Operational Risk Management

An Iceberg – but Icebergs can melt…

DMF Stakeholders' Forum

Berlin, May 2013

DEBT MANAGEMENT FACILITY

Mike Williams
mike.williams@mj-w.net

Operational risk is: "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 on-going business processes." *Basel II*

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 DMU: a practical approach

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

OR: Some Examples

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

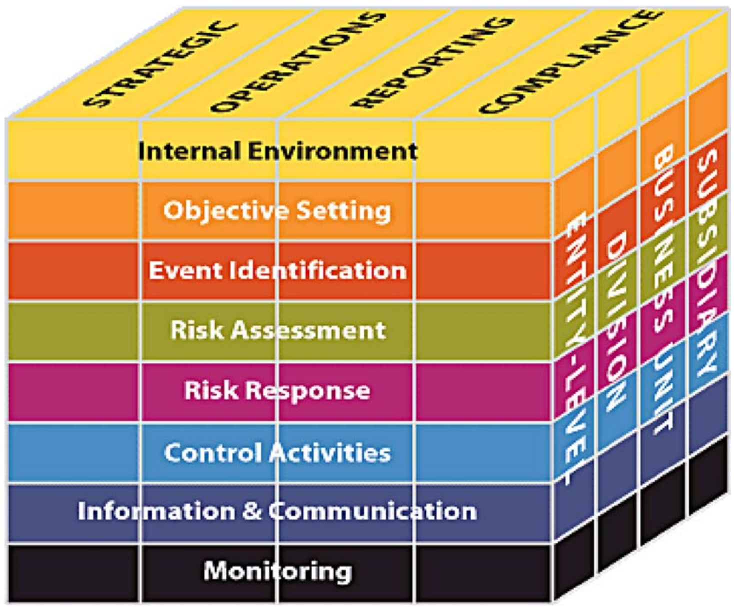
- Policy changes by Ministers, regulators, other stakeholders
- Poor high-level policy making, weak governance structures
- Failure or errors of suppliers, outsourcers or agents (a failure of their risk controls)
- Changes in legislation or the courts' interpretation
- Legal or commercial disputes, inc employment contracts
- Externally supported systems failure
- System attack (hacking)
- Business continuity events – of fire or flood, terrorist or industrial action; or natural disaster

But Management of OR is important…

- Significant risk exposures
  - Failure of transaction-processing systems
  - Exposure to suppliers (inc IT dept and central bank)
  - Business continuity events
- Made worse 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
- It is worse in the public sector
  - Added concerns associated with political and reputational risk
  - Increasing regulatory requirements and explicit compliance expectations in private sector (Basel II, Sarbanes Oxley, Dodd-Frank, MiFID, industry standards etc) also put pressure on public sector

Different ORM Techniques

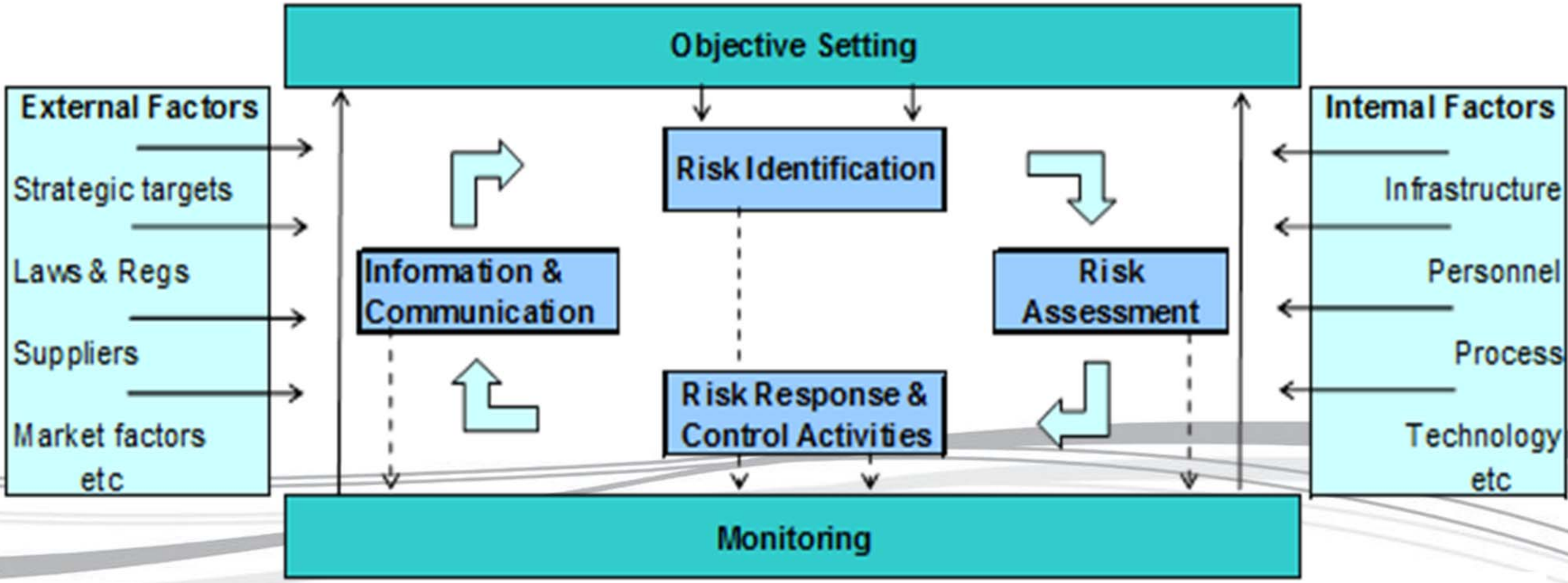
- There are different techniques and standards
  - ISO 31000: developed to provide guidance on the risk management process and its implementation.
  - COSO: widely-used standard for understanding and evaluating internal control structures, particularly in a transaction processing environment.
  - Risk Management Standards of UK, Australia /New Zealand…..



- But they have <u>the same</u> underlying approach
  - Developing an appropriate risk management environment: a responsibility of senior management
  - Systems for risk management: identification, assessment, monitoring, and mitigation/control

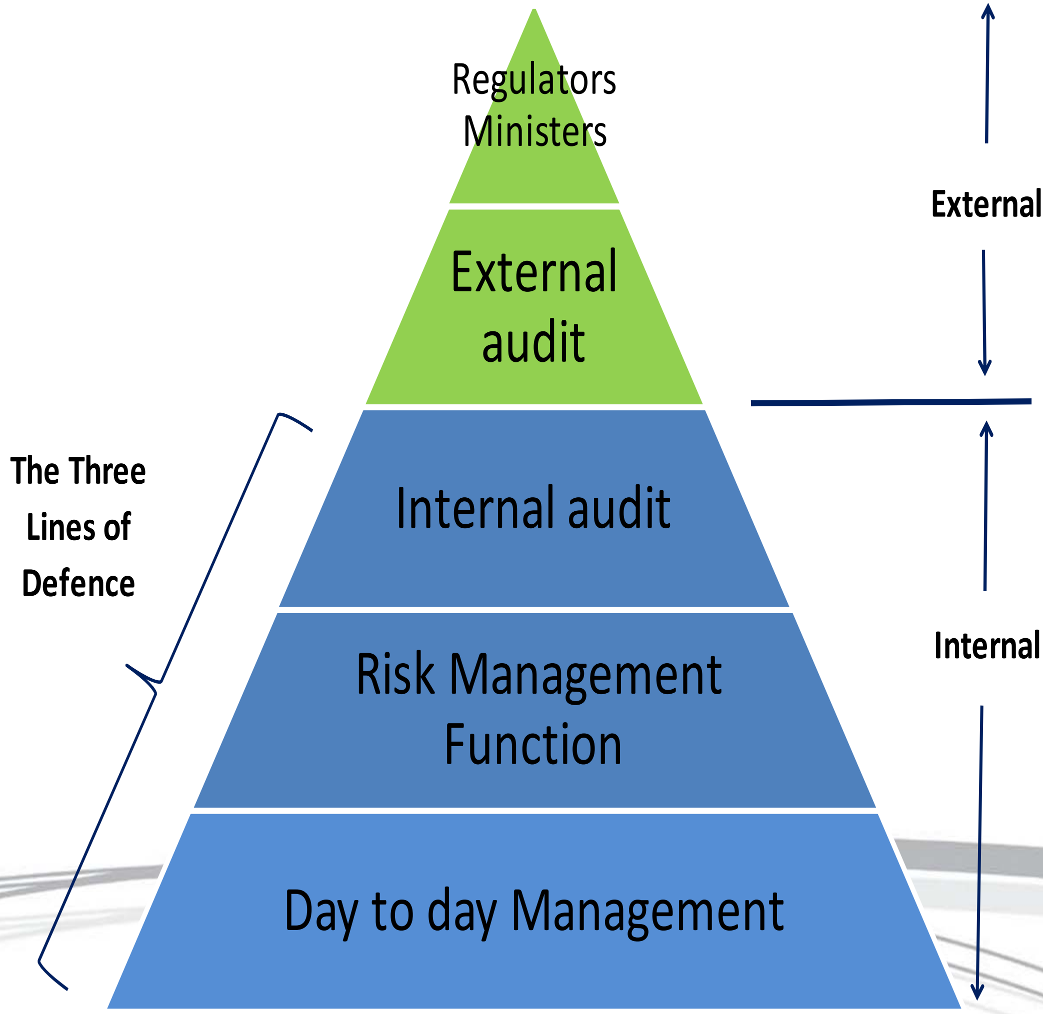
ORM is a Dynamic Process…

- ORM is not a one-off event or an add-on
  - It is a series of actions that permeate an entity's activities.
  - Processes should be repeatable and linked into day-to-day work – and hence to continuous incremental improvement
  - A data history, e.g. of key risk indicators (KRIs) or risk events, is built up gradually to enable effective trend analysis



...embedded in the wider Control Framework

- Corporate governance and decision-making structures
- The business plan
  - Identifying strategic or business risks
  - Setting DMU objectives
- Enterprise risk management
- Responsibilities and delegations
- HR policies; including a code of conduct or ethical practice and performance review
- The control environment supported by an internal audit function



What it means in a DMU: a Practical Approach

Initial Steps

- Senior management must signal to whole office the importance attached to ORM
  - A key component of the overall governance structure
  - Explicit attention to the risk culture, closely linked with HR and evaluation practices
  - Office meetings, office notices, attending workshops etc
- ORM is a middle office function
  - Appoint a "Risk Champion" – someone in middle office who will take OR responsibility – who leads and guides the process throughout the office; and coordinates reporting to management
  - Typically evolves over time, from being the main driver to being a facilitator or consultant
- Individuals at all levels have direct responsibility in their area

Suggested Process

- Key steps
  - Identify risks and assess key exposures
    - Exposure = likelihood of the relevant risk event multiplied by its impact
  - Collect risk data (risk registers) in a series of workshops across the office – Risk Champion ensures consistency
    - Important that everyone is involved, including the more junior staff – helps to develop risk understanding and a risk culture
  - Prepare a high-level summary of risk exposures that is consistent across the office
    - Identify priorities for management
  - Monitor risk events; regularly review and update the risk profile
- Technique is flexible – can initially be done in broad brush way; build and improve over time as experience develops
  - Coordinate with internal audit; inform external audit

Scoring the Risks

- Identify separate activities and the associated risks
- Rate each risk for both likelihood (low, medium, high) and impact (low, medium, high)
- Plot the combinations on a 3*3 (or 4*4) matrix
  - Most serious risk exposures are those of high likelihood and large impact
  - Identified for urgent management action

		Risk Impact		
		Low	Medium	High
Risk Likelihood	Low	Lowest Priority		
	Med			
	High			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

Action might include…

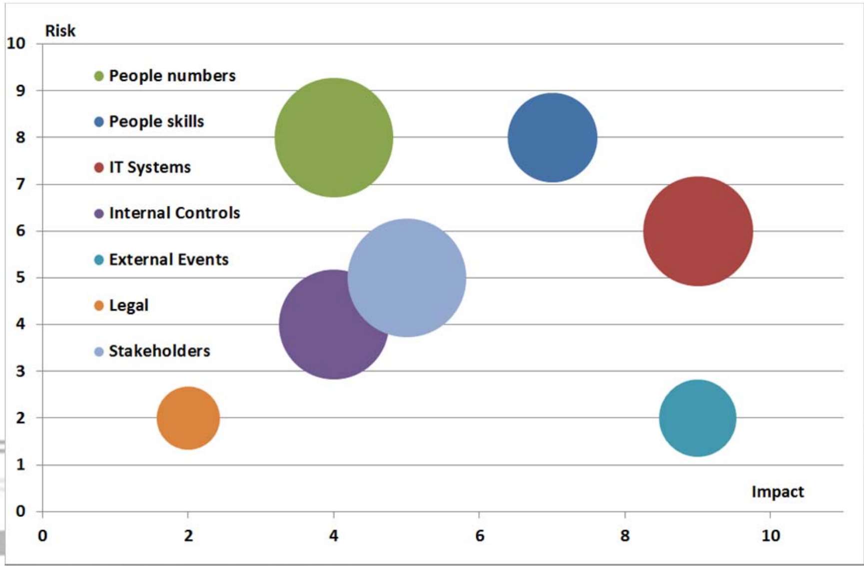
- Risk responses
  - Accept the (residual) risk
  - Avoid the risk (e.g. stop a certain service or choose a totally different technological solution)
  - Transfer the risk (e.g., insure against losses, outsource to specialists)
  - Mitigate (control) the risk, taking measures to reduce the probability of it materialising, and/or reduce the impact of the loss event.
- Development of controls
  - Aimed at prevention, detection or mitigation
  - Important to separate operations and processing, 4-eyes principle
  - Ensure consistent application, monitored by MO and/or internal audit
  - Process manuals incorporating controls – keep them simple, as working documents
- Expanded training programme
- Developing a business continuity plan

Business Continuity Plan

- BCP mitigates some – not all – risks
  - ORM is about all risks that impact on objectives
- Disaster recovery site is only a part of BCP
  - Must be able to manage all disruptions
- Requires
  - Documenting business activities and critical processes and systems
  - Impact analysis under different scenarios – links directly with risk assessment
  - Development of the BCP – must involve third party suppliers
  - Training and testing: everyone must know what to do, and how to respond depending on the business continuity event
  - Regular updating – and testing again

Supporting Techniques

- Identify risk drivers, summarising exposures
  - Causes: people, process, systems, legal, external…
  - Event types: e.g. fraud, lack of skills, error checking, business disruption, system failures…
  - Summarise patterns in bubble charts – showing exposure to key drivers



- Key Risk Indicators
  - Activity or volume-based measures that serve as early warning signals for management
- Risk Management Committee
  - Chaired by head of debt office or the main "customer" in MoF
  - Responsibilities cover market, credit & operational risk; MO/risk champion acts as secretary
  - Defines DMU's risk policies, inc. risk appetite, taking account of objectives
  - Develops and maintains risk policies, inc. methodology and setting risk limits
  - Considers reports from risk champion; agrees action accordingly
  - Commissions and approves BCP

Reporting

- Incidences or Exceptions [or Errors]
  - Report each incident or exception
  - 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 risk profile, identifying where better or worse; and priorities for mitigating action
  - Error reports part of this, but do not capture all vulnerabilities
- Possible technique:
  - 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 or Risk Committee, with recommendations

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 / external audit reports
  - Well-established precedent in financial services industry
- Contracts with external suppliers cover risk management, inc compensation for errors

Some conclusions…

- ORM is a process – to be developed over time and embedded
- No DMU is too big or too small
  - Benefits are in reach with a proportionately modest resource cost
  - Procedures outlined are consistent with good international practice; but also flexible, and can be applied proportionately to size, activities, risk appetites and capability.
- All staff should be involved
  - Individuals should know what risks they are facing and managing
  - All should be involved in refreshing of the data, incident reporting…
  - Continuing reporting, summarising and consultancy work will fall largely to the MO [maybe just 1-person equivalent in a small office]
- Whatever the scale and resources, senior management support is critical
  - ORM helps them to meet objectives

Thank You!