Operational Risk Management in a Debt Management Office

Based on Client Presentation

January 2008

mike.williams@mj-w.net

Outline

- The importance of operational risk management (ORM)
- International best practice
  - A high-level perspective, emphasising:
    - The dynamic nature of the process
    - The role of the ORM function
    - Top management responsibility
- ORM in a DMO

mike.williams@mj-w.net

Operational Risk is problematical...

- OR is least understood of the risk categories:
  - OR is endogenous to the institution – it cannot be captured and measured as easily as credit and market risk
  - The management processes are complicated - OR 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
- OR has many sources – e.g. a lack of discipline, unstable or poorly designed procedures, inertia, change, greed, lack of memory or knowledge, overconfidence, etc
  - all factors which cannot be easily quantified, monitored, and reported upon

mike.williams@mj-w.net

But Management of OR is important…

- Failure of transaction-processing systems is a major risk exposure
- OR increased by ever-changing environment
  - Heavy reliance on IT – reduces human error, but exposes new risks
  - Pressures to reduce costs
  - Increasingly sophisticated financial products
  - New technologies (e.g. increased use of the internet) accelerate market activity and increase interconnectivity, bringing new security concerns
  - Increasing regulatory requirements that have highly explicit compliance expectations (e.g., Basel II, Sarbanes Oxley, MiFID, and industry standards) – all of which put pressure also on public sector
- In public sector, added concerns associated with political and reputational risk

mike.williams@mj-w.net

The Definition of OR

- "The risk of loss (financial or nonfinancial) 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."

  Basel II

- Note that this definition:
  - is positive (it is possible to measure and manage operational risk)
  - is comprehensive: it does not concentrate only on specific functional areas (back office, IT, payments, etc) or risk categories (compliance, fraud, etc)
  - is flexible enough for each entity to tailor to its own specific business/needs
  - includes external events
  - includes legal risk
- Strictly the definition excludes strategic and reputation risk
  - But regulators and rating agencies typically expect reputation and strategic risk also to be monitored as an important part of the OR framework – and that is best practice

mike.williams@mj-w.net

The COSO Risk Management Framework

- COSO framework has become the accepted standard for enterprise-wide risk management and for understanding and evaluating internal control structures. It is:
  - Comprehensive
  - Industry-, sector- and territory- independent, and easily permits extensions in a particular field of interest

mike.williams@mj-w.net

COSO: Lifecycle Components - 1

- Internal Environment
  - Risk management philosophy and culture
  - Risk appetite – how much risk is "acceptable"
  - Oversight by senior management (corporate governance); principles for delegating authority and responsibility; management, organisation and development of staff
  - The integrity, ethical values and competence of all concerned
    - includes eg, code of conduct
- Objective Setting
  - Risks should be identified and evaluated against business objectives
- Event or Risk Identification; and Risk Assessment
  - Risk identification and assessment can be combined in a single process
  - Combine top down (identify strategic objectives; then identify related risks) with bottom up (identify risks, link to objectives)
  - Risk and Control Self-Assessment (RCSA), integrate with surveys brainstorming, scenario analysis, external review etc.
  - Importance of gradual build up of expertise over time
  - Focus on residual rather than inherent risk

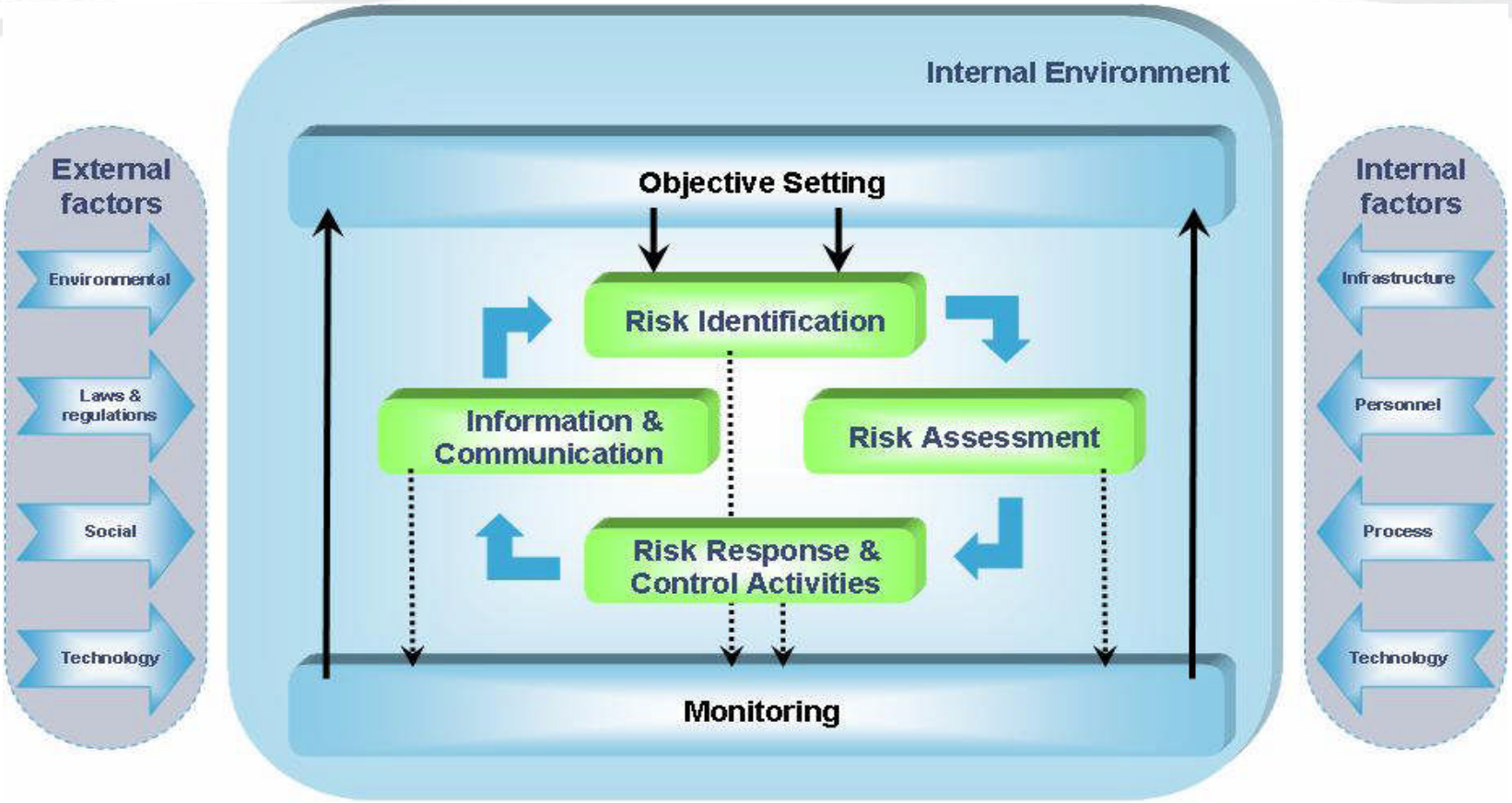
mike.williams@mj-w.net

COSO: Lifecycle Components - 2

- Risk Responses
  - Risk avoidance; Risk reduction (mitigation); Risk transfer; or Risk acceptance
- Control Activities, eg:
  - Approvals
  - Authorisations
  - Verifications
  - Reconciliations
  - Performance reviews
  - Segregation of duties
- Information and Communication
  - Includes OR escalation procedures and reporting to (top) management – right people need the right data at the right time
- Monitoring
  - Tracks and examines the implementation of ORM over time
  - Combination of ongoing monitoring activities and specific evaluation of the ORM process itself (inc by internal auditors)

mike.williams@mj-w.net

A Dynamic Process



NB: Operational risk management is not a one-off event but a series of actions that permeate an entity's activities

Indicators of Best ORM Practice

- ORM practices should be repeatable
  - one-off launch of an advanced technique is not itself best practice – improvement is intrinsically incremental
- ORM practices should be linked into day-to-day business, and hence to continuous improvement mechanisms built into the ORM cycle
- Policies and procedures should be fully embedded in working practices, with active top management support
- Framework is rolled out across the organisation, with buy-in from all
- Data history is built up gradually to enable effective trend analysis
  - Eg historical loss data and trends of key risk indicators
- ORM falls short of best or good practice where
  - It is no more than an 'add-on' in terms of practices, policies and procedures
  - It is a product of the ORM function only, and then rolled out for – or imposed on – a selected number of departments or processes

mike.williams@mj-w.net

Role of the Middle Office ORM Function

- The ORM function
  - co-ordinates the ORM process on a day-to-day basis
  - establishes the framework for reporting and evaluating results
  - facilitates and monitors the risk-response process, escalating problems as necessary
- The function typically evolves over time, from being the main driver to being a facilitator or consultant. This shift requires both:
  - The active support of senior management
  - A strong ORM function, to enforce a formalised and standardised approach for the implementation of ORM practices across the organisation
- But note that:
  - Control activities must be planned at all levels throughout the organisation and the responsibilities for their execution and follow-up clearly defined (this responsibility does not normally reside within the ORM function)
  - The responsibility for developing and implementing risk-response action plans lies with management (including the business units or process owners)
  - Monitoring is undertaken in parallel and is semi-independent of the ORM function insofar as is evaluating the effectiveness of the ORM process itself

mike.williams@mj-w.net

Top Management Responsibility

- ORM is a key component of the overall governance structure, ie a formal, structured response to managing the internal environment and the external factors influencing it
- Integration of ORM requires:
  - Explicit attention to the risk culture, closely linked with human resources development and evaluation practices
  - Explicit responsibility allocation for ORM objectives to employees across the organisation
  - ORM to be an integral part of communication & monitoring activity
- Degree of top management attention is an initial indicator of an organisation's ORM maturity level
  - It is top management's responsibility to establish an effective support structure for mature operational risk management practices
  - This includes providing leadership in interpreting and translating often intangible governance considerations into a practical policy

mike.williams@mj-w.net

OR Management in a Debt Office: a Practical Approach

mike.williams@mj-w.net

Initial Steps

- Senior management must signal to whole office the importance attached to operational risk management (ORM)
  - Office meetings, office notices, attending workshops etc
- Appoint a "Risk Champion" – someone in middle office who will take OR responsibility. The risk champion:
  - Leads and guides the process throughout the office; and coordinates reporting to management
  - Develops the control framework; acts as "consultant" to line managers; and monitors and chases progress – but does not detract from line managers' responsibilities for ORM in their own areas
  - Ideally has some professional OR training (but not always possible)

mike.williams@mj-w.net

Suggested Process

- Key steps
  - Identify risks and assess key exposures
    - Exposure = likelihood of the relevant risk event multiplied by its impact
  - Prepare a high-level summary of risks that is consistent across the office, as a way of identifying priorities for management
  - Monitor risk events
  - Regularly review and update of the risk profile
- Technique is flexible – can initially be done in broad brush way; build and improve over time as experience develops
- Collect risk data (risk registers) in a series of workshops across the office
  - Could be organised on a team basis; or with a meetings of mixed groups of staff; or using a committee taken from every part of the office
  - Important that everyone is involved, including the more junior staff - helps to develop risk understanding and a risk culture
  - Coordinate with internal audit; inform external audit

mike.williams@mj-w.net

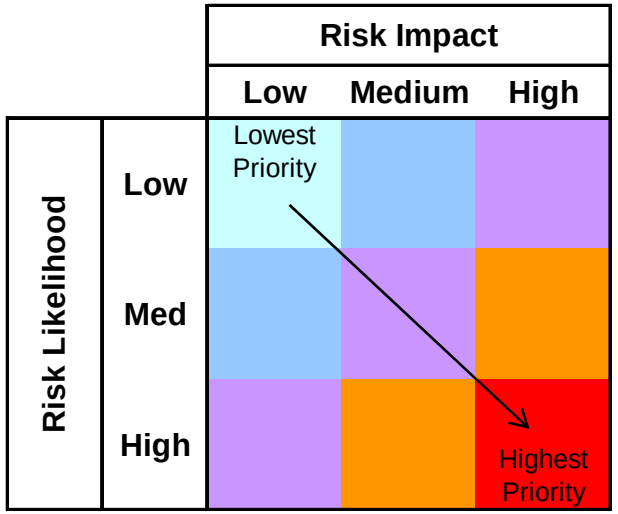
The Process in Practice

- Workshops convened/guided by the risk champion
  - He or she has understanding of risk across the range of functions
  - Can ensure a consistency of approach and terminology
- Break down the main business areas into business activities or processes, each with a stated objective
- Identify and describe in the workshops the key risks that might impact on each area of the business
  - Balance the amount of detail and usefulness to management
- Identify the key controls which mitigate each of the risks.
  - Many of the control techniques will apply to many of the risks
  - As experience develops a system to evaluate controls should be introduced

mike.williams@mj-w.net

Scoring the Risks

- Rate each risk for both likelihood (low, medium, high) and impact (low, medium, high)
- Plot the combinations on a 3 x 3 matrix
  - Most serious risk exposures are those of high likelihood and large impact.
  - Identified for urgent management action
    - Ideally scoring done separately before and after the mitigating controls, and decide whether the residual risk can be further reduced or is unavoidable. But initially scoring the present positions is highest priority



- Risk champion reports to management on greatest exposures, together with the control actions that have been taken or might be taken in future
- Refresh data periodically with repeat workshops

mike.williams@mj-w.net

Action might include…

- Expanded training programme
- Development of control tools
  - Possibly with professional/consultancy help
  - Separation of operations and processing, 4-eyes principle
  - Ensure consistent application, monitored by middle office/risk champion and/or internal audit
  - Process manuals incorporating controls
    - Keep them simple, as working documents
  - Ensuring use of process control and check lists
- Removing legal uncertainties
- Developing a business continuity plan

mike.williams@mj-w.net

Reporting

- Incidences or Exceptions [or Errors]
  - Report each incident or exception - summary in reports to senior management
  - Relevant for monitoring control framework - identifying badly managed risks and action needed to avoid repeat
  - Should not "blame" individual concerned - many incidents often fault of management failing to develop adequate control environment
- Report regularly to senior management on the risk profile, identifying where improving or deteriorating; and priorities for mitigating action
  - Error reports part of this, but do not capture all vulnerabilities
- Possible technique:
  - Indentify which manager has the lead responsibility for managing and controlling each of the identified risks
  - Ask each manager to report periodically [quarterly?] on the risks for which they are responsible - whether these have increased or reduced, and whether and what action should be taken
  - Risk champion collects the reports together with the error reports, and summarises the key points for senior management, with recommendations

mike.williams@mj-w.net

Managing "External" Risks

- Many risks arise outside the office
  - rest of MoF, main suppliers (inc IT), central bank
- Develop their understanding of the problem, seek co-operation
- In MoF
  - Bilateral meetings, communication of the results of their errors, reporting to senior management
  - Consider informal "contracts" eg with IT department
- For central bank, cover risk management in Memorandum of Understanding or Service Level Agreement
  - Require central bank to provide evidence of relevant ORM processes and their soundness – eg internal or external audit reports
  - Well-established precedent in financial services industry
- Contracts with external suppliers cover risk management, inc compensation for errors

mike.williams@mj-w.net

Benefits of a Risk Committee

- Chaired by senior official – eg head of debt office or the main "customer" in MoF
  - Could be sub-committee of eg Public Debt Management Committee
- Middle office/risk champion acts as secretary and provides most papers
- Responsibilities ideally cover market, credit & operational risk; and include
  - Defining debt office's risk policies, including risk appetite, taking account of business requirements
  - Development and maintenance of risk policies
    - valuation methodologies, market, liquidity, credit, and operational (including legal and business continuity) risk policy documents, and so on.
    - agreeing the approach to identification, quantification, and monitoring of risks.
  - Reviewing any limit/policy breaches and recommending action, where necessary.
- In relation to operational risk, in particular
  - Agreeing the OR processes applied across the office.
  - Considering reports from the risk champion; and agreeing action accordingly
  - Commissioning and approving business continuity plans

mike.williams@mj-w.net

References

- Best Practices in Qualitative Operational Risk Management: The ORM Reference Guide

  [The source for the charts above]

- Roadmap to Operational Risk Management Success: The ORM Maturity Benchmark

  [Both the above published in 2007 by TransConstellation, a not-for-profit entity established by industry leaders in the field of financial-transaction processing including Euroclear and SWIFT see www.transconstellation.com]

- COSO: The Committee of Sponsoring Organisations of the Treadway Commission: www.coso.org

mike.williams@mj-w.net