Principles for the Sound Management of Operational Risk

完善的操作风险管理的基本原则

Operational Risk Governance

- The Basel Committee on Banking Supervision defines operational risk as:
  - *" the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."*
  - The committee states that the definition excludes **strategic** and **reputational risks** but includes *legal risks*.
- Sound operational risk management practices cover governance, the risk management environment, and the role of disclosure. Operational risk management must be fully integrated into the overall risk management processes of the bank.
- The three common "*lines of defense*" employed by firms to control operational risks are:
  1. **Business line management**. Business line management is the first line of defense. Banks now, more than ever, have multiple lines of business, all with varying degrees of operational risk. Risks must be identified and managed within the various products, activities, and processes of the bank.
  2. **An independent operational risk management function**.
  3. **Independent reviews of operational risks and risk management**. The review may be conducted internally with personnel independent of the process under review or externally.

Corporate Operational Risk Function(CORF)

- The bank's specific business lines monitor, measure, report, and manage operational and other risks. The corporate operational risk function (CORF), also known as the corporate operational risk management function, is a functionally independent group that complements the business line' risk management operations.
- The CORF is responsible for designing, implementing, and maintaining the bank's operational risk framework. Responsibilities of the CORF may include:
  - *Measurement of operational risks.*
  - *Establishing reporting processes for operational risks.*
  - *Establishing risk committees to measure and monitor operational risks.*
  - *Reporting operational risk issues to the board of directors.*
- Larger, more complex banking institutions will typically have a more formalized approach to the implementation of the lines of defense against operational risks, including the implementation of the CORF.

Principles of Operational Risk Management

1. The maintenance of a **strong risk management culture** led by the bank's board of directors and senior managers.
2. The operational risk framework must be **developed and fully integrated into the overall risk management processes** of the bank.
3. The board should **approve the periodically review** the framework.
4. The board must identify the types and levels of operational risks the bank is willing to assume as well as approve **risk appetite** and **risk tolerance statements**.
5. Consistent with the bank's risk appetite and risk tolerance, senior management must **develop a well-defined governance structure** within the bank.
6. Senior management must **understand the risks, and the incentives related to those risks, inherent in the bank's business lines and processes**.

Principles of Operational Risk Management

7. New lines of business, products, processes, and systems should require an **approval process that assesses the potential operational risks**.
8. **A process for monitoring operational risks and material exposures to losses** should be put in place by senior management and supported by senior management, the board of directors and business line employees.
9. Banks must put strong **internal controls**, **risk mitigation**, and **risk transfer strategies** in place to manage operational risks.
10. Banks must have plans in place to survive in the event of a major business disruption. **Business operations must be resilient (**富有弹性的**)**.
11. Banks should make **disclosures** that are clear enough that outside stakeholders can assess the bank's approach to operational risk management.

The Role of the Board and Senior Management

- With respect to *Principle 1*, the board of directors and/or senior management should:
  - **Provide a sound foundation for a strong risk management culture** within the bank.
  - **Establish a code of conduct (or ethics policy) for all employees** that outlines expectations for ethical behavior.
  - **Provide risk training** throughout all levels of the bank.
- With respect to *Principle 2*, the board of directors and/or senior management should:
  - **Thoroughly understand both the nature and complexity of the risks** inherent in the products, lines of business, processes, and systems in the bank.
  - Ensure that the **Framework is fully integrated in the bank's overall risk management plan** across all levels of the firm (i.e., business lines, new business lines, products, processes, and/or systems).

The Role of the Board and Senior Management

- With respect to *Principle 3*, the board of directors and/or senior management should:
  - **Establish a culture and processes** that help bank managers and employees understand and manage operational risks.
  - **Regularly review the Framework**.
  - **Provide senior management with guidance** regarding operational risk management and approve policies developed by senior management aimed at managing operational risk.
  - Ensure that the Framework is subject to **independent review**.
  - **Ensure that management is following best practices** in the field with respect to operational risk identification and management.
  - **Establish clear lines of management responsibility** and establish strong internal controls.

The Role of the Board and Senior Management

- With respect to *Principle 4*, the board of directors and/or senior management should:
  - **Consider all relevant risks** when approving the bank's risk appetite and tolerance statements. The board must also consider the bank's strategic direction. The board should approve risk limits and thresholds.
  - **Periodically review** the risk appetite and tolerance statements.
- With respect to *Principle 5*, the board of directors and/or senior management should:
  - **Establish systems to report and track operational risks** and maintain an effective mechanism for resolving problems.
  - 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 responsible for market, credit, liquidity, interest rate, and other risks and with those procuring outside services, such as insurance or outsourcing.
  - Ensure that CORF managers should have **sufficient stature (**威望，声望**)** in the bank, commensurate with(与…相当) market, credit, liquidity, interest rate, and other risk managers.
  - Ensure that the staff is **well trained in operational risk management**.
  - Develop a **governance structure of the bank that is commensurate with the size and complexity** of the firm.

The Role of the Board and Senior Management

- With respect to *Principle 6*, the board of directors and/or senior management should:
  - **Consider both internal and external factors** to identify and assess operational risk.
- With respect to *Principle 7*, the board of directors and/or senior management should:
  - **Maintain a rigorous approval process for new products and processes**.
  - **Thoroughly review new activities and product lines**.
- With respect to *Principle 8*, the board of directors and/or senior management should:
  - **Continuously improve the operational risk reporting**.
  - **Ensure that operational risk reports are timely**.
    - ✓ Banks should have sufficient resources to produce reports during both stressed and normal market conditions. Reports should be provided to the board and senior management.

The Role of the Board and Senior Management

- With respect to *Principle 9*, the board of directors and/or senior management should:
  - **have a sound internal control system.**
    - ✓ Banks may need to transfer risk (e.g., via insurance contracts) if it cannot be adequately managed within the bank.
- With respect to *Principle 10*, the board of directors and/or senior management should:
  - **Establish continuity plans to handle unforeseen disruptive events** (e.g., disruptions in technology, damaged facilities, pandemic illnesses that affect personnel, and so on).
  - **Periodically review continuity plans**.
- With respect to *Principle 11*, the board of directors and/or senior management should:
  - **Write disclosures** such that stakeholders can assess the bank's operational risk management strategies.
  - **Disclosures should be consistent** with board of directors and senior management risk management procedures.

Operational Risk Management Framework

- The operational risk management framework must define, describe, and classify operational risk and operational loss exposure.
- The framework must be documented in the board of directors' approved policies.
- Framework documentation, which is overseen by the board of directors and senior management, should:
  - Describe reporting lines and accountabilities (责任) within the governance structure used to manage operational risks.
  - Describe risk assessment tools.
  - Describe the bank's risk appetite and tolerance.
  - Describe risk limits.
  - Describe the approved risk mitigation strategies (and instruments).
  - With respect to inherent and residual risk exposures, describe the bank's methods for establishing risk limits and monitoring risk limits.
  - Establish risk reporting processes and management information systems.
  - Establish a common language of operational risk terms to create consistency of risk identification and management.
  - Establish a process for independent review of operational risk.
  - Require review of established policies and procedures.

Tools for Identifying and Assessing Operational Risk

- Tools that may be used to identify and assess operational risk include:
  - **Business process mappings**, which do exactly that, map the bank's business processes. Maps can reveal risks, interdependencies among risks, and weaknesses in risk management systems.
  - **Risk and performance indicators** are measures that help managers understand the bank's risk exposure. There are *Key Risk Indicators* (KRIs) and *Key Performance Indicators* (KPIs).
  - **Scenario analysis** is a subjective process where business line managers and risk managers identify potential risk events and then assess potential outcome of those risks.
  - **Measurement** involves the use of outputs of risk assessment tools as inputs for operational risk exposure models. The bank can then use the models to allocate economic capital to various business units based on return and risk.

Tools for Identifying and Assessing Operational Risk

- **Audit findings** identify weaknesses but may also provide insights into inherent operational risks.
- **Analysis of internal operational loss data**. Analysis can provide insight into the causes of large losses. Data may also reveal if problems are isolated or systemic.
- **Analysis of external operational loss data** including gross loss amounts, dates, amount of recoveries and losses at other firms.
- **Risk assessments**, or *risk self assessments* (RSAs), address potential threats. Assessments consider the bank's processes and possible defenses relative to the firm's threats and vulnerabilities.
- **Comparative analysis** combines all described risk analysis tools into a comprehensive picture of the bank's operational risk profile. For example, the bank might combine audit findings with internal operational loss data to better understand the weaknesses of the operational risk framework.

Features of an Effective Control Environment

- An effective control environment must include the following five components:

1. A control environment.
2. Risk assessment.
3. Control activities.
4. Information and communication.
5. Monitoring activities.

Managing Technology Risk and Outsourcing Risk

- **Technology** can be used to mitigate operational risks but it introduces its own risks. The Basel Committee recommends an integrated approach to identifying, measuring, monitoring, and managing **technology risks**. Technology risk management tools are similar to those suggested for operational risk management.

- **Outsourcing** involves the use of third parties to perform activities or functions for the firm. Outsourcing may reduce costs, provide expertise, expand bank offerings, and/ or improve bank services. The board of directors and senior management must understand the operational risks that are introduced as a result of outsourcing.

Example

1. Griffin Riehl is a risk manager at Bluegrass Bank and Trust, a small, independent commercial bank in Kentucky. Riehl has recently read the Basel Committee on Banking Supervision's recommendations for sound operational risk management and would like to put several controls in place. He would like to start with the *three lines of defense* suggested by the committee. Which of the following is not one of the three common "lines of defense" suggested by the Basel Committee for operational risk governance?

   A. Business line management.

   B. Board of directors and senior management risk training programs.

   C. Creating an independent operational risk management function in the bank.

   D. Conducting independent reviews of operational risks and risk management operations.

Example

2. Garrett Bridgewater, a trader at a large commercial bank, has continued to increase his bonus each year by producing more and more profit for the bank. In order to increase profits, Bridgewater has been forced to increase the riskiness of his positions, despite the written risk appetite and tolerance statements provided to all employees of the bank. The bank seems happy with his performance so Bridgewater takes that as a sign of approval of his methods for improving profitability. Which of the following pairs of the 11 fundamental principles of risk management has the bank most clearly violated in this situation?

   A. Principle 1 (a strong risk management culture) and Principle 11 (the bank should make clear disclosures of operational risks to stakeholders).

   B. Principle 2 (develop an integrated approach to operational risk management) and Principle 7 (establish a rigorous approval process for new lines of business).

   C. Principle 3 (approve and review the operational risk framework) and Principle 4 (develop risk appetite and tolerance statements).

   D. Principle 5 (develop a well-defined governance structure) and Principle 6 (understand the risk and incentives related to risk inherent in the bank's business lines and processes).

Example

3. Gary Hampton is providing descriptions of the operational risk management assessment tools, reporting lines, and accountabilities to the board of directors. Hampton is most likely working on:

A. Framework documentation.

B. A corporate operational risk function (CORF) handbook of operations.

C. An outline of the fundamental principles of operational risk management.

D. An open group operational framework diagram.

Example

4. George Mathis works in risk analysis and management at a large commercial bank. He uses several tools to identify and assess operational risk. He has asked several business line managers to identify some risk events that would disrupt business. Each manager has also provided their thoughts on what would happen given worst case operational failures. The risk assessment tool Mathis is most likely using in this case is(are):

A. risk indicators .

B. comparative analysis .

C. scenario analysis.

D. business process mappings.

Example

5. A risk management officer at a small commercial bank is trying to institute strong operational risk controls, despite little support from the board of directors. The manager is considering several elements as potentially critical components of a strong control environment. Which of the following is not a required component of an effective risk control environment as suggested by the Basel Committee on Banking Supervision?

A. Information and communication.

B. Monitoring activities.

C. A functionally independent corporate operational risk function.

D. Risk assessment.

恭祝大家

FRM学习愉快！

顺利通过考试！