World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Emerging trends in risk management with Reference to banking industry

Madhaiyan. M *

AGM and PRINCIPAL, UCO Bank, Staff Training Centre, Chennai.
COE on Credit monitoring, Compliance and Risk management.

World Journal of Advanced Research and Reviews, 2026, 29(03), 1663-1673

Publication history: Received on 14 February 2026; revised on 20 March 2026; accepted on 23 March 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0705

Abstract

Risk management is a critical function in modern banking, ensuring financial stability, regulatory compliance, and sustainable growth in an increasingly complex and volatile economic environment. Banks are exposed to a wide range of risks, including credit risk, market risk, operational risk, liquidity risk, and reputational risk. Effective risk management frameworks enable banks to identify, measure, monitor, and mitigate these risks through robust policies, advanced analytics, internal controls, and governance mechanisms.

With rapid digitalization, globalization of financial markets, and evolving regulatory expectations, the role of risk management has expanded beyond traditional prudential safeguards to become a strategic driver of performance and resilience. The adoption of risk-based pricing, stress testing, early warning systems, and enterprise risk management practices helps banks enhance asset quality, protect stakeholder interests, and maintain public confidence.

This article examines the key dimensions of banking risk management, highlights emerging challenges such as cyber risk and climate-related financial risk, and emphasizes the importance of building a strong risk culture supported by technology, skilled human resources, and proactive supervision. Effective risk management not only safeguards banks against potential losses but also contributes to long-term financial inclusion, economic stability, and sustainable development.

Keywords: Risk History; Risk mitigation; Risk Management; Risk avoidance; Climate risk

1. Introduction

Risk management has always been central to the banking industry, but in the 21st century its complexity has expanded dramatically. Globalization, digital transformation, rising regulatory expectations, and emerging threats such as cybercrime and climate change have reshaped the risk landscape. As banking products and services evolve, so too must the frameworks, technologies, and strategies that institutions use to identify, assess, and mitigate risks.Post–global financial crisis reforms ushered in a new era of regulatory scrutiny, demanding greater transparency, higher capital buffers, and more robust risk governance. At the same time, technological innovation—artificial intelligence (AI), machine learning (ML), big data, cloud computing, blockchain—has revolutionized risk identification and predictive capability. Today, banks face a dual challenge: managing traditional financial risks while simultaneously addressing new categories of operational, technological, and environmental risk.

This article examines the major trends shaping risk management in the banking industry in 2025, exploring how institutions are adapting and the innovations that are defining the future of financial stability.

* Corresponding author: Madhaiyan. M

2. History of Risk Management in Banking

2.1. Early Banking Era (Before 1970s) – Traditional Risk Control

In the Early Banking Era (before the 1970s), risk control was largely traditional, informal, and heavily dependent on bankers' personal experience and judgment rather than structured frameworks. Banks focused primarily on credit risk, assessing a borrower's character, collateral, and repayment capacity through relationship-based lending practices. Decisions were guided by trust, local knowledge, and long-term customer relationships rather than quantitative analysis or statistical models. Regulatory oversight was relatively limited compared to modern standards, and there were few standardized risk measurement tools. As a result, risk management was reactive rather than strategic, with minimal diversification strategies and little emphasis on market, operational, or liquidity.

2.2. 1970s–1980s – Regulatory Awareness

During the 1970s–1980s, the banking sector entered a period of growing regulatory awareness as financial instability, oil shocks, inflation, and international debt crises exposed weaknesses in traditional risk practices. The collapse of institutions such as Herstatt Bank highlighted the dangers of settlement and foreign exchange risk, prompting greater global coordination among regulators. This era led to the establishment of the Basel Committee on Banking Supervision, which began developing international standards for bank supervision and capital adequacy. Banks started shifting from purely judgment-based lending toward more structured risk assessment processes, with increased attention to capital requirements, liquidity management, and country risk. Although quantitative models were still limited, this period marked the transition from informal risk control to more formal, regulation-driven risk management frameworks.

2.3. 1990s – Quantitative & Market Risk Focus

During the 1990s, banking risk management shifted strongly toward quantitative methods and a heightened focus on market risk, driven by rapid financial innovation, globalization, and the growth of complex financial instruments such as derivatives. Advances in computing technology enabled banks to adopt statistical models to measure and manage risks more precisely, including the widespread use of Value at Risk (VaR) to estimate potential losses. Regulatory developments such as Basel Committee on Banking Supervision's Basel I framework reinforced capital adequacy standards and encouraged more formalized risk measurement systems. Institutions increasingly monitored interest rate risk, foreign exchange risk, and trading portfolio exposures, reflecting a broader understanding that risk extended beyond traditional credit concerns. This decade marked the transformation of risk management into a more data-driven, model-based discipline integrated into strategic decision-making

2.4. Early 2000s – Integrated Risk Management

In the early 2000s, banks moved toward integrated risk management, recognizing that credit, market, operational, and liquidity risks were interconnected and needed to be managed holistically rather than in silos. Institutions began implementing enterprise-wide risk frameworks that aligned risk measurement with strategic planning, capital allocation, and corporate governance. Regulatory developments such as Basel II, introduced by the Basel Committee on Banking Supervision, emphasized risk-sensitive capital requirements, supervisory review, and market discipline, encouraging banks to adopt advanced internal rating systems and operational risk models. This period also saw the rise of enterprise risk management (ERM) practices, stronger internal controls, and increased reliance on technology and data analytics. Overall, risk management became more comprehensive, strategic, and embedded across all levels of financial institutions.

2.5. Post-2008 Global Financial Crisis – Strengthening Controls

Following the 2008 Global Financial Crisis, risk management entered a new era focused on strengthening controls, transparency, and resilience across the financial system. The crisis—triggered by excessive risk-taking, weak oversight, and the collapse of institutions such as Lehman Brothers—revealed major flaws in existing models and governance structures. In response, regulators introduced stricter reforms, including Basel III developed by the Basel Committee on Banking Supervision, which imposed higher capital requirements, leverage ratios, and liquidity standards. Stress testing, risk governance, and board-level oversight became central to banking supervision, while greater emphasis was placed on transparency, systemic risk monitoring, and macroprudential regulation. Overall, the post-crisis period marked a shift toward more robust, forward-looking and resilience-focused risk management practices

2.6. 2010s – Enterprise Risk Management (ERM)

During the 2010s, Enterprise Risk Management (ERM) became a central pillar of banking strategy, emphasizing a holistic, organization-wide approach to identifying, assessing, and managing risks. Rather than treating credit, market, operational, and liquidity risks separately, ERM integrated them under a unified governance framework aligned with corporate objectives and risk appetite. Regulatory reforms following the global financial crisis—particularly Basel III introduced by the Basel Committee on Banking Supervision—reinforced the need for strong risk culture, board oversight, and comprehensive stress testing. During this decade, banks also strengthened internal controls, enhanced data analytics capabilities, and adopted advanced risk reporting systems to improve transparency and decision-making. Overall, ERM in the 2010s reflected a shift toward proactive, strategic, and resilience-focused risk management embedded across all levels of the organization.

2.7. Recent Developments (2020s–Present) – Emerging Risks

In the 2020s to the present, risk management has evolved to address a new generation of emerging risks shaped by global uncertainty, digital transformation, and interconnected markets. The COVID-19 pandemic exposed vulnerabilities in liquidity, supply chains, and operational resilience, prompting banks to enhance stress testing and scenario analysis. At the same time, institutions are increasingly focused on cyber risk, fintech disruption, climate-related financial risk, and geopolitical instability. Regulators and standard-setting bodies, including the Basel Committee on Banking Supervision, have expanded guidance on operational resilience and climate risk management. Advances in artificial intelligence, big data analytics, and digital banking have improved risk monitoring but also introduced model risk and data privacy concerns. Overall, the current era emphasizes agility, technological integration, sustainability considerations, and proactive risk identification in an increasingly complex and rapidly changing financial environment

3. Expansion and Refinement of Traditional Risk Categories

3.1. Credit Risk Transformation

Credit risk remains the core risk faced by banks, but the methodologies used to measure it have undergone significant modernization.

3.2. Shift toward Behavioral and Real-Time Analytics

Traditionally, credit assessments relied heavily on historical financial statements, credit scores, and static borrower profiles. Today, dynamic data sources—cash flow trends, real-time transaction patterns, macroeconomic indicators, alternative data (e.g., mobile phone payments)—are providing deeper insight into borrower behavior.

Machine learning models enhance accuracy by detecting non-linear patterns and early warning signals that traditional models often miss. For instance, sudden fluctuations in spending or deposit patterns can help identify potential defaults weeks or months earlier.

3.3. Portfolio Diversification and Macro Stress Scenarios

With global markets increasingly interconnected, banks now conduct more frequent and granular stress testing. The rise of geopolitical tensions, inflationary pressures, and supply chain disruptions has forced banks to evaluate sector-specific vulnerabilities (e.g., retail, real estate, energy). These insights are integrated into credit decisions and loan pricing strategies.

3.4. Market Risk in an Era of Volatility

Market risk—exposure to losses arising from fluctuations in interest rates, exchange rates, equity prices, and commodity prices—has intensified.

3.5. Greater Volatility from Global Events

Events such as pandemics, wars, trade conflicts, and political instability create unpredictable market swings. Banks are therefore adopting dynamic risk management tools capable of real-time recalibration.

3.6. Improved Risk Modeling Techniques

Tools such as Value-at-Risk (VaR), Expected Shortfall (ES), and scenario modeling have evolved. Banks combine traditional models with AI-driven models that incorporate sentiment analysis, news analytics, supply chain data, and global market trends.

3.7. Algorithmic Trading and the Need for New Controls

Automated trading introduces both speed and complexity. New regulations require banks to monitor algorithmic behavior, ensure kill-switch mechanisms, and validate models more rigorously.

3.8. Operational Risk and the Technology Factor

Operational risk—arising from system failures, human error, or external events—has broadened with digital transformation.

3.9. Cybersecurity as the Most Critical Operational Risk

Cyber security has emerged as the most critical operational risk in modern banking due to the rapid expansion of digital services, online transactions, and interconnected financial systems. As banks increasingly rely on cloud computing, mobile platforms, and fintech partnerships, they face heightened exposure to cyber attacks such as data breaches, ransomware, phishing, and distributed denial-of-service (DDoS) attacks. Major incidents affecting institutions like JPMorgan Chase have demonstrated how cyber threats can disrupt operations, compromise sensitive customer data, and damage institutional reputation. Beyond financial losses, cyber incidents can undermine customer trust, trigger regulatory penalties, and pose systemic risks to the broader financial system. Consequently, regulators and global bodies such as the Basel Committee on Banking Supervision emphasize strong cyber security frameworks, continuous monitoring, incident response planning, and investment in advanced threat detection systems. In today's highly digital environment, effective cyber security is no longer just an IT function but a strategic priority embedded within enterprise-wide risk management.

3.10. Automation-Related Failure Risks

Automation-related failure risks have become a significant operational concern as banks increasingly depend on automated systems, algorithms, and artificial intelligence to process transactions, assess creditworthiness, detect fraud, and manage trading activities. While automation improves efficiency, accuracy, and cost reduction, system errors, coding flaws, model miscalculations, or technical outages can lead to substantial financial losses and reputational damage. For example, technology-driven incidents such as the trading glitch at Knight Capital Group demonstrated how automated system failures can cause severe market disruption within minutes. Automation also introduces risks related to over-reliance on models, insufficient human oversight, cyber security vulnerabilities, and challenges in explaining complex algorithmic decisions. As a result, regulators and global standard-setters like the Basel Committee on Banking Supervision emphasize strong model validation, governance controls, regular system testing, and clear accountability structures. In the digital banking era, managing automation-related risks is essential to maintaining operational resilience and financial stability.

3.11. Liquidity Risk Post–Financial Crisis

Liquidity risk—when a bank cannot meet its financial obligations—has remained a regulatory priority.

3.12. Regulatory Ratios Driving Discipline

Regulations such as the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR) require banks to maintain sufficient high-quality liquid assets. These safeguards proved invaluable during market disruptions, including the COVID-19 pandemic.

3.13. Real-Time Liquidity Monitoring

Advances in digital infrastructure allow banks to track liquidity daily or even hourly. Predictive analytics forecast potential funding shortages, improving preparedness for market stress events.

4. Technological Innovations Transforming Risk Management

Technology is reshaping every aspect of risk management, enabling faster detection, better modeling, and more precise mitigation strategies.

4.1. Artificial Intelligence and Machine Learning

4.1.1. Enhanced Predictive Capabilities

Artificial Intelligence (AI) and Machine Learning (ML) have transformed risk management in banking by providing enhanced predictive capabilities that allow institutions to anticipate, quantify, and mitigate potential threats more effectively. These technologies analyze vast volumes of structured and unstructured data, uncover complex patterns, and generate insights for credit risk assessment, fraud detection, customer behavior analysis, and market trend forecasting. For instance, AI-driven models can predict early signs of loan defaults, detect anomalous transactions in real time, or optimize portfolio risk exposure with greater accuracy than traditional statistical methods. However, their power comes with challenges, including model interpretability, bias in training data, and operational or cyber security vulnerabilities. Regulators, including the Basel Committee on Banking Supervision, emphasize the need for rigorous model validation, transparency, and governance frameworks to ensure AI/ML applications are reliable and aligned with risk appetite. Overall, AI and ML significantly enhance predictive capabilities, enabling proactive and data-driven risk management across the financial sector.

4.1.2. AI in Fraud Detection

Fraud detection systems now use ML to identify abnormal transaction patterns in real time. Models compare current behavior to historical patterns for each customer and flag anomalies instantly.

4.1.3. AI in Compliance and Reporting

RegTech tools automate regulatory reporting, transaction monitoring, suspicious activity identification, and risk-classification tasks—reducing both cost and human error.

4.2. Big Data and Predictive Analytics

The explosion of structured and unstructured data is revolutionizing banking risk management.

4.2.1. Customer-Level Risk Prediction

Customer-level risk prediction leverages advanced analytics, artificial intelligence (AI), and machine learning (ML) to assess the risk profile of individual clients with greater precision and timeliness. By analyzing diverse data sources—including transaction history, credit behavior, income patterns, and social data, and even macroeconomic indicators—banks can predict potential defaults, fraud, or credit deterioration at the individual level. This enables more personalized risk-based pricing, proactive account monitoring, and targeted interventions to mitigate losses. For example, predictive models can flag early warning signs of repayment difficulties or unusual transaction activity, allowing banks to act before issues escalate. While highly effective, customer-level risk prediction requires careful management of data privacy, algorithmic bias, and regulatory compliance, as emphasized by guidelines from the Basel Committee on Banking Supervision. When implemented responsibly, it strengthens decision-making, enhances portfolio quality, and supports a more resilient, customer-focused risk management strategy

4.2.2. Enterprise-Wide Risk Identification

Big data systems capture data across operational, financial, and market domains to offer a holistic risk profile, enabling more informed decision-making.

4.2.3. Block chain and Distributed Ledger Technology (DLT)

Block chain reduces risks associated with fraud, reconciliation errors, and counterparty exposure.

4.2.4. Transparency and Immutability

Every transaction recorded on a block chain is visible and tamper-proof, reducing opportunities for fraud and manipulation.

4.2.5. Smart Contracts

Self-executing digital contracts verify contractual conditions automatically, lowering operational risk and speeding settlement processes.

4.2.6. Cross-Border Payments

DLT reduces settlement time from days to seconds, lowering liquidity and counterparty risks.

4.2.7. Cloud Computing and Risk Management

Cloud computing offers scalability, flexibility, and cost efficiency, but also brings new risks.

4.2.8. Benefits for Risk Management

The adoption of advanced risk management techniques offers multiple benefits that strengthen a bank's resilience, efficiency, and strategic decision-making. First, it improves risk identification and measurement, allowing institutions to detect potential credit, market, operational, and emerging risks early. Second, it enables proactive decision-making, as predictive analytics, AI, and scenario modeling provide forward-looking insights rather than relying solely on historical data. Third, it enhances regulatory compliance, helping banks meet capital adequacy, liquidity, and governance standards set by bodies like the Basel Committee on Banking Supervision. Fourth, advanced risk management supports capital optimization, ensuring that resources are allocated efficiently to mitigate risk while maximizing returns. Finally, it boosts operational resilience and stakeholder confidence, reducing the likelihood of financial losses, reputational damage, or systemic disruptions. Overall, effective risk management transforms risk from a reactive challenge into a strategic advantage for modern financial institutions

4.2.9. Associated Risks

- Data security
- Vendor risk
- Regulatory restrictions around data storage

Banks therefore implement shared-responsibility frameworks and conduct rigorous vendor assessments.

5. Regulatory Developments and Compliance Trends

The regulatory landscape continues to evolve, emphasizing resilience, transparency, and consumer protection.

5.1. Capital and Liquidity Requirements

Basel III reforms introduced post-crisis mandates for higher capital buffers, leverage ratios, and liquidity requirements. Banks must conduct Internal Capital Adequacy Assessment Processes (ICAAP) and Internal Liquidity Adequacy Assessment Processes (ILAAP) regularly.

5.2. Shift toward Proactive Regulation

Regulators now emphasize risk culture, board accountability, and governance standards. Supervisory reviews focus not only on numbers but also on leadership effectiveness and risk awareness.

5.3. Cyber security Regulations

Cyber security regulations have become a cornerstone of modern banking oversight, reflecting the growing threat of cyber attacks and the need to protect sensitive financial data, critical infrastructure, and customer trust. Regulators worldwide mandate that banks implement comprehensive cyber security frameworks covering risk assessment, incident detection and response, data protection, and continuity planning. Standards often require regular vulnerability assessments, penetration testing, and reporting of breaches to supervisory authorities. For example, guidelines from the Basel Committee on Banking Supervision emphasize robust IT governance, operational resilience, and integration of cyber security into enterprise risk management (ERM). In addition, regional regulations—such as the EU's Network and Information Systems (NIS) Directive and the U.S. Gramm-Leach-Bliley Act (GLBA) cyber security provisions—set clear requirements for safeguarding customer data and maintaining secure financial systems. Overall, cyber security regulations aim to minimize operational disruptions, prevent financial losses, and ensure that banks remain resilient against evolving digital threats in an increasingly connected financial ecosystem

5.4. Stress Testing

Stress tests simulate extreme but plausible scenarios—economic downturns, market crashes, geopolitical conflicts—and evaluate whether banks can maintain capital adequacy.

5.5. Enhancements in Stress Testing

Enhancements in stress testing have become a critical component of modern risk management, enabling banks to evaluate their resilience under extreme but plausible adverse scenarios. Unlike traditional approaches that focused mainly on historical risk patterns, contemporary stress testing incorporates forward-looking simulations across credit, market, liquidity, operational, and systemic risks. Advanced models use macroeconomic indicators, scenario analysis, and even AI-driven predictive analytics to assess how shocks—such as economic recessions, interest rate spikes, cyber attacks, or climate-related events—could affect capital adequacy and liquidity positions. Regulatory bodies, including the Basel Committee on Banking Supervision, as well as national authorities like the U.S. Federal Reserve and the European Banking Authority (EBA), mandate regular stress tests to ensure banks maintain sufficient buffers under stress. Enhancements also include integrated enterprise-wide stress testing, automated reporting, and real-time monitoring, which improve decision-making, risk mitigation, and strategic planning. Overall, these developments have transformed stress testing from a regulatory compliance exercise into a proactive tool for resilience and risk-informed management.

6. Emerging Risks Reshaping the Banking Industry

Beyond traditional categories, new risk domains are rising in importance.

6.1. Climate Risk and Environmental Risk

Climate risk refers to the potential negative impacts of climate change on people, economies, ecosystems, and systems. Its importance is growing because it affects nearly every aspect of life and decision-making. Key reasons why climate risk is important include:

6.2. Environmental Protection

Climate risks such as rising temperatures, sea-level rise, floods, droughts, and extreme weather events threaten ecosystems, biodiversity, and natural resources that humans depend on for food, water, and clean air.

6.3. Human Health and Safety

Climate change increases risks of heat waves, disease spread, food insecurity, and water scarcity. Managing climate risk helps protect lives, especially vulnerable populations like children, the elderly, and low-income communities.

6.4. Economic Stability

Unchecked climate risks can damage infrastructure, agriculture, supply chains, and businesses. Assessing climate risk helps governments and companies avoid major financial losses and plan resilient investments.

6.5. National and Global Security

Climate risks can intensify conflicts over resources, drive migration, and destabilize regions. Addressing them is crucial for maintaining social and political stability.

6.6. Business and Financial Decision-Making

Investors and organizations increasingly consider climate risk to assess long-term profitability, insurance costs, and regulatory compliance. Ignoring it can lead to stranded assets and financial shocks.

6.7. Sustainable Development

Understanding climate risk supports better planning for cities, energy systems, transportation, and agriculture—ensuring development that meets present needs without harming future generations.

7. Policy and Governance

Governments use climate risk assessments to design effective climate policies, disaster preparedness plans, and adaptation strategies.

Climate risk has shifted from a theoretical concern to a financial reality. Natural disasters, rising temperatures, and climate-driven economic disruptions threaten asset values, supply chains, and borrower repayment capacity.

7.1. Types of Climate Risks

- **Physical Risk**: damages from extreme weather events.
- **Transition Risk**: financial impacts of moving toward a low-carbon economy.
- **Liability Risk**: legal claims related to environmental harm.

Banks now integrate Environmental, Social, and Governance (ESG) factors into investment and lending decisions.

7.2. ESG Integration and Sustainable Finance

7.2.1. What Is ESG?

ESG stands for **Environmental, Social, and Governance** — a framework used to evaluate how responsibly and sustainably a company operates beyond just financial performance. It has become a central factor in investment, corporate strategy, and risk management worldwide.

ESG (Environmental, Social, and Governance) is important because it helps organizations, investors, and governments evaluate long-term sustainability, ethical impact, and risk beyond traditional financial metrics.

8. Importance of ESG

8.1. Better Risk Management

ESG identifies non-financial risks such as climate change, labor issues, data privacy, and weak governance that can affect long-term performance and stability.

8.2. Long-Term Financial Performance

Companies with strong ESG practices often show better resilience, operational efficiency, and sustainable returns, making them more attractive to long-term investors.

8.3. Investor Confidence and Access to Capital

Investors increasingly use ESG criteria to guide decisions. Strong ESG performance improves transparency and helps companies attract funding at lower costs.

8.4. Regulatory Compliance

Governments worldwide are introducing ESG-related regulations. Adopting ESG early helps organizations stay compliant and avoid penalties.

8.5. Reputation and Brand Value

Good ESG practices enhance corporate reputation, customer trust, and employee loyalty, while poor ESG performance can lead to reputational damage.

8.6. Social Responsibility and Ethical Conduct

ESG promotes fair labor practices, diversity and inclusion, human rights protection, and ethical business behavior.

8.7. Climate and Environmental Protection

The environmental pillar supports responsible resource use, emissions reduction, and climate resilience, contributing to sustainable development.

8.8. Strong Corporate Governance

Governance ensures transparency, accountability, ethical leadership, and effective decision-making.

Banks are increasingly offering:

- Green bonds
- Sustainability-linked loans
- Renewable energy financing
- Climate risk disclosures

Regulators are pushing for greater transparency in ESG reporting.

8.9. Third-Party and Outsourcing Risks

Third-party and outsourcing risks have become a significant concern for banks as they increasingly rely on external vendors, technology providers, and fintech partners to deliver services and support operations. While outsourcing can improve efficiency, reduce costs, and provide access to specialized expertise, it also introduces operational, compliance, and cyber security vulnerabilities. Risks include service disruptions, data breaches, regulatory non-compliance, and dependency on a vendor's financial or operational stability. High-profile incidents, such as outages in cloud-based banking services, have highlighted how failures in third-party systems can directly impact customers and the broader financial system. Regulators, including the Basel Committee on Banking Supervision, emphasize that banks maintain robust vendor risk management frameworks, including due diligence, contractual safeguards, continuous monitoring, and contingency planning. Effective management of outsourcing risks ensures operational resilience, protects customer data, and safeguards institutional reputation while enabling banks to leverage external expertise safely.

8.10. Geopolitical Risk

Geopolitical tensions—sanctions, trade wars, regional conflicts—affect currency markets, investment flows, and supply chains. Banks are creating geopolitical risk dashboards to evaluate exposures in sensitive regions.

9. The Future of Risk Management in Banking

As the financial environment becomes more complex, banks are shifting from a reactive approach to a predictive and proactive model of risk management.

9.1. Enterprise Risk Management (ERM) as a Strategic Function

Risk management is becoming a driver of competitive advantage, not merely a compliance tool. Boards are integrating risk strategy into:

- Digital transformation plans
- Product development
- Market expansion strategies
- Capital planning

ERM functions are gaining influence in strategic decision-making.

9.2. Rise of Integrated Risk Management Platforms

Banks are implementing unified, cloud-based platforms that consolidate data across departments and provide a 360-degree view of risk. These platforms incorporate AI, analytics, and visualization tools for faster decision-making.

9.3. Real-Time Risk Monitoring

Banks are moving toward continuous risk monitoring:

- Real-time liquidity dashboards
- Ai-enabled cyber threat detection
- Real-time fraud alerts
- Daily stress testing simulations

This enables immediate corrective action.

9.4. Ethical and Responsible Use of AI

As AI becomes central to decision-making, ethical risks emerge:

- Algorithmic bias
- Privacy concerns
- Model explainability issues

Regulators require transparency in how AI models make decisions, especially in credit scoring and fraud detection.

9.5. Model risk governance in Indian banks

Model risk governance in Indian banks requires significant investment in technology, data infrastructure, and skilled human resources. Banks need advanced analytics platforms, robust data management systems, and independent model validation frameworks. Investment is also needed in training professionals with expertise in quantitative modeling, AI, and risk analytics. However, challenges include high implementation costs, limited availability of quality data, and dependence on legacy IT systems. Smaller banks may struggle with resource constraints. Additionally, ensuring regulatory compliance under the Reserve Bank of India adds complexity. Balancing innovation with strong governance and transparency remains a key challenge for sustainable model risk management.

9.6. Risk-Based Supervision (RBS)/SPARC

Risk-Based Supervision (RBS) is an approach used by the Reserve Bank of India to monitor banks based on their risk levels. Instead of uniform supervision, RBI focuses more on banks with higher risks. It evaluates risks like credit, market, liquidity, and operational risks, along with governance and internal controls. Banks are assigned risk scores, and supervision intensity is decided accordingly. RBS helps in early detection of problems, efficient use of resources, and promotes better risk management. This approach strengthens financial stability and reduces the chances of bank failures in the banking system.

9.7. Data quality issues

Data quality is a critical challenge in risk management for banks. Inaccurate, incomplete, or outdated data can lead to faulty risk assessment, mispricing of credit, and inadequate capital allocation. Poor data quality affects stress testing, model validation, and early warning systems, increasing the likelihood of non-performing assets. Indian banks often face fragmented data across legacy systems, inconsistent reporting standards, and limited integration, making timely and reliable risk evaluation difficult. Under the supervision of the Reserve Bank of India, banks are encouraged to improve data governance, standardize processes, and implement robust IT systems to enhance accuracy and support effective risk management.

9.8. What went wrong ?

A notable case of risk management failure in Indian banks is the **Punjab National Bank (PNB) fraud in 2018**. Bank officials failed to detect fraudulent Letters of Undertaking (LoUs) issued to Nirav Modi and associates. Weak internal controls, poor monitoring, and inadequate risk assessment allowed ₹11,400 crore in undetected exposures. The incident highlighted lapses in operational risk management, internal audits, and data verification processes. It exposed how over-reliance on manual approvals, lack of cross-verification, and insufficient governance can lead to massive financial losses. This case became a landmark example for strengthening risk management frameworks under RBI supervision.

Another notable case is the **Yes Bank crisis of 2020**. Rapid credit growth, aggressive lending, and weak internal risk controls led to a surge in non-performing assets (NPAs). The bank's overexposure to stressed sectors, coupled with inadequate monitoring and poor governance, caused liquidity stress and eroded investor confidence. Delayed recognition of bad loans and gaps in credit risk assessment worsened the situation. The Reserve Bank of India had to intervene, imposing a reconstruction plan and management changes. This case illustrates how poor credit risk management and governance failures can threaten the stability of a financial institution.

A recent example of risk management failure in Indian banking is the **₹590 crore suspected fraud at** IDFC First Bank**'s Chandigarh branch**, disclosed in early 2026. Officials allegedly colluded with external parties using forged instruments to siphon funds from government-linked accounts, exposing gaps in internal controls, verification processes, and

operational risk oversight. The incident led to regulatory reporting, suspension of staff, forensic audits, and market backlash, highlighting weaknesses in governance, transaction monitoring, and risk detection systems. It underscores the importance of robust risk management practices and strong internal controls to prevent large-scale fraud and protect financial stability.

10. Conclusion

Risk management in banking has shifted from a compliance task to a strategic imperative, critical for resilience and competitiveness. As financial systems become more interconnected and digital, banks face not only traditional credit, market, and operational risks, but also cyber threats, climate-related challenges, geopolitical uncertainty, and technology-driven vulnerabilities. Advanced tools like AI, machine learning, and blockchain enhance real-time risk assessment and predictive insights, yet introduce new oversight and ethical demands. Strengthened regulatory standards and the rising importance of ESG metrics make robust governance and climate-conscious strategies essential. In this dynamic landscape, effective risk management is no longer optional—it is the foundation of sustainable banking.

References

[1] Risk Management — by K. Ramakrishna**;** General risk management book with banking applications.

[2] Reserve Bank of India (2002).; Risk Management Systems in Banks**.** RBI Circular / Guidance Note. This guideline explains that banks face multiple financial and non-financial risks such as credit risk, liquidity risk, market risk, operational risk and reputational risk. It emphasizes board-approved policies, risk measurement systems and prudential limits for effective risk control.

[3] Reserve Bank of India (Basel II – ICAAP Guidelines). Supervisory Review Process (SRP) and Internal Capital Adequacy Assessment Process (ICAAP). RBI requires banks to internally assess all material risks and maintain adequate capital buffer consistent with their risk profile. ICAAP must be Board-approved and include stress testing and monitoring systems.

[4] Reserve Bank of India (Risk-Based Supervision Framework – SPARC). Risk Based Supervision of Banks in India. RBI introduced a forward-looking supervisory framework focusing on identification of major risks, adequacy of capital and effectiveness of risk management controls in banks.

[5] Reserve Bank of India – Interest Rate Risk in Banking Book (IRRBB) Master Directions. Banks must assess capital requirement for interest rate risk and develop internal methodologies aligned with their risk appetite and ICAAP framework.

[6] Reserve Bank of India Committee Report on Risk Based Supervision. Highlights migration from compliance-based supervision to risk-focused supervision to enable early identification of vulnerabilities and improve overall risk culture in banks.