Operational Risk Management

The Framework and Techniques; and making them work for Debt Managers

Based on Client Presentation
November 2020

Outline

The importance of operational risk management (ORM)

International best practice

ORM in a DMU: a practical approach

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 [an entity's] ability to operate its on-going business processes." *Basel II*

Operational Risk is problematical…

OR is less well understood than other risks

- OR is endogenous to the institution: it is more difficult to capture and measure than credit and market risk
- The management processes are complicated
  - OR is linked to nature and complexity of the activities, to processes and systems in place, and to quality of management and 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, cyder crime)
- Business continuity events: fire or flood; terrorist or industrial action; natural disaster – or a pandemic bring lockdowns/staff shortages

But Management of OR is increasingly 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…

- Reliance on IT: reduces human error, but exposes new risks (inc cyber crime)
- Pressures to reduce costs
- New technologies (e.g. increased internet use) accelerate activity and increase connectivity, but bring new security concerns

…and especially in the public sector

- Added concerns associated with political and reputational risk
- Increasing private sector regulatory and compliance requirements (Basel, Sarbanes Oxley, Dodd-Frank, MiFID, industry standards, impact of climate change etc) also put pressure on public sector

Outline

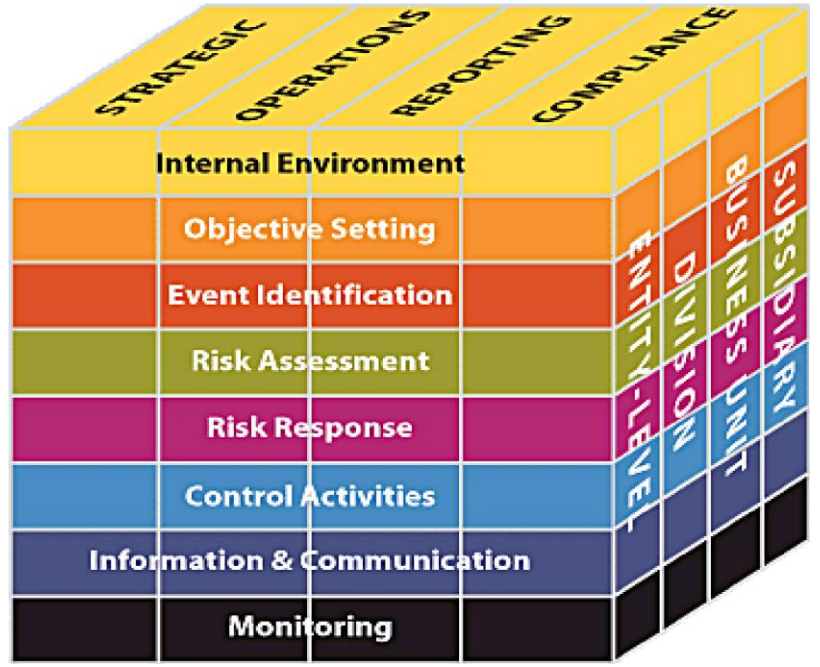
The importance of operational risk management (ORM)

International best practice

ORM in a DMU: a practical approach

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 the same 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

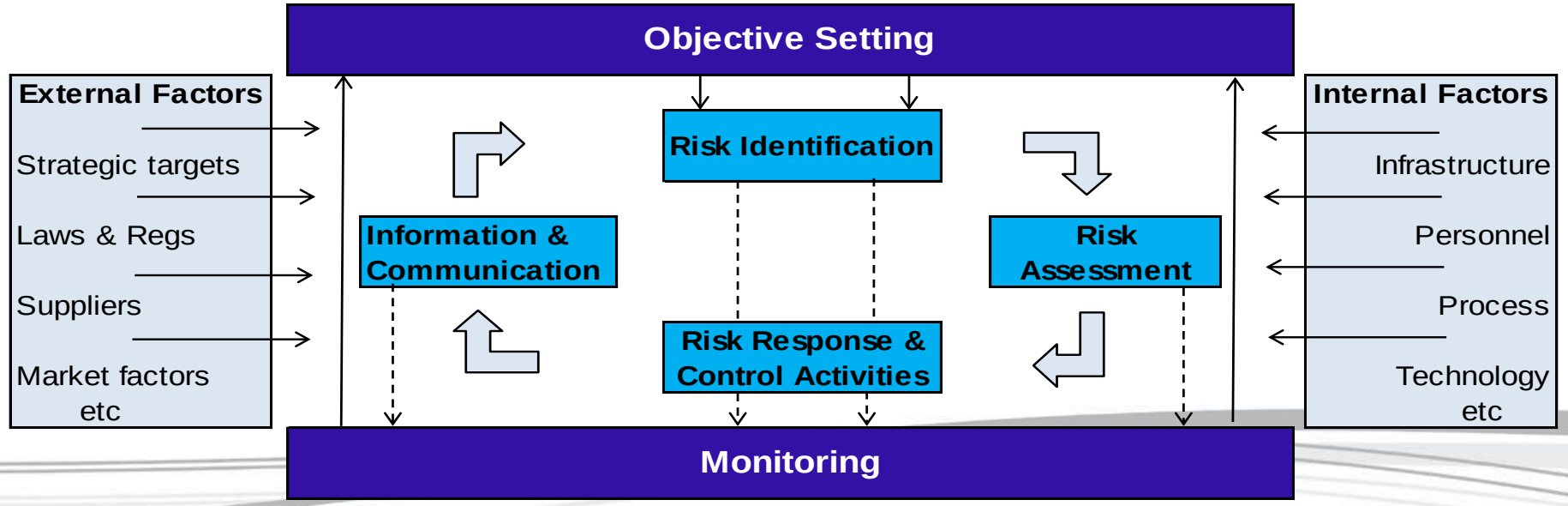
It is a series of actions permeating an entity's activities.

Processes should be repeatable and linked into day-to-day work

Supports continuous incremental improvement

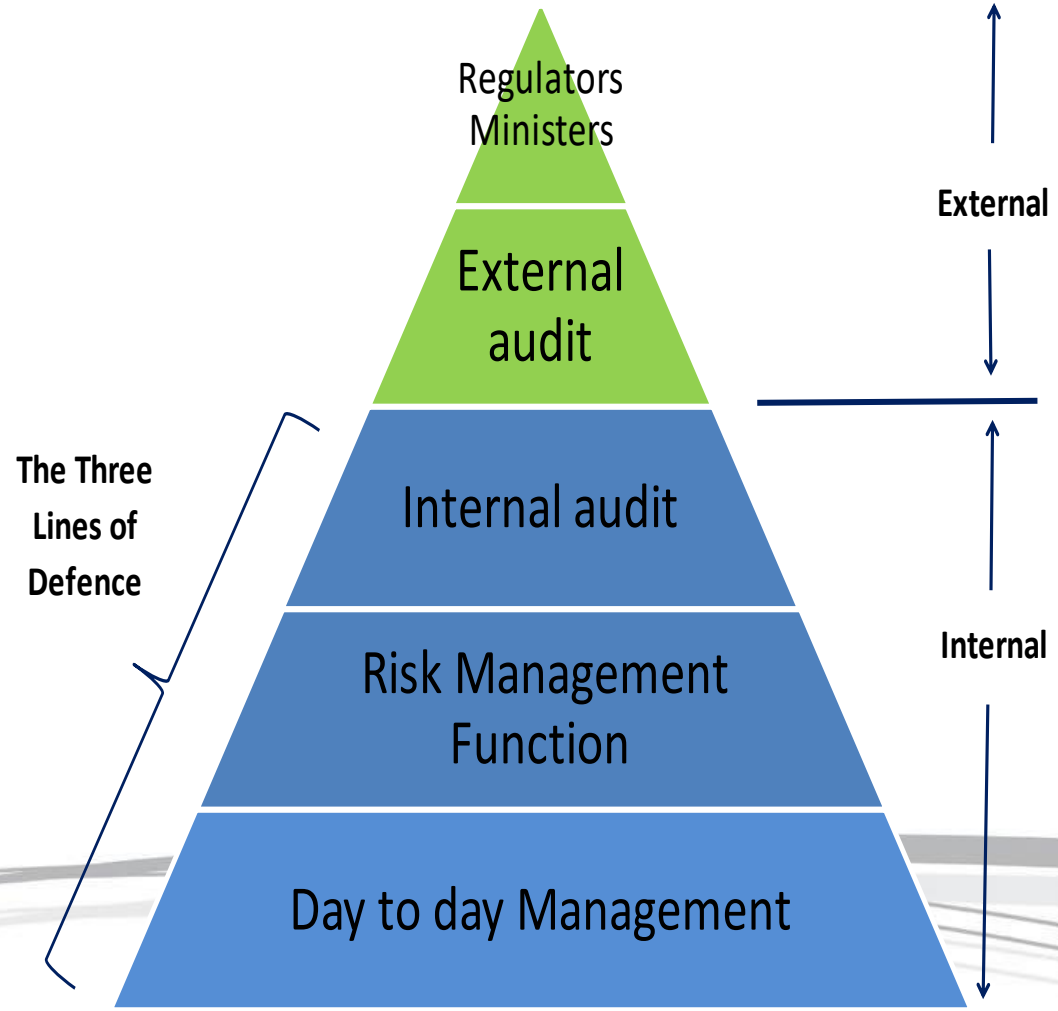
Data history, e.g. key risk indicators (KRIs) or risk events, is built up gradually

Enables 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
  - Linkage to wider ministry risk management framework
- 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



Outline

The importance of operational risk management (ORM)

International best practice

ORM in a DMU: a practical approach

Annexes attached with examples of Controls and Key Risk Indicators (KRIs)

To Emphasise…

The OR function does not change the responsibilities of individuals and their managers for risk management in their areas

Senior management must signal 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

Technique is flexible – can initially be done in broad brush way; build and improve over time as experience develops

Suggested Steps

Appoint a "Risk Champion" – someone in middle office to take OR responsibility

- He/she 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

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,- 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

Scoring the Risks

1. Identify separate activities and the associated risks

2. Rate each risk for both likelihood (low, medium, high) and impact (low, medium, high)

3. Plot the combinations on a matrix
   - Most serious risk exposures those of high likelihood & large impact
   - Identified for urgent management action

Likelihood level of risk	Impact level of risk				
	Insignificant	Minor	Moderate	Major	Catastrophic
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

Source: Tokaç & Williams 2013

4. Risk champion reports to management on greatest exposures, together with the control actions that have been taken or might be taken in future

5. 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

- 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

BCP mitigates some – not all – risks

Requires

- Documenting business activities and critical processes and systems
- Impact analysis under different scenarios; links 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

Reporting

- Incidences/Exceptions/Errors
  - Report each incident
  - Identify badly managed risks and action needed to avoid repeat
  - Should not "blame" individual concerned –incidents often fault of management failing to develop adequate control environment
- Key Risk Indicators
  - Activity or volume-based measures that serve as early warning signals for management (see Annex)
- Report regularly to senior management on risk profile
  - 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

- Others in Ministry/Treasury, main suppliers (inc IT), central bank

Develop their understanding of the problem, seek co-operation

In Ministry/Treasury

- 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 MoU or Service Level Agreement

- Require central bank to provide evidence of relevant ORM processes and their soundness
- Example: internal / external audit reports; well-established precedent in financial services industry

Contracts with external suppliers cover risk management, inc compensation for errors

Some Governance Issues

ORM, Internal Audit and Compliance

- Internal Audit
  - Independent of ORM
  - Reports directly to head of DMU or wider ministry
- Compliance
  - Checks to see that controls and regulatory requirements are followed
  - May be part of middle office, even of ORM team
- IA work includes evaluating OR and compliance processes
  - Although IA, ORM and compliance have different functions they should work closely to avoid duplication

Risk Management Committee

- Chaired by head of DMU or the main "customer" in wider Ministry/Treasury
- 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

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

References

- Bank for International Settlements (2003) "Sound Practices for the Management and Supervision of Operational Risk" (BIS, Basel) www.bis.org/publ/bcbs96.htm
- OECD (2005) "Management of Operational Risk by Sovereign Debt Management Agencies" Chapter 5 in Advances in Risk Management of Government Debt (OECD)
- Tokaç, Hakan and Mike Williams (2013) "Government Debt Management and Operational Risk: A Risk Management Framework and its Application in Turkey" (Sigma Papers, No. 50, OECD) http://dx.doi.org/10.1787/5k483jnqxtms-en
- World Bank (2010), "Guidance for Operational Risk Management in Government Debt Management" (World Bank) https://documents.worldbank.org/en/publication/documents-reports/documentdetail/419301468153852761
- There is a range of papers on operational risk and enterprise risk management on the website of COSO (Committee of Sponsoring Organizations of the Treadway Commission) at www.coso.org

Annex: Controls: Some Examples

- **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

Annex: Key Risk Indicators: Some Examples

- **Systems**
  - Downtime; Recorded software/hardware problems
- **Risk Issues**
  - Concerns or issues raised proactively by individuals or managers, or 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; sick leave
  - Training days/skill profile
- **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].