SIGMA
A joint initiative of the OECD and the EU, principally financed by the EU
Creating Change Together

GOVERNMENT DEBT MANAGEMENT AND OPERATIONAL RISK:

A RISK MANAGEMENT FRAMEWORK AND ITS APPLICATION IN TURKEY

Hakan Tokaç and Mike Williams

SIGMA PAPER No. 50

2 Rue André Pascal
75775 Paris Cedex 16
France

mailto:sigmaweb@oecd.org
Tel: +33 (0) 1 45 24 82 00
Fax: +33 (0) 1 45 24 13 05

www.sigmaweb.org

THE SIGMA PROGRAMME

SIGMA is a joint initiative of the OECD and the EU, principally financed by the EU. SIGMA has been working with countries on strengthening public governance systems since 1992.

SIGMA currently works with:

- Croatia as an EU accession country
- Albania, Bosnia and Herzegovina, the former Yugoslav Republic of Macedonia, Kosovo*, Montenegro, Serbia, Turkey as EU candidate and potential candidate countries
- Algeria, Armenia, Azerbaijan, Egypt, Georgia, Jordan, Lebanon, Moldova, Morocco, Tunisia and Ukraine as EU Neighbourhood countries

SIGMA provides assistance in 5 key areas:

- Civil service management and administrative legal framework
- Public finance and audit
- Public procurement
- Policy making and co-ordination
- Public governance strategy and reform

SIGMA assesses:

- Governance systems and institutions
- Legal frameworks
- Reform strategies and actions plans
- Progress in reform implementation

and provides :

- Methodologies and tools to support reforms
- Recommendations on improving laws and administrative arrangements
- Advice on the design and implementation of reforms
- Opportunities to share good practice form a wide range of countries
- Policy papers and multi-country studies

For further information on SIGMA, consult our website:
www.sigmaweb.org

* This designation is without prejudice to positions on status, and is line with UNSCR 1244 and with the ICJ opinion on the Kosovo declaration of independence.

TABLE OF CONTENTS

Acronyms

CBT	Central Bank of Turkey
CC	Coordinating Committee (within DGPF)
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DeMPA	Debt Management Performance Assessment
DGER-IT	Directorate General of Economic Research and IT (in the Turkish Treasury)
DGFER	Directorate General of Foreign Economic Relations (in the Turkish Treasury)
DGPF	Directorate General of Public Finance (in the Turkish Treasury)
DMU	Debt Management Unit
DRC	Debt and Risk Committee (of the Turkish Treasury)
ERM	Enterprise Risk Management
IA	Internal Audit
KRIs	Key Risk Indicators
MC	Managing Committee (in DGPF)
MoF	Ministry of Finance
MoU	Memorandum of Understanding
ORM	Operational Risk Management
ORMU	Operational Risk Management Unit (in DGPF)
PDC	Public Debt Committee
PFMC Law	Public Financial Management and Control Law
RC	Risk Champion (in DGPF)
RCSA	Risk and Control Self-Assessment
RPFDM Law	Regulating Public Finance and Debt Management Law
SDU	Strategy Development Unit
SLA	Service Level Agreement
TCA	Turkish Court of Account

EXECUTIVE SUMMARY

The management of operational risk is at the heart of efficient government and of growing interest among SIGMA's partner countries. Managers in the public sector and international organisations have (irrespective of their area of work) a legal obligation to make sure that effective and documented systems of internal control are in place and applied. If anything goes wrong – whether as a result of external events or internal failure – the financial and political consequences and consequences to reputation can be severe.

Governments often fail to apply good or even routine operational risk management practices. Many have difficulty in understanding or knowing how to start putting the processes in place. This Paper provides information on just where to start and on how to develop a framework for managing operational risks, i.e. those arising from people, processes, systems and external events. The analysis provides senior managers with a clear oversight of key operational risks, and how necessary actions can be taken to manage them in a way that is consistent with the objectives of the organisation.

This Paper contributes to SIGMA's work with its country partners and follows earlier work done by the OECD as well as with the World Bank and the International Monetary Fund in learning and sharing experiences on governance and the management of operational risk. SIGMA's experience in working with the Treasury in Turkey illustrates how the general approach to operational risk and the techniques used can be applied across a wide range of activities, not only financial activities.

Specifically this Paper outlines for senior treasury managers, and government debt managers in particular, how an effective operational risk management process can be developed by:

- defining what operational risk is and from where it derives;
- identifying and assessing these risks;
- embedding a culture and a process to manage and report on key operational risks;
- addressing the challenges arising.

Operational risk is the least understood of the debt management risk categories. It cannot be captured and measured as easily as credit or market risk, and it is often endogenous to the institution. But it is no less important. Not only can financial losses be severe, there is potentially also severe reputation and political damage associated with operational error or failure, reflecting on the competence of the debt managers or of ministers.

In the case of the Turkish Treasury, the General Director of Public Finance appointed a 'risk champion' to start the process. This person was responsible for conducting the risk identification and assessment process, and prepared reports to the top management on behalf of other managers about the progress in managing risks and any changes in the risk profile. The risk champion has an important role through active surveillance to ensure consistency and in underlining the key issues for management. In Turkey the head of the middle office of the debt management unit is the risk champion. In practice many risks will be generated by the front or back office and the location of the

operational risk management function in the middle office can facilitate a degree of independence and overview.

Templates adapted to the Turkish Treasury were used to guide the assessment of operational risks. Such generic tables usually need adaptation to fit the organisation's differing internal priorities and external environment. The respective roles of the risk team and line managers or the reliance on hard or soft data can also vary.

Main risks should be identified and their importance (whether financial, political or reputational) should be measured within the organisation:

- by developing a clear framework to assess the significance of each risk;
- by evaluating and weighing both the likelihood of the risk being realised and its impact if it is (risk exposure is the product of likelihood and impact);
- by identifying the action to mitigate the risks and monitor their progress;
- by prioritising management actions;
- by recording all risks in a risk register to facilitate monitoring and the identification of risk priorities; and finally;
- by clarifying the different types of risk and distinguishing between inherent and residual risk.

The most effective way of identifying and assessing risks and developing a risk register is usually to run a series of workshops – which the Turkish Treasury did. Decisions should then be made on how to manage these risks. Risks can be accepted, avoided, transferred or controlled. These controls will in turn be linked to roles and responsibilities of staff for managing risks and related exposures. These decisions should give staff authority and delegation to handle those risks as well as the ability to operate in the event of any internal or external event that affects business continuity.

The risk profile is the summary document of the assessment. It facilitates review and subsequent monitoring of risks. The risk profile captures risk exposures and the reasons for decisions made about what is and what is not tolerable. It identifies the most significant risk issues on which senior management should focus.

In the case of the Turkish Treasury, it is the line managers' responsibility to complete regular monitoring reports. These reports include errors, incidents and changes in the risk profile of their units. The operational risk management unit analyses and summarises those and prepares quarterly operational risk bulletins. Those bulletins are submitted to the Debt and Risk Management Committee. The risk bulletin also includes information on actions needed, e.g. to respond to a worsening risk profile, with action-oriented recommendations prompted by managers' comments for further decision making by top management.

In establishing a process to report on key operational risks it is crucial that the culture of the institution does not make staff reluctant to report incidents if they fear that doing so can impact on their career prospects or performance assessment. There must be a "no-blame" culture; and the management should be supportive and avoid reprisal. Everyone in the office has risk management responsibilities. Risk awareness takes time to develop, and once established it must be reinforced. Basic training should be given to new personnel, with all staff being given periodic refresher courses.

This study also captures some challenges in developing the operational risk management process. The governance of the Ministry and the wider governance framework is of crucial importance and it

is necessary to ensure there is a mechanism that can properly weigh competing requirements. The main role of the Debt and Risk Management Committee in Turkey, as in many other countries, is to set a strategic debt management policy objective and mandate people responsible for strategy execution. Management should therefore set the boundaries of the operational risk management unit. These boundaries will depend on the size of the Treasury or Ministry where the debt management unit is established and a balance needs to be drawn where control of risk exposures lies largely outside the relevant managerial unit, i.e. in the Ministry or the wider Government. Other relationships such as those between the Ministry of Finance and the Central Bank, which is often an important service supplier, should be addressed at a senior level.

The benefits of operational risk management are difficult to measure as they can only be defined strictly in terms of what did not happen. Although risk management should be conceptually similar for all organisations, its application should take account of resource availability and the range of its responsibilities. In a smaller organisation it can be done without significant extra staff resources: a little time, thought and guidance is enough. A shortened process or partial framework is better than none: this is an embryonic process and practical experience is important to build upon. The experience in Turkey shows that such benefits are in reach with a proportionately modest resource cost.

INTRODUCTION

Objective of the Paper

This Paper is designed to be of value to financial managers, especially to government debt and treasury managers, and to all those who are looking to develop their management of operational risk as one type of risk that they have to deal with. It sets out a widely-applicable and relevant policy approach and management framework; the practical application is illustrated by the experience of using the framework in the Turkish Treasury.

The authors believe that the arrangements set out below and the lessons learnt can be applied across a wide range of debt management units (DMUs – this expression is used broadly throughout this Paper, and does not refer to any specific structure) and related treasury functions. The task may appear daunting: many DMUs are short of skilled staff, very few operational risk management professionals will be available elsewhere in the public sector, and DMUs are often precluded from recruiting from the private sector, whether by civil service rules or an inability to compete with private sector salaries. Nonetheless, a truncated process and a partial or broad-brush framework is better than none. The Paper sets out how policy and practical choices can be made in applying the techniques and in using the resources available, while also taking advantage of a positive internal culture and public sector standards of integrity. Similarly, the framework can be applied to all DMUs, however constituted, ranging from a fully integrated branch of a ministry of finance to a self-standing debt management office, whether or not it uses the central bank as fiscal agent. The difference will be in the risk assessments, which may depend on the unit's roles and respective responsibilities and its dependence on others.

Operational Risk and Debt Management

Risk management is central to the debt manager's task. Risk depends on exposure to future events, however driven, with exposure depending both on the probability of the event happening and its impact if it does. Risk management is about identifying and assessing these risk factors, and deciding whether and how to respond to them and mitigate their impact. Among the risks managed by debt managers, market risk has perhaps received the most attention, i.e. the risks associated with changes in market prices, such as interest rates and exchange rates, on the cost of the government's debt servicing. The assessment of market risk is underpinned by a range of widely-promulgated quantitative techniques. Also important is rollover risk, which depends on how interest rate volatility interacts with the redemption profile, and liquidity risk, the ability to access cash in a short period of time. Both can be seen as a category of market risk. Credit risk, the impact of a failure of a counterparty, may be important in some cases. The debt manager's task is to assess the magnitude of these risks, or the sensitivity of outcomes to changes in the risk factors, and develop a strategy for managing the trade-off between expected cost and risk.

Operational risk is perhaps the least understood of the debt management risk categories. But it is no less important. The DMU will be directly responsible for stewardship of very substantial government

liabilities (and also in some cases assets) and for managing a large value of transactions, probably much more than any other governmental body. The large sums involved mean that any risk exposure can have damaging financial consequences including on debt service costs. But there is potentially also severe reputation and political damage associated with operational error or failure, reflecting on the competence of the debt managers or of ministers.

Risk management should be a holistic and comprehensive process within a DMU. A larger DMU would have its own senior management risk committee or enterprise risk management framework to define its risk policies, covering market and credit as well as operational risk, to monitor exposures and identify the trade-off between risk and operational goals. Within this context, the exposures associated with operational risks and the importance of developing policies and procedures for managing those risks have been drawn to debt managers' attention.[1] . However, their implementation in practice has, for various reasons, been deficient. Operational risk management is difficult and may be seen as unfashionable and of relatively low status in the high pressure and politicised environment faced by many debt managers. Responding to this gap, the World Bank has recently published a guidance note on operational risk management in government debt management. Its Debt Management Performance Assessment (DeMPA) tool developed by the World Bank also has two debt performance indicators that cover important aspects of operational risk management.[2]

Good practice calls for the development of operational risk management policies and procedures that give senior managers a clear oversight of key operational risks, and for necessary actions to manage these risks in a way that is consistent with wider debt management objectives. This Paper, after setting out a general framework, draws on the work done in the General Directorate of Public Finance (GDPF) in the Undersecretariat of the Treasury in Turkey – in effect the Turkish government DMU. The GDPF has developed an operational risk management framework that is in line with good practice as widely adopted across the financial services industry internationally, while also taking into account the somewhat different objectives of a public sector body.

The work in the Turkish Treasury was supported by SIGMA, a joint initiative of the EU and the OECD, that supports potential EU (candidate) candidates and neighbours in their public administration reforms. Debt management operations were identified as an area of co-operation between the Treasury and SIGMA under a peer process and as part of the support to be provided more generally for the implementation of Turkey's Public Financial Management and Control Law No.5018, enacted in 2003 (PFMC Law). This public finance framework law, and the legislation flowing from it, introduces modern fiscal planning, budgeting, auditing and control procedures. The law does not specifically require the development of an operational risk management framework as described in this Paper, although it is fully in tune with it. An improved ORM framework was identified as a crucial part of an efficient wider internal control system as well as being necessary to bring this part of the Treasury's work into line with good international practice. [3]

---

1 Not least in International Monetary Fund and World Bank (2001), ("The Guidelines") where there are a number of references.

2 See World Bank (2009) and World Bank (2010).

3 The authors are grateful for SIGMA's support throughout the project (Mike Williams was the external consultant), and in particular of Ulrika Klingenstierna; Bianca Brétéché and Joop Vrolijk also made valuable comments on this Paper; and for helpful comments from other reviewers, including Lars Jessen (World Bank), Gunilla Liljeroth (Swedish National Debt Office), Ian Storkey and Enrique Cosio-Pascal (consultants), and colleagues in the Turkish Treasury particularly Coşkun Cangöz (DG of Public Finance), Sevgi Bakircı and Abdullah Kantarcı. Errors and judgements remain the authors' own; in this context it should be noted that the Turkish Treasury has not formally

SECTION I: MANAGING OPERATIONAL RISK

What is Operational Risk?

Operational risk is usually defined as "the risk of loss (financial or non-financial) resulting from inadequate or failed internal processes, people and systems, or from external events that impact a company's ability to operate its ongoing business processes."[4]

It should be noted that this definition:

a) is positive (it is possible to measure and manage operational risk);

b) is comprehensive: it does not concentrate only on specific functional areas (back office, IT, payments, etc) or risk categories (compliance, fraud, etc).

c) is flexible enough for each entity to tailor to its own specific needs;

d) includes external events.

On a narrow reading this definition excludes reputation risk (reputation is public information or perception about an entity's capability or credibility; and the risk exposure arises from events having a negative impact on those perceptions). But reputation risk is especially important in the public sector and indeed is increasingly regarded as the greatest all-pervasive threat in the financial services area. Even if the cost in the first instance falls on the market or creditors not the entity, there are plenty of routes through which the cost can be reflected back onto it. Certainly regulators and rating agencies usually expect reputation to be monitored as an important part of the operational risk framework – and that is good practice. The definition also excludes strategic risks, *i.e.* those compromising the entity's high-level goals. They should also be monitored and controlled. In a DMU it may be convenient to do so alongside operational risks – the same tools are appropriate – and many entities handle them, together with credit, market, and liquidity risk, in a wider enterprise risk management (ERM) framework, as discussed below. In an internal audit context, strategic, operational and reputation risk may be considered together.

Not all the regulations and standards that are being increasingly applied in the private sector (such as the Basel II capital accord and, the Sarbanes Oxley Act in the US as well as the statements on risk exposures and internal control procedures expected under accounting standards) formally apply also in the public sector. But public sector entities and debt managers in particular, are increasingly expected to follow private sector good practice where it is relevant. The public sector is also highly exposed both to reputation risk and to closely-related political risk. The loss of reputation can prove costly as well as embarrassing if for example the market and investors in future prove unwilling to

---

endorsed all the implicit judgements of this Paper.

[4] This definition was adopted for the Basel II capital accord, following work by a private sector industry group. See also BIS (2003). In some contexts legal risk, information security risk, settlement risk, new project risk, etc may be identified and handled separately; here they are all included within operational risk.

give the DMU the benefit of the doubt in the event of further errors or uncertainties, however prosaic they might be.

Enterprise Risk Management

Operational risk management (ORM) should be seen as part of the wider ERM framework. ERM deals with risks and opportunities affecting overall value creation or preservation and has been defined as "a process, effected by an entity's [board or senior management], applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[5] As well as operational risk, ERM extends to the high-level alignment of strategy with the willingness to accept risk, and deals with multiple and cross-enterprise risks, and the potential interactions between different risk categories.

In a debt management context, the entity may be the DMU or the ministry as a whole; and the range of risk factors may be similarly wide. At the level of the enterprise, therefore, operational risk cannot be abstracted from market and credit risk. But it has some distinguishing features:

a) It is endogenous to the institution; it is linked to the nature and the complexity of the activities, to the processes and the systems in place, and to the quality of the management and of the information flows.

b) It cannot be captured and measured as easily as credit or market risk.

c) It flows from many sources. These include a lack of discipline, poorly designed procedures, inertia, change, greed, inadequate knowledge, and overconfidence. Box 1 includes some examples applying to a DMU. None of these factors is easily quantified, monitored, or reported upon; but most apply in one way or another across any entity's activities, and would be taken into account in any ERM framework.

[5] COSO (2004). COSO is the Committee of Sponsoring Organisations of the Treadway Commission. See: www.coso.org.

Box 1. : Examples of Operational Risk Exposures

A distinction can be made between risks that are internal to the DMU – which should be under the control of management – and those that are external – but management should have mitigation or other policies in place. The distinction is not hard-edged and in practice exposures often arise from the interaction between external and internal factors.

Internal to the DMU

Policy and analysis failure

Poor process design

Personnel failure – key person risk, error, processes followed incorrectly, weak code of practice or other HR policies

Insufficiently clear legal or other documentation

Project failure

Internally supported systems failure – IT software or hardware, other systems

Incomplete data

Premises failure – power etc – and physical security

Failure to follow employment law or health & safety standards

Fraud, theft or other crime

External to the DMU

Policy changes by Ministers, regulators, other stakeholders

Poor high-level policy making, weak governance structures

Failure or errors of suppliers, outsourcers or agents (a failure of their risk controls)

Changes in legislation or the courts' interpretation

Legal or commercial disputes, inc employment contracts

Externally supported systems failure

System attack (hacking)

Business continuity events – of fire or flood, terrorist or industrial action; or natural disaster

Operational Risk Management Techniques

A number of ORM techniques or tools have been developed. The differences, however, are relatively small. Many are applicable at the level of the enterprise as a whole, and they all have the same important elements in common.

a) Developing an appropriate risk management environment. Senior management should be aware of the major operational risk exposures as a distinct risk category that should be managed; it should approve and periodically review the ORM framework, ensure clarity in implementation priorities and responsibilities and put in place appropriate independent audit arrangements that could challenge the operational risk management system.

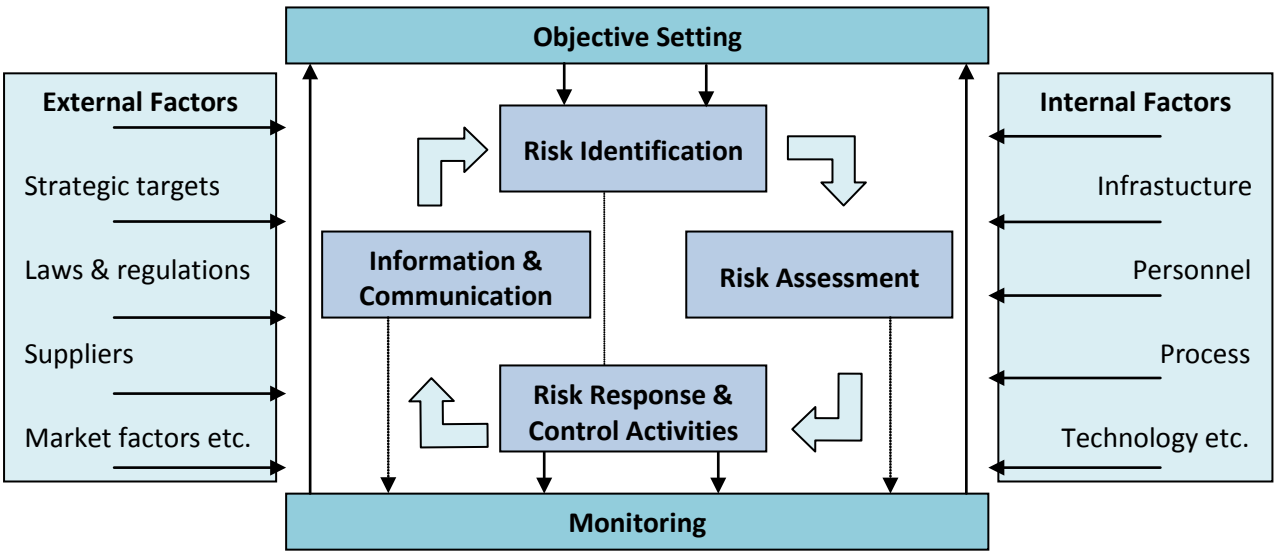
b) Systems for risk management: identification, assessment, monitoring, and mitigation/control. That requires identifying and assessing operational risks, both those arising externally and those inherent in all activities, processes and systems; implementing a process to regularly monitor operational risk profiles and exposures; and having policies, processes and procedures to control and/or mitigate material risks, including contingency and business continuity events.

There is no one template that fits all organisations. There will be differing internal priorities and external environments; and the respective roles of the risk team and line managers or the reliance on hard or soft data will vary. The tools are nevertheless useful as a guide or aid. The technique set out here broadly follows that established by COSO.[6] The COSO approach is a widely-used standard for understanding and evaluating internal control structures particularly in a transaction processing environment. Although designed for ERM, it is equally applicable just to ORM, and has the advantage of being comprehensive, sector- and territory-independent, and also sufficiently flexible for extension to a specific area of interest. A summary of the COSO approach is at Annex A. It identifies eight inter-related components: the internal environment; objective setting; risk identification; risk assessment; risk responses; control activities; information and communication; and monitoring.

It is also important to stress that ORM is a dynamic process; it is not a one-off event or an add-on. It is a series of actions that permeate an entity's activities. The ORM processes should be repeatable and linked into day-to-day work across the organisation, and hence to continuous incremental improvement mechanisms built into the ORM cycle. A data history, *e.g.* of key risk indicators (KRIs) or risk events, is built up gradually to enable effective trend analysis.

The cyclical process is illustrated in Figure 1. The internal environment (and influencing factors) provides the setting within which top management establishes objectives. All staff and management are responsible for maintaining the ORM process with the formal ORM function having a coordinating responsibility and also establishing an information and communication framework for reporting and evaluating results. Monitoring is undertaken in parallel and is semi-independent of the ORM function as its purpose is to evaluate the effectiveness of the ORM programme itself.

Figure 1: the Dynamic ORM Process [7]



[6] Other techniques include the "Risk Management Standard" of the UK-based Association of Insurance & Risk Managers and others (AIRMIC/ALARM/IRM 2002); and the Australia /New Zealand Standard AS/NZS 4360:2004. Since the Turkish Treasury started its work an international standard on risk management ISO 31000 has been developed to provide guidance on the risk management process and its implementation. Both ISO 31000 and the COSO framework are built on the same model of selecting an objective and using it as a standard for evaluating risk management effectiveness and efficiency. The practical steps for a debt office are essentially the same.

[7] Adapted from a chart in TransConstellation (2007a), page 19.

The ERM and ORM framework should be integrated in the internal control environment in the DMU, or entity of which it is a part, as summarised in Box 2. These elements are not entirely independent; indeed they feed positively off each other when embedded in a supportive culture that is aware of risk and the importance of its management.

Box 2. : Internal control

The system of internal control for a DMU potentially includes a number of components, some of which may operate at the level of the wider treasury or ministry of finance:

The corporate governance management structures (*e.g.* a public debt committee, an advisory board, cross-function managing committee, policy making committees; also an audit committee where applicable), and the related accountability processes.

A process for establishing objectives supported by regular review of performance, and the entity's priorities and targets.

A risk management framework covering the range of enterprise risks. This includes strategic, credit, market risk, etc; and also operational risk (as discussed in this Paper), including the business continuity plan, incorporating any disaster recovery site.

Arrangements to ensure that management in each business function is responsible for ensuring that the operations within their area are compliant with plans, policies, procedures and legislation. This may include controls on market and credit risk exposures.

Internal budgetary controls, including a mechanism for approving and attaching priorities to internal capital expenditures or projects and managing their implementation.

HR policies; including a code of conduct or ethical practice.

The control environment will be supported by an internal audit function providing an opinion on the adequacy and effectiveness of internal control systems and recommendations for improvement.

SECTION II: OPERATIONAL RISK MANAGEMENT IN A DEBT MANAGEMENT UNIT

Responsibilities

Middle Office

The management of operational risk must be a responsibility shared and understood by all staff in the DMU. Staff should be aware of the risk exposures in their area, and how they might undermine objectives, and have responsibility for managing those exposures within their own control. Line managers should be responsible for identifying and monitoring the risks in their own units and for ensuring that the control activities work as intended and in line with priorities set by senior management. But the ORM framework itself, and the associated processes, should be established and maintained by the ORM function that lies within the middle office of a DMU with other risk management functions (the ORM unit will often be very small, at most 2 full-time persons and possibly less than one person in a small DMU). In practice many of the risk exposures will be generated in front or back office; but the location of the ORM function in middle office facilitates a degree of independence and overview.

The ORM function has two roles: it drives the process and monitors performance and execution, reporting to senior management; but it also acts as a consultant to line managers in identifying risks and planning control activities. In practice the function typically evolves over time, from being the main driver when first establishing the framework, to being more of a facilitator or consultant when it is running smoothly.

It is also important to note:

a) Control activities must be planned at all levels throughout the organisation and the responsibilities for their execution and follow-up clearly defined.

b) The responsibility for developing and implementing risk mitigation plans lies with management (including the administrative units or process owners).

c) Monitoring and reporting is undertaken in parallel. Insofar as monitoring includes evaluating the effectiveness of the ORM process itself (*e.g.* by internal audit), it should have some independence of the ORM function.

Senior Management

ORM is a key component of the overall governance structure, *i.e.* the structured internal processes of specifying objectives, making decisions and monitoring performance within the wider environment, including the strategic objectives and accountability processes applying to the DMU itself.

The degree of top management attention is arguably an initial indicator of an organisation's ORM maturity level. Full Integration and recognition of ORM requires senior management:

a) To give explicit attention to the risk culture, closely linked with human resources development and evaluation practices.

b) To provide leadership in interpreting and translating often intangible governance considerations into a practical policy.

c) To allocate responsibility for ORM objectives to employees across the organisation.

d) To ensure that ORM is an integral part of communication and monitoring activity.

e) To embed fully policies and procedures in working practices.

Some thought also needs to be given as to how the ORM function relates to related functions, such as internal audit (IA) and a separate compliance function if there is one. The IA function should be independent of the ORM function, not least because part of its role is to evaluate ORM processes, and should report to the head of the DMU. It should be governed by an audit charter that gives the unit sufficient authority and freedom. The IA function may sometimes be referred to as the "third line of defence" in a model where the first line of defence is line management and the internal control system, and the second line is the risk management and compliance functions. Many DMUs will be too small to have a dedicated IA function and they will in practice share that of the wider ministry of finance. But it is important that the IA plan of work takes proper account of the DMU's risk profile; and the risk managers can usefully have an input into that.

Compliance is the process for ensuring that procedures and controls are consistent with rules and regulations (legislation, codes of conduct etc) and also that they are properly operated. In the past the organisational distinction between compliance and the IA function may have been unclear but more recently a separate function has been developed for financial services activities to cope with the complexity of the regulatory environment; the compliance officer will often be the main day to day contact with the regulators, although that is less relevant for a DMU. The compliance function will carry out its own checks to ensure that controls are operating as they should; and it may be dispersed in individual operating units in a way that is not usually the case for IA (and compliance's work is also potentially subject to audit by IA), or it may be part of middle office. It is likely that only larger DMUs and those operating in a more sophisticated environment would have a separate compliance function. In any event compliance would work closely with both the IA and ORM functions to avoid unnecessary duplication.

General Approach

First Steps

To discharge its responsibilities senior management needs:

a) A process for identifying key risks which might impact on objectives, and for quantifying or assessing them.

b) A high-level summary of risks that is consistent across the DMU, and a technique for assessing key exposures as a way of identifying priorities.

c) Controls or other techniques for managing risks and exposures. Controls will in turn be linked to roles and responsibilities (clarity, segregation of duties, etc); authorities and delegation; and robustness (ability to operate in the event of any internal or external event that affects business continuity).

d) An opportunity to review regularly the risk profile and reassess priorities in the light of changes in the environment and risk events.

These management needs must mesh with the procedures that operate at working level, *i.e.* the preparation of risk registers, the development and operation of controls and the preparation of procedures that embody them.

The approach set out here is designed to be consistent with good practice but to take account of the constrained resources of many DMUs and their integration in wider ministerial or governmental organisations. It is an approach that has been tested in a number of DMUs.

The first step is to identity an individual in the middle office to lead the process – often referred to as the "risk champion". More developed DMUs will have an ORM professional; others will need to identify an official who will be tasked to organise, develop and drive forward the framework, advise line managers as required, maintain risk data and report to senior management on the risk profile. In the smallest DMUs, this official may have other middle office responsibilities.

Risk Identification and Assessment

The risk register then needs to be populated. This can be done in different ways (brainstorming, scenarios etc); but the most effective is usually to run a series of workshops. Consultants can be involved in this process, perhaps as a facilitator. But the raw data must come from those familiar with the organisation. Local managers and staff must "own" the process throughout, with full support of course from top management. The workshops can be organised on a team basis across the DMU, by using a mix of individuals across teams, or on an administrative process basis (smaller DMUs may decide to engage all staff directly). Either way all staff need to be involved somehow, directly or indirectly; the process must not only be top down. One of the dangers of working team by team is that linkages between teams are not given due weight. Some organisations instead focus on more horizontal processes, including the interfaces between managerial units. However, horizontal assessment tends to takes longer and to have a higher organisational cost. At an early stage, it may be wiser to focus on teams or managerial units, not least because that links with developing the responsibility of individual managers for the risks in their area. As the work develops it could be enhanced to include cross-cutting processes. As will be explained in Section III a working group was formed in Turkey with cross-team membership; but their work was periodically tested in a much wider group, meetings of which also helped to develop risk awareness.

The workshops should be guided by someone, probably the risk champion, who has an understanding of risk across the range of functions; and can also ensure a consistency of approach and terminology. In practice there will be far bigger risks in some areas of the DMU's work than in others – and without some process to ensure consistency, there is a significant risk that the result will be lists of risks that have been 'scored' by very different criteria.

The workshops identify and describe key risks that might impact on each the DMU's objectives. The approach is to break down the main areas into activities or processes, each with a stated objective. There is a balance to be drawn between the amount of detail and usefulness to management. If the initial exercise involves many staff it may generate several hundred separately identifiable risks. But in practice many of the risks will be similar to each other; and smaller organisations find it more convenient to boil the number down somewhat, maybe to 100 or less. There will probably be a further summary in reporting to senior management.

The risk exposures then need to be put in priority. “Exposure” is the likelihood of the relevant risk event multiplied by its impact. In the private sector good practice is now to try to quantify the risks in financial terms. Operational risk can then be added to measures of credit and market risk to set against total risk appetite. But this is not recommended for a DMU, at least in the first instance:

a) It is time consuming and resource intensive to set up the system in an internally consistent way.

b) By reducing everything to financial numbers there is a danger of downplaying reputation or political risk.

c) It is all too easy to focus effort on risks that can be quantified, at the cost of overlooking risk exposures that may be just as great if more nebulous.

But some technique is needed to weigh exposures. A convenient way of doing this is to rate each risk for both likelihood and impact and plot the combinations on a matrix – see the next Section. The most serious risk exposures are those of high likelihood and large impact; they will be identified for urgent management action. In a full exercise this scoring process would be done separately before and after the mitigating controls, and some view formed both as to the effectiveness of controls and whether the residual risk can be further reduced or is unavoidable. In practice, in a resource-constrained environment, the initial focus should be on residual risk, not inherent risk, i.e. reflecting the current risk environment.

There is further information to be gained from analysis of risk drivers, summarising exposures for example by:

a) Causes: people, process, system, legal, external ;

b) Event types: *e.g.* internal fraud, external fraud, employment practices, error checking, business disruption, system failures.

If there are patterns emerging, for example the frequency with which IT drives high exposures, that is highly relevant to management.

In Turkey the process of risk identification and assessment was done thoroughly and took a number of workshops, as described in the next section; but in the smallest DMU just 2 or 3 workshops may generate sufficient data to identify the main risk exposures for senior management, even if they are defined in generic or broad brush terms.

Risk Response and Controls

There is a policy progression from identifying a risk exposure, to deciding the risk response, and then implementing the necessary control or other action. Risk responses are often categorised into four headings:

a) Accept the (residual) risk.

b) Avoid the risk (*e.g.* stop a certain service – which may not be open to a DMU – or choose a totally different technological solution).

c) Transfer the risk (*e.g.*, insure against losses, outsource to a specialised party).

d) Mitigate (control) the risk, taking measures to reduce the probability of it materialising, and/or reduce the impact of the loss event.

Ideally there should be an assessment process to judge the most effective approach, trading-off cost and risk appetite. For major risks, the response decision should be made by senior management. In practice in a DMU, as in other transaction processing bodies, mitigation controls will be especially important.

Control activities are the policies, procedures, practices, and organisational structures that help to ensure that residual risk levels are brought to their target levels, and that risk-response action plans are carried out. Many of the control techniques will apply to many of the risks. Some examples are in Box 3. There is advantage where possible in combining controls (*e.g.*, prevention and detection measures, automated process controls and manual monitoring controls, etc). The effectiveness of the control can be followed up and evaluated (*e.g.* by monitoring the impact on KRIs, see Section IV below). By its nature, the ORM cycle is iterative, and lessons should be learned on what does or does not work.

Box 3.: Examples of Controls

Prevention

- Automation and process standardisation and instructions
- Access controls
- Segregation of duties, dual verification (“four eyes”)
- Formal sign-offs
- Training
- Trialling/testing

Detection

- Confirmation matching
- Reconciliations
- System monitoring
- Compliance reviews, security inspections, internal and external audit

Mitigation

- Investigation procedures
- Business continuity and disaster recovery plans
- Back-up systems and support, archives
- Insurance

Documenting Procedures and Controls

Once the key controls are identified, it is possible to write operating procedures, which should incorporate those controls. This is best done by those who have designed the procedures and identified the controls, in practice probably the relevant team leaders; this ensures ownership at

operational level. Similarly, procedures should not be written by an external consultant; that guarantees that they will be ignored. The procedures should be written in a way that makes sense to those who are operating them, although they should be subject to review by the risk champion or other expert, who could facilitate the process by supplying templates.

The purpose of documenting the procedures is twofold:

a) To provide a check-list for the relevant member of staff or his/her manager to ensure that all the necessary actions underpinning an activity have been executed and the relevant controls or checks evidenced.

b) To provide a basis for the risk manager, auditor or compliance officer to confirm that actions are being taken in accordance with agreed procedures and to investigate whether the embedded controls are effective, efficient and proportionate.

The procedures should be written in summary form, and should not be any more detailed than is needed. However, there should be sufficient detail so that if a staff member was taken ill or unexpectedly leaves, his or her replacement could step into the relevant functions.

Reporting

The risk champion should report to management on the overall risk profile. This will require identifying the greatest exposures from the workshops, together with suggested control or risk management actions. Regular reports (say, quarterly) should then be made on changes in the risk profile. This is best linked with individual managers themselves reporting on the risk profile in their area. Once the relevant spreadsheets have been prepared, summarising the output from the workshops, this should be relatively straightforward. Managers should report their experience over the previous period, and indicate how their risks have changed, any changes in controls, and any recommendations for further mitigation action. Their reports would be co-ordinated and summarised by the risk champion. The smaller the DMU, the more streamlined must be the process; but it follows essentially the same steps.

The risk workshops should be held again periodically to refresh the data. This is particularly important, *e.g.* following a team or office re-organisation. The same technique may be useful to brainstorm the risks associated with any new policy instrument or other change in the way in which the DMU interacts with stakeholders or customers.

Part of the regular report to senior management should be a summary of incidences and exceptions. They are relevant both as a way of monitoring the control framework and in identifying new or poorly managed risks. Each incident should be reported, with proposals as to how to avoid the same problem in future. It must be emphasised to staff that this is not a matter of their having to "own-up", nor does it in any way expose them to disciplinary action – it is a "no blame" culture. But it is important to learn lessons so that the same problem does not recur. Many incidents and even staff errors are often not the fault of the individual concerned, but of management who has failed to develop an adequate control environment.

Reporting is discussed further in Section IV, along with some of the practical challenges that arise. But it is first useful to set out in more detail how the approach was applied in Turkey.

SECTION III: OPERATIONAL RISK MANAGEMENT IN THE TURKISH TREASURY

The Treasury and the Reform Programme

The Turkish Treasury, which is affiliated to the Prime Minister's office, has a lead economic management role within the central government. Its range of functions is diverse, covering debt and cash management, foreign economic relations, assisting government in economic policy design, regulating the insurance market, and monitoring and supervising state aids in line with European Union *acquis*. The most senior official is the Undersecretary of the Treasury; he has three deputies, and they manage seven General Directorates, of which GDPF is one, and various audit, consulting and support units. Around 1200 people work at the headquarters of the Treasury, of which 160 people work for DGPF. An organisation chart is at Annex B.

The PFMC Law, which was enacted in 2003, marks a fundamental reform in public financial management. It addresses long running problems of the Turkish financial administration including wastefulness, poor productivity and undue focus on the short-term. It introduces modern financial administration concepts, including accountability, financial transparency, fiscal discipline, internal audit and control, a better balance between authority and responsibility, fiscal planning, and improved budget and expenditure processes. Since the PFMC Law almost all public institutions have prepared three year strategic plans setting out their mission, vision and strategic goals; performance budgeting requirements ensure that these strategic goals are linked to budgets. Importantly the new law also requires all public institutions to establish an internal control framework.

In the area of debt management, the Government has initiated a further series of reforms following the ratification in 2002 of the Law on Regulating Public Finance and Debt Management (RPFDM Law). This Law defines the Treasury as the sole borrowing authority on behalf of the government, introduces changes in the debt management organisation structure in the Treasury (see Annex B), and determines the main principles and procedures for debt and receivables management and guarantee issuance. A Debt and Risk Management Committee (DRC) has been established and is responsible for determining strategies for the management of public assets and liabilities, taking into account the risk and cost targets. At the same time a new risk management unit, or middle office function, was created in DGPF, to monitor the risks associated with public debt and receivables and develop strategy proposals for the DRC. This middle office is applying sophisticated models for monitoring market and credit risk, commended by the World Bank and other international organisations as in line with good practice.

The PFMC Law mandated all public institutions to set up a Strategy Development Unit (SDU) and an internal audit (IA) function. The Treasury created its SDU in early 2006 with responsibility for establishing the internal control framework and associated systems and standards within the Treasury, within a framework to be set by the Ministry of Finance (MoF) which acts as the Central Harmonisation Unit for all line public institutions for establishing the internal control framework. An IA unit was established in the Treasury in early 2008, reporting directly to the Undersecretary. External audit is conducted by the Turkish Court of Accounts (TCA). In its 2005 Audit Report the TCA

recommended the Treasury to develop an internal control framework according to the guidelines which would be developed by the MoF.

Against the background of these initiatives, DGPF, also conscious that the risk management work done in middle office lacked an ORM component, took the initiative to establish an ORM framework as part of the wider internal control system.

Initially DGPF developed an ORM framework in the back office which is responsible for servicing of domestic and foreign debt, receivables management and debt accounting and statistics. The back office was chosen as a pilot area because the number of transactions is relatively high and the processes somewhat easier to analyse than the middle and front offices. After completing the work at the back office DGPF carried out similar work in the rest of the DG. Eventually the framework of the all three offices and the support units were combined in a coherent way.

The Process

Organisational Arrangements

The first step was an analysis of the current ORM arrangements. This work identified poor risk awareness and a lack of risk systems (i.e. limited risk evaluation against activities and objectives, no internal audit and few administrative guidelines). In the light of these results DGPF developed an action plan and timetable, setting out the detailed steps towards an ORM framework.

A new organizational structure was formed to carry out the ORM work within the DGPF: see Annex B. The head of the middle office was appointed as the Risk Champion (RC); and a new operational risk management unit (ORMU) of two people was established under him. A management committee (MC) was formed, chaired by the General Director with his deputies (*i.e.* the heads of front, middle and back office) as members. The RC chaired a coordination committee (CC) which included representatives from all units of the DG. Working groups were formed in each of the three offices and support units of DGPF (although each of the three offices proceeded separately initially, the MC and CC were DG-wide). Around 4 to 5 people were assigned to these working groups from each office and they were required to act as liaison between their colleagues and the CC. All these changes were announced by the Director General in a letter to staff, who were asked to support the new initiative.

The RC led and coordinated the whole process. The CC met regularly once a week throughout and executed the action plan in line with the timetable. In each meeting all work of the previous week was revised and the next week planned. MC met regularly once a month to oversee the process and ensure that it was kept to timetable. MC also approved decisions taken by the CC, which were taken forward by the working groups, meetings of which were attended by members of the CC to ensure a consistent approach application across the DG. These arrangements ensured that everything was being done in harmony at all levels of DGPF. The RC and the ORMU met with the SIGMA team from time to time to review and revise the procedures, and confirm that they were in line with international good practice.

Building the Risk Profile

The next step was to provide training to the DG staff, led by the ORMU, on both the concept of ORM and the process to be followed. It was important at this stage to involve all the staff and raise risk awareness. After the training sessions, the working groups started to build up the risk profile tables of their units; workshops identified activities, activity purposes, associated risks and current controls.

All relevant line managers attended these workshops, as did the ORMU (in many cases the RC) to ensure a consistent approach. The working groups identified both the specific risks which would hinder timely and accurate achievement of activity goals and sources of risks (classified simply as people, external, legal and institutional).

Once risks were identified, they were measured according to their impact (whether financial, reputational or political) and likelihood. DGPF used qualitative measures taking into account the nature of the work of a DMU. This work was done in workshops in which all working groups (and in some cases the SIGMA consultant) participated under the RC's coordination; the collective workshops were followed up by workshops in each unit. In this way a common understanding of how to measure risks was established. The final result was a matrix with nine columns as shown.

Activity Area	Activities	Objectives of Activities	Encountered Risks	Source of Risk	Existing Controls	Likelihood Level	Impact Level	New Controls

An example of some rows in the risk matrix is in Annex C. Likelihood was scored in five levels from very low to very high; impact also in five levels from insignificant to catastrophic. Among the more serious impacts would be significant data errors that lead to errors in debt servicing or create a misleading redemption profile; or a failure to comply with legislation After scoring all risks, a risk exposure matrix was formed, i.e. showing the product of likelihood and impact – see Figure 2.[8] The matrix was used to prioritise the risks and craft new control mechanisms to mitigate the high level risks. The darker colours (the "heat map") indicated the higher priority areas; those in area 3, 4 and 5 in Figure 2 were identified for early action.

Figure 2: Risk Exposure Matrix

		Impact level of risk				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood level of risk	Very Low	1	1	2	2	3
	Low	1	2	2	3	4
	Medium	2	2	3	4	4
	High	2	3	4	4	5
	Very High	2	4	4	5	5

All risk profile tables of the three offices in DGPF were combined by the senior management team. Several workshops were run in which the Director General, his deputies and all other line managers participated for the combination of risk profile tables. The DG himself led these workshops and the tables were combined by eliminating repetitions and covering the whole functions of the DGPF.

[8] A smaller DMU might use a smaller impact/probability matrix; but the scoring process of itself is not very time consuming; indeed, the first rough cut is likely to add the most value, and the scoring can be refined as the risk matrix and heat map are updated in future periods.

Reporting

Error reporting formats were developed as a tool for monitoring and improving risk assessment; and staff encouraged to report errors as soon as they were encountered. "Errors" is defined broadly to include all incidents, including those that are system-related. In order to help them understand the report format and methodology, the ORMU provided training to all staff. Error reports are received and monitored by the ORMU. To make reporting easier the risk profile tables and error reporting formats are on the DGPF intranet. In their reports staff link the errors to the risk profile table (by noting the relevant row number). This process not only helps the ORMU to assess the sources of risk or changes in the risk profile, it also contributes to improved risk awareness among the staff, and better understanding of the linkage between risks and controls.

Line managers are required to fill in monitoring reports on the errors reported by their units and changes in the risk profile of their units and send these reports to ORMU. This ensures that managers are notified about errors and also adds a management level perspective. Managers are asked also to give feedback about the measures taken, make suggestions for future prevention, and give their opinion on how the risk in their area are evolving, whether they are decreasing or increasing in these reports. The columns of managers' quarterly report are shown.

Main Risk Area	Risks	Evolution	Measures	Suggestion	Additional Notes

The ORMU prepares quarterly operational risk bulletins for the DRC in which analysis and information on the risk profile table and errors of the previous quarter are summarised. This encourages the involvement in the ORM process of senior managers, who closely monitor changes in the risk profile. The bulletins are discussed in DRC and new control mechanisms or other mitigation strategies developed (*e.g.* training, sharing external risks with other departments or providers). The focus of course is on the highly-scored risk exposures.

Looking Forward

DGPF staff will continue to produce error or incident reports which will enable the RC to test the risk exposures and concentrations identified in the risk profile table; line managers will complete quarterly monitoring reports; and the RC will present the Risk Bulletin to the DRC. The implementation of controls, as well as their impact on risks, will be closely monitored. There are plans to update the risk matrix once a year, involving staff at all levels. During this process, the lessons of error reports and monitoring reports will be taken into consideration.

The risk profile tables, risk matrixes and error reports were originally built in excel spreadsheets. Even though excel was a sufficient tool, DGPF has developed an operational risk management software programme in order to enable the system to operate more quickly and more securely.

Early Messages

The initial setting up of the ORM framework required some time and attention, with many meetings and workshops. The need for staff to work overtime initially caused some of them to see the process as a burden. But in time they realised that it in fact made their work easier and reduced the number of mistakes and errors; and they became more supportive. This change in attitude was related to the

increase of risk awareness, particularly in more operational areas. The full and visible support of senior management also helped counter any reluctance. Staff have also been able to use the ORM framework (including the error reports and risk bulletins) to convey their needs to the senior management, *e.g.* for training or office equipment.

The decision to start with DGPF's back office as a pilot, only subsequently rolling the framework out to the rest of the DG, created a few problems. In part this was about different parts of the DG working at different stages which created some delay in implementing the whole system across DGPF. It took one year to set up the framework at the back office and one year to roll it out to the rest of the DG (middle office, front office and support units). Then it took six months to combine the risk profile tables of the back office and the rest of the DG. Although the experience obtained in the back office was helpful in extending the framework to the rest of the office, setting up the system in all of DGPF at the same time would have saved time.

The numbers of rows in the risk profile tables is an indicator of the work involved. The total of rows, i.e. separately identified activities, for the different offices (front, middle, back and the support units) was around 1 250. By eliminating the overlaps, taking into account the processes of the whole DG, the number is around 750 in the final risk profile table. There are fewer separately identified risks than activities, about 600 across all offices, although following rationalisation the combined risk exposure matrix has about 400. About 13% of these risks fall into the high exposures areas 4 and 5 of the heat map; 46% of the risks fall into areas 3 and 4, and 52% into the low exposure areas 1 and 2. (Some other organisations have anecdotally reported broadly similar distributions.)

DGPF started to benefit from the ORM framework right away. Immediately after it was set up in the back office, new control mechanisms were developed for the risks of highest priority, including the development of a disaster recovery plan and establishment of an IT Disaster Recovery Centre to provide for the continuity, restoration and recovery of critical data and systems. Additional control mechanisms have been developed, and are being implemented, for the risks in categories 3, 4 and 5. Detailed guidelines for debt management information systems have been prepared (some 400 pages) as well as control lists of relevant processes.

Using the Technique in a small debt management unit

The discussion above has noted at some points how the technique might be modified for a smaller DMU. Although it is conceptually similar for all DMUs, in practice its application can take account of resource availability and the range of responsibilities. Where a central bank is fiscal agent and paying agent (possibly also managing the debt database) the risk exposures within the DMU will be less than when those functions are in-house. But the same processes of risk identification and assessment, risk response and control, and monitoring and review are important in any environment. The difference may lie in the thoroughness with which the processes are applied at least in the first instance. As experience grows and capacity builds, so the ORM framework can also be developed.

In a small DMU of say less than 15 people, the approach might be along the lines suggested in box 4.

Box 4.: The Technique in a Small DMU

- A "risk champion" is appointed by the head of the DMU – this role may only be a share of his or her time; but it should probably be at least 40% of a full time equivalent.
- The risk champion, possibly with consultant support but certainly with the visible support of senior management, briefs the whole DMU on the process and its relevance. If the ministry's internal or external auditors can be involved, so much the better.
- Workshops for risk identification and assessment are held. There might be only 2 or 3 groups (maybe one each for front middle and back office); but the risk champion attends them all (again an external consultant could act as facilitator) and takes responsibility for identifying and recording issues that cut across the groups. It may be wise in the first instance to keep the total number of identified activities and separate risks identified to no more than 100 in each case. One meeting of each group may be sufficient – but more may be preferred.
- The risk champion records the matrices and summarises the results for senior management or the head of the DMU, identifying priority actions. The head of the DMU, with the support of the risk champion, may want to pursue concerns with senior management or others in the ministry, or with the central bank.
- There is a process of regular review, perhaps with the head of each office reporting quarterly on whether the profile in their area has changed. This should be buttressed by incident reporting. The risk champion summarises this material for management, adding his or her own recommendations. The development of performance or risk indicators comes later.
- The risk data are periodically refreshed with future workshops. As capacity develops the thoroughness and detail of this process, and the associated reporting, also increase.

SECTION IV: HANDLING PRACTICAL CHALLENGES

This section draws on experience of using the framework in the Turkish Treasury to illustrate some of the practical challenges that arose. Its coverage, however, is not on primarily Turkish issues but on those challenges that many DMUs are likely to face. Similarly the discussion of data reporting that follows is intended to have wider relevance.

The Unit Boundary and Managing "External" Risks

The Problem

One of the decisions in setting up the ORM framework is the boundaries of the relevant unit. Where a DMU is constituted as a semi-autonomous DMO that will probably be straight forward; but if it is part of a larger treasury or ministry there will be a balance to be drawn. The smaller the unit, the more straightforward it is to put a framework in place, but the more complications arise because control of risk exposures lies outside the relevant managerial unit. All DMUs will have external relationships with the central bank and other suppliers or agents outside their direct control; but if the DMU is embedded in a ministry or treasury:

a) The DMU will also be dependent on the larger body's support services, some of which may be crucial, including IT, personnel or HR, business continuity and internal audit (as in the case in Turkey). Those units will be subject to the ERM framework that applies to the ministry as a whole; but it may not be as developed or thorough as the framework that applies to the DMU.

b) It is more likely that there will be other managerial units with some related responsibilities. In some countries those setting the debt management policy framework may be separate from those who execute the policy, at least in domestic markets. There are many cases where the front office functions associated with external borrowing, or at least external loans and credits from donors, are separate from other debt management functions (as they are in Turkey). The DMU is not only dependent on the relevant directorate for data, it may find it difficult to insist that external borrowing terms are kept within the agreed policy parameters emerging from the debt management strategy. The separation between cash management and debt management responsibilities can give rise to similar problems, depending on the ORM framework covering the wider treasury functions.

There is no simple solution to this trade-off. As noted above, in Turkey the ORM framework was originally applied to the back office, then the DGPF as a whole, which internalised many of the back office's linkages; but the DG is still part of the Treasury; and a comparable framework has yet to be rolled out across all directorates. Whatever the decision on boundaries there will be wider linkages that have to be managed.

Solution: "Internal" Suppliers

Where part of the debt management function is separate from the main DMU (and particularly from the transactions-intensive back office functions), it is important that it is governed by the same strategic and operational imperatives. It strengthens the case for some form of Public Debt Committee (PDC), i.e. a committee chaired by the Finance Minister or senior official that includes representatives from all relevant debt management functions, as well as those responsible for macro-economic policy and fiscal policy. The main role of the PDC is the formulation of strategic debt management policy objectives; the mandating of those responsible for strategy execution; and the setting of targets and objectives and subsequent monitoring of performance. But part of this process should be to ensure that operational risk issues are properly addressed.[9] This should include clarity about data and information exchange requirements, as well as establishing agreed policy parameters. The peripheral divisions, even if much smaller than the main DMU, should be encouraged to apply similar ORM techniques. In practice it is sensible to back this up with regular meetings at working level to ensure a smooth flow of data and a shared understanding of operational priorities. A similar approach can be applied to the management of cash surpluses and deficits.

Services that are supplied across the whole ministry or treasury are potentially more problematical. Within this group IT is often a particular problem:

a) Debt management is a systems-intensive area, whether for data handling or transaction processing.

b) All parts of the ministry will have demands on the IT team and IT budget; and there is a risk that priorities may be set by whoever shouts loudest.

c) The IT team is itself likely to be short of resources, whether skilled staff or financial resources for developing new capabilities.

Business continuity planning may especially suffer: disaster recovery sites are expensive, and the requirements in terms of resilience and recovery times for most administrative functions are likely to be much less demanding than those for debt management.

The governance of the ministry and the wider ERM framework is of crucial importance. There should be a mechanism for setting staff and budget priorities under which senior officials and ministers are able properly to weigh competing requirements. But that will not be enough without also risk management machinery at the ministry level, of the kind outlined here for the DMU. Mechanisms might also usefully include:

a) An effective internal audit function that is tasked to consider administrative processes that straddle directorates.

b) A senior management team that formally considers the ministry's risk profile and identities control and mitigation priorities, *i.e.* the same mechanism that operates within the DMU although with a wider perspective (and risk register).[10] The process might be facilitated in a larger DMU by a Risk Committee that supports senior management.

---

9 In Turkey, as well as the Debt and Risk Committee, there are two risk and credit committees which include representatives of middle and back office functions in the DGPF and the front office functions of the DGFER; and these can also be a useful forum to identify problems.

10 In Turkey, the Treasury's SDU has responsibility for establishing the internal control framework and associated systems and standards within the Treasury.

c) Where an Audit Committee has been established it should assist the head of the ministry in ensuring that decision making and risk management processes are sound. More generally, the Audit Committee should review the governance, the financial reporting process, the ERM framework, the effectiveness of internal controls, and the processes for monitoring compliance with external legislation and internal policies. The Audit Committee would normally expect to receive reports from head of IA and, where relevant, also from the head of the DMU's middle office.

All these mechanisms should identify problems that exist between the DMU and other parts of the ministry; and ensure that they are properly addressed. In practice, however, in many countries the ministry-wide governance structures may be less sophisticated than those that apply to or within the DMU. The formal structures should therefore be supported by more informal mechanisms. In Turkey regular meetings have proved helpful; thus DGPF is able to show to DGER-IT its data on IT-related errors and the consequences, and DGER-IT is better able to explain the type of information needed to correct a problem. This in turn has been buttressed by more focus in the ORM process on the specification of objectives. Some kind of informal Memorandum of Understanding (MoU) or protocol can also help by making explicit the information flows required, both ways, and the timescales and responsibilities for providing them.

In those less developed environments where the DMU is ahead of the rest of the ministry in recognising the imperative of an ORM framework, greater responsibility falls on the senior DMU staff. They may not always have the necessary status within the ministry to insist on a wider application of these principles. But it is still possible to apply the techniques outlined in this note to a small unit, albeit that the process of risk identification and assessment is truncated; and many controls lie outside the unit. For interactions beyond the unit, the problem may be how to push ORM up the agenda of senior officials or ministers. Support for this will usually be available from the external auditors, internal auditors (where there are any), and the international financial institutions. Again informal mechanisms and pressures will play a part.

Solution: "External" Suppliers

Whatever the size of the DMU and its interaction with others in government, there will be some "external" suppliers. For suppliers of non-specialised goods and services there is not much of a problem: a combination of competition, past record and contract and consumer protection law is likely to be sufficient. Large IT procurements are always challenging; although there are well documented techniques for managing project risks, the implications for the internal control environment also need to be addressed. For significant suppliers with a continuing contract, regular meetings are appropriate to test their commitment and to ensure that there is no weakening of their underlying financial or operational performance; risk of failure of the contractor often implies a credit as well as an operational exposure.

Potentially much more difficult are the interactions with the central bank. In practice the central bank may have more developed ORM processes than the ministry of finance, reflecting a longer experience of market operations. This is helpful, but there is still a complicated relationship to be managed, particularly where the bank is fiscal agent.

From the DMU's perspective the main operational risks in this relationship are likely to be errors or other problems:

a) in handling auctions, where the bank is fiscal agent, whether the processing, announcement or settlement;

b) in processing transactions, *e.g.* as settlement agent or as banker;

c) in exchanging data, *e.g.* on cash flows or market developments;

d) as a result of a failure to follow understandings (or to consult) on market operations.

The relationship between a ministry of finance and the central bank of course has to operate at many levels, ranging from fundamental policy issues to operational understandings to the central bank as supplier of services. Policy issues will have to be addressed as a high level; but there will be a range of operations where the need is for consultation, advice and data exchange. These areas would normally be covered by some form of Protocol or MoU. But the central bank will also supply a number of services to the ministry or DMU. The most important of these will be as banker, although some services will fall under the general heading of debt and cash management, *e.g.* fiscal agent (managing auctions), settlement agent or registrar/paying agent. Although the central bank may in practice be handling many debt-related operations that does not mean that all risks are transferred; the DMU still remains primarily responsible (not least to ministers) for ensuring that the risks are managed by its agent. It may not be appropriate to have a fully fledged contract between two organisations that are in effect guaranteed by central government. But some form of "service level agreement" (SLA) would be advisable to give effect to the expectations on both sides. The SLA would normally include targets for operational performance, covering for example auction or other transaction turnaround times and timeliness of data exchange. But it is possible to go further from a risk management perspective:

a) By including in the SLA understandings about how operational risk is managed and to what standard. This will include the handling of any business continuity problem.

b) This might include providing for compensation in the event that there is an operational failure, thereby improving risk management incentives.[11]

c) By requiring the central bank to provide evidence of relevant ORM processes and their soundness. This may be a sensitive issue between the DMU or ministry and the central bank but it is well established in the financial services sector where suppliers are expected to reveal, for example, relevant reports by external auditors.[12] A compromise may be to give the ministry confidential access to unpublished audit reports of the central bank.

In any event, as with internal suppliers, these formal arrangements should be backed up with bilateral meetings, communication of the results of error reports, and reports to senior management on both sides, with mechanisms to resolve any areas of disagreement before they become a source of contention.

---

11 The French debt office (Agence France Trésor, AFT) and the central bank (Banque de France, BdF) have agreed an innovative SLA, the broad details of which have been made public. It includes provisions for compensation for investment opportunities that are missed because the BdF is unable to honour its contractual commitments, primarily arising from incidents (such as software unavailability) that disrupt the flow of information to AFT or prevent some transactions. See: http://www.aft.gouv.fr/article_787.html.

12 In the UK for example, the local settlement system (part of the Euroclear group) publishes an external audit report which provides clients with substantive information on the operation of controls and procedures including their design in relation to control objectives. The Bank of England also publishes for customers an audit in relation to its banking services. Similar audits are used widely by outsourcing organisations that require Sarbanes-Oxley certification.

Data and Reporting

Incident Reporting

One of the challenges is what data to collect and how to collect them. A key objective of ORM is to provide actionable information to allow decision-makers to assess the true extent of risks in order to determine the way forward.

Incident reporting is crucial. If that can be linked with actual loss data, so much the better; but as argued above, not if such financial calculations are simply a distraction. Moreover, many significant incidents do not result in serious direct losses (*e.g.* unavailability of processing capacity). Incidents should be analysed to risk drivers and to risk exposures. It will be helpful to design a standard template for incident reporting (which should also identify action to avoid a repeat), and build an internal database that lists all incidents attributable to operational problems.

It is good practice to score incidents (critical, significant, minor etc); and monitor over time the process of assessment, agreed action and its implementation by management.

There are often two problems in practice:

a) In more analytical areas the concept of an error or incident may be less clear cut. In Turkey there was also initially some uncertainty about who should report errors when more than one unit was involved in the process. Ideally it is the originating team not the impacted team that should report the incident.

b) The culture of the DMU may make staff reluctant to report incidents if they fear that it will affect their prospects or performance assessment. It is very important that there is a "no-blame" culture; and management should be seen both to insist on a report and to avoid anything in the way of reprisal. Constant reminders will probably be necessary at first. In Turkey incidence reporting has improved as staff have gained reassurance from the attitude of management. Persistent error of course is to be discouraged; but more often than not it will be management's fault – because of insufficient training, poorly targeted checking or inadequate system design. The risk team can use its own information and informal sources as a ways of encouraging and monitoring the completion of reports.

One other point is worth noting, important for incident reporting but of wider relevance. Risk awareness takes time to develop, and once established it must be reinforced. Basic training should be given to new personnel, with all staff being given periodic refreshers.

Incident reports are only one part of the reporting processes; they say nothing about exposures that have not materialised in the period. Incident reports should be backed both by managers' own assessment of the risk profile in their area – and whether it was deteriorating or improving. Also helpful are key risk indicators (KRIs) as potential indicators of risk exposures.

Managers' Assessment of Changes in the Risk Profile

A fully-fledged updating of the risk matrices is not sensible more frequently than once as year. A full exercise is time-consuming and frequent updating carries the risk of managers treating it as a simple repetitive exercise. Some organisations do this on a rolling basis, *e.g.* a quarter of the teams each calendar quarter. Managers should, however, regularly (say each quarter) be asked to comment on the risk profile in their area, in particular whether there had been any significant changes in the assessed risk scores – upwards or downwards. This could be done most simply by adding a column to

the matrices that provided for a simple "worse/better/no change" indicator. There could then be another column for managers to indicate, where they had identified a significant change, what the nature of the problem was and what, they thought, should be done about it. Alternatively, or preferably alongside this, the risk champion or other member of the risk team could, drawing on their own knowledge, discuss recent risk developments with the line managers; if the resources are available this can often produce richer information, as well as facilitate well-designed responses. Whatever the route, the assessments should be brought together by the risk champion for presentation to the Risk Committee or senior management team.

The regular (quarterly) summary report from the risk champion should include some discussion of whether action needs to be taken, *e.g.* to respond to a worsening risk profile, with action-oriented recommendations, perhaps prompted by managers' comments. One possibility is to use the information in the matrices on risk drivers. Thus in Turkey the middle office team usefully summarised the different risks into relatively few categories of risk drivers or risk sources (which were also linked to control categories). Presentational devices showing how each of these categories contributes to risk exposure can also be helpful. The linkage between the risk driver and the risk scores on the matrices provides a measure of this. Errors can also be indentified to risk drivers, to explore any emerging trends. Such charts need not necessarily be produced every quarter. They are really an aid to discussion, i.e. to ensure that senior management focuses on the risk exposures; and identifies where mitigating action is necessary (and indeed possible).

Key Risk Indicators (KRIs)

KRIs are activity or volume-based measures that serve as early warning signals for management, pointing to changes in risk conditions before the risk events materialise, and enabling management to take anticipatory action. KRIs measure changes to operational risk causal categories, i.e. the risk drivers. They are particularly useful as indicators of operational stress. Inevitably no one indicator can encapsulate everything that is important; and the temptation to focus only on what can be measured must again be resisted. But showing how indicators are changing over time is useful information for management. The number and type of incidents is an important indicator itself; other examples might include system availability, transaction turnaround times, auction reporting lags, staff sickness levels, and the time lags in preparing publications, data releases or replies to requests. (Some debt offices publish at least some KRIs or related performance indicators, including both the UK and France, although it is probably wise to gain some experience of KRIs before publishing them.)

Line management might find KRI information particularly useful as a way of focusing on risk exposures in their area. It may be that only those risks with exposures that require immediate attention are escalated to senior management. KRI reporting can be useful on a monthly basis, between fuller reviews, particularly when data are stored centrally.

A fuller discussion of KRIs, with examples that might be used in a DMU, is at Annex D.

The Risk Champion

It is worth stressing the central role of the risk champion, or the ORM unit, in all these processes. Over time data will improve and KRIs will put policy choices on a sounder footing. But subjective assessment will always play a part and that requires active surveillance by the risk champion to ensure consistency; and an ability to underline the key issues for management. He or she also needs a good sense of how the controls are working in practice and where the weaker points or unreported incidences might lie. That will mean walking the floor to gain an informal understanding of problems

and indentify where the risk processes may be poorly or unenthusiastically applied. There will be a time for emollience (*e.g.* telling some individuals that the risk impacts in their area work perhaps do not score quite so heavily as they would like to think), as well as times for actively chasing returns or follow-up action. In a smaller DMU much of the essential risk awareness and training work is also likely to fall to the risk champion. It is an important task.

CONCLUSION

The importance of operational risk management in debt management units is not in doubt. The benefits are difficult to measure, as they can be defined strictly only in terms of what did not happen. But they are clear enough:

a) a better understanding of risk and more informed and improved decision making, with greater focus by senior management on what is important;

b) more effective and efficient risk management processes and controls, and speedier corrective mechanisms, all underpinning the protection of the government balance sheet and transactions;

c) an enhanced external reputation, which potentially brings benefits in the DMU's or treasury's interaction with, for example, the central bank and market intermediaries;

d) a stronger and more risk-aware culture internally, with wider business planning benefits in terms of focus on objectives and collaborative work within the DMU.

In the Turkish Treasury, there were some early benefits as some high risk exposures were brought into focus and new control mechanisms were developed accordingly, particularly in the IT and disaster recovery areas. Staff gave their full support once they realised that the new framework made their work easier and reduced the number of mistakes and errors. They also found it useful to use the ORM framework and tools to convey their needs to the senior management. Although the formal technique is currently used only in the DGPF, discussions with the DGFER and DGER-IT, as well as with the senior management of the Debt and Risk Committee, have widened understanding of risk, its assessment and control priorities. The DGPF has also made strides in terms of reporting, developing indicators, and improving process documentation.

The experience in Turkey and in other DMUs shows that such benefits can be achieved with a proportionately modest resource cost. The procedures outlined are not only consistent with good international practice, taking into account the distinct public sector characteristics of a DMU, they are also flexible, and can be applied proportionately to size, activities, risk appetites and capability. In Turkey, the cost includes the staff of the ORMU and the time taken by the working groups, to which some management time must be added. All staff will be involved in periodical updating of the data, incident reporting etc.; but much of the continuous reporting and summarising work will be the ORMU's responsibility. For a smaller DMU, it might identify an existing member of the middle office as risk champion, and establish a working group, engaging all staff directly to draw up the initial matrices through two or three workshops. Whatever the scale and resources, the support of senior management will be critical, and, at the end of the day, ORM helps them to meet their and the entity's objectives.

BIBLIOGRAPHY

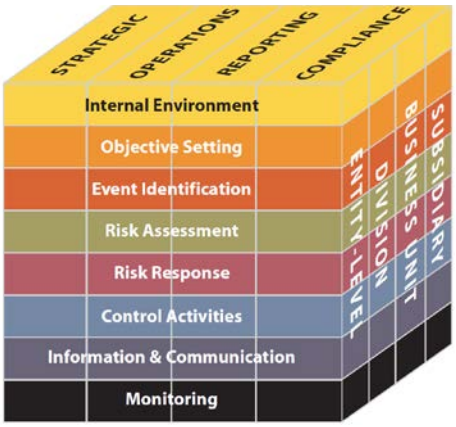
- BIS (Bank for International Settlements) (2003), *Sound Practices for the Management and Supervision of Operational Risk - final documents*, BIS, Basel, www.bis.org/publ/bcbs96.htm
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) (2004), "Enterprise Risk Management - Integrated Framework", COSO, www.coso.org
- IMF (International Monetary Fund) and World Bank (2001) (amended 2003), *Guidelines for Public Debt Management*, IMF and World Bank, Washington D. C., http://treasury.worldbank.org/bdm/htm/guidelines_publicdebt.html
- OECD (2002), "Risk Management Practices Concerning Assets and Liabilities of Debt Managers in OECD Countries" in *Debt Management and Government Securities Markets in the 21st Century*, OECD, Paris, pp. 135-148
- OECD (2005), "Management of Operational Risk by Sovereign Debt Management Agencies" in *Advances in Risk Management of Government Debt*, OECD, Paris, pp. 67-88
- TransConstellation (2007a), *Best Practices in Qualitative Operational Risk Management: The ORM Reference Guide*, TransConstellation, Brussels, www.transconstellation.com [13]
- TransConstellation (2007b), *Roadmap to Operational Risk Management Success: The ORM Maturity Benchmark*, TransConstellation, Brussels, www.transconstellation.com
- Turkey - Undersecretariat of Treasury (2009), "Public Debt Management Report 2009", Turkey - Undersecretariat of Treasury, Ankara, www.treasury.gov.tr
- World Bank (2009), *Debt Management Performance Assessment (DeMPA) Tool*, World Bank, Washington, D.C. , http://go.worldbank.org/4VX651FHB0
- World Bank (2010), *Guidance for Operational Risk Management in Government Debt Management*, World Bank, D. C., http://go.worldbank.org/48MIDC8BH0
- Risk Management Practices concerning assets and liabilities of debt managers in OECD countries, Chapter 7 in: *Public Debt Management and Government Securities Markets in the 21st Century*, Paris, OECD, 2002
- Management of operational risk by sovereign debt management agencies, Chapter 5 in: *Advances in Risk Management of Government Debt*, OECD, 2005

[13] 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 are Atos Worldline SA/NV, Euroclear, SWIFT and The Bank of New York Mellon (Brussels).

ANNEX A: THE COSO RISK MANAGEMENT FRAMEWORK

Introduction[14]

The COSO enterprise risk management (ERM) framework was designed as a coherent internal control structure covering compliance, reporting and strategic risk management next to ORM. In concept ERM incorporates the internal control framework, although COSO recognised that would be used both to satisfy their internal control needs and move toward a fuller risk management process. In practice the components of the COSO lifecycle apply equally to ORM.



There is a direct relationship between an entity's objectives, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube.

The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction summarises the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, or entity unit.

Risk Management Lifecycle Components

I. Internal Environment: this encompasses the tone of an organisation, and sets the basis for how risk is viewed and addressed by everyone within it. It includes:

a) integrity and ethical values, and the environment in which they operate (including a code of conduct);

b) risk management philosophy and culture;

c) risk appetite – how much risk is "acceptable".

II. Objective Setting: risks should be identified and evaluated against entity objectives.

III. Event or Risk Identification

IV. Risk Assessment

These two processes are often integrated, with an emphasis on self assessment techniques, and that is considered good practice. A process is needed to identify internal and external events affecting achievement of an entity's objectives. Risks are then analysed, considering likelihood and impact, as

[14] This summary (and the cube) is taken partly from COSO (2004) but also the helpful summaries of the framework in TransConstellation (2007a) and (2007b).

a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis (although residual risk is likely to be the initial focus).

There is a variety of tools. The main Paper outlines a combined top down (identify strategic objectives; then related risks) and bottom up (identify risks, link to objectives) process, emphasising the need to involve management and staff at all levels. The emphasis is on Risk and Control Self-Assessment (RCSA), i.e. that the people with the best knowledge of the relevant activities identify potential sources of risk. Related tools are questionnaires, surveys, brainstorming, scenario analysis, external review and so on. In all cases there will be, and should be, a gradual build up of expertise over time.[15]

V. Risk Responses: the approaches include risk avoidance; risk reduction (mitigation); risk transfer; or risk acceptance. It is for management to select a set of actions that align risks with the entity's risk tolerances and risk appetite.

VI. Control Activities: policies and procedures are established and implemented to help ensure the risk responses are effectively carried out. They include:

a) approvals

b) authorisations

c) verifications

d) reconciliations

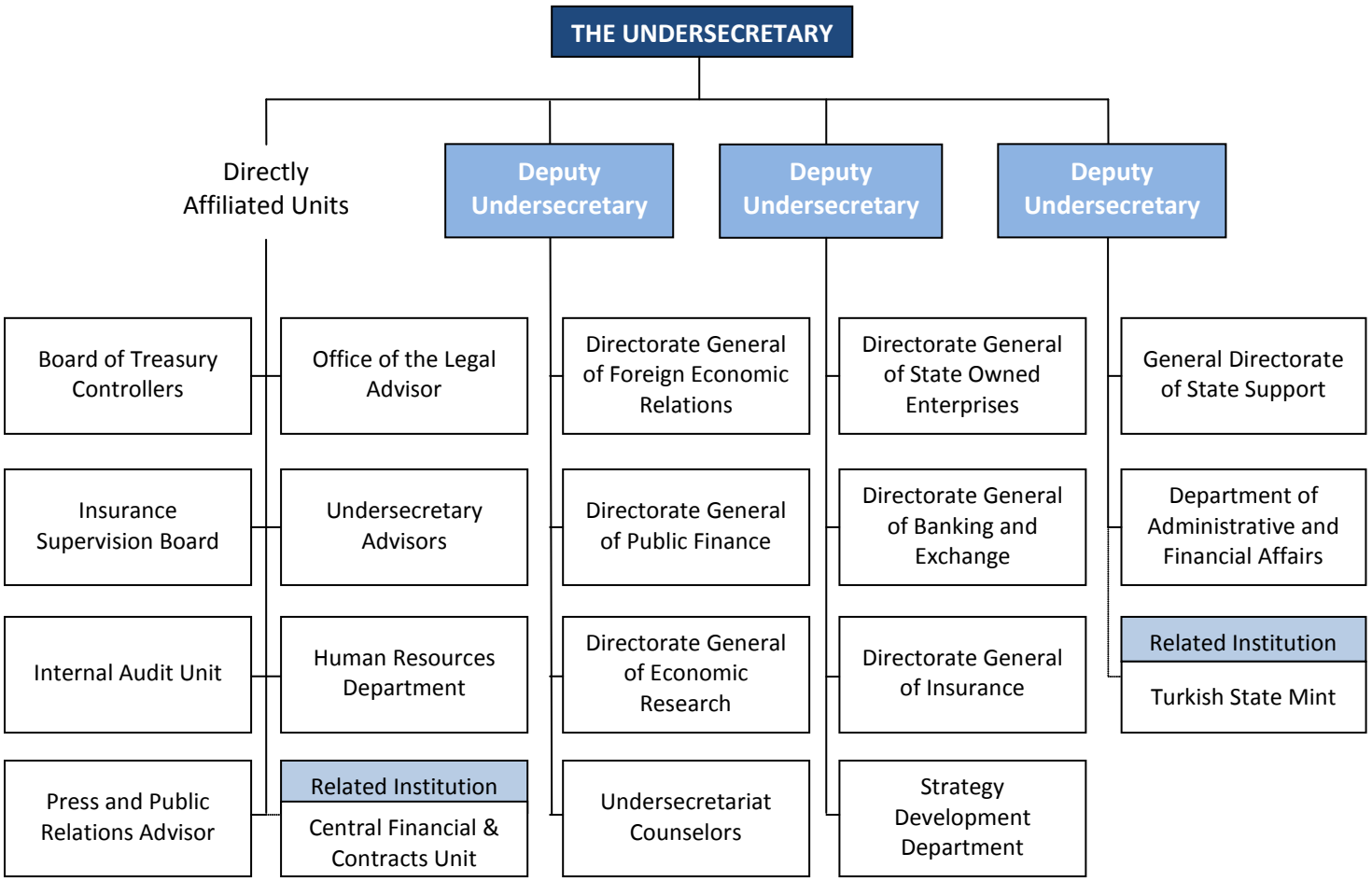
e) segregation of duties

VII. Information and Communication: includes the operational risk escalation procedures and reporting to (top) management. The right people need the right data at the right time.

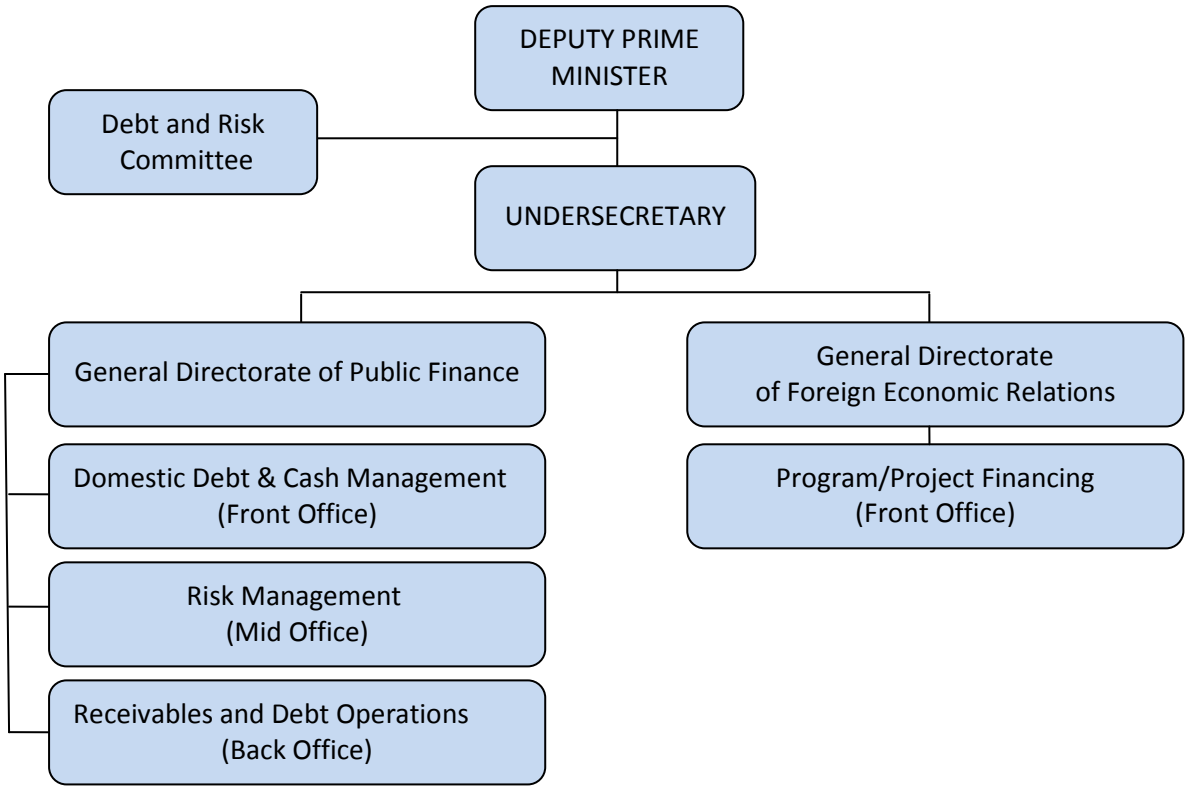
VIII. Monitoring: the implementation of ORM should be tracked and examined over time. This requires a combination of ongoing monitoring activities and specific evaluation of the ORM process itself (including by IA).

[15] For a much fuller discussion of RCSA and other techniques see TransConstellation (2007a).

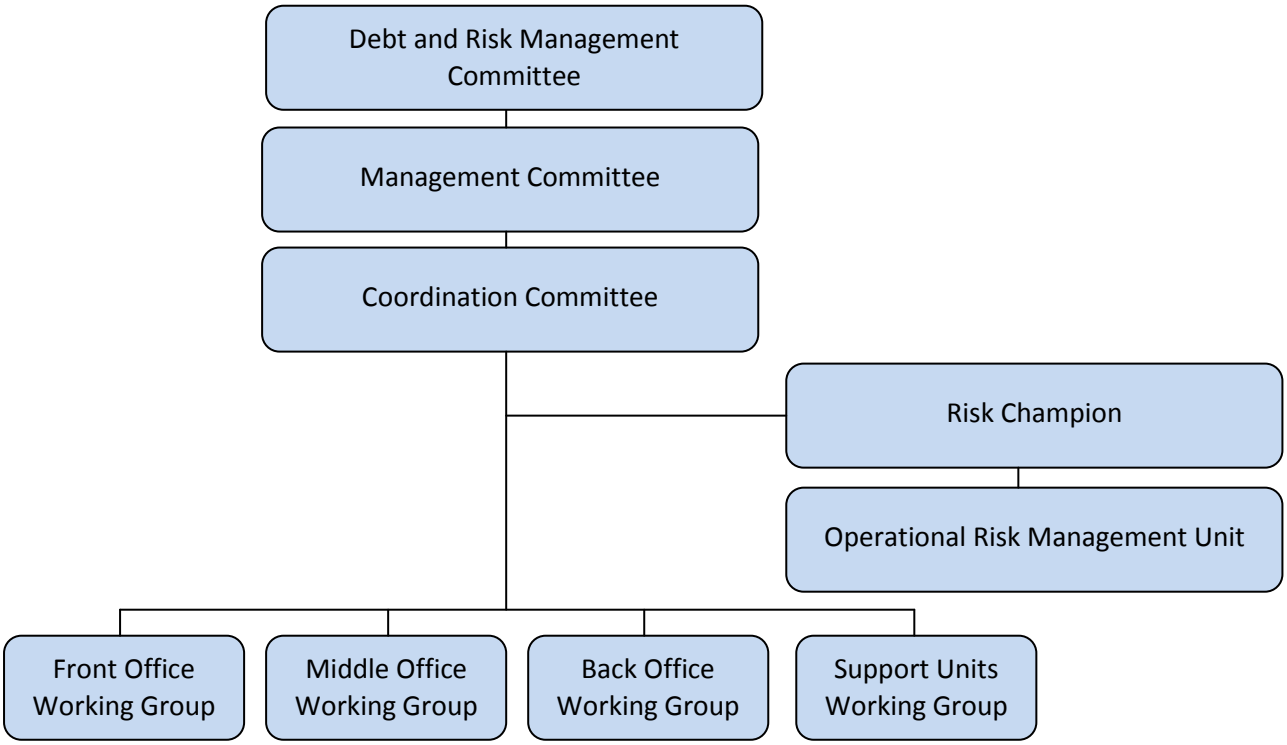
ANNEX B: ORGANISATION OF THE TURKISH TREASURY



Debt Management Organisation



Operational Risk Management Organisation



ANNEX C: THE RISK MATRIX: SOME EXAMPLES

Activity area-I	Activity area-II	Activities	Sub Activities	Objectives of (Sub) Activities	Encountered Risks	Source of Risk	Existing Controls	Likelihood	Impact	New Controls
Cash management	Cash program	Transactions related to the Treasury Cash Program	Preparing the Cash Program	Preparing the tables that will serve as a basis for the financing need	Incorrect data which come from the related units	External (Related institution)	Horizontal control, Vertical Control	Very low	Major	1.Technology Based Solutions 2. Efficient coordination with related units
					Incorrect entry of the data	Personnel	Using excel files by separating them first.	Low	Catastrophic	1.Technology Based Solutions 2.Training of staff
						External(Software)				
Accounting operations	Accounting operations	Carrying out the transactions related to the non-tax collections among the amounts transferred to the accounts of the Internal Payments Accounting Unit	Classifying the amounts according to the legislation	Registering the amounts collected to the State accounts correctly and completely according to the legislation	Incorrect or incomplete classification of the notification	Personnel	Horizontal control, Vertical Control	Low	Major	1.Personnel training
					Incorrect and/or missing information in the documents	External	Staff Experience	Medium	Moderate	1. Efficient coordination with related units
			Ensuring the accounting of transactions		Wrong or Incomplete Data Entry	Personnel	Cross checks, say2000i	Very high	Minor	1.Personnel training
								Low	Major	1. Efficient coordination with Ministry of Finance
			Preparing the financial tables		Incorrect or incomplete data entry		Cross checks	Low	Medium	1.Control list
Statistics	Developing statistics	Preparing statistics related to debt, receivables and financial data	Preparing statistical data on a weekly, monthly and quarterly basis	Publishing the statistics on time	Incorrect calculation of data	Personnel	Horizontal control, Vertical control	Low	Major	1.Update Information Systems
						External(Information System)	Horizontal control, Vertical control			
					Incorrect data received from the related units	Personnel (Related institution)	Horizontal control, Vertical control	Very low	Medium	1.Technology Based Solutions 2. Efficient coordination with related units
		Preparing the Public Debt Management Report (PDMR)	Preparing and publishing PDMR in monthly and yearly basis	Publishing the PDMR on time	Incomplete/incorrect data received from the related unit	Personnel	Horizontal control, Vertical control	Low	Catastrophic	
					Delay in the preparation of report	Personnel	Vertical control	High	Catastrophic	1. Designing format and layout of report in Treasury
						External				
					Delay in the publishing of report	Personnel	Vertical control, coordination with the related units	Very low	Catastrophic	
						External				

ANNEX D: KEY RISK INDICATORS

KRIs point to changes in risk conditions before risk events materialise. They are aimed to show whether the organisation in under strain – that the exposure to risks (especially likelihood) is increasing even if there is no increase in errors or incidents (although the number and type of errors are themselves important indicators). KRIs should therefore enable management to take appropriate steps to avoid the event.

Although the purpose of KRIs is essentially forward-looking, they should be composed of both forward-looking and backward-looking indicators. It would be possible to identify a multitude of KRIs around a given risk event. However, the number should be manageable, perhaps 10 per management level. The difficulty lies in selecting the most significant ones, particularly the 10 or so that will be going to the Board or Risk Committee. Essentially, effective KRIs should match the following criteria:

a) Relevant: a KRI's trend should be positively correlated with the frequency with which the variable contributes to risk events materialising.

b) Measurable: KRIs should be easily and objectively quantifiable.

c) Comprehensive: taken together, KRIs should cover all risk factors, and potentially all relevant types of activity and risk categories.

Related concepts – and potential sources for selecting or deriving KRIs – are:

a) Key Performance Indicators (KPIs) are used to monitor operational efficiency (*e.g.* auction turn round times, percentage of back office transactions successfully processed; transaction turn round times; time to respond to external queries; etc).

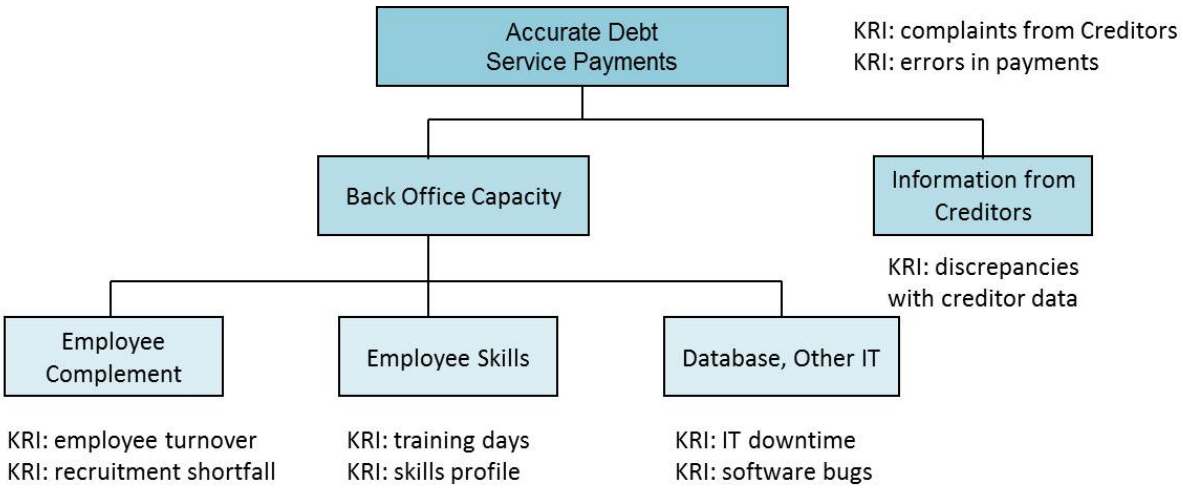
b) Key Control Indicators (KCIs) are used to demonstrate the effectiveness of controls (*e.g.*, the number of audit exceptions, the number of outstanding confirmations, etc.).

There is not a very hard line between indicators of operational performance and risk indicators – for example: "number of errors per [100] transactions" or "systems downtime" could be both.

One potentially useful technique is to establish KRIs for each of the influencing factors within a process hierarchy. Figure B1 shows an example for the common task of making an interest payment to an external creditor.[16] Several organisations establish benchmarks or targets for their KRIs; the monitoring focus is then on those indicators falling short. Other choices include whether to calculate the KRIs from centrally held data or collect them from administrative units.

[16] There is a full discussion of KRIs, including many examples, at TransConstellation (2007a) page 79-85; it also includes the diagram on which Figure B1 is based.

Figure B1: A Hierarchy of KRIs



Some possible KRIs, relevant to a DMU, are summarised in Box B1.

Box B1: Examples of KRIs

Systems

- Downtime
- Recorded software/hardware problems

Risk Issues

- Concerns or issues raised proactively by individuals or managers, compared with the number emerging as a result of *e.g.* incidents or audit comments.
- Time taken to resolve the issues that have been raised by whatever route.

Transactions

- Numbers of transactions processed
- Average turnaround times
- Data discrepancies
- (Justified) complaints from debtors/creditors

Reporting

- Lags in reporting or data publication
- Errors on website
- Failing to meet publication or announcement timetables

People

- Staff turnover; average period in post of staff
- Overtime
- Gaps in staff complement
- Training days/skill profile

- Sick leave

Business Continuity

- Readiness [qualitative assessment; or measured against indicators for *e.g.* possible recovery times, availability of system back-up; availability of electrical/ fuel back-up].