Grant Thornton Bharat

ICAI - Physical cum Virtual Regional Banking Summit

Risk Management through Technology and Artificial Intelligence / Data Analytics / Blockchain

February 2021

Learning Objectives

01 Evolution of risk management

02 Risk management - Overview

03 Future of risk management across banks

04 Regulatory landscape – Risk management in banks and key risks

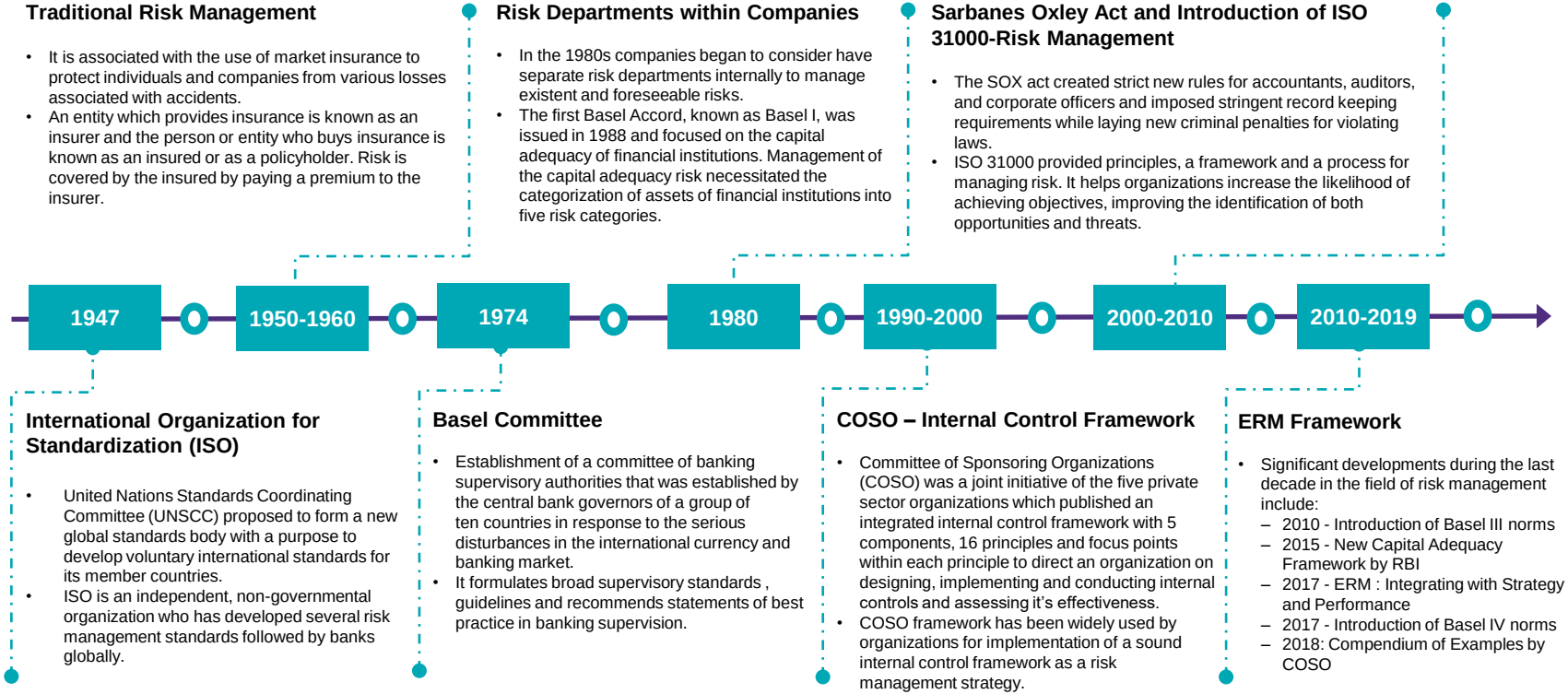
05 Risk management and technology

06 Case studies

Grant Thornton Bharat

1. Evolution of risk management

Evolution of risk management - Timeline



Traditional Risk Management

- It is associated with the use of market insurance to protect individuals and companies from various losses associated with accidents.
- An entity which provides insurance is known as an insurer and the person or entity who buys insurance is known as an insured or as a policyholder. Risk is covered by the insured by paying a premium to the insurer.

Risk Departments within Companies

- In the 1980s companies began to consider have separate risk departments internally to manage existent and foreseeable risks.
- The first Basel Accord, known as Basel I, was issued in 1988 and focused on the capital adequacy of financial institutions. Management of the capital adequacy risk necessitated the categorization of assets of financial institutions into five risk categories.

Sarbanes Oxley Act and Introduction of ISO 31000-Risk Management

- The SOX act created strict new rules for accountants, auditors, and corporate officers and imposed stringent record keeping requirements while laying new criminal penalties for violating laws.
- ISO 31000 provided principles, a framework and a process for managing risk. It helps organizations increase the likelihood of achieving objectives, improving the identification of both opportunities and threats.

International Organization for Standardization (ISO)

- United Nations Standards Coordinating Committee (UNSCC) proposed to form a new global standards body with a purpose to develop voluntary international standards for its member countries.
- ISO is an independent, non-governmental organization who has developed several risk management standards followed by banks globally.

Basel Committee

- Establishment of a committee of banking supervisory authorities that was established by the central bank governors of a group of ten countries in response to the serious disturbances in the international currency and banking market.
- It formulates broad supervisory standards , guidelines and recommends statements of best practice in banking supervision.

COSO – Internal Control Framework

- Committee of Sponsoring Organizations (COSO) was a joint initiative of the five private sector organizations which published an integrated internal control framework with 5 components, 16 principles and focus points within each principle to direct an organization on designing, implementing and conducting internal controls and assessing it's effectiveness.
- COSO framework has been widely used by organizations for implementation of a sound internal control framework as a risk management strategy.

ERM Framework

- Significant developments during the last decade in the field of risk management include:
  - 2010 - Introduction of Basel III norms
  - 2015 - New Capital Adequacy Framework by RBI
  - 2017 - ERM : Integrating with Strategy and Performance
  - 2017 - Introduction of Basel IV norms
  - 2018: Compendium of Examples by COSO

Grant Thornton Bharat

2. Risk management - Overview

Risk management - Overview

Risk management is the process of identifying, evaluating, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters. It involves making and carrying out decisions that will minimize the adverse effect of risks on an organization through various risk management strategies.

Risk management process

1. **Risk identification :** The bank identifies and defines potential risks that may negatively influence a process or project. Risk sources must be identified and classified at the earliest to ensure that an effective overall risk assessment process is established.
2. **Risk analysis :** The bank determines the odds of the identified risks occurring, as well as its consequences. The goal of the analysis is to further understand each specific instance of risk, and how it could influence the company's projects and objectives.
3. **Risk evaluation :** The risk is then evaluated after determining it's overall likelihood of occurrence and consequence. The bank can then make decisions on whether the risk is acceptable and whether it is willing to take it on based on its risk appetite.
4. **Risk mitigation :** Banks assess their highest-ranked risks and develop a plan to alleviate them using specific risk controls. These plans include risk mitigation processes, risk prevention tactics and contingency plans in case the risk materializes. It involves development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level basis the bank's risk appetite. One of the 4 risk management strategies are identified and implemented.
5. **Risk monitoring :** Part of the mitigation plan includes following up on both the risks and the overall plan to continuously monitor and track new and existing risks. The overall risk management process is also to be reviewed and updated accordingly. Once a risk mitigation plan is implemented in the previous phase, it is continuously monitored to assess its efficacy with the intent of revising the course-of-action, if needed.

Risk management strategies

1. **Risk avoidance :** While the complete elimination of all risk is rarely possible, a risk avoidance strategy is designed to deflect as many threats as possible in order to avoid the costly and disruptive consequences of a damaging event.
2. **Risk transfer** : Sometimes, the consequences of a risk is shared, or distributed amongst several of the project's participants or bank's departments. The risk could also be shared with a third party, such as a vendor or business partner.
3. **Risk reduction** : Banks are able to reduce the amount of effect certain risks can have on their processes. This is achieved by adjusting certain aspects of an overall project plan or bank process, or by reducing its scope post risk value analysis.
4. **Risk retaining (Accept) :** Sometimes, banks may decide whether a risk is worth it from a business standpoint or not and choose to retain the risk and deal with any potential fallout. Banks will often retain a certain level of risk that a project has, where the anticipated profit is greater than the costs of its potential risk.

ISO 31000 is a family of standards relating to risk management codified by the International Organization for Standardization. The ISO recommended that the following target areas or principles should be a part of the overall risk management process:

1. It should create value for the organization.
2. It should be an integral part of the overall organizational process.
3. It should factor into the company's overall decision-making process.
4. It must explicitly address any uncertainty.
5. It should be systematic and structured.
6. It should be based on the best available information.
7. It should be tailored to the project.
8. It must take into account human factors, including potential errors.
9. It should be transparent and all-inclusive.
10. It should be adaptable to change.
11. It should be continuously monitored and improved upon.

Source : blog by* Hadi Fadlallah on *towardsdatascience.com

Grant Thornton Bharat

Risk management - Key concepts

Governance, Risk and Compliance (GRC)

- Governance, risk and compliance (GRC) is the **umbrella term covering an organization's approach across these three areas**: Governance, risk management, and compliance.
- GRC is formally defined as "the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity."
- GRC is a discipline that **aims to synchronize information and activity across governance, risk management and compliance** in order to operate more efficiently, enable effective information sharing, report activities more effectively and avoid wasteful overlaps.
- Although interpreted differently in various organizations, **GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance** with applicable laws and regulations.
- Each of these three disciplines creates information of value to the other two, and **all three impact the same technologies, people, processes and information**.
- Substantial duplication of tasks evolves when governance, risk management and compliance are managed independently. **Overlapping and duplicated GRC activities negatively affect both operational costs and GRC matrices**.

Enterprise Risk Management (ERM)

- COSO 2017 ERM Framework defines ERM as the culture, capabilities and practices , integrated with strategy-setting and performance that organizations rely on to manage risks in creating, preserving and realizing value.
- It focuses on managing risks through recognizing culture, developing capabilities, applying practices, integrating with strategy setting and performance, managing risk to achieve strategy and business objectives and linking it to value.
- The Institute of Internal Auditors (IIA) states that ERM is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.
- It encompasses all stakeholders and not merely those who are directly affected by the product or service offerings of a company.
- ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators and society overall.

Operational Risk Management (ORM)

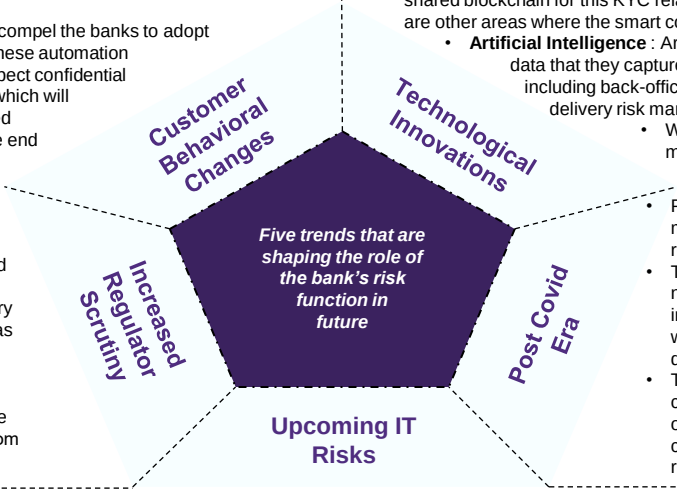
- Operational Risk Management (ORM) is a subset of Enterprise Risk Management. It includes operational and legal risk only. It is generally measured in terms of operational losses and foregone income through control and self assessment (CSA).
- It is a continuous cyclic process which includes risk assessment, risk decision making and implementation of risk controls, which results in acceptance, mitigation or avoidance of risk. ORM is the oversight of operational risk, including the risk of loss resulting from inadequate or failed internal processes, systems, human factors or external events.
- Unlike ERM which flows down from a "tone at top" , ORM is embedded at the more micro level of individual processes.
- Banks often have an independent operational risk management function which conducts a periodic self assessment of functions across the bank to identify and assess risks, define and implement relevant controls and manage the likelihood and potential impact of any foreseeable risks.
  - The basic principles of ORM are:
  - Accept risk when benefits outweigh the cost.
  - Accept no unnecessary risk.
  - Anticipate and manage risk by planning.
  - Make risk decisions at the right time and at the right level.

3. Future of risk management across banks

Future of risk management across banks

- Over the last decade, an increase in the technological innovations in the BFSI space has resulted in multiple startups and financial technology players emerge as competitors to banks. Through apps and simplified mode of digitized banking solutions, they have been attracting customers that have been over the years inclined towards traditional banking methods.
- In line with these, banks will need to quickly digitize their banking model to ensure seamless and instant responses to retail and corporate customer requests on account opening, disbursal, re-payment and re-financing.
- While in the longer run, behavioral changes of the customer will compel the banks to adopt technology that will enable banks to offer customized services, these automation changes will create new risks not previously anticipated with respect confidential data protection and usage of personally identifiable information which will need to be managed and mitigated. This will necessitate the need for risk management processes to become an integral part of the end to end customer lifecycle.

- **Augmented Reality :** The end-state in the banking sector by using augmented reality is to give customers complete autonomy in actions and transactions they could perform at home. Hybrid branches are envisioned by technology experts who believe that bank branches as we know them today are a thing of past.
- **Blockchain** : Banks will see a huge saving by using blockchain technology in the KYC operations. Business models are being developed currently which would ensure that they could rely on a shared blockchain for this KYC related activities. Syndicated loans, trade finance and payments are other areas where the smart contracts on blockchain could be highly effective.
- **Artificial Intelligence** : Artificial Intelligence allows banks to use the large histories of data that they capture to make much better decisions across various functions including back-office operations, customer experience, marketing, product delivery risk management, and compliance.
- While such technologies will help banks expedite processes, management of associated risks will become critical as well.



- With an increase in the technological innovations in the field of financial services, the regulators have been following a sandbox approach that allows time-bound testing of financial products and innovations under their oversight.
- The future of internal bank models for the calculation of regulatory capital, as well as the potential use of a standardized approach as a floor (Basel IV) has been agreed on in 2017 and is due for implementation in January 2023.
- New regulations, norms and revised regulatory guidelines have resulted in enhanced scrutiny by the regulator with a focus on the bank's ability to successfully identify and mitigate risks arising from the use of these innovations.

- Post the pandemic, the pressure on banks to maintain adequate margins along with appropriate capital and liquidity requirements will be their key focus area.
- To maintain sufficient margins, the operating costs of banks will need to be substantially lower and cost savings will become as important as generating revenues. The most effective measures would be simplification and standardization of processes and digitization of models.
- The risk function of a bank will need to play its part in reducing costs in ways that help achieve the overall risk management objective of the bank such as implementing a strong automated control framework that can reduce human intervention and thus, reduce associated costs

- **Social engineering attack :** It is the psychological manipulation of people into performing actions or divulging confidential information. The risk function of banks will need to be ensure that customers are made more aware of these risks and are well informed and equipped to deal with them.
- **Cybersecurity risk** : It is the probability of exposure or loss resulting from a cyber attack or data breach on the bank. With new age technologies coming into the fore the risk faced by banks from external sources such as hackers has increased manifold. Data protection will be the key focus of the risk management function of banks while managing ancillary risks emerging from leveraging technologies.

- By understanding these key risks, banks will be better positioned to leverage relevant technologies and use them appropriately to manage risks. Prudent risk management will also help banks improve profits as they sustain fewer losses on loans and investments.
- Information risk management system must also be made an integral part of the overall risk management framework of the bank with a focus on emerging IT and IS risks.

Grant Thornton Bharat

Future of risk management – How banks can prepare themselves

Diversify the talent pool

- Building the right mix of talent with technology is important. Data scientists will be needed to collaborate across the bank to translate data points to organization objectives.
- Risk managers would need to become an integral part of business areas, while traditional operational areas will work with lower human intervention and increased automation.
- Hiring talented employees will be tricky for traditional banks , as potential candidates would prefer financial technology firms unless banks strengthen their value propositions.

Leverage technological innovations

- Risk functions should leverage advanced analytics, machine learning and artificial intelligence tools to enhance the accuracy of their predictive models.
- Risk functions can be expected to leverage tools for a number of purposes including financial-crime detection, transaction monitoring, early-warning systems and collections in the retail and small and medium size enterprise segments.

Improves risk reporting framework

- Replacing paper-based reports with system based reports that offer information in real time and enable risk managers to conduct a root-cause analysis and would enable banks to make better decisions.
- While regulatory requirements have been pushing towards improving the quality of data used in risk reports and improving the timeliness of the same, focus need to be given to the format of reports or how they could be used to make decisions which may be driven internally by the bank's risk management function

Strengthen the risk-management culture

- A strong central risk management culture which is drilled down by following a top down approach will help the banks prepare for the future.
- The detection, assessment, and mitigation of risk must become part of the daily job of all bank employees and not only those in risk functions.
- With automation and more sophisticated analytical and technical capabilities, human intervention will be needed to ensure appropriate and ethical application.

Automate business processes

- Digitization of core business processes such as client onboarding, KYC verification and credit score generation will help to reduce both potential nonfinancial risks and operating expenses.
- Risk function can help speeden up the digitization of core risk processes, such as credit applications and underwriting, by approaching businesses with potential solutions from an integrated risk standpoint.
- Improved efficiency and a better overall customer experience will be potential additional benefits.

Grant Thornton Bharat

4. Regulatory landscape – Risk management in banks and key risks

Regulatory landscape - Risk management in banks

Key regulatory requirements pertaining to risk management in banks in line with the "**RBI Notification on Risk Management in Banks**"

Organisational Structure

- Banks should have an appropriate structure for risk management.
- Well defined structure provides a clear path for risk assessment.

Risk Measurement

- The risk measurement approach adopted in terms of the various financial and non-financial risks in the banking system should be comprehensive.

Risk Management Policies

- The risk management policies should clearly spell out the quantitative prudential limits on various segments of banking operations.
- Such policies should be able to identify new risks as well.

Guidelines and Parameters

- Banks should have comprehensive guidelines and parameters in place which act as a cushion to the various risks to which the banks are exposed.

Strong MIS capability

- There should be a strong MIS system in place for reporting, monitoring and controlling risks.
- The MIS should be consistent in quality and should ensure the integrity and reliability of data.

Risk Reporting Framework

- There should be well laid out procedures, effective controls and a comprehensive risk reporting framework.

Risk Management Framework

- There should be a separate risk management framework independent of the operational departments and with clear delineation of levels of responsibility for management of risk.

Periodic Reviews

- Periodic reviews are essential to assess the effectiveness of a bank's risk management framework. It is necessary to ensure that the framework continues to evolve and meet the needs of the bank

Overall objectives of the Banking Regulations

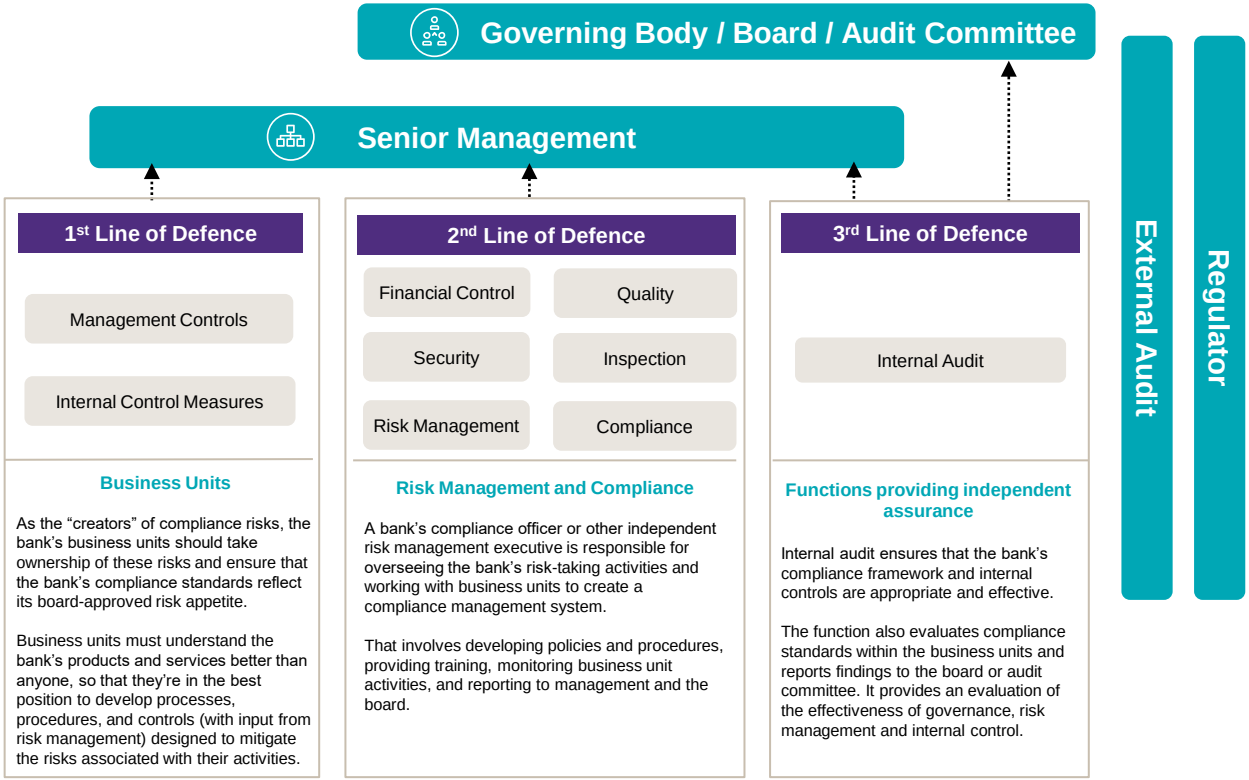
- **Protection of depositors:** Deposits held by banks belong to public and they needs to be protected. Banking in most countries works on the concept where deposits are only partially backed by reserves. The objective of banking regulations is to reduce the level of potential risk faced by depositors.
- **Systemic risk reduction:** Banking regulations are enforced to ensure that fluctuations in business activities and issues at an individual bank do not impact the overall flow of transactions in the economy.
- **Efficient and competitive financial system:** Regulatory framework encourages competition and ensures adequate level of banking services throughout the economy. It enables a competitive environment conducive to changing economic conditions and technological advances.
- **Avoiding money laundering:** Another aim of banking regulations is to avoid the misuse of the banking system to disguise the true source of funds or conceal the ultimate disposition of the funds.
- **Credit allocation:** Banks play an important role in taking care of small scale sectors that may impact large segments of the population or employment intensive sectors such as agriculture.

Key areas of RBI focus governed through its banking regulations

1. Liquidity management requirements like maintaining minimum capital ratios.
2. Financial reporting and disclosure requirements to ensure accuracy and reliability.
3. Restrictions on large exposures of banks to individuals or groups to safeguard capital from unnecessary risk.
4. Market discipline through transparency and financial disclosure requirements.
5. Credit rating requirements to provide an estimation of the absolute and relative risk undertaken the bank.
6. Supervisory reviews by providing directions and ensuring compliance.

Grant Thornton Bharat

Banking risk management framework



- The "three lines of defence" model helps banks to identify and structure interactions amongst and responsibilities of key stakeholders. This helps in achieving alignment to business objectives, effective collaboration, and clear accountability across functions.
- It encourages the governing body to provide direction and delegate responsibilities to each line of defence. This simplifies the overall management of risks that can be identified across the bank.
- This approach significantly improves the bank's risk governance and provides greater assurances to both regulators and shareholders.

Grant Thornton Bharat

Key risks faced by banks

Environmental, Social & Governance Risk (ESG)

ESG risk is the consideration of nonfinancial risks arising from environment and sustainability, reputation or brand, legal, technological, product or service quality, labor, ethical conduct, compliance, and strategic considerations. Currently, the FS sector is witnessing a shift of focus from the financial aspects of internal control systems to the nonfinancial aspects. The risks arising from these non-financial aspects such as environmental and customer detriment need to be taken into consideration while developing the risk culture of any bank. The last decade has seen a significant rise in the consumer awareness due to easy access to information and data and hence , the impact of ESG risks must be built into the integrated risk management framework of the bank.

Credit Risks

Credit risk is the biggest risk for banks. It occurs when borrowers or counterparties fail to meet contractual obligations such as when borrowers default on a principal or interest payment of a loan, failure to meet obligational contracts in areas such as derivatives and guarantees provided. While banks cannot be fully protected from credit risk due to the nature of their business model, they can lower their exposure in several ways. Since deterioration in an industry or issuer is often unpredictable, banks lower their exposure through diversification. Recent innovations have resulted in development of multiple credit risk management tools and technologies which help banks in managing and mitigating the credit risk faced by them.

Market Risks

Market risk mostly occurs from a bank's activities in capital markets. It is due to the unpredictability of equity markets, commodity prices, interest rates, and credit spreads. Banks are more exposed if they are heavily involved in investing in capital markets or sales and trading. Commodity prices also play a role because a bank may be invested in companies that produce commodities. As the value of the commodity changes, so does the value of the company and the value of the investment. Artificial intelligence and machine learning tools are being used by banks globally to predict movements in markets and commodities helping the bank choose the risk mitigation strategy accordingly.

Liquidity Risks

Liquidity risk refers to how a bank's inability to meet its obligations (whether real or perceived) threatens its financial position or existence which is why it is highly prioritized and managed. Financial institutions manage their liquidity risk through effective asset liability management (ALM). Liquidity risks are easier to manage with technology due to its quantitative nature through analysis of quantifiable data, updation of the model built or adopted by a bank within the risk management software and constant monitoring of defined limits or financial ratios. Key risk indicators or metrics that directly or indirectly affect risks can be tracked in real-time and help banks detect emerging risks.

Regulatory Risks

Regulatory risks have always been uniquely important for heavily regulated industries such as banking. RBI guidelines, Basel norms and several other applicable regulations steer the operations of the banking industry by aligning it with the prevalent economic environment of the country. Assessing the severity of regulatory changes and understanding the changes themselves is now built into the scope of several risk management solutions post the development of natural language processing. It gives computers a better understanding of the written word which has resulted in risk management solutions gaining the ability to parse regulatory documents, quickly detect additions and changes and manage regulatory risks more effectively.

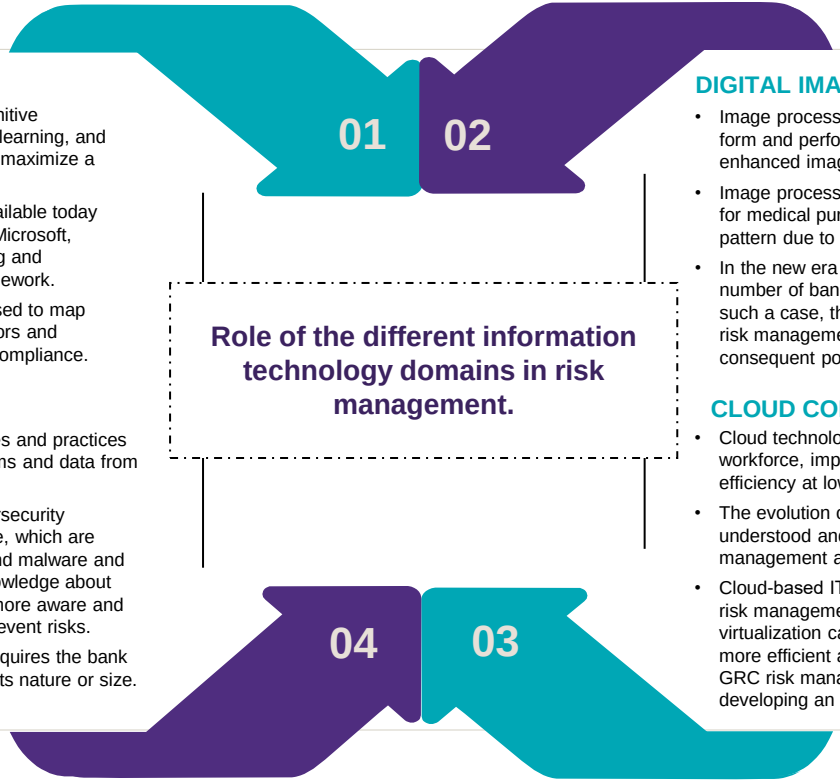
Operational Risks

Operational risks largely revolve around the actions of employees and businesses instead of data or numbers. Operational risks arise when there is a process that may be violating a regulation or compliance requirement and increasing the overall risk exposure of the organization. One cannot keep a track of all the actions taken by all employees in an organization in real-time, which is why banks have struggled a lot in minimizing these risks. Centralized operational risk management solutions track these actions and detect problems instantly. The technology focuses on making these assessments as fast and accurate as possible. This is accomplished by providing a centralized platform that accepts standardized data, ensuring that operational risk data is easily available for analysis. This means that risk managers can easily access all the data they need for which previously they had to spend hours collecting and extracting the data for analysis.

Grant Thornton
Bharat

5. Risk management and technology

Risk management and technology



ARTIFICIAL INTELLIGENCE

- Intelligence exhibited by machines that mimic cognitive functions and human processes such as thinking, learning, and predicting is embedded in networked machines to maximize a certain goal or achieve an objective.
- In addition, since the technology is often freely available today from major developers such as Google, IBM and Microsoft, banks are able to leverage the same for enhancing and strengthening their existent risk management framework.
- In risk management artificial intelligence can be used to map policies, procedures, and controls with the regulators and regulatory changes to improve the organizations compliance.

CYBERSECURITY

- Cybersecurity is a body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
- Risk managers can benefit from the leading cybersecurity companies like Symantec, Kaspersky and McAfee, which are publishing periodically stating the latest threats and malware and system breaches. This would give them more knowledge about risks that can occur by using technologies to be more aware and to choose the appropriate security defenses to prevent risks.
- The constantly evolving nature of security risks requires the bank to manage all foreseeable threats irrespective of its nature or size.

Role of the different information technology domains in risk management.

DIGITAL IMAGE PROCESSING

- Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it.
- Image processing was introduced as a tool for risk assessment for medical purposes by observing asymmetry in the heat pattern due to temperature differences.
- In the new era post covid, the virtual world will necessitate a number of banking processes to be virtual and digitized. In such a case, the use of digital image processing in the field of risk management to ensure early detection of errors and consequent potential risks will be critical for banks.

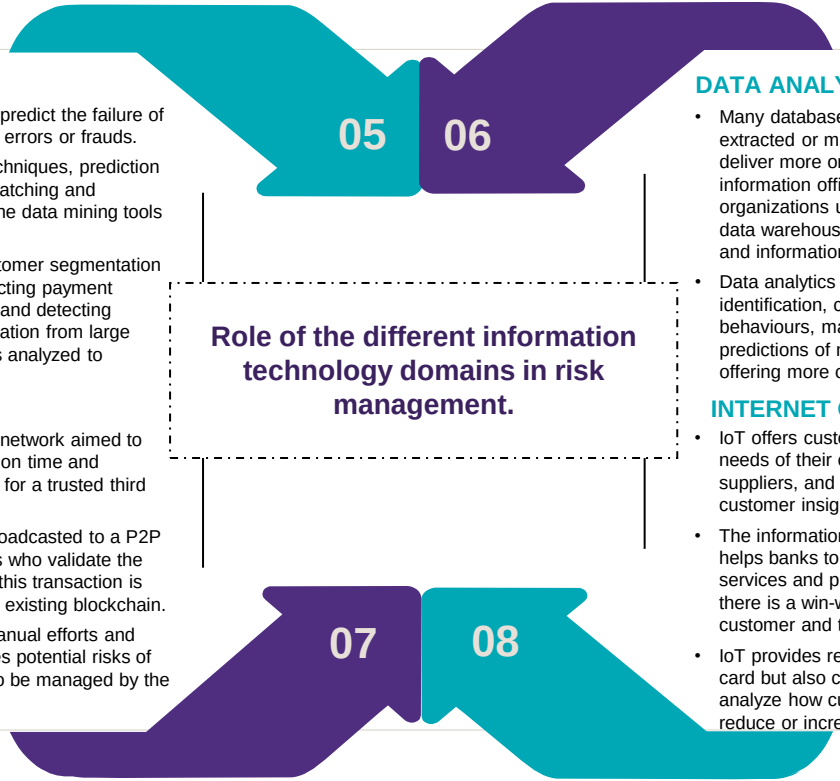
CLOUD COMPUTING

- Cloud technologies are providing greater flexibility for the workforce, improved productivity, broader insight, and higher efficiency at lower costs as compared to on-premise solutions.
- The evolution of cloud-based IT environment needs to be understood and considered when evaluating GRC risk management applications.
- Cloud-based IT environments that provide “on-demand” GRC risk management software as a service (SaaS) exploit the virtualization capabilities and provide tenant users with even more efficient and cost-effective alternatives than buying a GRC risk management application and running it in house or developing an in-house tool.

Source : blog by* Hadi Fadlallah on *towardsdatascience.com

Grant Thornton Bharat

Risk management and technology



DATA MINING

- Banks can benefit from data mining techniques to predict the failure of components or internal systems to identify system errors or frauds.
- Used in combination with the other data mining techniques, prediction involves analyzing trends, classification, pattern matching and mapping. By analyzing past events or instances, the data mining tools can make predictions about an event.
- Leading banks are using data mining tools for customer segmentation and profitability, credit scoring and approval, predicting payment defaults, operational risk management, marketing and detecting fraudulent transactions. These tools extract information from large sets of data and ensure that the right set of data is analyzed to identify anomalies.

BLOCKCHAIN

- It is a decentralized ledger of all transactions in a network aimed to increase security, reduce cost, decrease transaction time and increase transparency, while eliminating the need for a trusted third party.
- Once a transaction is requested by a user, it is broadcasted to a P2P network consisting of computers, known as nodes who validate the transaction using cryptography. Post verification, this transaction is represented as a new block which is added to the existing blockchain.
- While blockchain increases efficiency, reduces manual efforts and improves collaboration amongst peers, it increases potential risks of data leakage and security concerns which need to be managed by the bank.

Role of the different information technology domains in risk management.

DATA ANALYTICS

- Many databases contain risk data points that can also be extracted or mined by more powerful computing platforms to deliver more organizational value over time. Tools that chief information officers (CIOs) and chief risk officers (CROs) of organizations use to help facilitate such efforts include electronic data warehouses (EDWs), business intelligence (BI) applications, and information analytical technologies.
- Data analytics can help manage fraud risk by timely fraud identification, credit risk by analysing and predicting user behaviours, market risk by allowing better simulations and predictions of market and companies and operational risk by offering more control and knowledge over interaction with clients.

INTERNET OF THINGS (IoT)

- IoT offers customer data that helps banks identify the business needs of their customers, their value chain for including retailers, suppliers, and distributors. The data also helps banks to gain customer insights.
- The information about customers that is available through IoT helps banks to provide value-added services, customized banking services and products, and financial assistance to ensure that there is a win-win situation for the parties involved i.e. the customer and the bank.
- IoT provides rewarding, easy-to-access services not only to debit card but also credit card customers. The banks are able to analyze how customers use ATM kiosks in various areas and reduce or increase the installation of ATMs accordingly.

Source : blog by* Hadi Fadlallah on *towardsdatascience.com

Grant Thornton Bharat

Tools and technologies in risk management

1 Robotic Process Automation (RPA) for operational efficiencies

- Banks, FIs and insurance companies can improve the speed and accuracy of their core business processes by using robotic process automation (RPA) to replicate user actions to reduce human intervention in manually intensive processes.
- RPA is helpful to track and monitor compliance-evidencing & audit trails by integrating front and back-end systems. Further, improving control by ensuring consistent adherence to set rules, with minimum human intervention.
- Compliance processes like addressing reporting obligations & supervision related to regulatory reporting are automated by using RPA. FIs are targeting on increasing process efficiency while reducing the time taken to complete the process by incorporating RPA.

2 Natural Language Processing (NLP) for KYC verification

- Banks and FIs can use NLP to assess in amending and updating their internal policy requirements by anticipating process regulations, guidelines and compliance requirements.
- Banks can also monitor customers for KYC compliance requirements by using NLP and can even apply it to customer interactions.
- Banks can apply NLP to customer interactions to scrutinise it and identify policy deviations, if any.
- Banks and FIs are reducing the client onboarding and KYC timelines by leveraging NLP. Quick documentation turnaround time in the virtual environment is possible with the use of NLP.

Key technologies leveraged in risk management

3 AI-ML based compliance and transaction monitoring

- Banks detect & determine fraudulent transactions by leveraging AI-ML models based on self-learning algorithms which is an approach to monitor & highlight fraudulent transactions. The models study customer activities & transactions to analyse patterns & identify suspicious activities.
- AI-ML helps in developing a review & monitoring framework such as implementing a 4-eye mechanism for signing-off on the transactions reported to the regulator, creating a dashboard to perform an aging analysis of the responses received from regulators to help the team address reporting obligations.

4 Augmented and Virtual Reality (AR-VR) for training

- FIs are enhancing employee skill set by leveraging augmented and virtual reality (AR-VR) for providing trainings.
- Banks can create a virtual experience of simulations or role plays to train their employees on compliance norms.
- These tools can prove to be very helpful in preparing the employees to be equipped to meet the ever-changing requirements of the banking sector an enhance the digital experience of customers.

5 Voice/Speech and Facial Recognition Software for compliance monitoring

- Banks and FIs conduct trade surveillance and compliance monitoring with the help of voice & speech recognition software which enables them to minimize unauthorized & insider trading and activities related to money laundering.
- Voice/speech and facial recognition software is further used to meet KYC requirements and reduce the compliance burden.
- On real time basis, speech recognition technology helps to automate workflow and mitigate risk of fines.
- The speech recognition capability assists in mitigating the bank's risk of being penalized thus helping them to reduce their liability for fines.

6 Big Data and Machine Learning for superior risk and asset management

- Reducing risk in asset management and removing cognitive biases by detecting patterns in transactions and trades.
- For making informed decisions related to credit monitoring, guideline monitoring, and breach remediation of portfolios banks make use of structured and unstructured data.
- Banks can use Big Data for shaping policies by giving pop ups regarding latest regulations and guidelines
- Machine learning can help with most portfolio construction tasks like idea generation, alpha factor design, asset allocation, weight optimization, position sizing and the testing of strategies.

7 Cloud based software solutions

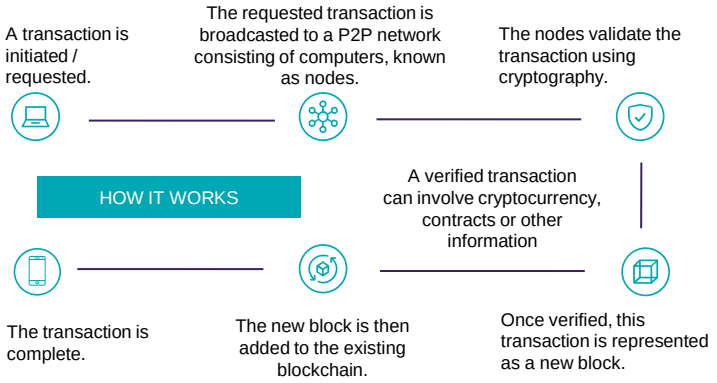
- Banks and Financial Institutions use cloud-based software solutions for :
  - Validating and standardizing their transactional details
  - Identifying accounting entries with a heightened risk of potential fraud
  - Streamlining the transaction of information for effective project management
  - generating dashboards to explore analytics in real time.

8 Aadvanced Analytics and Risk Reporting

- To improve data quality, risk aggregation and risk reporting timelines, advanced risk reporting capabilities in management information systems is used.
- To identify deviations and anomalies quicker and more precisely and in real time, risk reporting systems analysis the granular behavioral patterns of customer behavior.
- To identify, prevent and decrease cross-market and cross-sector financial risks, People's Bank of China leverages AI, Big Data and cloud computing capabilities.

Grant Thornton Bharat

Risk management and blockchain



Cryptography - Integrity and security of the information on the blockchain are ensured with cryptographic functions.

Distributed Ledger - Every participant in the network has simultaneous access to view the information.

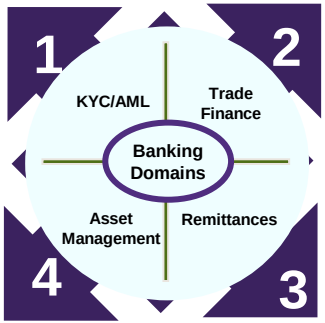
Consensus - Verification is done by participants confirming changes with one another thereby replacing the need for a third party to authorise transactions.

Workload optimization - Facilitates near real-time data availability and transparency that can eliminate the need for reconciliation.

Reduced latency and higher efficiency - Combination of distributed data and pre-determined rules further reduce errors and lag time.

Utility of the blockchain technology across key banking domains

- Utilising the immutable nature of the blockchain, banks have implemented this technology to minimise log tampering and assist in monitoring complex transactions in an automated and effective manner.
- The blockchain technology is applied to identify and use all the valid existing data already stored in multiple systems of record, such as those relating to loan applications and bank account openings, thereby reducing the need for manpower focused on KYC tasks and shortening the processing time for applications.
- The distributed ledger technology (DLT) permits the banks to remove intermediaries and provide a trusted and shared view of authorized and permissioned data amongst key stakeholders.
- It enhances transparency, reduces intermediaries and creates direct linkage between fund managers and distribution platforms.

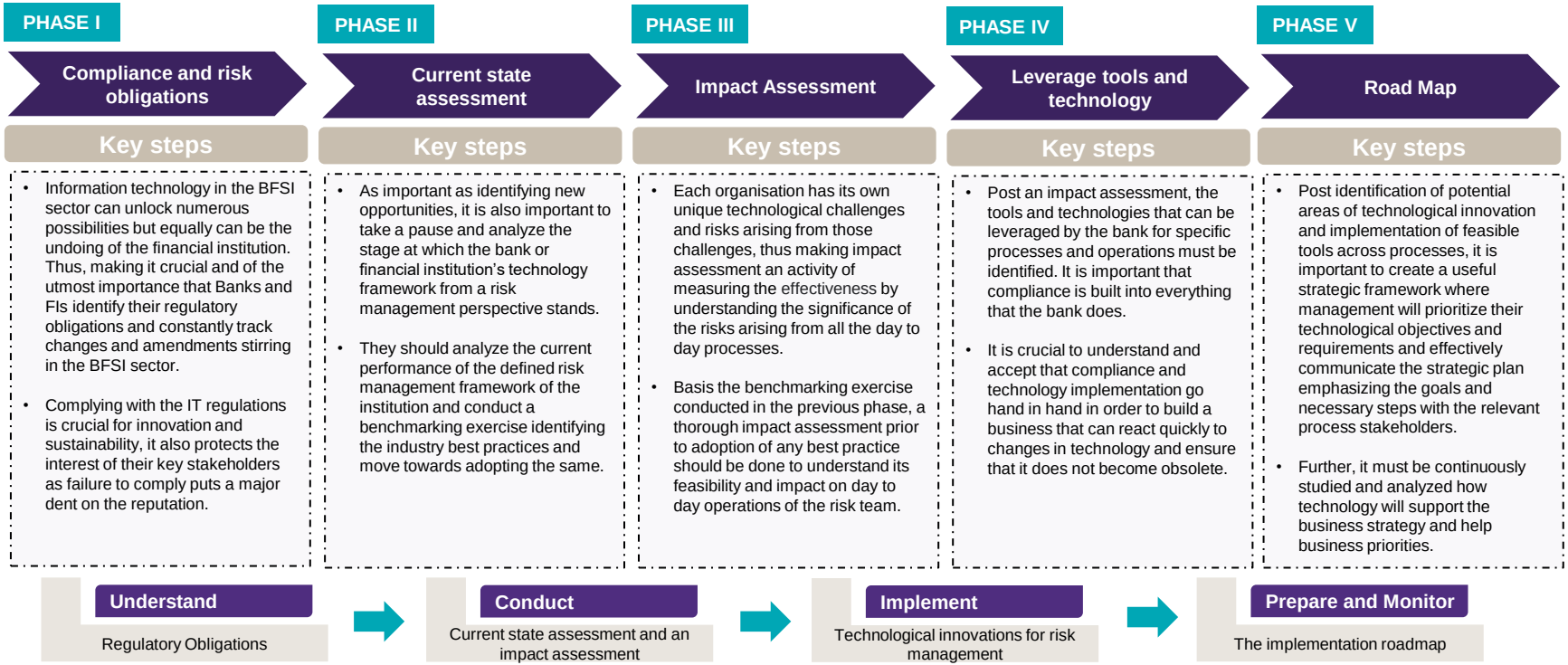


- A blockchain-based infrastructure to drive efficiencies, reduce costs and open up new revenue opportunities in trade finance, like new models of credit and funding guarantees backing the trade is being explored and implemented by banks.
- Customisation of the infrastructure to provide real time review of financial documents, mitigate the risk of delayed or denied payments by modelling self-executing contracts and provide delivery assurance for buyers by enabling real-time shipment status tracking and visibility is being done globally by banks.
- Blockchain technology is being considered to be used in both domestic and international fund transfers. International transfers stand to gain due to the huge disparity between rules and regulations as well as IT systems between banks across countries. Cross-border payments normally take several days to complete as many developing countries lack the IT infrastructure to process the transactions.

- ***Management of associated risks -*** To mitigate the risks arising from blockchain, banks must design control environments surrounding their blockchain systems and business processes transacting on those systems. The risk managers of banks conducting IT and system audits will need to extend their focus to third party (smart) contracts, cybersecurity controls around the business processes and how consensus is configured within the blockchain – both from a technical as well as a process standpoint.
- Extended focus on information risk management using an integrated risk management system will be the key to ensure that banks are able to leverage the benefits of the upcoming technologies while managing the risks created due to their implementation and use.

Grant Thornton Bharat

The approach to identify innovation opportunities within the risk management function



Grant Thornton Bharat

6. Case studies

Leading Indian nationalised bank

Synopsis

Strengthening the risk management framework through an early warning system for a leading Indian nationalised bank. The engagement required implementation of the Early Warning System (EWS) for monitoring Special Mention Accounts (SMA) which involved developing the entire software solution (web based application) along with a front end with three level user interfaces to detect 45 early warning signals which would put the bank in alert regarding wrong doing as per Reserve Bank of India circular dated July 01,2015.

Credit monitoring challenges faced by the Bank

1. Multiple sub-systems operating under one single function
2. Lower participation of end business user in requirements sharing
3. Ability to apply right set of monitoring parameters on borrowers risk profile
4. Absence of single source of truth and repository for internal data
5. Issues related to data availability, accessibility and usability
6. Responsibility sharing between internal and external IT support
7. Behavioral and change management issues for user adoption
8. Managing issues around false positives and negatives
9. Adherence to deployment, data and cyber security policies

Grant Thornton Bharat

Leading Indian nationalised bank

Approach

- Scoping of the data and reviewing the existing governance framework from documentation and IT perspective
- Detailed data mapping of the source system to data points as prescribed in the RBI guidelines and internal policies
- Technical and functional blueprint development of the integrated framework, output formats and output red flags
- Phase wise implementation with external data integration based red flag alert mechanism, Complete set data integration and Internal data-mart + external data integration
- Integration testing of the system
- Training and support to the end users
- Maintenance including updates and bug fixes

Value delivered

- Implementation of the Early Warning System in partnership with a leading financial technology company into production and provided trainings to the end users
- Effective monitoring reliably lowers both credit and capital requirement by identifying opportunities to de-risk and improve asset quality:
  - Reduced loan-loss provision by 10-20%
  - Reduced risk-weighted assets and required regulatory capital by 10%

Grant Thornton Bharat

American multinational investment bank and financial services company

Synopsis

- In August 2020, the investment bank faced a class-action lawsuit over two separate data breaches involving missing equipment that exposed clients' personal identifiable information, including Social Security Number and account numbers to third parties. The Office of the Comptroller of the Currency (OCC) levied a fine of 60 million $ against the said financial services company.
- When the Bank decommissioned two data centers related to it's wealth management business in 2016, it did not properly oversee the third-party company responsible for ensuring that all personal data was removed. The old servers, which still contained customers' data, were thought to be encrypted, but the Bank subsequently learned that a 'software flaw' on the servers left previously deleted data on the hard drives in an unencrypted form. In connection with the decommissioning, the Bank failed to effectively assess or address the risks associated with the decommissioning of its hardware.
- They also failed to adequately assess the risk of using third-party vendors, including subcontractors and failed to maintain an appropriate inventory of customer data stored on the devices. Such data could be illegally used by third parties to use the Bank's current and former customers' personally identifiable information to steal their identities and to make fraudulent purchases among other things. The current and former customers face a lifetime risk of identity theft.

Potential Causes

1. **Absence of a strong vendor risk management framework** :
   - Vendor risk management is a key area of focus of enterprise wide risk management frameworks which necessitate having sufficient oversight and controls over the work of vendors.
   - Centralised vendor management systems and tools for banks developed by experts track the end to end vendor lifecycle from due diligence, risk assessment, planning, and contract review to ongoing monitoring and review of the data and information accessible by the vendors.
   - The Bank failed to maintain an appropriate inventory of customer data stored on the devices, exercise adequate due diligence in selecting the third-party vendor and adequately monitor the vendor's performance.

2. **Inadequate Cyber Security Risk Control Framework:**
   - Appropriate cyber security risk management policies and processes with respect to the collection, storage, protection and disposal of personally identifiable information should be thoroughly implemented and monitored.
   - They should include the monitoring procedures, and contracts of IT asset disposal services they use. Tools such as using IoT to assist in tagging assets with Radio Frequency Identification (RFID) tags could be used to ensure centralized tracking of all assets including servers con be done.

Impact

1. **Customer Detrimental Impact**:
   - The Bank's customers filed a lawsuit against it , claiming that it failed to properly safeguard personally identifiable information while discarding the equipment.
   - The lawsuit damaged the Bank's image towards its other potential clients. Loss of trust amongst the customers could impact the Bank severely in the long run.

2. **Increased Reputational Risk**:
   - Regulatory fines have a major reputational impact on any bank. The regulator and public scrutiny rises leading to an increased reputational risk in the longer run.
   - The Bank developed a hidden threat to it's brand name which had the potential to impact future revenues of the company.

3. **Attributable Financial Impact:**
   - The Office of the Comptroller of the Currency (OCC) fined the investment bank $60 million for the it's failure to properly oversee the decommissioning of several data centers, putting customer data at risk of exposure.

Grant Thornton Bharat

Leading global investment bank and financial services firm

Synopsis

- In December 2020, a global investment bank and a leading financial services firm along with one of its former bank managers was indicted by Swiss prosecutors over the lender's alleged failure to prevent money laundering by a Bulgarian drug ring. The lender was first accused by the Office of Attorney General (OAG) of failures in its anti-money laundering processes in 2013, and the case traced back to 2008 when it first started criminal proceedings against some of the bank's clients, when prosecutors opened a probe into a Bulgarian wrestler who they allege had turned to drug trafficking.
- Allegedly , one of the bank's employee actively helped the drug ring by laundering 16 million francs using solely a "back-to-back" credit structure. Overall, the employee helped obscure the illicit origins of transactions worth more than 140 million Swiss francs. The prosecutors' indictment alleged that a senior relationship manager at the bank systematically ignored or sidestepped money-laundering reporting requirements between 2004 and 2008 to aid the criminal group.
- Further, the Swiss officials and the financial regulator can order the lender to disgorge it's profits and the criminal court can impose a fine up to 5 million Swiss franc.

Potential Causes

1. **Ineffective transaction monitoring by the AML function** :
   - There seems to be potential failure on the part of the bank while conducting the screening or due diligence of clients for ties to illicit activities and employees.
   - Further, the AML and FCU function should've set up an effective and efficient end use and transaction monitoring system within the centralised risk management framework of the Bank.
   - Artificial intelligence and machine learning models need to be built into the self assessment framework of the banks to track, monitor and identify any anomalies at the earliest. These models help identify patterns in spending and transactions of customers and pinpoint to suspicious activities which can be analyzed by risk managers.

2. **Absence of consistent and strong risk management framework:**
   - The prosecutors in the indictment said that the lender had been aware of these deficiencies from at least 2004, The fact that the lender let it continue until 2008, or even beyond, is an act of mere negligence on it's part.
   - While the Swiss investigators stated that the Bank failed to take organizational measures that were reasonable and required to guard against the laundering of cash made from the sale of cocaine that was then used to buy real estate in Switzerland and Bulgaria, the alleged failure may be attributed to an absence of a strong and consistent risk management framework at the top.

Impact

1. **Operational Losses:**
   - In January 2021, a Quint article stated that the Bank expects to post a fourth quarter loss" despite a strong year from an operational standpoint. This prediction was attributed to huge amount (approx 850m$) set aside for legal cases to tackle the legacy issues faced by the Bank.

2. **Increased Scrutiny from regulators:**
   - The Bank eventually emerged in the U.S. regulatory scrutiny for alleged money laundering as well.
   - The U.S. Federal Reserve imposed a 90-day deadline for the Bank to improve its weaponry against illicit money making its way into the financial system through its accounts.

3. **Increased Reputational Risk**:
   - If the Swiss officials and the financial regulator impose a fine and order the Bank to disgorge their profits, the attributable financial impact will be significant consequently dampening the reputation of the bank as well.
   - Increased regulatory scrutiny has a major reputational impact on any bank. The public scrutiny rises leading to an increased reputational risk in the longer run. The global financial services firm has developed a hidden threat to it's brand name which had the potential to impact future revenues of the company.