Risk and control in Government Treasury management and systems

Some definitions

This paper is concerned with concepts and management of risk in Government treasuries and in particular the issues that arise with the implementation of computerised systems for budget execution, transaction processing and reporting. As a starting point some definitions of the terms are considered below. Note that for each term there are a number of definitions. Those quoted are the most appropriate and widely accepted.

- The definition of **risk** as a general concept has been much debated, but the following accords with both common sense and general usage "*The probability and magnitude of a loss, disaster or other undesirable event*"[1]
- The same writer defines **risk management** as "*The identification, assessment and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor and control the probability and/or impact of unfortunate events*"[2] As we shall see this differs from some of the definitions used in accounting literature.
- **Fiduciary risk** is a concept introduced by the UK Department for International Development (DFID) and is particularly relevant in this context "*the risk that funds are not properly accounted for, not used for the intended purposes or that the expenditure does not represent value for money*"[3]
- The term **control** is used in variety of contexts. This paper is concerned with management control and in particular internal financial control. Herbert Mockler defines management control as "*a systematic effort by business management to compare performance to predetermined standards, plans, or objectives in order to determine whether performance is in line with these standards and presumably in order to take any remedial action required to see that human and other corporate resources are being used in the most effective and efficient way possible in achieving corporate objectives*"[4]
- Internal (or **internal financial) control** is used in a narrower sense and is defined by Wikipedia as follows: "*At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations. At the specific transaction level, internal control refers to the actions taken to achieve a specific objective (e.g., how to ensure the organization's payments to third parties are for valid services rendered.) Internal control procedures*[2] *reduce process variation, leading to more predictable outcomes*".

[1] "The Failure of Risk Management" Douglas W Hubbard 2009
[2] Douglas Hubbard, op cit
[3] DFID internal working paper on Fiduciary Risk, 2004
[4] Robert J. Mockler (1970). *Readings in Management Control*. New York: Appleton-Century-Crofts. pp. 14–17

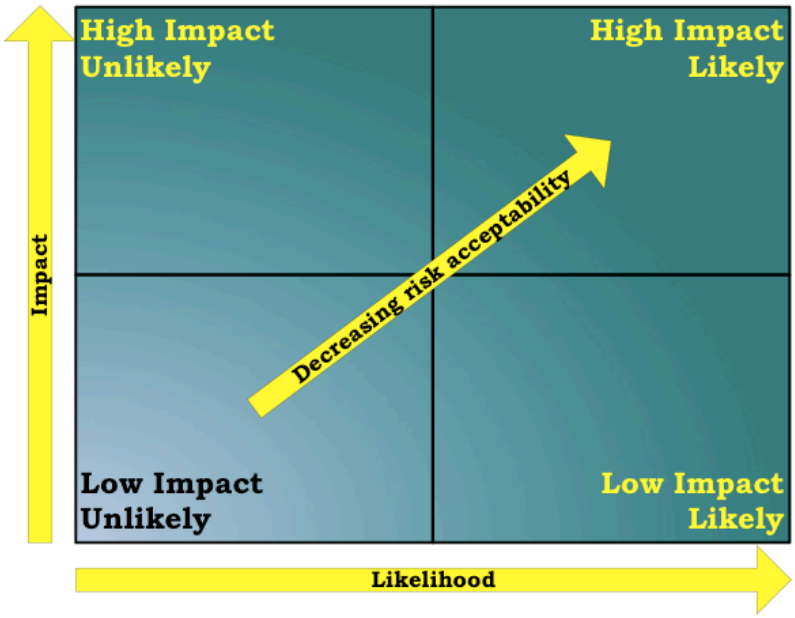
- **Government treasury** is used to refer to the budget execution, accounting and reporting functions within a Ministry of Finance.

The nature of risk

Risk has been defined above. It is noteworthy that risk has two dimensions:

- The likelihood (probability) of risk, and
- The impact (cost) if the risk becomes a reality.

Figure 1: Risk likelihood and impact



Both axis can be expressed quantitatively – impact as a monetary cost and likelihood as a probability. Mathematically it is possible to multiply:

Cost ($) X Probability (P) = expected value of loss

However, there are dangers in simply multiplying risk and cost because this looses important information about the impact of the risk, e.g. the risk of a plane crashing as compared to the risk of the loss of cash. Clearly only a very small risk of the former may be acceptable whereas a significant risk of the loss of cash may me accepted.

Risks are often correlated and linked sequentially. For example the risk of fraud in an entity will probably involve a series of control failures each with risk of such failure, e.g.

- Failure of budget management
- Failure of a supervisor to check the work of a clerk
- Bank reconciliation not carried out.

Each failure has its own probability, but all have to occur for the fraud to take place. Consequently the probabilities have to be multiplied to arrive at the overall probability. The risk could be reduced by addressing just one risk factor – but there might be other risks this would not address.

Modern approaches to risk management involve quantifying risk probabilities and costs, and also identifying correlation of risk factors. These approaches will be discussed further in the last section of this paper.

Risk in the context of government treasury operations

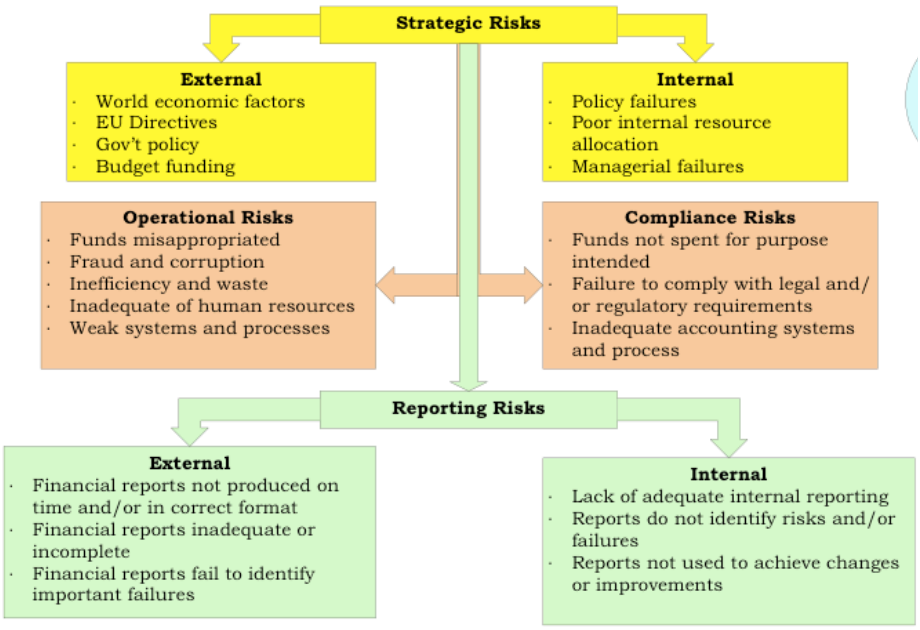
Government financial management is characterised by high levels of risk from external factors. For example the risk of adverse impact from external financial events, e.g. interest rate rises, changes in exchange rates. Whilst this paper is not concerned with such external risks it would be perverse to establish a sophisticated risk management and control system for internal financial management processes whilst ignoring such external risks. Risk management should be system wide and embrace all risks not just those related to internal systems.

However, this paper is concerned with risks in the context of internal actions within the public financial management processes. Examples of risks include:

- Revenues legally owed to the government not being collected, or if collected not being deposited for the benefit of government
- Payments not being made for the purpose intended
- Loss of public money or other assets
- Inefficient or wasteful use of public resources.

It is this type of risk that the DFID refer to as fiduciary risk (see definition above). The model in the diagram below provides and overview of the strategic risks facing a government treasury.

Figure 2: Treasury risk framework



COSO internal control approach

As a result of many high-profile business scandals and increased awareness of the level of corruption in many countries, as noted by the Corruption Perception Index published by Transparency International, calls were made for enhanced corporate governance and risk management, with new law, regulation, and listing standards. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control – Integrated Framework*[5]. *However, t*he need for an

[5] "Internal Control– Integrated Framework" published by the Committee of Sponsoring Organizations of the Treadway Commission, 2000

overall risk management framework for the entity as a whole, providing key principles and concepts, a common language, and clear direction and guidance, became even more compelling. Thus, COSO published Enterprise Risk Management – Integrated Framework in 2001 that fills this need. This framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. This does not replace the internal control framework, but rather incorporates the internal control framework. Entities may decide to look to this framework both to satisfy their internal control needs and to move toward a fuller risk management process.

According to the COSO approach among the most critical challenges for managements is determining how much risk the entity is prepared to and does accept as it strives to create value. Using the integrated framework, legislation has been enacted or is being considered by many countries to extend the long-standing requirement for governments to maintain systems of internal control.

The underlying premise of risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Risk management enables management to deal with uncertainty and associated risks and opportunities.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth, returns and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Risk management encompasses:

- *Aligning risk appetite and strategy* – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- *Enhancing risk response decisions* – Risk management provides the rigour to identify and select among alternative risk responses—risk avoidance, reduction, sharing, and acceptance.
- *Reducing operational surprises and losses* – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- *Identifying and managing multiple and cross-entity risks* – Every entity faces a myriad of risks affecting different parts of the organization, and risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- *Seizing opportunities* – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- *Improving deployment of capital* – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

These capabilities inherent in risk management help management achieve the entity's performance and prevent loss of resources. Risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

COSO defines risk management as "*a process, effected by an entity's legislative body, management and other personnel, applied in strategy setting and across the entity, 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*". Contrast this definition with the definition at the start of the paper. THE COSO definition views risk management as a process; it

also introduces the concept of "risk appetite" – the willingness of an entity to accept certain levels of risk.

Within the context of an entity's established mission or vision, management establishes strategic objectives, selects strategy, and sets objectives cascading through the entity. The risk management framework is geared to achieving an entity's objectives, set forth in the following categories:

- *Strategic* – high-level goals, aligned with and supporting its mission
- *Operations* – effective and efficient use of its resources
- *Reporting* – reliability of reporting
- *Compliance* – compliance with applicable laws and regulations

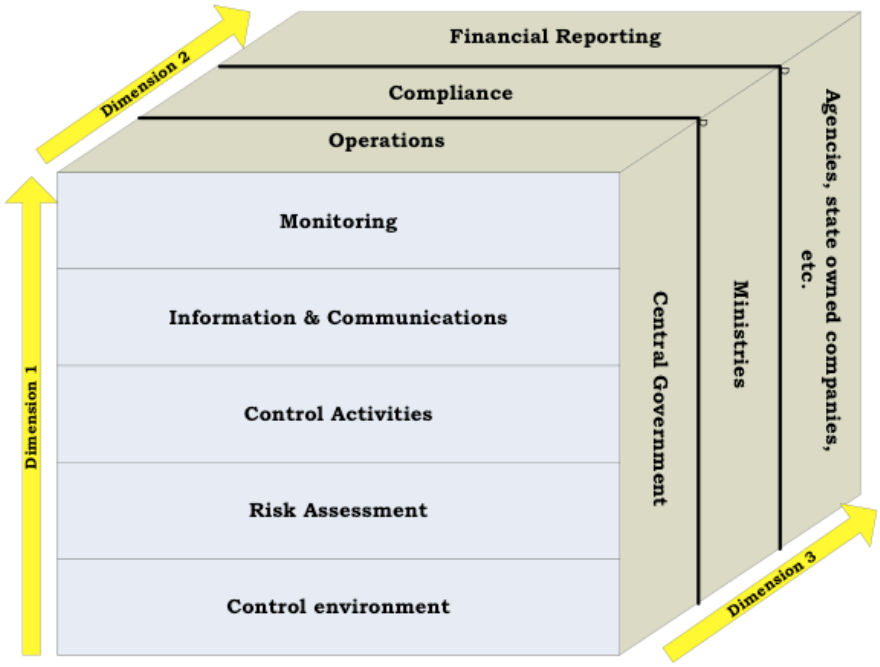
Because objectives relating to reliability of reporting and compliance with laws and regulations are within the entity's control, risk management can be expected to provide reasonable assurance of achieving those objectives.

Risk management consists of eight interrelated components. These are derived from the way management operates an entity and are integrated with the management process. These components are:

1. *Internal Environment* – The internal environment encompasses the culture of an organization, and sets the basis for how risk is viewed and addressed by an entity's staff, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
2. *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
3. *Event Identification* – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
4. *Risk Assessment* – Risks are analyzed, considering likelihood (probability) and impact, as a basis for determining how they should be managed.
5. *Risk Response* – Management selects risk responses—avoiding, accepting, reducing, or sharing risk.
6. *Control Activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
7. *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.
8. *Monitoring* – The entirety of risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations or both.

There is a direct relationship between objectives, which are what an entity strives to achieve, and risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix as illustrated in the model below.

Figure 3: The COSO risk management model



Under the COSO approach determining whether an entity's enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective risk management. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite.

When risk management is determined to be effective in each of the four categories of objectives, respectively, the legislative body and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved. Further, they are assured that the entity's reporting is reliable and that applicable laws and regulations are being followed.

The EU Public Internal Financial Control (PIFC) approach

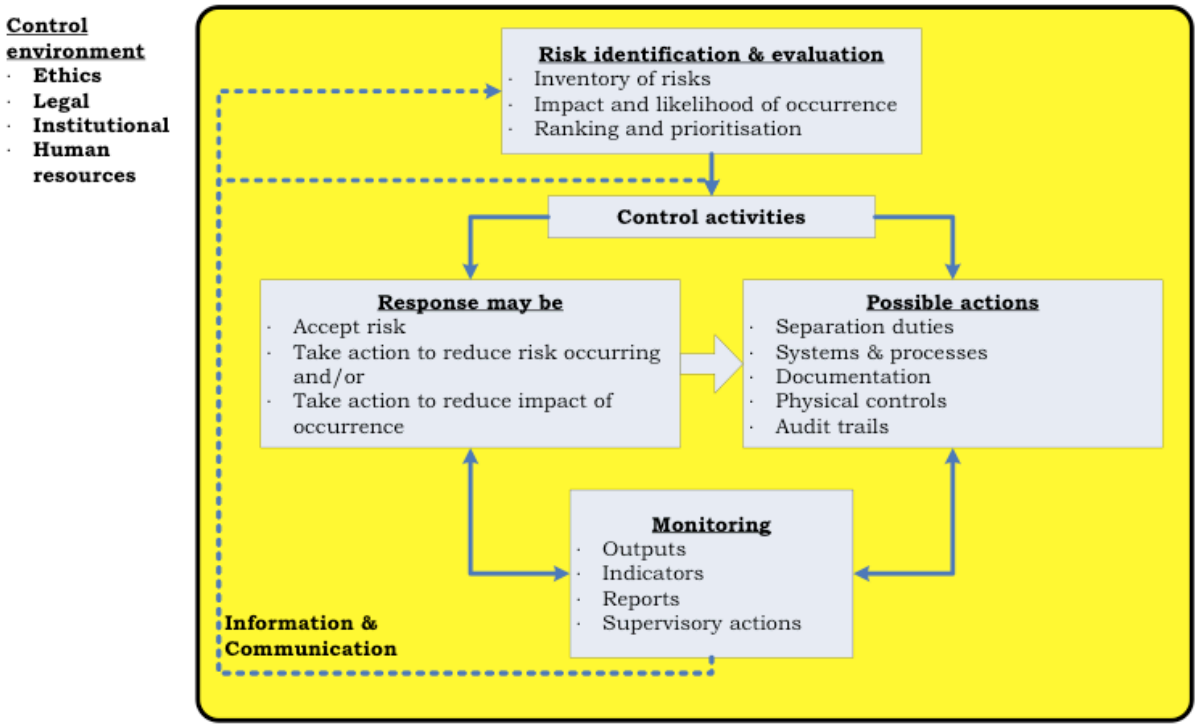
The EU has developed the PIFC structure based on COSO approach to internal control and risk management. Public Internal Financial Control (PIFC) is an exercise in risk management. All transactions involving the use of other people's money involve an element of risk that the resources will be lost, used improperly, not used for the purpose intended, or used properly but inefficiently. PIFC seeks to balance the risks of such events against the costs of their prevention.

The PIFC approach provides an institutional approach to risk management and it envisages three aspects:

1. Internal financial control established in every entity financed from the public budget
2. Internal audit in every entity
3. A Central Harmonization Unit coordinating internal control and internal audit.

The PIFC model is mandatory for EU accession countries. The approach to risk management is based on the COSO framework and summarised in the model below.

Figure 4: Risk management framework



This model summarises current approaches to risk management in public financial management and is being widely implemented in EU accession countries.

Impact of IT systems on control and risk management

As countries implement Treasury IT systems and move towards Integrated Financial Management Information Systems (FMIS) these present a new type and level of risk and hence control requirements.

The new or increased risks fall into a number of categories, for example:

- Implementation risks – the very substantial risks that implementation of such complex systems fail are delayed, or cost more than expected.
- Operational risk – because Government financial operations become dependent on the new systems a system failure could have catastrophic consequences
- Data risk – because all data is held electronically there are risks of corruption, unauthorized access or actual loss of data
- Transaction processing risk – automated transaction processing makes it easier to hide unauthorized transactions either through system or operator manipulation.

On the other hand automated systems also provide opportunities to reduce risk and increase control. Controls can be automated; processes always follow specified sequences; control actions can be made mandatory; and so on.

What this means is that risk management and control in automated systems present a new set of challenges and opportunities, and these increase as systems become more integrated. However, the principles of risk management remain the as above.

There exists an international Information Security Standard set by the International Organization for Standardization ISO SO/IEC[6]. This standard applies generally to all IT systems and not specifically to financial management systems. The standard is concerned with information security rather than with the broader risk framework described above. Nevertheless the standard contains much that is useful in the context of an IFMIS and the risk management and control strategy should ensure compliance with this standard.

As part of the implementation of an IFMIS there should be an IT security policy. This policy then becomes part of the overall control and risk management strategy. The following is a list of suggested contents for such a policy:

1. Ensuring Suitable Environmental Conditions for Computer Installations
2. Controlling Physical Access to Information and Systems
3. Controlling Logical Access to Information and Systems
4. System Operations and Administration
5. Data Management
6. Backup, Recovery and Archiving
7. Production of Documents and Reports
8. Document Handling
9. Securing Data
10. Information Handling and Processing
11. Maintaining Commercial Software
12. Combating Cyber attacks and crime
13. Personnel Issues Relating to Security
14. Training and Staff Awareness
15. Disaster Recovery and Business Continuity Plans
16. Information Security Weaknesses, Incidents and Breaches
17. Security Classification of Information and Data.

Because the management of risk within an integrated IT system is so important, there should be appointed an "information security officer" at a sufficiently senior level to ensure that the security and control procedures are properly observed. This person should form part of the overall internal control structure.

A structured approach to risk management will include the risks specific to an IFMIS as part of the overall risk structure and develop appropriate control procedures. As processes become paperless organisational controls become increasingly important. For example the system may require a supervisor authorisation, but if the supervisor gives his password to a junior staff member to perform the check, then the value of the control is lost.

6 The ISO/IEC 27000 family of standards, is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is "ISO/IEC 27001:2005 - Information technology – Security techniques -- Information security management systems – Requirements".

High impact unforeseen events

The 2007 banking crisis and the failure of risk management within the financial sector has led to reconsideration of approaches to risk management. Although developed in a different context the lessons and new approaches have direct relevance to the management of risk in public financial management.

Nassim Taleb has introduced the concept of "Black Swans"[7] – events that are completely unforeseen but have a considerable impact. He argues that such unforeseen events are more common that usually perceived and that their occurrence can make carefully designed control systems irrelevant. Whilst it is not possible to predict a specific event, risk management should anticipate random events with a significant impact. Taleb argues that this is of particular importance in the financial world where a number of well established risk models underestimate the risk of such random events.

This suggests that risk management for PFM should take account of possibility of external events that can have a very substantial impact. Procedures should incorporate suitable levels of redundancy and alternative operating modes.

A quantitative approach to risk management

The approaches of the COSO and PIFC framework are essentially non-quantitative. They rely on subjective judgements of likelihood and impact of risk factors. Risks are ranked in on a general scale, e.g. high, medium, low.

However, a more scientific approach to modelling and quantifying risk is well established and increasingly used for risk management. The key elements of such an approach comprise:

1. Assigning costs (or a range of costs) to risk factors together with estimates of probability. Probability estimates can be subjective, based on historic experience or there can be specific research to assess event probabilities.
2. Building a model of the risk relationships. Bayesian theory can be used to model dependencies and relationships. Monte Carlo simulation can be used to test the model through a number of different scenarios.
3. Use the model to assess the benefits of risk management strategies. This can enable an informed decision on the benefits of spending on different controls, and also how much it is worth spending to provide more reliable estimates of the probability and costs of uncertain outcomes.
4. Test and amend the model against actual experience.

The quantitative approach to risk management enables a number of questions to be answered. For example, it may be worth expenditure to provide a better understanding of the probability of certain types of risk. The approach will certainly provide a mechanism for cost/benefit evaluation of expenditures to reduce risk.

A quantitative approach does not change the nature of risk management but it does provide a less subjective basis for decisions. As far as is known the quantitative approach has not so far been used in public financial management but is likely to be developed in the future.

[7] Nassim Nicholas Taleb "The Black Swan" 2007

Some conclusions

Risk and control in public financial management must be seen in the context of overall risk management of public finances. In reality the greater risks to public finances are likely to be external and very large. These external risks include both foreseeable events, such as exchange rate movements, and unforeseen "black swan" events.

However, managing risk and establishing controls over public financial management is necessary not only because of the scale of risks and possible losses but also as part of the process of building good governance. To establish both internal and external confidence in government processes there must be a degree of assurance that public finances are properly managed. Hence, to see this as an exercise in risk management is too narrow. Control over finances is part of confidence building in the process of governance.

There are now well developed and structured approaches to control and risk management for public financial management. The implementation of an IFMIS provides new challenges and requires the issue of information security and controls of the system to be specifically addressed. However, the nature of the requirements for risk management and control of public financial management remains the same.

In the future it is likely that risk management and the design of controls will become increasingly based on quantitative approaches and modelling of risks.