FRM Part II

Operational Risk And Resilience

RISK GOVERNANCE

Learning Objectives

After completing this reading you should be able to:

- ✓ Explain the **Basel regulatory expectations** for the governance of an operational risk management framework.
- ✓ Describe and compare the **roles of different committees** and the **board of directors** in operational risk governance.
- ✓ Describe the "**three lines of defense**" model for operational risk governance and compare roles and responsibilities for each line of defense.
- ✓ Explain best practices and regulatory expectations for the development of a **risk appetite** for operational risk and for a strong **risk culture**.

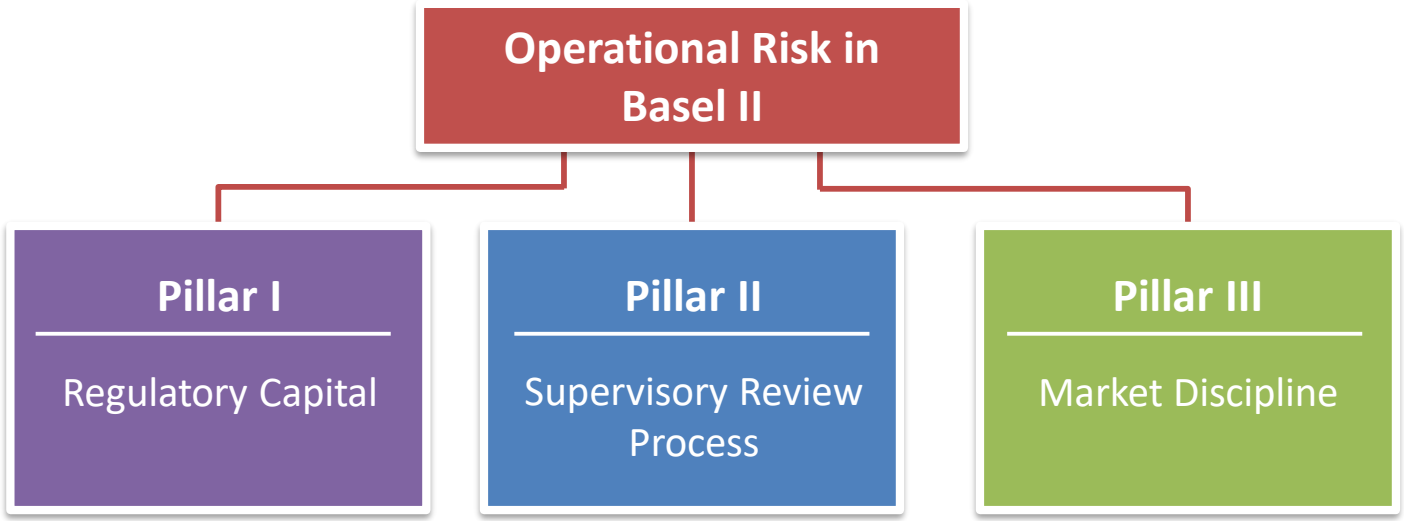
Basel Regulations

LO: Explain the Basel regulatory expectations for the governance of an operational risk management framework.

The Basel Committee defines operational risk in Basel II and Basel III as:

*"The risk of loss resulting from **inadequate** or **failed internal processes**, **people** and **systems** or from external events. This definition **includes legal risk**, but **excludes strategic and reputational risk**."*

Basel II introduced three regulatory pillars:



Basel Regulations

Pillar 1 (Regulatory Capital)

- Ensures that banks maintain **sufficient capital** to absorb unexpected losses.
- Includes mandatory principles of management.
- Recognises that **capital alone** is not **sufficient.**
- Proper **governance and management** are key **to cover the risks** of operational exposure.

Basel Regulations

Pillar 2 (Supervisory Review Process)

- Regulated entities must **self-assess** operational risks not covered in Pillar 1.
  - E.g., **concentration of activities**, **compliance exposure**, **governance/management gaps, aggressive growth strategies.**
- Supervisors use this information to review entity's **risk profile** and **assess capital adequacy.**
- Regulator can then **validate or ame**nd self-assessed capital requirements if necessary.

Basel Regulations

Pillar 3 (Market Discipline)

- Requires financial institutions to **disclose** their financial information and risks regularly.
  - On a **yearly** or **quarterly basis.**
- Encourages **market discipline** and **informs investors** of potential risks associated with **riskier activities.**
- **Safeguards investors** by requiring firms to maintain **adequate capital** to cover increased risk exposure.

Basel Regulations

BCBS Revisions to the Principles for the Sound Management of Operational Risk

01 Culture

- Emphasises on **operational risk awareness** throughout the organization.
- Achieved through **support** and **promotion** by **board and senior management.**

02 ORM Framework

- Identifies, assesses monitors, and controls operational risks.

03 Risk Appetite and Tolerance Statement

- A **clearly defined** statement outlining organization's **risk appetite.**

04 Senior Management Role in ORM Policies

- Must ensure ORM policies are **clearly understood** and **implemented.**
- Through **active oversight**, **continual training programs** and **proper communication channels.**

Basel Regulations

BCBS Revisions to the Principles for the Sound Management of Operational Risk

05 Comprehensive Risk Identification and Assessment

- **Ongoing identification** of all types of potential risks — **both internal and external.**

06 Change Management Process

- A **proactive** change management process for **efficiently** managing changes which could result in **new or modified operational risks.**

07 Regular Monitoring

- **Effective control systems** to continuously **monitor** and report operational risks.

08 Strong Control Environment

- Comprehensive and effective controls, ranging from **corporate governance** structures to **operational policies, processes and procedures.**

Basel Regulations

BCBS Revisions to the Principles for the Sound Management of Operational Risk

09 Robust ICT Management Program

- *A sound ICT management program:*
- Involves establishing a comprehensive framework of **policies, procedures, structures** and other measures.
- Ensures implementation of **effective IT security** measures across all areas of the institution's operations.

10 Business Continuity Plans (BCPs)

- Financial institutions must have a BCP in place.
- Outlines strategies for responding to **disruptions** in **normal operations.**
- Disruptions might be due to **accidents or disasters.**

11 Public Disclosures

- Promote **transparency** for institutions.
- Provide an overview of internal policies addressing **material operational risks factors…**
    - And relevant external developments impacting the entity's ability to attain its strategic goals.

Role of Committees and Board of Directors

LO: Describe and compare the roles of different committees and the board of directors in operational risk governance.

Governance of operational risk is managed by different **committees**.

- They **make decisions based on reports** and other **relevant information** from various **levels of the organization.**

Number and scope of committees put in place to tackle operational risks depends on:

- **Size and complexity** of the organization.

Collegial decisions are taken within these committees.

- Rely on **reports and escalated data** from multiple sources within the firm's decision-making hierarchy.

All committee members can contribute their ideas and analyze reports generated by different departments.

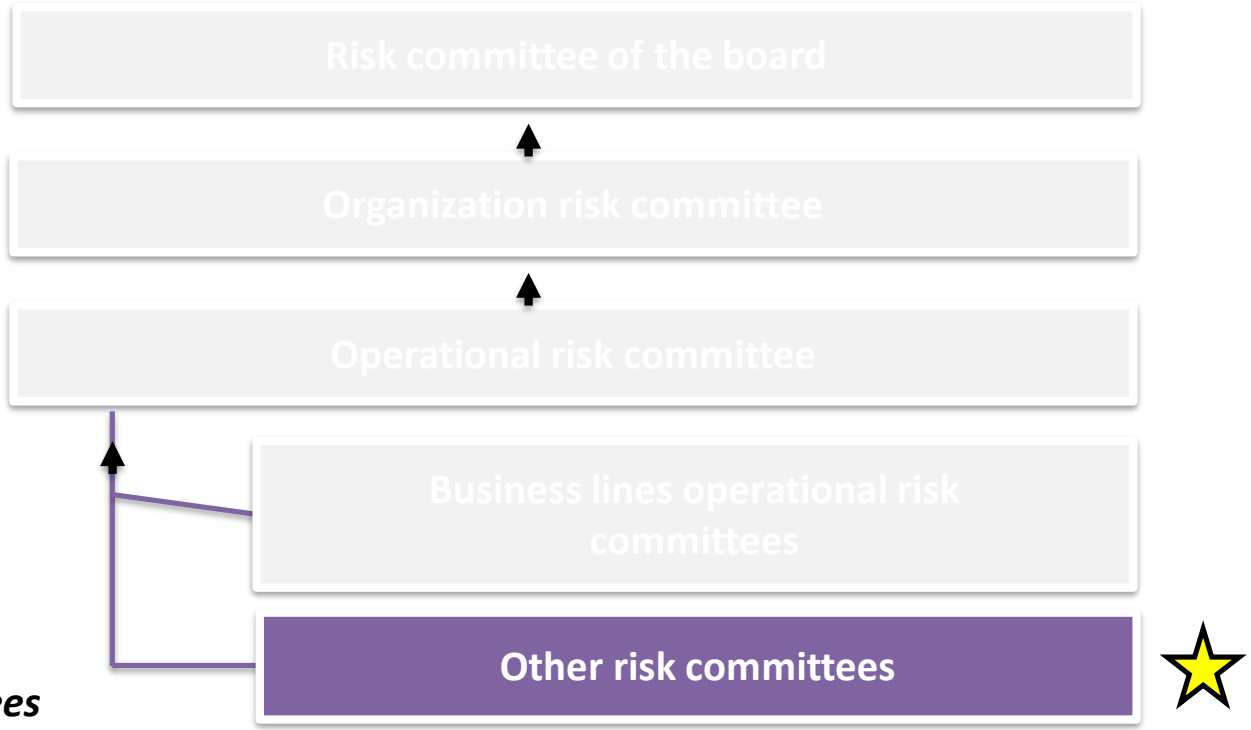
- Ensures an understanding of all areas at risk.

Role of Committees and Board of Directors

The Standard Risk and Committee Structure

Role of Committees and Board of Directors

The Standard Risk and Committee Structure



Other risk committees

- Consists of individuals **within a business line.**
- Tasked with **risk identification** and **evaluation** in a department.
- E.g., credit business line at a bank.
- Deals with **specific issues,** e.g., employee fraud, external fraud, and credit authorization controls.

Role of Committees and Board of Directors

The Standard Risk and Committee Structure

Business line operational risk committee:

- **Reviews reports** from departmental committees.
- **Issues directives.**
- **Escalates** major issues to the operational risk committee.

Role of Committees and Board of Directors

The Standard Risk and Committee Structure

Operational risk committee:

- **Reviews reports** detailing the risk status at the **business line level.**
- **Escalates significant issues**, or those **exceeding** predetermined limits.

Role of Committees and Board of Directors

The Standard Risk and Committee Structure

Organizational operational risk committee:

- **Oversees, manages, monitors, and reports the consolidated picture** to the board risk committee.

Role of Committees and Board of Directors

The Standard Risk and Committee Structure

Board risk committee

- **Oversees** all operational risk.
- Makes **recommendations to the full board** on risk-based decisions, risk exposure, and risk management.

The Three Lines of Defense

LO: Describe the "three lines of defense" model for operational risk governance and compare roles and responsibilities for each line of defense.

1st Line of Defense

- Front-line employees (risk owners).
- Oversee business processes.
- Ensure adherence to **risk management policies** and **frameworks.**

2nd line of defense

- Independent corporate operational risk management function (CORF).
- Oversee activities and behavior of the business lines.

3rd line of defense

- **Provides assurance** on alignment with policy objectives.
- Focuses on ensuring reliable evidence for compliance with **applicable laws, regulations and internal policies.**

Risk Appetite Risk and a Strong Risk Culture

LO: Explain best practices and regulatory expectations for the development of a risk appetite for operational risk and for a strong risk culture.

Regulatory Guidance on Risk Appetite for Operational Risk

- Essential for board members to **understand their role in defining acceptable risk levels.**
  - **Risk appetite** - Amount of risk an organization is willing to take to **achieve its strategic objectives.**
- Crucial to **consider both financial and non-financial risks when determining the risk appetite.**
- Board should develop a **clear framework** for **assessing** and **limiting operational risk.**
  - **Regularly review** and **update** this framework to ensure relevance.
- **Historical data, current trends, industry standards, legal requirements, and internal policies** should be considered **when developing this framework.**

Risk Appetite Risk and a Strong Risk Culture

Regulatory Guidance on Risk Appetite for Operational Risk

- Should include a **clear definition of what constitutes acceptable levels of risk**.
  - Should be established and communicated to all stakeholders and..
  - **Documented** in the policies and procedures.
- Risk appetite should be **regularly reviewed and adjusted as needed**.
  - Should consider **severity, probability,** and **impact of potential risks**.
- Organizations should establish **clear guidelines** for **risk-appetite assessment.**
  - Ensures **consistency** and **compliance** with regulatory standards.
- Organizations are encouraged to use tools such as **key risk indicators (KRIs), stress tests, scenario analysis…**
  - To **better assess exposure to current and future threats.**

FRM Part II

Operational Risk And Resilience

RISK GOVERNANCE

Learning Objectives Recap:

- ✓ Explain the **Basel regulatory expectations** for the governance of an operational risk management framework.
- ✓ Describe and compare the **roles of different committees** and the **board of directors** in operational risk governance.
- ✓ Describe the "**three lines of defense**" model for operational risk governance and compare roles and responsibilities for each line of defense.
- ✓ Explain best practices and regulatory expectations for the development of a **risk appetite** for operational risk and for a strong **risk culture**.