PERSPECTIVE

OPERATIONAL RISK MANAGEMENT IN BANKS: THE WAY FORWARD

Abstract

Risk management has always been a complex function for banks. Today the scope of regulatory compliance and risk management has become much broader, and the potential impact of noncompliance is significantly high. The risk function at banks is evolving from being a number-crunching function to a more dynamic business enabler, focusing on risks arising from complex products, diversified operations, diverse workforce, multiple channels, and regulatory compliance at regional and global levels. The intent being on proactive risk management and mitigation rather than event-based response.

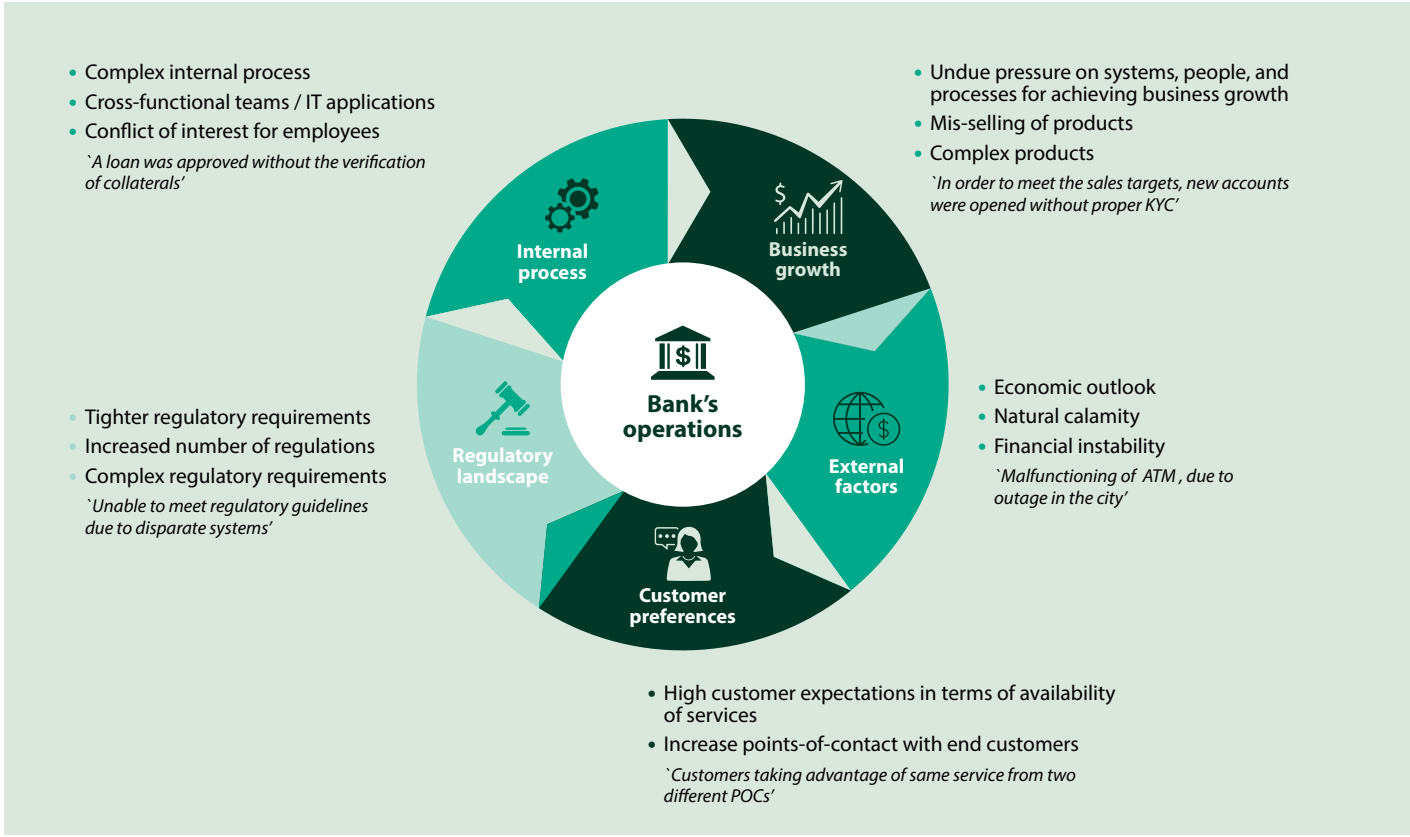
Operational risk has come to the fore since 2001 when it was recognized as a distinct class of risk outside credit and market risk, by Basel II. Though the Basel committee proposed some approaches to measure operational risk, their level of sophistication varies across banks. This is also because operational risk is the most complicated risk type, when it comes to risk quantification, identification, and mitigation. Operational risk is highly dynamic in nature and is impacted by numerous factors such as internal business processes, regulatory landscape, business growth, customer preferences, and even factors external to the organization.

Infosys®
Navigate your next

Introduction

Risk management has always been a complex function for banks. Today, the scope of regulatory compliance and risk management has expanded and the potential impact of noncompliance has significantly risen. As a result, the risk function at banks is evolving from being a number cruncher to a more dynamic business enabler focusing on risks arising from complex products, diversified operations, diverse workforce, multiple channels, and stricter regulatory compliance both regionally and globally. The underlying intent is proactive risk management and mitigation rather than event-based response.

Operational risk came to the forefront in 2001 when it was recognized as a distinct class of risk outside credit and market risk, by Basel II. Though the Basel committee proposed some approaches to measure operational risk, their level of sophistication varies across banks. This is mainly because operational risk is the most complicated risk type when it comes to risk quantification, identification, and mitigation. In fact, operational risk is highly dynamic in nature and impacted by numerous factors such as the internal business process, regulatory landscape, business growth, customer preferences, and even factors external to the organization. Some factors are:



Key challenges in operational risk management (ORM)

- **Inefficient risk identification parameters:** The current KRIs, KCIs, and KPIs used for ORM reporting in most banks are inefficient and do not provide a holistic data view, leading to incorrect risk identification. These KRIs are assessed in silos and a correlation among them is not quantified. Further, there is inconsistent risk measurement across business lines.
- **Large data processing and complex logic:** For ORM, the number of transactions that need to be monitored is growing at an exponential rate. This directly puts pressure on the current banking infrastructure and the existing processing logic is unable to handle the steep increase.
- **No single aggregated view for the enterprise:** Perhaps the biggest challenge in ORM is the lack of centralized and synchronized data. This can be further attributed to challenges around risk data aggregation. Most banks have incomplete coverage of data sources across business lines and hence, are unable to extract the full potential of huge data warehouses.
- **Lack of vision:** It is a known fact that ORM is widely recognized as a problem area within most banks but not many have a defined strategy which articulates how the bank intends to arrest operational risk.

In this article, we attempt to define a unified strategy for ORM and components of a futuristic ORM system.

Infosys solution approach

Using our experience of working with multiple customers, we have defined a comprehensive, three-point approach towards managing ORM:

- Enhance the risk coverage
- Integrate operational risk
- Decentralize operational risks

Enhance the risk coverage

The `three lines of defense' model is widely used to define and manage operational risk. To complement the three lines of the defense model, we propose a solution framework which works at a more granular level to help identify and control operational risk incidents. The target framework should include the following risk sources, which in our experience, is lacking in most banks today:

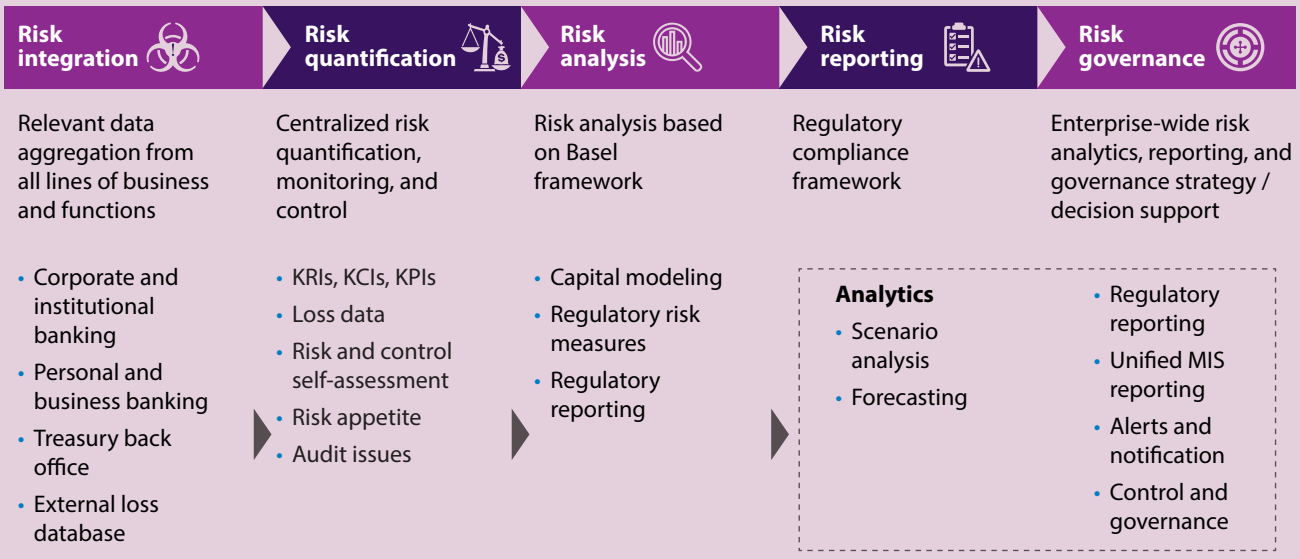
- Uniform monitoring of all potential risk exposure sources such as customer onboarding, portfolio management, employee tracking, or even disaster management
- Product fitment based on the customer profile and risk appetite to minimize potential defaults in future
- Inclusion of non-customer-facing functions / processes under the purview of the first line of defense
- Clear definition of accountability at each level within the risk plan
- Clearly established lines of communication and feedback with various levels of management, including business sponsors

The key objective here is to move beyond the traditional risk types and focus on all business processes and interactions to ensure they are well covered.

Integration of operational risk

Each risk classification – credit risk, market risk, and operational risk – differs widely in its assessment, on-ground execution, and quantification. It is highly recommended to have a holistic view of all of these risk classifications. Basel III reporting requirements need capital reporting for each risk classification to be done separately. The approach to address this in most banks today is to have disjointed systems which work like watertight compartments that result in duplication of costs as well as effort.

- **Integrated risk management platform:** We propose integration of these independent risk management systems under a composite umbrella for a more effective risk management strategy. This integrated risk platform created on top of a data lake can be further leveraged for a one–stop shop of all data requirements for trend analysis, scenario analysis, and to enable an equally powerful dashboard and on-demand analysis. This would help reduce the costs of platform maintenance, faster compliance with regulations such as BCBS239, and to send all risk-related regulatory reports to regulators from a single source.
- **Enterprise case management for risk:** A `case' typically is an instance of operational risk. We propose an enterprise case management system to manage alerts across different risk types. This will help to create a common risk catalog within the enterprise. Further, it will reduce operational and technology costs of managing such systems separately.



Target operational risk process

Decentralize operational risk

ORM is not just a function of the operational risk team. It should be embedded in roles across the organization. We propose a thin dedicated team to ensure overall compliance and participation of all units and business functions on the ground to ensure 100% coverage. This will help serve the twin purpose of decentralizing the ORM function at banks and cut costs to a great extent by reducing the dedicated ORM system and personnel.

The risk team can focus on overall regulatory compliance and the business functions can work on the ground to close gaps in business processes and operations. For example, the retail banking LOB manager can access, monitor, and mitigate the possible risks in the current customer onboarding process and the operational risk manager can define policies and standards for customer onboarding based on risk modeling, audit results, and past data analysis.

Monetizing the investment and the way forward

Most banks are approaching ORM reactively. As a result, solutions are tactical and costs and effort are duplicated. Given that ORM compliance and reporting is mandatory for all banks, we recommend having a central and holistic view of compliance across the bank. The objective should be to look beyond the short-term regulatory milestones and focus on re-engineering redundant processes. It is also essential to develop the right `risk culture' across the enterprise to achieve the desired return on compliance investment.

About the Authors

Venkatesha N. Vysya

Sr. Industry Principal, Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Venkatesha has over 20 years of industry experience leading several large and complex IT consulting, process re-engineering, system integration, and business transformation programs across marquee clients globally. Over the years he has built teams and multiple COEs to address business needs across industry domains.

He can be reached at **venkateshavn@infosys.com**

Navdeep Gill

Lead Consultant, Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Navdeep has nearly nine years of experience. She has worked on large transformational programs in risk areas, for leading financial service providers, and has extensive experience in defining the strategy and roadmap of such programs. She has an MBA degree with a specialization in finance. Her areas of interest include liquidity risk and regulatory reporting.

She can be reached at **navdeep_gill@infosys.com**

For more information, contact askus@infosys.com

Infosys®
Navigate your next