6

Operational Risk Management

Principles, Practice and Preparedness among Indian Banks

Richa Verma Bajaj

6.1. Introduction

The rising frauds (e.g. rogue trading, cyber and phishing attacks), infrastructure failures (e.g. information technology, terrorist attacks), and legal and regulatory risks (e.g. fines, penalty) have made it essential for banks and financial institutions to manage these risk, under the gamut of operational risk. Basel Committee (2006, paragraph 644) defines this risk 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." This definition focuses on causes of operational losses to control their future occurrences. Unlike, credit and market risk, operational risk is intrinsic in all business activities and processes (Hoffman, 1998 and Curry, 2012[1]). Post the release of COSO's (Committee of Sponsoring Organization) Internal Control-Integrated Framework in 1992 and the Sarbanes-Oxley Compliance Act in 2002, it became important for the banks to make operational risk, as an important part of risk management framework, which comprises of credit risk, market risk, operational risk and other Pillar II risk. It is interesting to note that operational risk constitute about 9-13 percent of the total risk pie (Ames et al, 2015).

The head of OCC, Thomas Curry, during his speech (2012) said that, "bank supervisors are seeing, operational risk eclipse credit risk as a safety and soundness challenge". This risk is mainly on the cost side, unlike credit risk (Alexander, 2003) and it destroys value for all stakeholders, Crouhy et al. (1998) and even run on the bank (Alexander, 2003). Moreover, the capital requirement for operational risk at large US banks is often observed higher than the capital requirement for market risk, (Fontnouvelle et al, 2006). According to Reserve Bank of India (RBI)'s, Systematic Risk Survey (SRS), even in Indian financial system operational risk has increased (RBI, 2022).

The Basel committee and RBI have suggested various top down[2] approaches like Basic Indicator Approach (BIA), The Standardised Approach (TSA) and Alternative Standardised Approach (ASA) and Bottom-up[3] approach for the computation of operational risk capital charges (ORCCs), i.e. Advanced Measurement Approach (AMA) through Basel II. Post the global financial crises, the Basel committee (2014) assessed the effectiveness of these Basel II approaches and found that these approaches are ineffective to assess the true operational risk profile of the banks. This is mainly on account of the method of exposure indicator estimation used in top-down approaches and the subjectivity involved in bottom-up and model based approach, like AMA. Rebonato (2007) argued that risk can be managed effectively using a simpler methodology, than following a quantitative approach. Same argument was put forward by Herring

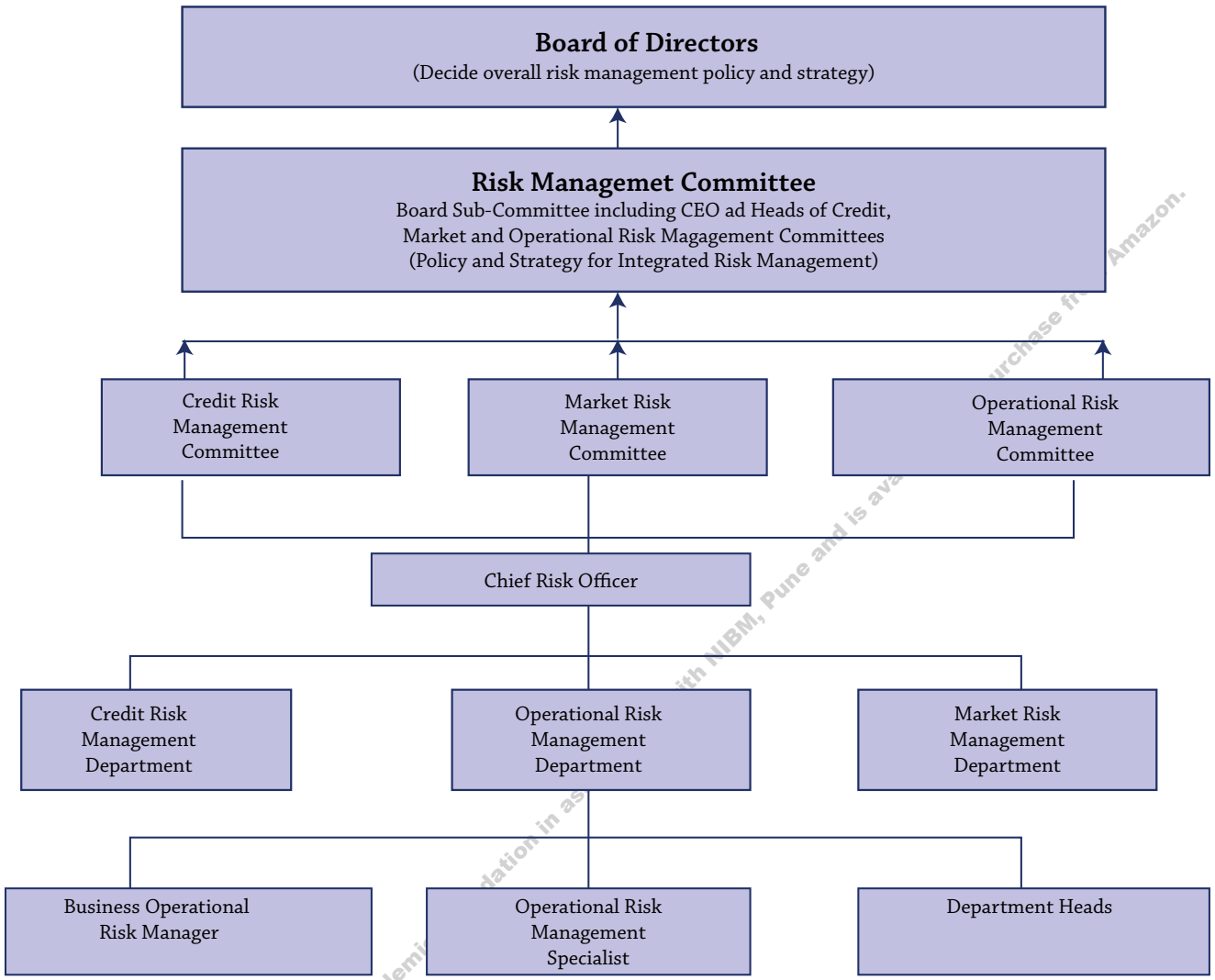
1. https://www.occ.gov/news-issuances/speeches/2012/pub-speech-2012-77.pdf

2. Regulatory driven methodology.

3. Bank-driven inputs for capital estimation.

FIGURE 6.1

Typical Organizational Structure for Operational Risk Management



Source: rbi.org.in

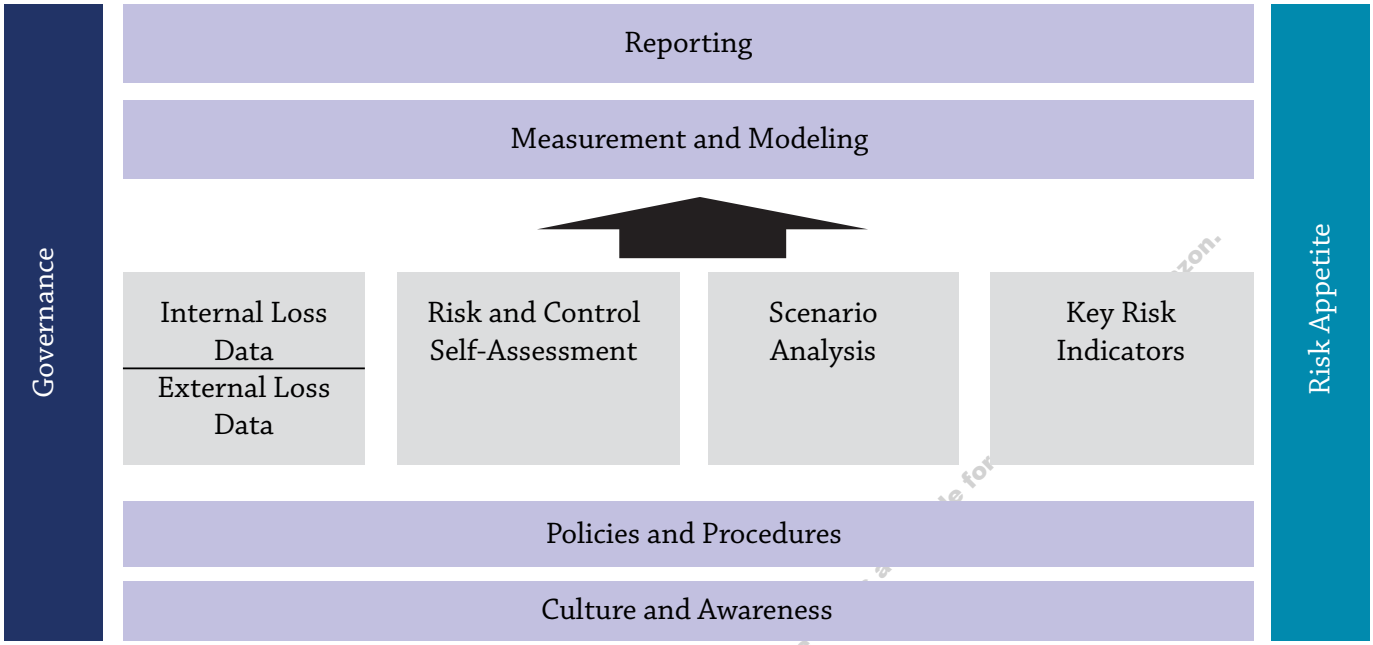
(2002). Currie (2004) suggested simultaneous use of top-down and bottom-up approaches to estimate capital charges for operational risk. Given this, in an effort to strengthen the soundness standards and to reduce risk weighted assets variability, the Basel Committee introduced Standardised Approach, a non-model based methodology of operational risk capital charge estimation through, Basel III - post crises reforms in December, 2017 (Basel 2017). This is both top-down and bottom up in nature. In response, Reserve Bank of India issued the "Master Direction on Minimum Capital Requirement for Operational Risk" in June 2023[4].

Banks are facing numerous implementation challenges to comply with this changed Basel methodology and to implement tools like operational risk event database, risk and control self-assessment (RCSA), key risk indicators (KRIs) and scenario analysis, for operational risk assessment and management. Banks are also expected to abide by the Prin-

4. https://rbidocs.rbi.org.in/rdocs/content/pdfs/DraftMDMCRO15122021.pdf

FIGURE 6.2

Operational Risk Management Framework (ORMF)



Source: Girling, P. X. (2013). Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework. John Wiley & Sons.

ciples of Sound Management of Operational Risk -PSMOR (2003, revised and updated in 2011 and 2021) (Basel, 2021). These principles provide detailed guidelines to banks to develop an effective operational risk management framework (ORMF). A comprehensive Operational Risk Management Framework (ORMF), includes an organisational structure for operational risk management comprising of the Board of Directors, the Risk Management Committee (RMC) of the Board and the Operational Risk Management Committee (ORMC). The organisation structure as suggested by RBI (2005), through its "Guidance Note on Operational Risk Management" is given in Figure 6.1.

In addition to governance structure, the ORMF, as presented in Figure 6.2, covers risk culture, risk appetite, operational risk policies and processes, tools of operational risk assessment, measurement and reporting. The cases of: (i) significant loss in one of the largest bank in Nigeria[5], The Diamond Bank[6], because of weak governance structure, poor risk culture and the board's inability to determine bank's risk appetite; (ii) the high frequency and severity of operational losses, during sub-prime crises, because of poor management action and control (ALGO First Research Database); and (iii) governance failure in India in ICICI[7], Yes[8] bank etc. call for an urgent need for bank and financial institutions to have in place strong ORMF, governance structure and risk culture for effective management of operational risk. Australian Prudential Regulatory Authority (APRA), defines risk culture as, "an entity's attitudes and behaviours towards risk management"[9]. The Institute of International Finance[10], cited the cultural failures as the major reason behind the credit and liquidity crises of 2008. In the similar direction, the white paper by Mckinsey and Levy[11] cited

5. https://disclosures.ifc.org/project-detail/SPI/9923/diamond-bank
6. https://guardian.ng/business-services/how-intrigues-lapses-losses-caused-diamond-banks-fall/
7. https://blog.ipleaders.in/corporate-governance-failure-in-icici-bank-ltd/
8. https://www.elearnmarkets.com/school/units/corporate-governance/landmark-corporate-governance-failures-in-india-yes-bank
9. https://www.apra.gov.au/transforming-risk-culture-observations-from-apra%E2%80%99s-pilot-survey
10. https://www.moneylife.in/article/risk-culture-in-indias-financial-sector-a-long-way-to-go/63022.html
11. Taking control of Organizational Risk Culture,

cultural flaws as the reason behind corporate failures like Societe Generale and Enron.

Given this background, it is important and urgent for banks and financial institutions to follow best practices as far as implementation of ORMF, governance structure, risk culture, tools for operational risk assessment and management etc. in line with PSMOR (2021). In order to gauge the level of preparedness of the banks in India with respect to below mentioned principles (12 as per Basel), the disclosures and annual report of all 12 public sector and 21 private sector banks were looked at, as on March 2022. The Basel Committee and RBI, provide directives to banks regarding reporting and disclosures, through Pillar III[12] i.e. Market Discipline, whereas Pillar I and II, focuses on capital estimation methodology. Pillar III, consists of various disclosures on the capital adequacy and risk management framework. It enables the market participants' information relating to best practices followed by the banks.

This chapter is divided into four sections. An introduction to operational risk management and Principles of Sound Management of Operational Risk (PSMOR) has been given in this section. The principles are detailed in Section 6.2. Results are discussed in Section 6.3. Section 6.4 concludes.

6.2. Principles of Sound Management of Operational Risk (PSMOR), Basel (2021)

The focus of each principle under PSMOR is briefed below:

Principle I Risk Management Culture: *"The board of directors should take the lead in establishing a strong risk management culture, implemented by senior management. The board of directors and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behaviour, and ensure that staff receives appropriate risk management and ethics training",* (Basel, 2021).

The criteria to observe preparedness of banks with respect to this principle is:

- Board of director's Responsibility for establishing the Risk Management Culture in bank
- Senior Management's Responsibility for implementing Risk Management Culture in bank
- The corporate culture focuses on standards of professional behaviour, training for staff on risk management and ethics. As, stronger the risk management culture, lower the operational risk
- Bank to develop policy to deal with conduct risk - code of conduct or an ethics policy – may be different for specific positions (treasury dealers, senior management) in bank
- Frequent review of these policies
- Setting up of Ethics Committee or Board Level Committee to oversee the implementation of code of conduct policy in bank
- Disclosure of such committees on Bank's website
- Ensure thorough understanding of staff about their roles and responsibilities for risk management
- Linkage of bank's compensation policy with risk appetite of the bank
- Mandatory training programmes for business unit heads, head of Internal controls and senior management on operational risk

Principle 2: Develop, Implement and Maintain Operational Risk Management Framework (ORMF): *"Banks should develop, implement and maintain an operational risk management framework that is fully integrated into the bank's overall risk management processes. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

12. RBI (2015), Master Circular – Basel III Capital Regulations

- Development of Operational Risk Management Framework (ORMF) in line with size and complexity of bank's operations and document the same
- Board of Director and Senior Management to have awareness about operational risk profile of the bank, i.e. risk intrinsic in business products, services, activities, processes and systems
- Frequent review of the bank's operational risk profile
- The understanding of ORMF by the business units, i.e. First Line of Defence (LoD)
- The training of ORMF to Business units by Corporate Operational Risk Management (CORM) team, i.e. Second Line of Defence
- Review of ORMF by Third Line of Defence
- Linkage of bank's operational risk assessment to bank's overall business strategy development process
- Assessment of Risk in New Product - higher the risk, higher the monitoring
- Clear definition of Operational Risk or Operational Loss in bank
- Frequent review and revision of Operational Risk Management Policy

Governance

Principle 3: Board of Directors approve and review the ORMF: *"The board of directors should approve and periodically review the operational risk management framework, and ensure that senior management implements the policies, processes and systems of the operational risk management framework effectively at all decision levels",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

- Board of Directors approve policy[13] for operational risk management in the bank
- Ensure alignment of Bank's ORMF with PSMOR Principles
- Frequent review of ORMF to ensure best practices in designing ORMF in the bank
- Ensure effectiveness of bank's ORMF in controlling risks emanating from external environment, risk associated with new products, activities, process or system
- Review of all material risks the bank is exposed to
- Conduct of the independent review of ORMF – either by third line of defence or third party from external sources
- Board of Director's responsibility for establishing Internal Controls in bank, like lines of reporting, compliance, separation of duties between operational risk function, business units and support function (like, outsourcing/business continuity planning)
- Assessment of effectiveness of abovementioned controls
- Frequent review of the effectiveness of controls by Board of Directors

Principle 4: Board of Directors approves Risk Appetite and Tolerance Statement[14]: *"The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

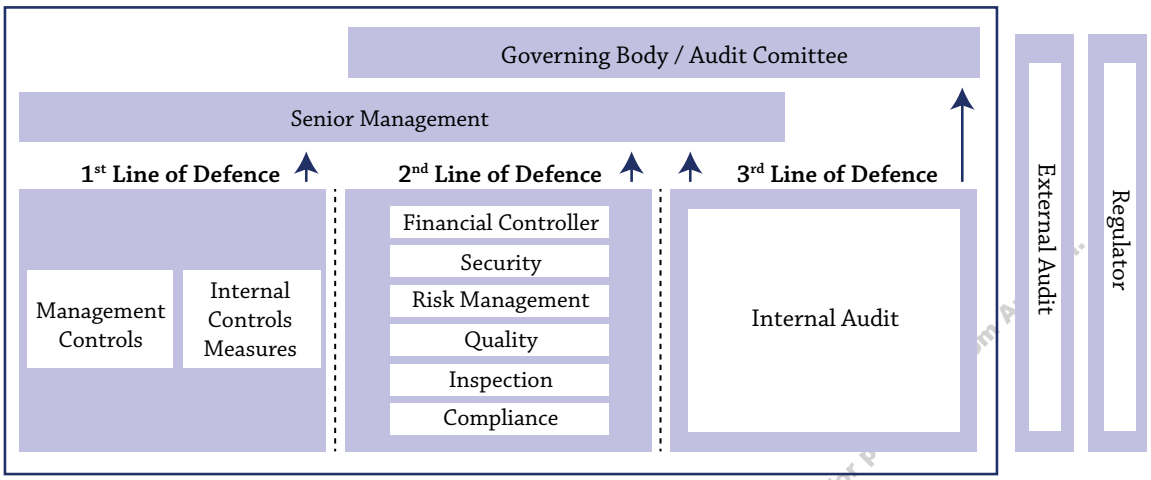
- Bank to have Risk Appetite and Tolerance statement (RATS) for operational risk
- Clearly understandable by all stakeholders
- Board of directors approves and review this statement
- Linkage of RATS with long-term and short term financial plan, strategic plans or regulatory requirements in bank

13. The focus of the policy is on identification, assessment/measurement, monitoring and management of operational risks associated with banking activities.

14. Financial Stability Board defines risk appetite, "as an aggregate level and types of risk an organisation is willing to assume within its risk capacity to achieve its strategic objectives and business plan" and risk tolerance refer to "as the acceptable variability around the risk limit", by the Central Bank of Ireland

FIGURE 6.3

Bank's ORMF Representing Three Lines of Defence



Source: CIAA website

- Risk Appetite Statement can be Qualitative or Quantitative in nature
- Ensure proper flow of risk statement to business units
- Stress testing of the statement
- Clearly defined acceptable level of limit breach by top management and remediation of breaches
- Should consider external environment

It is important for banks to undertake business activities in line with risk appetite statement approved by the board. It should take into account (i) current and expected change in external environment; (ii) material increase in business volume; (iii) quality of control environment; (iv) effectiveness of risk management; (v) mitigation strategy; (vi) loss experience; (vii) nature of limit breaches. It is interesting to note that only 26 percent of companies have a defined Risk Appetite Statement, (National Association of Corporate Directors[15]).

Principle 5: Senior Management develops Governance Structure: *"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 bank's risk appetite and tolerance statement"*, (Basel, 2021).

The Senior Management establishes roles and responsibilities for three lines of defence. For an effective operational risk governance, the bank need strong operational risk culture and clear communication between the three lines of defence. These three lines of defence (Figure 6.3) are defined below:

The first line of defence is the business line responsible for identification and management of operational risk, inherent in bank's products, activities, etc, in their respective units. They should have adequate resources and training to ensure awareness of operational risk

The Second line of defence is an independent Operational Risk Management Department (ORMD), which is responsible for implementing the ORMF across the Bank. They review the effectiveness of governance, risk management and internal controls within the Bank. The compliance function within the bank is also

15. https://www.nacdonline.org/analytics/

part of second line of defence. This line independently review, challenge and oversight the activities conducted by the first line and periodically report the same to the Board.

The third line of defence is Internal Audit. They are responsible for independent review of operational risk management framework, as they are not involved in development and implementation of ORMF.

The criteria to observe preparedness of banks with respect to this principle is:

- Ensures Senior Management's responsibility for development of governance structure i.e. Three Lines of Defence within the bank
- Senior Management in line with board approved ORMF, develops policies and procedures for operational risk in bank
- Senior Management defines roles and responsibilities at Business Unit level
- Bank to have a policy to define inter-departmental i.e, credit, market and operational risk, co-ordination and communication
- Bank to develop policies for obtaining external services like insurance or outsourcing to reduce severity of operational losses
- Ensure stature of head, Corporate Operational Risk Function – CORF. It should be at par with other risk functions such as credit/market and liquidity risk
- Ensure necessary experience and technical capabilities of the individual heading the department
- Sufficient experience of the staff required to enter the department
- Operational Risk head to look after compliance of risk policy in the bank
- Appropriate frequency of meeting of risk committee in bank and bank to have committee structure in line with bank's size
- Ensure proper composition of such committees

Risk Management Environment

Principle 6: Identification and Assessment of Operational Risk: *"Senior management should ensure the comprehensive 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",* (Basel, 2021).

The only way to manage operational risk is to identify it properly, Bocker and Kluppelberg (2005). Banks can consider following tools (Operational Risk Event Data, Self-Assessment, Event Management, Control Monitoring and assurance framework, Metrics) for risk identification and assessment. The criteria to observe preparedness of banks with respect to this principle is:

- Senior Management responsibility to ensure comprehensive identification and assessment of Operational Risk in bank
- List tools consider for risk identification and assessment
- Bank to identify both external and internal factors impacting bank's operational risk profile
- Bank to have comprehensive event database
- Document the external sources to collect event data in bank
- Provides information about losses that are common across industry
- Ensure business process, activities, organization function wise self-assessment with associated risk and control weakness
- Conduct Business Process Mapping exercise in bank
- Maintenance of Risk and Control Register (RCR) in bank
- Oversight of RCR by senior management, risk committee and Board of Directors
- Implementation of event management approach to recognise new risks, understand the primary causes and control weakness and control occurrence of similar event

- Bank to have control monitoring and assurance framework in place to identify effective controls to capture risks and operate effectively
- Segregate controls, as preventive and detective in bank
- List different controls across different business areas
- Develop Metrics[16] using event data and RCSA to monitor OR exposure
- Fix thresholds/limits for these metrics and monitor them frequently
- Conduct Scenario Analysis (SA) to assess magnitude of loss from potential events
- Senior Management, Business Management, Senior OR Staff, Functional areas like compliance, HR, IT Risk management may participate in conducting SA workshop
- Collect inputs for scenario analysis from internal loss data, external loss data, risk and control self-assessment, metrics, root cause analysis, process framework, etc
- Link scenario analysis process with disaster recovery and business continuity plan (BCP) in bank in order to test operational resilience
- Bank to have separate governance framework in place for scenario analysis, which is subject to separate independent review
- Conduct Benchmarking and Comparative Analysis – may be internal or external benchmarking
- Integrate[17] different risk measurement and management tools within bank
- Benchmarking or peer comparison of bank's metrics with other banks
- Robust verification and validation procedures
- Factor them into internal pricing and performance measurement

Principle 7: Comprehensive Change Management Process: *"Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and adequately articulated between the relevant lines of defence",* (Basel, 2021).

It is important for ORMF of the bank to address the operational risk exposure related to new activities, new product and services, entry into unfamiliar market or jurisdictions, new or modified business process, technology system, geographically distant businesses etc. The criteria to observe preparedness of banks with respect to this principle is:

- Ensure Change Management Process in bank
- The first Line of Defence performs assessment of New Products and initiatives
- Second Line of Defence challenges and review the assessment
- Ensure involvement of various control groups, like Finance, Compliance, Legal, Business, ICT and Risk Management in assessment in bank
- Bank to have policy and committee to assess inherent risk, control risk and residual risks in new product, activities, process, systems etc.
- Bank to strengthen their Human and IT infrastructure before changes are introduced in the bank
- Maintain centralized record of all products and services (including the outsourced one) to aid scrutiny of changes in bank

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

16. Metrics provides information about Event Counts, Model Results, Early Warning Signals to management about performance of business and control environment, risk profile
17. Comparison of results generated from scenario analysis with the output generated through analysis of ILD and ELD

of operational risk", (Basel, 2021). The coverage on Operational Risk Reporting includes: Operational risk event, control deficiency, process inadequacy, non-compliance and breach with operational risk appetite and tolerance statement (RATS), discussion on key or emerging risk, internal and external operational risk events and losses, and regulatory changes. On the whole reporting should incorporate financial, operational, compliance and external market information. The criteria to observe preparedness of banks with respect to this principle is:

- Senior Management is responsible for implementing a process to monitor the operational risk profile of the bank
- Ensure reporting structure for effective operational risk management
- First Line of Defence is responsible to ensure reporting of residual[18] operational risk in bank
- Bank to have operational risk reporting in line with bank's RATS
- Bank to report operational risk profile to top management, both in normal and stressed conditions
- Ensure linkage of reporting with changes in Operational Risk environment in bank in terms of Frequency/severity
- ORMF in bank is assessed by Internal or External Auditors or Risk Management Function
- Reports created by or for supervisory authority are reported to Board of Directors and Senior Management

Principle 9: Control and Mitigation: *"Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

- Focus of control function is on safeguard of bank's assets, produce reliable financial reports, compliance with laws and regulation
- The focus of compliance assessment in bank is on review of progress, compliance with controls, review of instances of non-compliance, evaluation of approvals, tracking reports of approved exceptions
- Bank to have clearly segregated duties of individuals or teams
- Ensure appropriate staffing and expertise to address operational risk
- Vacation policy for not less than two consecutive weeks
- Ensure sound technology governance and infrastructure risk management programme for automated processes
- Bank to have outsourcing arrangements in place
- Ensure Board of Director and Senior Management understanding of risks relating to outsourcing activities
- Clearly defined policies and practices to manage outsourcing risk
- Bank to have insurance policy to mitigate/transfer operational risk
- Board of directors to ensure review of insurance management programme

Principle 10: Bank's Information and Communication Technology (ICT) Risk Management Programme: *"Banks should implement a robust ICT risk management programme in alignment with their operational risk management framework",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

- Bank to have ICT risk management programme in place
- Ensure it is in line with Risk Appetite and Tolerance Statement of the bank
- Effective to control risk in bank and reduce bank's exposure to direct losses, legal claims, reputational damage, ICT disruptions and misuse of technology

18. Risk after considering controls. It is Inherent Risk minus Control Effectiveness

- Board of Directors and Senior Management to evaluate its design and effectiveness
- Ensure data and system confidentiality
- Appropriate reporting of ICT risks, controls and events

Principle 11- Business Continuity Planning (BCP): *"Banks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Business continuity plans should be linked to the bank's operational risk management framework",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

- Ensure effective business continuity plan to reduce losses from business disruptions
- Regular review of BCP in bank by Board of Directors
- Implementation of BCP by senior management and Business Unit Leaders
- First and Second line of defence designs BCP in bank
- Third Line of Defence review BCP in bank
- Prepare impact assessment of BCP in bank, with a coverage on financial, operational, legal and reputational consequences
- Conduct scenario analysis to assess effectiveness of BCP
- Fix the thresholds for maximum tolerable outrage, while conducting the scenario analysis
- Focus of BCP in bank is on business units, critical service providers, third parties, like central bank and clearing house
- Based upon qualitative or quantitative analysis
- Conduct of training and awareness programme for staff to execute contingency plan
- Conduct testing of business continuity procedures considering current operations, risk and threats
- Frequently report the same to board of directors and senior management
- Conduct business continuity testing with key service providers

Principle 12: Role of Disclosure and Role of Supervisors: *"A bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure",* (Basel, 2021). The criteria to observe preparedness of banks with respect to this principle is:

Role of disclosure

- Bank to have disclosure policy, in line with bank's risk profile, size and complexity of operations
- Disclose Operational Risk Exposure information to stakeholders - Operational Risk Capital Charges, Operational Risk Losses, tools, etc.
- Frequent approval and review of policy by Board of Director and Senior Management of banks

Role of Supervisor

- Focus on Industry Best practice
- Frequent assessment of ORMF of bank by evaluating policies, procedures, systems, and all other areas as disclosed in PSMOR
- Assessment of ORMF by external auditors
- Exchange of information with other supervisors (about assessment)
- Frequent reporting of operational risk related information to Regulator
- Peer comparison of operational risk processes

Given the principle-wise requirement, now it becomes important to assess the level of implementation of these principles, as obtainable from Basel III disclosures and annual reports of the banks in India. The study by Samanta et al (2016) and Kumar et al (2019), who examined the disclosures of the public and private sector banks, reported that operational risk disclosures in banks are weak, with minimal to no disclosures on many keys areas of operational

risk management. Thus, this study is most recent and new with respect to best practices on operational risk management as per PSMOR (2021). The operational risk disclosures of all twelve public sector and twenty-one private sector banks in the India forms the basis of the analysis.

6.3. Database and Methodology

In order to assess and review the principles, as listed in previous section, the banks are compared with respect to disclosures on ORMF, risk culture and the tools used by them for operational risk assessment and management. The information for the same has been collected from the Basel III Disclosures (DF-8) and annual reports, as on March 2022, for the banks included in the study.

Following methodology was used to review the best practices followed by the banks in India for operational risk assessment and management, policies developed and committees set up in banks to deal with operational risk. In total, 160 key words as per PSMOR were identified by going through the annual report of a large bank. Then mapping of these words was done with information available in annual reports of all banks under study. The words coming ten times and above were considered to design the text cloud to comment on the elements most frequently used by the banks relating to operational risk assessment and management.

Given this information, the next step was to prepare a disclosure index. The disclosure index is an extent of disclosure presented by a particular firm in their annual report. The disclosure index was first used by Cerf (1961). The Disclosure Index has been computed using the following formula:

$$\text{Disclosure Index of the Bank} = \frac{\text{No of Items disclosed by the Bank}}{\text{No of the items expected to be dislosed by the Bank}}$$

The study takes into account dichotomous scoring method, Paulhus (1991), whereby an item is scored as 1, if disclosed and zero, if undisclosed, particularly for qualitative statements given in the bank's annual reports. The disclosure Index was prepared in line with Kumar et al (2019), who followed the following methodology:

TABLE 6.1
Disclosure Index Category and Index Value

Disclosure Index Category	*Index Value*
FD, "fairly disclosed" category.	Above 80 percent
DSE, "disclosed to some extent" category.	Between 60-80 percent
L, "low level of disclosure" category.	Between 40-60 percent
VL, "very low level of disclosure" category.	Between 30-40 percent
EL, "extremely low level of disclosure" category.	Below 30 percent

Source: Author's construction.

The quantitative disclosure (RBI, 2015) relating to capital charge estimation method is presented next. All banks in India are estimating their operational risk capital charges (ORCC) as per Basic Indicator Approach (BIA). The data for the same has been collected from the annual report and Basel III disclosure, DF-8 and a comparative chart is presented. In the end, the Operational Risk Weighted Assets (OpRWA) to Total Risk Weighted Assets (TRWA) was presented, the data for the same is collected from Disclosure – 11 (Composition of Capital) from the Basel III disclosures of the banks under study.

Analysis and Interpretation

The results of the analysis are presented through following Sections: (i) Word Cloud Analysis; (ii) Analysis of PSMOR implementation in the Banks; (iii) Disclosure index of Banks; (iv) Disclosure on Operational Risk Capital Charge (ORCCs) as per Basic Indicator Approach (BIA); (v) Ratio of Risk weighted assets for Operational Risk to Total Risk Weighted assets of the Banks in India.

i. Word Cloud Analysis

A text cloud, shown in Figure 6.4, is created to view the elements most frequently used by banks and disclosed in annual reports of the banks relating to operational risk assessment and management. For example, operational risk management, committee, products etc.

FIGURE 6.4

Word Cloud Analysis

Source: Author's construction.

Although, the analysis shows that urgent focus is required on items, which are infrequently used, but forms an important part of operational risk management framework like, governance, risk culture, line of defence, tools used by the banks, such as loss data, risk and control self-assessment (RCSA) and key risk indicators (KRIs), etc.

ii. Analysis of PSMOR Implementation in Banks

In order to review the bank-wise preparedness with respect to principles of sound management of operational risk, i.e. PSMOR (2021), as presented in Section 6.2, following list was prepared (Table 6.2), covering operational risk governance, framework, systems, tools for assessment (like RCSA, KRIs, loss data and their root cause analysis, scenario analysis and stress testing), the policies and committees to manage operational risk. In addition to the qualitative parameters, the analysis present the quantitative disclosures in line with RBI (2015), i.e. operational risk capital charge estimation, as per BIA and intention of the banks to migrate to advanced approaches.

It is interesting to note that ORMF and ORMS has been implemented in more than 90 percent of banks. More than 75 percent of the banks are disclosing the information regarding tools like RCSA, KRIs and loss data, used for operational risk assessment and management. Improvement in disclosure of information relating to root cause analysis, scenario analysis and external loss data may help the market participants with the best practices followed by the banks under study. It is interesting to note that in more than 50 percent of the public and private sector banks, board of directors and senior management, have established strong risk culture. Moreover, banks have appropriate policies and committees in place to deal with this risk, with an exception of forex risk management and vacancy policy.

iii. Disclosure Index of Banks in India

Table 6.3 clearly shows that the Disclosure Index is low in eight out of 12 public sector banks in the country. These results are in line with Hossain (2008). In contrast, same holds true for only seven out of 21 private sector banks in the country. The Disclosure Index of the public sector banks (58%) is better than the old private sector banks (55%), however, it is significantly lesser than the new private sector banks (64%) (Table 6.3). These results are in line

TABLE 6.2

Comparative Representation of the Disclosures on Operational Risk Management (in percent)

Parameters	*Overall*	*Public Sector Banks in India*	*Private Sector Banks in India*
	33	12	21
Risk Culture	51.52	66.67	42.86
Operational Risk Management Framework	96.97	91.67	100.00
Operational Risk Management Structure	96.97	91.67	100.00
Statistical Analysis Software (SAS)	15.15	33.33	4.76
Risk Appetite Framework	78.79	91.67	71.43
Operational Risk Management System	45.45	75.00	28.57
Line of Defence	36.36	25.00	42.86
Risk and Control Self-Assessment	87.88	83.33	90.48
Key Risk Indicator	87.88	83.33	90.48
Internal Loss Event Data	75.76	75.00	76.19
Root Cause Analysis of Loss Incidents	51.52	41.67	57.14
External Loss Data	6.06	16.67	-
Stress Testing and Scenario Analysis	18.18	16.67	19.05
Insurance	30.30	25.00	33.33
Operational Risk Capital Charges			
Basic Indicator Approach	100.00	100.00	100.00
Standardised Approach of Basel III	18.18	16.67	19.05
Advanced Measurement Approach of Basel II	15.15	33.33	4.76
Policies and Committees for Operational Risk Management			
Information System Security	84.85	66.67	95.24
Outsourcing of Services	57.58	50.00	61.90
Business Continuity Planning	87.88	75.00	95.24
Disaster Recovery	81.82	58.33	95.24
Cyber Security	72.73	58.33	80.95
Compliance	60.61	50.00	66.67
Information Technology	15.15	8.33	19.05
Fraud Risk Management	78.79	75.00	80.95
Anti-Money Laundering	72.73	75.00	71.43
Know your Customer	66.67	75.00	61.90
Forex Risk Management Policy	9.09	16.67	4.76
Whistle Blower Policy	81.82	91.67	76.19
Vacation Policy	3.03	8.33	-
Product and Process Approval Committee (PPAC)	66.67	41.67	80.95
Risk Management Committee	100.00	100.00	100.00
Enterprise/ Integrated Risk Management Committee	87.88	100.00	80.95

TABLE 6.3

Disclosure Index of Banks (in percent)

Banks	*Disclosure Index*	*Banks*	*Disclosure Index*
State Bank of India	85	CSB Bank	76
Bank of Baroda	70	City Union Bank	58
Bank of India	52	Dhanlaxmi Bank	64
Bank of Maharashtra	64	Federal Bank	61
Canara Bank	58	Jammu and Kashmir Bank	45
Central Bank of India	64	Karnataka Bank	67
Indian Bank	48	Karur Vysya Bank	64
Indian Overseas Bank	52	Nanital Bank	33
Punjab and Sind Bank	52	RBL Bank	42
Punjab National Bank	58	South Indian Bank	48
UCO Bank	48	Tamilnadu Mercantile Bank	48
Union Bank of India	48	Average Disclosure of Old Private Sector Banks	55
Average Disclosure of Public Sector Banks	58	Axis Bank	64
		DCB Bank	58
		HDFC Bank	61
		ICICI Bank	76
		INDUS Ind Bank	67
		Kotak Mahindra Bank	73
		Yes Bank	73
		IDFC First Bank Limited	33
		Bandhan Bank	64
		IDBI Bank	70
		Average Disclosure of New Private Sector Banks	64
		Average Index of all Private Sector Banks	59

with Kumar et al (2019). The highest disclosure index of 85 percent clearly point towards the better disclosure in a large size bank like State Bank of India, followed by Bank of Baroda (70 percent). It is interesting to observe disclosure index of 70 percent and more in five private sector banks, in India.

iv. Disclosure on Operational Risk Capital Charge

To comply with Basel III framework (RBI, 2015), Banks in India estimate their regulatory capital requirement for Pillar I risks on a quarterly basis. The Basic Indicator approach (BIA) is used to estimate capital charges for operational risk and same is presented next.

The Figures 6.5, 6.6 and 6.7, present that as on March 2022, capital requirement for operational risk is highest in the case of State Bank of India and it is found the lowest in the case of Punjab and Sind Bank. In contrast, it is highest in HDFC bank and lowest in Nainital bank in private sector. These results are in line with Basel (2014) that operational risk capital charge increases in proportion to bank's revenue.

FIGURE 6.5

Capital Requirement for Operational Risk for Public Sector Banks in India (in crores)

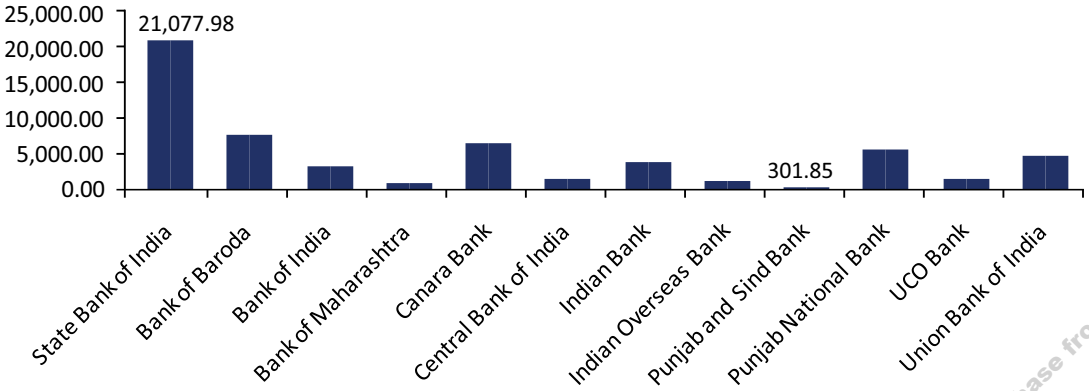


FIGURE 6.6

Capital Requirement for Operational Risk for Old Private Sector Banks in India (in crores)

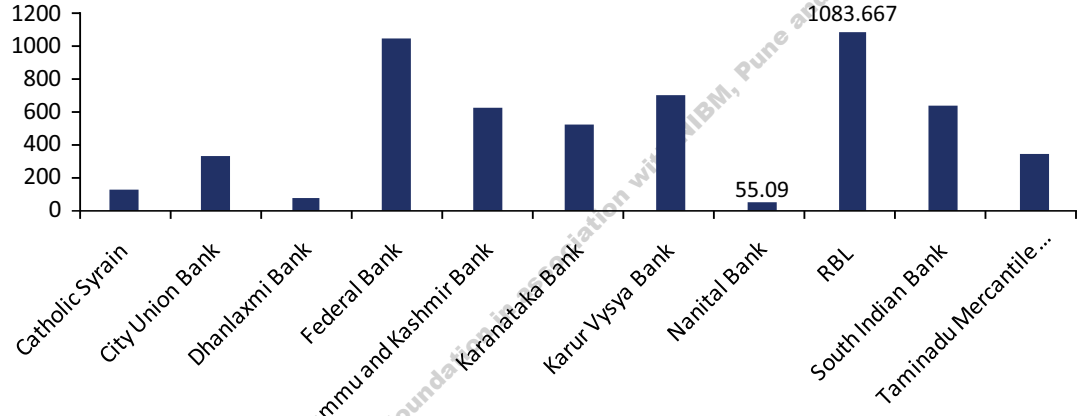


FIGURE 6.7

Capital Requirement for Operational Risk for New Private Sector Banks in India (in crores)

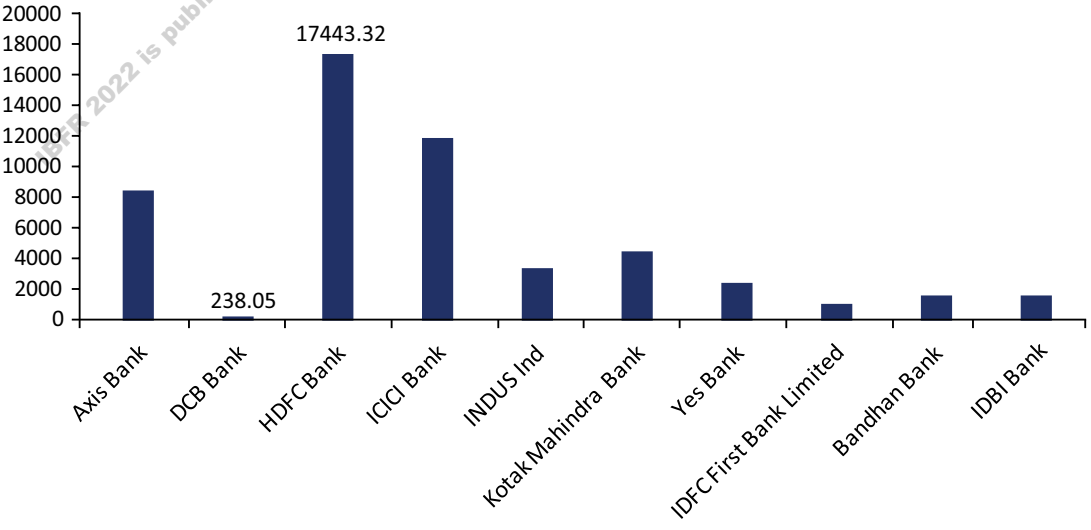


FIGURE 6.8

Risk Weighted Assets for Operational Risk to Total Risk Weighted Assets for Public Sector Banks in India

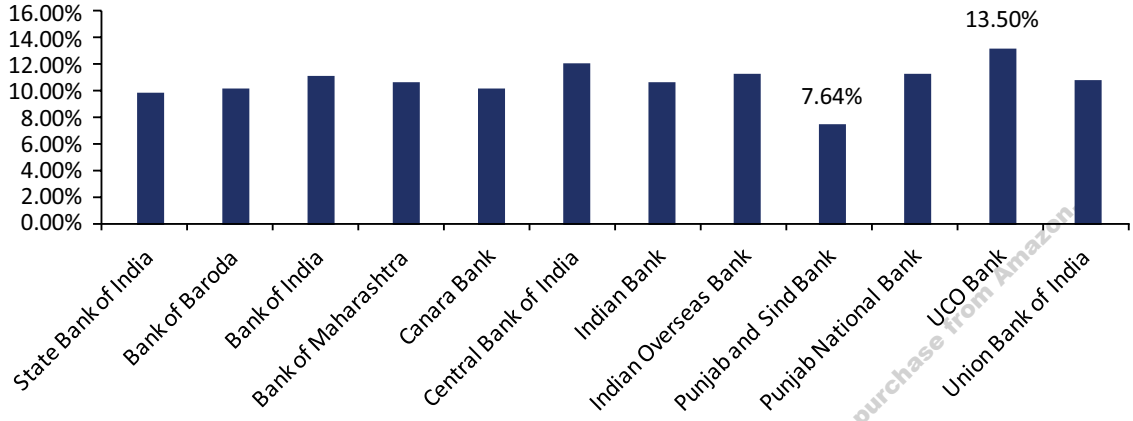
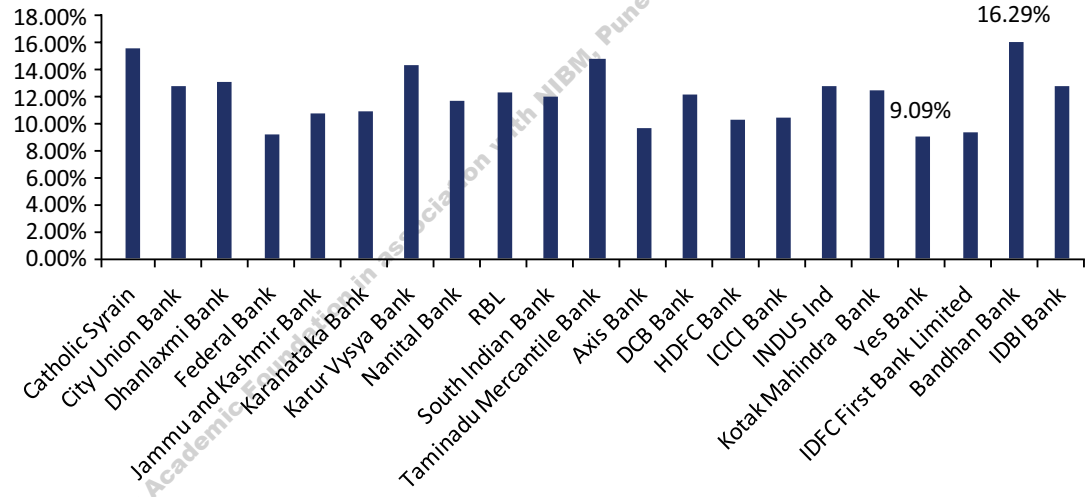


FIGURE 6.9

Risk Weighted Assets for Operational Risk to Total Risk Weighted Assets for Private Sector Banks in India



v. Ratio of Risk Weighted Assets for Operational Risk to Total Risk Weighted Assets

Further, the operational risk weighted assets to total risk weighted assets was presented through Figure 6.8 and 6.9. These figures clearly indicate that the ratio of risk weighted assets for operational risk to Total Risk Weighted Assets is highest in UCO bank followed by Central Bank of India. In contrast, same is found the lowest in Punjab and Sind bank. Whereas, in private sector banks, Bandhan Bank has the highest operational risk weighted assets (OpRWA) to total risk weighted assets (TRWA) and Yes bank has the lowest. The study found that operational risk weighted assets to total risk weighted assets of the bank is in the range of 7 to 13 percent in banks in public sector and 9 to 16 percent in private sector banks in the country.

6.4. Concluding Observations

This chapter is an attempt to view best practices, as per sound practice principles (PSMOR), for operational risk management followed by public sector and private sector banks in India.

These principles are detailed in Section 6.2 of this chapter and to comment on bank level preparedness with regard to these principles, the data has been collected from Basel III disclosures and annual reports of the banks, as on March 2022.

It is interesting to note that disclosure index relating to PSMOR implementation is found superior in new private sector banks followed by public sector and old private sector banks in the country. The disclosures on BIA capital charges clearly shows that big banks like State Bank of India and HDFC bank needs to maintain high capital for operational risk, as stated by Bajaj (2016). Moreover, banks are preparing themselves for migration to advanced approaches. As far as Regulatory Consistency Assessment Programme (Basel 2015) is concerned, the operational risk weighted assets to total risk weighted assets was 7.8 percent for India. It is interesting to note from the disclosures that recently this percentage is more than ten percent in 28 out of 33 banks in the country, which requires urgent regulatory attention and focus. These results are in line with Ames et al (2015). Moreover, low disclosure index on PSMOR, relating to few parameters, calls for top management attention in order to provide market participants required information relating to operational risk management.

References

Alexander, C. (2003). "Statistical Models of the Operational Loss", Pp. 129–170 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. Prentice Hall-Financial Times.

Ames, M., Schuermann, T. and Scott, H.S. (2015). "Bank capital for operational risk: a tale of fragility and instability", *Journal of Risk Management in Financial Institutions*, 8(3), pp. 227-243.

Bajaj, R. V. (2016). "Operational risk capital estimation under BIA and TSA: a study of public sector and private sector banks in India", *Decision*, 43(1), pp.67-92.

Basel Committee on Banking Supervision (2006). Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework, BCBS Publications, June.

Basel (2014), Operational risk - Revisions to the simpler approaches, October, available at *www.bis.org/publ/bcbs291.htm*.

Basel Committee on Banking Supervision (2021). Revisions to the Principles for the Sound Management of Operational Risk (PSMOR), March.

Basel (2015): Regulatory Consistency Assessment Programme (RCAP) - Assessment of Basel III risk-based capital regulations – India, June.

Basel (2017). Basel III - Finalizing post-crises reforms, December 7.

Bocker, K. and C. Kluppelberg (2005). "Operational VAR: A Closed-Form Approximation", Risk, December: pp.90–93.

Cerf, A. R. (1961). "Corporate Reporting and Investment Decisions", University of California Press, Berkeley, CA.

Crouhy, M., D. Galai, and R. Mark (1998). "Key Steps in Building Consistent Operational Risk Management and Measurement", Pp. 45–62 in *Operational Risk and Financial Institutions*, London: Risk Books.

Currie, C. V. (2004). "Basel II and Operational Risk: An Overview", Pp. 271–286 in *Operational Risk Modelling and Analysis*, ed. M. Cruz. London: Risk Books.

Curry, T. (2012). *https://www.occ.gov/news-issuances/speeches/2012/pub-speech-2012-77.pdf*

De Fontnouvelle, P., Dejesus-Rueff, V., Jordan, J. S. and Rosengren, E. S. (2006). "Capital and risk: new evidence on implications of large operational losses", *Journal of Money, Credit and Banking*, pp.1819-1846.

Herring, R. J. (2002). "The Basel 2 Approach to Bank Operational Risk: Regulation on the Wrong Track", Unpublished paper, University of Pennsylvania.

Hoffman, D. G. (1998). "New Trends in Operational Risk Measurement and Management", Pp. 29–44 in *Operational Risk and Financial Institutions*. London: Risk Books.

Hossain, M. (2008). The extent of disclosure in annual reports of banking companies: The case of India.

Kumar, M., Soni, H. and Mocanu, M. (2019). "The operational risk disclosure practices of banks: evidence from India and Romania", *Journal of Operational Risk*, 14(2).

Paulhus, D. L. (1991), "Measurement and control of response bias". In J. P. Robinson, P. R. Shaver, & L. S. Wrightsman (Eds.), *Measures of personality and social psychological attitudes* (pp. 17-59). San Diego: Academic Press.

Rebonato, R. (2007). *Plight Of The Fortune Tellers*. Princeton University Press.

Reserve Bank of India (2015). *https://rbidocs.rbi.org.in/rdocs/notification/PDFs/58BS09C403D06BC14726AB61783180628D39.PDF.*

RBI (2022). Financial Stability Report, December, Issue No – 26. *https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/0FSRDECEMBER2022F93A2F188A394ACDB2FDDC2FCC0D07F0.PDF.*

Samanta, P. and Dugal, M. (2016). "Basel disclosure by private and public sector banks in India: assessment and implications", *Journal of Financial Regulation and Compliance*.