their experiences show that operational policies and procedures that are embedded in day-to-day DeM operations together with ongoing monitoring and reporting by a middle office, risk monitoring and compliance unit or risk champion in the DMU are the key to successful management of operational risk.

REFERENCES

Bank for International Settlements (2003), "Sound Practices for the Management and Supervision of Operational Risk", Basel Committee on Banking Supervision [http://www.bis.org/bcbs/index.htm]

Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2008), "Internal Control – Integrated Framework: Guidance on Monitoring Internal Control Systems" [http://www.coso.org]

TransConstellation (2007), "Best Practices in Qualitative Operational Risk Management: The ORM Reference Guide" [http://www.transconstellation.com]

TransConstellation (2007), "Roadmap to Operational Risk Management Success: The ORM Maturity Benchmark" [http://www.transconstellation.com]

World Bank (2007), "Debt Management Performance Assessment (DeMPA) Tool" [http://go.worldbank.org/4VX651FHB0]

World Bank (2007), "Guide to the Debt Management Performance Assessment (DeMPA) Tool" [http://go.worldbank.org/4VX651FHB0]

ANNEX 1: RESULTS FROM THE DEMPA EXERCISE[15]

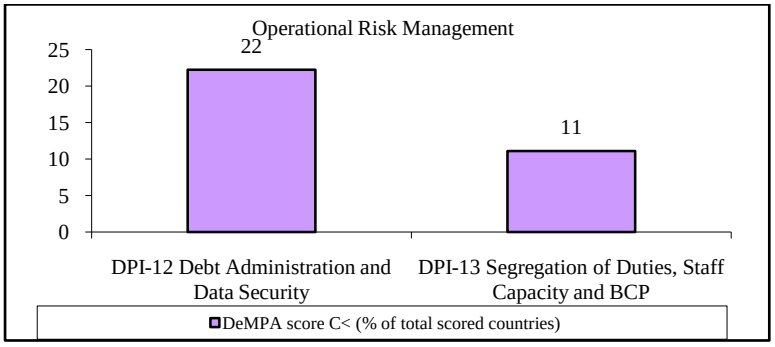
The DeMPA indicators that relate to the assessment of operational risk management in debt management operations are:

DPI-12 covering debt administration and data security assesses the availability and quality of documented procedures for (i) processing of debt service, (ii) debt data recording and validation, and (iii) controlling access to the central government debt recording/management, as well as the secure storage of debt recording/management system backups.

DPI-13 covering segregation of duties, staff capacity and business continuity assesses (i) the segregation of duties for some key functions, (ii) presence of a risk monitoring and compliance function, (iii) staff capacity and human resource management, and (iv) presence of an operational risk management plan including business continuity and disaster recovery arrangements.

The experience with undertaking the DeMPA assessments across 27 developing countries (as at end-December 2009) shows that most of these countries do not meet the minimum requirements in these two areas. As shown in Chart 1 only 22 percent of countries met the minimum requirements for DPI-12 Debt Administration and Data Security while only 11 percent met with the minimum effectiveness requirements on DPI-13 Segregation of Duties, Staff Capacity and Business Continuity.

Chart 1: DeMPA Results on Operational Risk Management

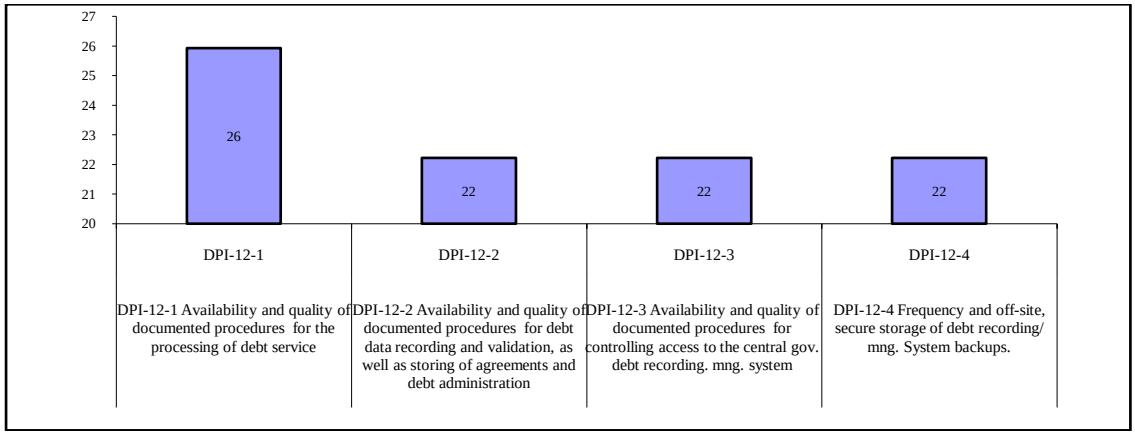


Source: DeMPA results

Chart 2 indicates that that less than a quarter of countries meet the minimum requirements for the first, third and fourth dimensions of DPI-12, which require documented procedures for processing debt service, controlling access to central government debt recording, management. Several countries were deficient in storage of debt management system backups and records in a secure location. Only few countries demonstrated sound practice in this area by taking daily backups and storing them in a secure location.

[15] Results are based on early results from 27 finalized DeMPA reports.

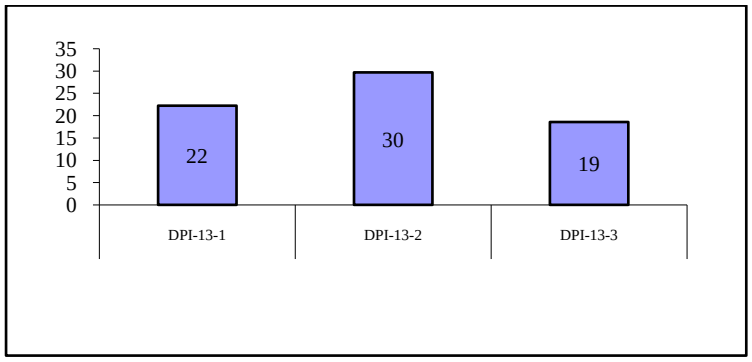
Chart 2: DeMPA Results on Debt Administration and Data Security Disaggregated by Dimensions



Source: DeMPA database, authors' calculations

Likewise, Chart 3 indicates that most of the assessed countries had weak debt management staff capacity; only one third met the minimum requirements for the dimension that examined whether staff are adequately trained with formal job descriptions. Twenty-two percent of the sample countries had clear separation between the debt managers with the authority to negotiate and contract debt, and staff which would service debt payments and those which would record and account other debt related transactions. Moreover, only 19 percent countries met the minimum requirements for the third dimension of this indicator and had business continuity and disaster recovery plan in place (Chart 3).

Chart 3: DeMPA Results on Segregation of Duties, Staff Capacity and Business Continuity Disaggregated by Dimensions



Source: DeMPA database, authors' calculations

During assessment missions, it was clear that the concept of operational risk and how this should be identified, assessed, monitored, and where necessary controlled/mitigated is not well known or understood. This is particularly the case in the Ministry of Finance. The Central Bank often had a better understanding, which in part is due to the need to meet with the BIS and other international compliance requirements. More importantly, none of the assessed countries have established a risk monitoring and compliance function for oversight of government debt management.

This clearly identifies a need to: (i) build awareness of operational risk and how to identify, assess, monitor and where necessary control/mitigate those areas that can impact government DeM operations from a cost and/or reputation risk perspective; (ii) build capacity in risk monitoring and compliance for government DeM operations.