CHAPTER 2. REGULATORY FRAMEWORK OF OPERATIONAL RISK.

BASEL II.

**2.1 Principles for the Sound Management of Operational Risk and the Role of Supervision**

Sound Practices for the Management and Supervision of Operational Risk (Sound Practices) is a document that was published in February 2003 by the Basel Committee on Banking Supervision (Committee) that articulate a framework of principles for the industry and supervisors. After, in the “2006 International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version” known as “Basel II”, the Committee anticipated that industry sound practice would continue to evolve.

Since then, banks and supervisors have implied their knowledge and experience in implementing operational risk management frameworks (Framework). Loss data collection exercises, quantitative impact studies, and range of practice reviews covering governance, data and modelling issues have also contributed to industry and supervisory knowledge and the emergence of sound industry practice. [[1]](#footnote-1)

Given the changes, the Committee decided that the 2003 Sound Practices paper should be updated to reflect the improved sound operational risk management practices used in the industry. In this document is incorporated the evolution of sound practice and it detail 11 principles covering (1) governance, (2) risk management environment and (3) the role of disclosure. By keeping the paper updated, the Committee upgraded it with specific principles for operational risk management.

A Framework for Internal Control Systems in Banking Organisations (Basel Committee, September 1998) underpins the Committee’s current work in the field of operational risk. The Core Principles for Effective Banking Supervision (Basel Committee, October 2006) and the Core Principles Methodology (Committee, October 2006), both for supervisors, and the principles identified by the Committee in the second pillar (supervisory review process) of Basel II are also important reference tools that banks should consider when designing operational risk policies, processes, and risk management systems. [[2]](#footnote-2) The banks are encouraged by the Supervisors to continue developing more sophisticated tools and practices to face the operational risk.

The Committee believes that the principles mentioned establish sound practices relevant to all banks. The Committee intends that when implementing these principles, a bank will take account of the nature, size, complexity, and risk profile of its activities.

**2.1.2 Role of Supervisors**

Supervisors conduct, directly or indirectly, regular independent evaluations of a bank’s policies, processes and systems related to operational risk as part of the assessment of the Framework. Supervisors ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at a bank. [[3]](#footnote-3)

Supervisor also pursue to ensure that, if the banks are part of a financial group, the procedures and processes are inline to ensure that the operational risk management is appropriated across the group. To achieve this request the cooperation and exchange of information with other supervisors will be necessary.

If there are deficiencies on the supervisory review, should be faced by a range of actions. Depending on the situation the supervisors will use the most suited tool. To ensure that they are receiving the information from the banks, supervisors may will to stablish a reporting mechanism with the bank and external auditors.

Operational risk can be found 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. As a result, sound operational risk management reflects the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems. The Committee desires to promote and improve the effectiveness of operational risk management through the banking system.

Risk management generally covers the process of identifying risks to the bank, measuring exposures to those risks, 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 and reporting to senior management and the board on the bank’s risk exposures and capital positions. Internal controls are typically embedded in a bank’s day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each. [[4]](#footnote-4)

Sound internal governance create the foundation of an effective operational risk management Framework. Though, internal governance issues related to the management of operational risk are likely those met in the management of credit or market risk.

The Committee is seeing sound operational risk governance practices adopted in an increasing number of banks. 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 and.

(iii) an independent review. [[5]](#footnote-5)

Depending on the bank’s nature, size and complexity, and the risk profile of a bank’s activities, the degree of formality of how these three lines of defence are implemented will vary.

As discussed in the Committee’s paper Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, June 2011, independent review includes the following components:

1. Verification of the Framework done on a periodic basis and is conducted by the bank's internal or external audit.
2. Verification activities test: the effectiveness of the overall Framework consistent with policies approved by the board of directors, and test validation processes to ensure they are independent and implemented in a manner consistent with established bank policies.
3. Validation: ensures that the quantification systems used by the bank is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes, and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.

Sound Practices for the Management and Supervision of Operational Risk 3 governance function should be fully integrated into the bank’s overall risk management governance structure.

In the industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise 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 defence, generally complementing the business line’s operational risk management activities. The degree of independence of the CORF will differ among banks. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance, and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines’ inputs to, and outputs from, the bank’s risk management, risk measurement and reporting systems. The CORF should have enough personnel skilled in the management of operational risk to effectively address its many responsibilities. The third line of defence is an independent review and challenge of the bank’s operational risk management controls, processes, and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation, and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review but may also involve suitably qualified external parties. [[6]](#footnote-6)

It's an important characteristic the use of a strong risk culture and good communication among the 3 lines of defence. Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively.

Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures but should also be evaluating whether the Framework meets organisational needs and supervisory expectations.

Given the evolution of operational risk management and the environment’s continuously changing management should ensure that the Framework’s policies, processes, and systems remain sufficiently robust. Improvements in operational risk management will depend on the degree to which operational risk managers’ concerns are considered and the willingness of senior management to act promptly and appropriately on their warnings. [[7]](#footnote-7)

**2.1.2 Fundamental principles of operational risk management:** [[8]](#footnote-8)

As introduced in the biggening of this chapter, we will analyse the evolution of sound practice and the 11 principles covering governance, risk management environment and the role of disclosure.

*Principle 1:* “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”.

While higher is the culture of risk management and ethical business practices, the banks are less likely to face damaging operational risk events and are better positioned to deal whit the potentially events that may occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.

The board must create a code of conduct that reflect clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. It ensures that the bank staff understand the roles and responsibilities and authority to act again risk. Strong and consistent senior management support for risk management and ethical behaviour strongly supports codes of conduct and ethics, compensation strategies, and training programmes.

The compensation policies should be in line to the bank’s statement of risk appetite and tolerance, strategy, and objectives. The proper balance between risk and reward must be found.

Senior management must ensure that a proper level of operational risk training is available at all levels through the organisation. The provided training must be in line with the seniority, role, and responsibilities of the employees.

*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”.

The main goal of sound risk management is that the board of directors and managers understand the nature and complexity of the risk related in the products, services, and activities.

A fundamental 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 organisation.

Sound Practices for the Management and Supervision of Operational Risk including those at the group and business line levels, as well as into new business initiatives’ products, activities, processes, and systems. In addition, results of the bank’s operational risk assessment should be incorporated into the overall bank business strategy development processes.

The Framework must be well documented in the board of directors, and they should approve policies and include definitions of operational risk and loss. If they don’t the effectiveness of the framework will be harm.

**Framework documentation should clearly**[[9]](#footnote-9)**:**

1. identify the governance structures used to manage operational risk, including reporting lines and accountabilities.
2. describe the risk assessment tools and how they are used.
3. 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.
4. describe the bank’s approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure.
5. establish risk reporting and Management Information Systems (MIS).
6. provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives.
7. provide for appropriate independent review and assessment of operational risk.
8. require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs and revised as appropriate.

**Governance:**

*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.”

The board of directors should[[10]](#footnote-10):

1. establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank’s strategies and activities, and develop comprehensive, dynamic oversight and control. An inconsistent taxonomy of operational risk terms may increase the likelihood of failing to identify and categorise risks, or allocate responsibility for the assessment, monitoring, control, and mitigation of risks that are fully integrated into or coordinated with the overall framework for managing all risks across the enterprise.
2. provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management.
3. regularly review the Framework to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes, or systems, including changes in risk profiles and priorities (e.g., changing business volumes).
4. ensure that the bank’s Framework is subject to effective independent review by audit or other appropriately trained parties; and
5. ensure that as best practice evolves management is availing themselves of these advances.

A critical aspect of the operational risk is the strong internal controls, and it must be stablished by the board of directors with clear lines of management responsibility and accountability. The control environment should provide proper independence of duties between operational risk management functions, business lines and support functions.

*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”.

While approving and reviewing the risk appetite and tolerance statement, all the relevant risks, bank’s risk aversion, financial situation and strategic direction must be considered. The risk appetite and tolerance statement should summarise the various operational risk appetites within a bank and ensure that they are steady. Then the board of directors must approve suitable limits for specific operational risks, and an overall operational risk appetite and tolerance. It should be regularly reviewed by the board of directors, considering changes in the environment, materials and activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume, or nature of limit breaches. The board should supervise management adherence to the risk appetite and tolerance statement and provide for appropriate detection and remedy of breaks.

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 the bank’s material products, activities, processes and systems consistent with the risk appetite and tolerance”.

Senior manager is the responsible for creating and keeping robust challenge mechanisms and appropriate problems-solving processes; must include reporting systems, track, and analyse issues to ensure the solving. Banks must be able to prove that the three lines of defence methodology is operating adequately and to clarify how the board and senior management ensure that this approach is implemented and operating in an appropriate way.

Senior management must interpret the operational risk management Framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility, and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank’s risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit’s activity. Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank’s overall risk management programme. [[11]](#footnote-11)

Senior management must guarantee that bank activities are led by staff with the required experience, technical capabilities, and access to resources. The responsible staff for monitoring and applying the compliance with the institution’s risk policy must have independence from the units that they supervise.

A bank’s governance structure should be commensurate with the nature, size, complexity, and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration: [[12]](#footnote-12)

1. Committee structure – Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee report. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country,

business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board’s risk management committee.

1. Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include independent non-executive board members, which is a requirement in some jurisdictions.
2. Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

**Risk Management Environment:**

*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”.

The risk identification and evaluation are important characteristics for an effective operational risk management, it considers internal and external factors. The sound risk assessment allows banks to understand its risk profile and position the risk management resources and strategy in a more effective way.

Examples of tools that may be used for identifying and assessing operational risk include: [[13]](#footnote-13)

1. 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.
2. 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 to obtain a more complete view of their operational risk exposure.
3. 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 organisations 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.
4. Risk Assessments: 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 is considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls is 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.
5. Business Process Mapping: Business process mappings identify the key steps in business processes, activities, and organisational 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 prioritise subsequent management action.
6. Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank’s risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans.
7. 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.
8. 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.
9. Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank’s operational risk profile. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank’s exposure to potential risk events.

The bank must ensure that the internal pricing and performance measurement mechanisms properly consider the operational risk. If isn’t, risk-taking incentives could not be properly aligned with the risk appetite and tolerance.

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”.

A bank’s operational risk exposure is enlarged when a bank participates in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Besides, the level of risk may intensify when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business critical operations. A bank must ensure that its risk management control infrastructure is suitable at origin and that it keeps pace with the rate of growth of products activities, processes, and systems.

A bank must have policies and procedures that report the process for review and approval of new products, activities, processes, and systems. The review and approval process should consider:

1. inherent risks in the new product, service, or activity.
2. changes to the bank’s operational risk profile and appetite and tolerance, including the risk of existing products or activities.
3. the necessary controls, risk management processes, and risk mitigation strategies.
4. the residual risk.
5. changes to relevant risk thresholds or limits.
6. the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process must also ensure that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The application of new products, activities, processes, and systems must be checked to identify any differences to the expected operational risk profile, and to manage any risks.

*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”.

Banks are stimulated to improve the quality of operational risk reporting. A bank must ensure that its reports are comprehensive, accurate, consistent, and actionable across business lines and products. Reports must be adaptable in scope and volume; effective decision-making is obstructed by excessive amounts and scarcity of data.

Reporting must be appropriate, and a bank should be able to produce reports in normal and stressed market conditions. The regularity of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The outcome of the monitoring must be included in regular management and board reports, as must evaluate the Framework performance done by the risk management functionaries. Reports generated by supervisory authorities should also be reported internally to senior management and the board, where requires.

Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making.

**Operational risk reports should include:**

1. breaks of the bank’s risk appetite and tolerance statement and limits.
2. Details of the recent significant internal operational risk events and losses.
3. relevant external events and any possible impact.

It’s necessary to analyse periodically the data capture and risk reporting processes to continuously enhancing risk management performance and advanced risk management policies, methodologies, and practises.

*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”.

A sound internal control programme consists of five components that are essential to the risk management process: 1) control environment; 2) risk assessment; 3) control activities; 4) information and communication; 5) monitoring activities.

An effective control environment also requires proper separation of duties. Assignments that create conflicting duties for individuals or a team without double controls may enable cover-up of losses, errors, or other inappropriate actions. Consequently, areas of potential conflicts of interest should be identified, minimised, and be subject to careful monitoring and review.

Effective use and sound implementation of technology can contribute to the control environment. 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.

Management must ensure that the technology infrastructure meets the business requirements by providing sufficient capacity for the activity levels in normal and stress situation, ensuring data and system integrity, security, and availability; and supporting integrated.

*Technology infrastructure refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environments.*

Mergers and acquisitions resulting in divided and separated infrastructure, cost-cutting measures or scarce investment can challenge a bank’s ability to aggregate and analyse 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 must elaborate an appropriate capital’s investment or always provide for a robust infrastructure, before mergers are completed, high growth strategies are started, or new products are added.

*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”.

Banks are exposed to disrupting events, that may be severe and result in an incompetence to achieve some business obligations. Incidents that harm the bank’s facilities, telecommunication or information technology infrastructures can result in significant financial losses to the bank. A bank must establish business plans in accordance with the nature, size, and complexity of their operations to provide resiliency against the risk. The plans should consider different types of possible scenarios in which the bank may be vulnerable.

Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes. A bank should identify critical business operations, key internal and external dependencies, and appropriate resilience levels.

Possible disrupting circumstances must be evaluated for their financial, operational, and reputational impact, and the result of the risk assessment must be the basis 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, and suppliers.

To ensure that the contingency strategies remain consistent with the current operations, risk and threats, resiliency requirements and recovery priorities, the bank should execute periodically reviews on its continuity plans.

A bank should participate in stress testing with key service providers. The results must be reported to the directives and managers.

**Role of Disclosure**

*Principle 11:* “A bank’s public disclosures should allow stakeholders to assess its approach to operational risk management”.

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 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. [[14]](#footnote-14)

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. [[15]](#footnote-15)

1. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-1)
2. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-2)
3. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-3)
4. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-4)
5. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-5)
6. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-6)
7. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-7)
8. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-8)
9. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

   ‌ [↑](#footnote-ref-9)
10. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-10)
11. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-11)
12. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-12)
13. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-13)
14. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-14)
15. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-15)