Operational and Integrated Risk Management (OR)

The broad areas of knowledge covered in readings related to Operational and Integrated Risk Management include:

- Principles for sound operational risk management
- Enterprise risk management (ERM)
- Risk appetite frameworks and information technology (IT) infrastructure
- Internal and external operational loss data
- Modeling operational loss distributions
- Model risk
- Risk-adjusted return on capital (RAROC)
- Economic capital frameworks and capital allocation
- Liquidity risk:
    - Liquidity adjustments to value at risk (VaR) measures
    - Liquidity risk in financial and collateral markets
    - Repurchase agreements and refinancing
- Failure mechanics of dealer banks
- Stress testing banks
- Regulation and the Basel Accords

"Principles for the Sound Management of Operational Risk"

"Principles for the Sound Management of Operational Risk" (Basel Committee on Banking Supervision Publication, June 2011)

After completing this reading you should be able to:

- Describe the three "lines of defense" in the Basel model for operational risk governance.
- Summarize the fundamental principles of operational risk management as suggested by the Basel committee.
- Evaluate the role of the board of directors and senior management in implementing an effective operational risk structure per the Basel committee recommendations.
- Describe the elements of a framework for operational risk management.
- Identify examples of tools that can be used to identify and assess operational risk.
- Describe features of an effective control environment and identify specific controls that should be in place to address operational risk.
- Describe the Basel committee's suggestions for managing technology risk and outsourcing risk.
- Describe and outline business resiliency and continuity plans for banks under the Basel committee framework.
- Identify and discuss the role of a bank's public disclosures.

Reading note: BIS readings are notoriously text-dense and nearly useless. For example, this reading has multiparagraph definitions of what a supervisor is, including this insight: Supervisors ensure that procedures are followed. This isn't anything in this reading that isn't common sense and is a low priority on exam day.

Learning objective: Describe the three "lines of defense" in the Basel model for operational risk governance.

In the industry practice, the first line of defense is business line management. This means that sound operational risk governance will recognize that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes, and systems for which it is accountable.

A functionally independent corporate operational risk function (CORF) is typically the second line of defense. A key function of the CORF is to challenge the business line's inputs to, and outputs from, the bank's risk management, risk measurement, and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities

The third line of defense is an independent review and challenge of the bank's operational risk management controls, processes, and systems.

Learning objective: Summarize the fundamental principles of operational risk management as suggested by the Basel committee.

Principle 1: The board of directors should take the lead in establishing a strong risk management culture.

Principle 2: Banks should develop, implement, and maintain a framework that is fully integrated into the bank's overall risk management processes.

Principle 3: The board of directors should establish, approve, and periodically review the framework.

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.

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.

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.

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.

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses.

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

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.

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

Learning objective: Evaluate the role of the board of directors and senior management in implementing an effective operational risk structure per the Basel committee recommendations.

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 behavior. 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 organization.

Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur.

The board should establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act.

Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organization. Training that is provided should reflect the seniority, role, and responsibilities of the individuals for whom it is intended.

Learning objective: Describe the elements of a framework for operational risk management.

The fundamental premise of sound risk management is that the board of directors and bank management understand the nature and complexity of the risks inherent in the portfolio of bank products, services, and activities. A vital means of understanding the nature and complexity of operational risk is to have the components of the framework fully integrated into the overall risk management processes of the bank. The framework should be appropriately integrated into the risk management processes across all levels of the organization.

The framework should be comprehensively and appropriately documented in board of directors' approved policies and should include definitions of operational risk and operational loss.

The framework should:

- Identify the governance structures used to manage operational risk, including reporting lines and accountabilities.
- Describe the risk assessment tools and how they are used.
- Describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments.
- Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure.
- Establish risk reporting and management information systems (MIS).
- Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating, and risk management objectives.
- Provide for appropriate independent review and assessment of operational risk.
- Require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

Learning objective: Identify examples of tools that can be used to identify and assess operational risk.

- **Audit findings:** While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors.

- **Internal loss data collection and analysis:** Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure.
- **External data collection and analysis:** External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organizations other than the bank. External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures.
- **Risk sssessments:** In a risk assessment, often referred to as a risk self-assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, Risk Control Self-Assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment.
- **Business process mapping:** Business process mappings identify the key steps in business processes, activities, and organizational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness; they also can help prioritize subsequent management action.
- **Scenario analysis:** Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process.
- **Measurement:** Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return.

Learning objective: Describe features of an effective control environment and identify specific controls that should be in place to address operational risk.

Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations, safeguard its assets, produce reliable financial reports, and comply with applicable laws and regulations. A sound internal control program consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.

Control processes and procedures should include a system for ensuring compliance with policies. Examples of principal elements of a policy compliance assessment include:

- Top-level reviews of progress toward stated objectives.
- Verifying compliance with management controls.
- Review of the treatment and resolution of instances of noncompliance.
- Evaluation of the required approvals and authorizations to ensure accountability to an appropriate level of management.
- Tracking reports for approved exceptions to thresholds or limits, management overrides, and other deviations from policy.

In addition to segregation of duties and dual control, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. Examples of these controls include:

- Clearly established authorities and/or processes for approval.
- Close monitoring of adherence to assigned risk thresholds or limits.
- Safeguards for access to, and use of, bank assets and records.
- Appropriate staffing level and training to maintain expertise.
- Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations.
- Regular verification and reconciliation of transactions and accounts.
- A vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other countermeasures may enable concealment of losses, errors, or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and be subject to careful independent monitoring and review.

Learning objective: Describe the Basel committee's suggestions for managing technology risk and outsourcing risk.

Having automated processes introduces risks that must be addressed through sound technology governance and infrastructure risk management programs.

The use of technology-related products, activities, processes, and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring, and managing technology risks. Sound technology risk management uses the same precepts as operational risk management and includes:

- Governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives.
- Policies and procedures that facilitate identification and assessment of risk.
- Establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk.

- Implementation of an effective control environment and the use of risk transfer strategies that mitigate risk.
- Monitoring processes that test for compliance with policy thresholds or limits.

Management should ensure that the bank has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated, fragmented, and disconnected infrastructure, cost-cutting measures, or inadequate investment can undermine a bank's ability to aggregate and analyze information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth. Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high-growth strategies are initiated, or new products are introduced.

Outsourcing is the use of a third party—either an affiliate within a corporate group or an unaffiliated external entity—to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:

- Procedures for determining whether and how activities can be outsourced.
- Processes for conducting due diligence in the selection of potential service providers.
- Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights.
- Programs for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider.
- Establishment of an effective control environment at the bank and the service provider.
- Development of viable contingency plans.
- Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

Learning objective: Describe and outline business resiliency and continuity plans for banks under the Basel committee framework.

Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfill some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system. To provide resiliency against this risk, a bank should establish business continuity plans commensurate with the nature, size, and complexity of their operations. Such plans should

take into account different types of likely or plausible scenarios to which the bank may be vulnerable.

Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programs, and communication and crisis management programs. A bank should identify critical business operations, key internal and external dependencies, and appropriate resilience levels. Plausible disruptive scenarios should be assessed for their financial, operational, and reputational impact, and the resulting risk assessment should be the foundation for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and—where appropriate—civil authorities.

A bank should periodically review its continuity plans to ensure that contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programs should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.

Learning objective: Identify and discuss the role of a bank's public disclosures.

A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile, and complexity of a bank's operations, and evolving industry practice.

A bank should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors, and controls/mitigates operational risk effectively.

A bank's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.

A bank should have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them.