Lecture

IAQS | INSTITUTE OF ACTUARIAL & QUANTITATIVE STUDIES

Class: TY BSc

Subject : Basel

Subject Code:

Chapter: Unit 1 Chapter 1

Chapter Name: Operational risk and principles of sound management

Today's Agenda

1. Introduction

2. Role of supervisors

3. Operational risk
    1. Causes of operational risk
    2. Why is operational risk management important?

4. History

5. Principles for management of operational risk

6. Fundamental principles

7. Revised fundamental principles

1 Introduction

Principles for the Sound Management of Operational Risk and the Role of Supervision – incorporates the evolution of sound practice and details eleven principles of sound operational risk management covering
(1) governance,
(2) risk management environment
(3) the role of disclosure.

2 Role of supervisors

- Supervisors conduct regular independent evaluations of a bank's policies, processes and systems related to operational risk.
- Supervisors ensure that there are appropriate mechanisms in place.
- Supervisors also seek to ensure that, where banks are part of a financial group, there are processes and procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group.
- Supervisors identify deficiencies in the banking mechanism and use tools most suited to the particular circumstances of the bank and its operating environment.
- Supervisors continue to take an active role in encouraging ongoing internal development efforts by monitoring and evaluating a bank's recent improvements and plans for prospective developments.

3 Operational risk

Operational risk is any risk that arises from your company's business processes and could result in financial loss or disruption to your ability to serve customers.

- Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme.
- Operational risk management (ORM) is the art of protecting your company from such risks and minimizing any damage that may occur.
- Operational risk is a broad concept.
- Examples include internal issues such as employee misconduct, human error, poorly designed business practices, and weak internal processes. External events such as cyber security breaches and natural disasters qualify as operational risks, too. The common factor in all these events is their ability to affect your daily operations and create a risk of loss.

3.1 Causes of operational risk

- Natural disasters, such as earthquakes, hurricanes or wildfires and Man-made disasters, such as terrorism, cyberterrorism and cybercrime.
- Embezzlement, insider trading, insider cybercrime, negligence and other workplace-related torts.
- Regulatory compliance violations, breach of contract, antitrust, market manipulation and unfair trade practices.
- Failure to adhere to the company's policies or procedures or, conversely, a failure to enforce policies.
- Outdated or unpatched information technology (IT) systems and software.
- Unfair or inconsistent work policies.
- Human errors, such as data entry errors or a missed deadline.
- Poorly conceived or inefficient internal processes.

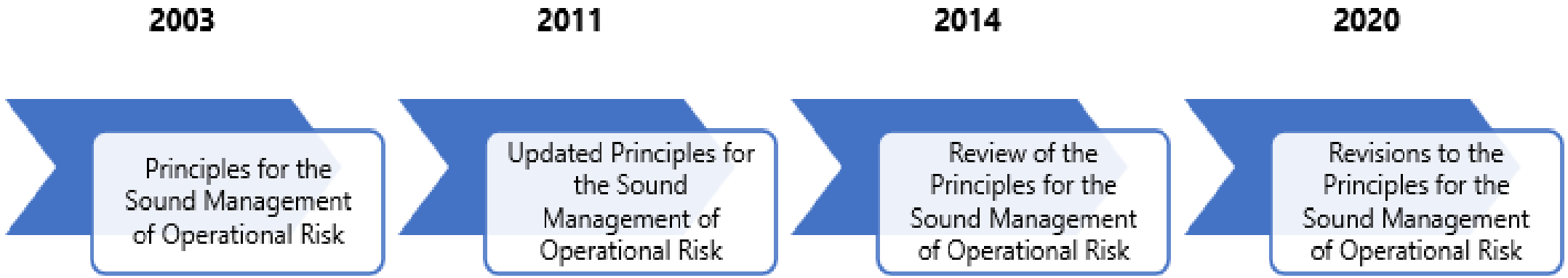
3.2 Why is operational risk management important?

Operational risk management (ORM) is important because it can help organizations:

- Improve decision-making
- Reduce costs
- Identify unsafe practices
- Improve manufacturing
- Boost consumer satisfaction
- Provide accurate financial forecasting
- Respond resiliently to disruptions
- Improve product performance
- Ensure continuous improvement

4 History

The Basel Committee on Banking Supervision (BCBS) published the PSMOR in 2003 to provide a framework of principles related to operational risk to guide industry practitioners and supervisors. The BCBS updated the principles in 2011 and conducted a review of the implementation in 2014. In August 2020 the BCBS published a further revision to the PSMOR for consultation, with comments to be provided by 6 November.



5 Principles for management of operational risk

- Risk management generally encompasses
  - the process of identifying risks to the bank,
  - measuring exposures to those risks (where possible),
  - ensuring that an effective capital planning and monitoring programme is in place,
  - monitoring risk exposures and corresponding capital needs on an ongoing basis,
  - taking steps to control or mitigate risk exposures
  - reporting to senior management and the board on the bank's risk exposures and capital positions.

- Sound internal governance forms the foundation of an effective operational risk management

- Common industry practice for sound operational risk governance often relies on three lines of defence –
  (i) business line management,
  (ii) an independent corporate operational risk management function
  (iii) an independent review

6 Fundamental principles

Principle 1:
The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

With respect to Principle 1, the board of directors and/or senior management should:

1. Provide a sound foundation for a strong risk management culture
2. Establish a code of conduct (or ethics policy) for all employees
3. Provide risk training

6 Fundamental principles

Principle 2:
Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

With respect to Principle 2, the board of directors and/or senior management should:

1. Thoroughly understand both the nature and complexity of the risks
2. Ensure that the Framework is fully integrated in the bank's overall risk management plan

6 Fundamental principles

Principle 3:
The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

With respect to Principle 3, the board of directors and/or senior management should:

1. Establish a culture and processes that help bank managers and employees understand and manage operational risks.
2. Regularly review the Framework.
3. Provide senior management with guidance regarding operational risk management.
4. Ensure that the Framework is subject to independent review.
5. Ensure that management is following best practices.
6. Establish clear lines of management responsibility.

6 Fundamental principles

Principle 4:
The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.

With respect to Principle 4, the board of directors and/or senior management should:

1. Consider all relevant risks when approving the bank's risk appetite and tolerance statements.
2. Review the risk appetite and tolerance statements

6 Fundamental principles

Principle 5:
Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

With respect to Principle 5, the board of directors and/or senior management should:

1. Establish systems to report and track operational risks and maintain an effective mechanism for resolving problems.
2. Translate the Framework approved by the board into specific policies and procedures used to manage risk. Ensure that operational risk managers communicate clearly with personnel
3. Ensure that CORF managers should have sufficient stature in the bank.
4. Ensure that the staff is well trained in operational risk management.
5. Develop a governance structure of the bank that is commensurate with the size and complexity

6 Fundamental principles

Principle 6:
Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

With respect to Principle 6, the board of directors and/or senior management should:
1. Consider both internal and external factors to identify and assess operational risk

6 Fundamental principles

Principle 7:
Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

With respect to Principle 7, the board of directors and/or senior management should:
1. Maintain a rigorous approval process for new products and processes.
2. Thoroughly review new activities and product lines.

6 Fundamental principles

Principle 8:
Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

With respect to Principle 8, the board of directors and/or senior management should:

1. Continuously improve the operational risk reporting.
2. Ensure that operational risk reports are timely.

6 Fundamental principles

Principle 9:
Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

With respect to Principle 9, the board of directors and/or senior management should :
Have a sound internal control system as described in LO 35.e (an effective control environment)and LO 35.f (managing technology and outsourcing risks).
Banks may need to transfer risk (e.g., via insurance contracts) if it cannot be adequately managed within the bank. However, sound risk management controls must be in place and thus risk transfer should be seen as a complement to, rather than a replacement for, risk management controls. New risks, such as counterparty risks, may be introduced when the bank transfers risk. These additional risks must also be identified and managed.

6 Fundamental principles

Principle 10:
Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

With respect to Principle 10, the board of directors and/or senior management should:

1. Implement an information and communication technology (ICT) program
2. Oversee the effectiveness of ICT risk management on a frequent basis.
3. Ensure the ICT program can accommodate potential stress and disruptive events.

6 Fundamental principles

Principle 11:
A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

With respect to Principle 11, the board of directors and/or senior management should:

1. Establish continuity plans to handle unforeseen disruptive events (e.g., disruptions in technology, damaged facilities, pandemic illnesses that affect personnel, and so on).
2. Periodically review continuity plans.

6 Fundamental principles

With respect to Principle 12, the board of directors and/or senior management should:

1. Write public disclosures such that stakeholders can assess the bank's operational risk management strategies.
2. Write public disclosures that are consistent with risk management procedures. The disclosure policy should be established by the board of directors and senior management and approved by the board

7 Revised Fundamental principles

Principle 1: Risk Culture

- New wording places the emphasis on senior management's responsibility to implement a strong risk culture and the steps the board of directors must take to facilitate this.
- Clarity that poor risk culture includes inappropriate provision of financial services (whether wilful or negligent).
- Added recommendation that the Code of Conduct should be reviewed and approved by the board, attested to by employees, its implementation overseen by a senior ethics committee, and be publicly available.
- Management should now set clear accountabilities so bank staff understand their roles and responsibilities for risk management.
- Clarity that customised training programmes should be mandatory for specific roles (e.g. heads of business units).

7 Revised Fundamental principles

Principle 2: Operational risk management framework (ORMF)

- Addition of a recommendation for the board of directors and management to understand the nature and complexity of risks inherent in their systems.
- Clarity that integration of ORMF into the bank's overall risk management processes is the first line's responsibility.
- Added detail on inclusions to the ORMF, including: mandates and membership of operational risk governance committees; reference the relevant operational risk management policies and procedures; increased focus on control identification and assessment; and the approach to ensuring controls are designed, implemented and operating effectively.
- Requires that policies be reviewed and revised, as appropriate, based on the continued assessment of the quality of the control environment, addressing internal and external changes.

7 Revised Fundamental principles

Principle 3: The Board of Directors

- Change in emphasis on board responsibility and movement to greater ownership by senior management . For example, the board's role is now articulated as oversight of material operational risks and effectiveness of key controls, and ensuring senior management implement the ORMF.
- Additional recommendation for the board to ensure controls 'be regularly reviewed, monitored and tested to ensure ongoing effectiveness'

Principle 4: Risk Appetite

- There are new recommendations that the operational risk appetite should: be easy to communicate and understand; include key background information and assumptions; clearly articulate the motivations for assuming or avoiding certain types of risk, and the boundaries or indicators to monitor these risks; ensure the strategy and risk limits of each business unit and legal entity, as relevant, align with the bank-wide risk appetite statement; and be forward looking and, where applicable, subject to scenario and stress testing.

7 Revised Fundamental principles

Principle 5: Senior Management

- The previous title was 'Three lines of defence and senior management', now this only references senior management. Wording related to the three lines of defence has been removed from the principle and detail has been added to the front of the document, where it is stressed that the three lines of defence model should be adequately and proportionally used by financial institutions to manage every kind of operational risk sub-category, including ICT risk

7 Revised Fundamental principles

Principle 6: Identification and Assessment in BAU

- Substantive changes to the list of tools used to identify and assess risk. Changes include: the removal of audit findings and capital as an example tool to identify and assess risk; further detail on the qualitative and quantitative analysis involved in the RCSA process and the documentation required; the addition of 'event management'; addition of control monitoring and assurance framework requiring a 'structured approach to the evaluation, review and ongoing monitoring and testing of key controls, sufficiency of control coverage' and that 'control monitoring should be appropriate for the different operational risks and key controls'; more detail has been provided on scenario analysis, specifically how to conduct scenarios and potential uses; and the addition of 'benchmarking' in the comparative analysis section.
- Addition of the specification that data to be accurate and subject to the Corporate Operational Risk Function (CORF) monitored action plans and remediation plans where necessary

7 Revised Fundamental principles

Principle 7: Identification and Assessment in Change

- Greater clarity on the three lines of defence during change. Line 1 should perform the initial assessment; Line 2 conducts review and challenge of all stages of the process and ensures all control groups are involved as appropriate.
- New recommendation to assess the evolution of associated risks from inception to termination (i e. throughout the full life-cycle of the product).
- Addition of paragraph 40 'Banks should maintain a central record of their products and services to the extent possible (including the outsourced ones) to facilitate the monitoring of changes'.
- Change management policies and procedures should be subject to independent and regular review and update.

7 Revised Fundamental principles

Principle 8: Monitoring and Reporting

- The onus of the principle has been moved to senior management and removal of the word ‘losses’ from the principle, broadening it.
- Detail makes it clear that Line 1 should be conducting ‘reporting on any residual operational risks, including operational risk events, control deficiencies, process inadequacies and non-compliance with operational risk tolerances’
- Addition of text on 'a discussion of key and emerging risks assessed and monitored by metrics' and the need to report on 'root cause analysis' for significant events and losses.

7 Revised Fundamental principles

Principle 9: Control and Mitigation

- Removal of detail regarding technology risk (now it is clarified that they must follow the same process as operational risk)
- New wording around concentration risk and the complexity of outsourcing.
- The addition of paragraph 54 'banks should have unified classification, methodology, procedures of operational risk management established by the CORF'

Principle 10: ICT

- New principle stating: 'Banks should implement robust ICT governance that is consistent with their risk appetite and tolerance statement for operational risk and ensures that their ICT fully supports and facilitates their operations. ICT should be subject to appropriate risk identification, protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness, and convey relevant information to users on a timely basis'

7 Revised Fundamental principles

Principle 11: Business continuity planning

The previous principle was titled ‘business resiliency and continuity plans’, the 'resiliency' wording has been dropped and separate principles are to be provided in the Principles for Operational Resilience paper..
There is new text now on the need for board and senior management involvement in reviewing and implementing business continuity plans (BCP).
Clarity that BCP must be grounded in scenario analysis and the need to now set thresholds and limits for the activation of BCP.

Principle 12: Disclosure

New wording around including operational risk exposures in disclosures. Historically banks have only disclosed their processes and capital holdings for operational risk. Now it is recommended that bank’s include operational loss events, while not creating additional operational risk through this disclosure (e.g. description of unaddressed control vulnerabilities). This may be a material shift in reporting