

View Point



Integrated Operational Risk Management Beyond Basel II

Navin Shankar Patel and Godwin George

An integrated approach towards Operational Risk Management (ORM) initiatives is required for a bank to be risk compliant

The New Basel Capital Accord, also known as the Basel II Accord, was proposed in 2001 by the Bank of International Settlements. It explicitly recognized operational risk as a distinct class of risk, different from credit and market risks, and as a significant contributor to a financial services bank's risk profile ^[1]. The Basel II Accord proposed various approaches for measuring a bank's operational risk exposure. These approaches and their adoptions by banks have evolved over time and the levels of sophistication of methodologies under these approaches vary widely.

As significant investments are made in ORM initiatives, banks should look beyond Basel II and ORM should be used as a transformational initiative. Riskmanagement efforts need to be seen from an operational excellence perspective and should be part of an integrated compliance platform. Before we try and look beyond Basel II, a look within Basel II is required for this discussion to be self-explanatory.

For more information, contact askus@infosys.com

Basel II Revisited

The Basel Committee on Banking Supervision defines operational risk as “the risk of loss resulting from inadequate or failed processes, people and systems or from external events”.^[3]

As a part of the accord, Basel II proposed three pillars to play an important role in the operational risk capital framework^[1]:

- Pillar 1: Minimum regulatory capital requirement for operational risk
- Pillar 2: Supervisory review process to enforce a rigorous control environment to limit exposure to capital risk
- Pillar 3: Market discipline requirements.

Pillar 1 requires firms to quantify the operational risk capital charges and to set the considerations for the quantification; Basel II Accord proposed three broad approaches^[2].

- Basic Indicator Approach: Considering operational risk, firms need to hold capital to a fixed percentage of a single indicator (e.g., gross income).
- Standardized Approach: An extension of the basic indicator approach where the firm is seen as an amalgamation of a hierarchy of business units and business lines. For each business line, the regulator proposes an indicator on which the capital charge will be based.
- Advanced Measurement Approach (AMA): The regulator allows the firms a flexibility of using the output of the internal operational risk measurement systems.

There are qualifying criteria for banks to follow one of the above approaches and all the approaches can also be used in a bank in different business-lines based on the qualification standards.

Banks had the liberty to choose the measurement approach that suited them. But the adoption of measurement approaches has changed over time along with the evolution of ORM frameworks and risk appetite in banks. The choice of options for the estimation of operational risk capital charges turns out to be vast and banks can choose between two macro approaches: top-down models based on balance indicators (the Basic Indicators Approach and the Standardised approach) and advanced, quali-quantitative bottom-top models (the Advanced measurement approach). Increasingly AMA is preferred over other methods and recently, the Office of Comptroller and Currency approved Basel II Capital Rule which advocates AMA for ORM^[5].

Lifecycle Approach to ORM

A persistent quest for a convenient ORM platform has led banks to experiment with various approaches. Recently it has been observed that the ‘lifecycle’ approach to ORM is increasingly being adopted [Fig. 1]. In this approach, ORM is seen as a series of lifecycle steps:

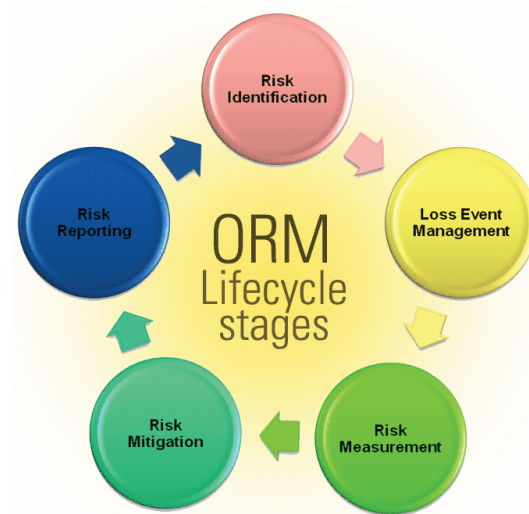


Figure 1:ORM Lifecycle stages
Source: Infosys Experience

- It involves a process to capture the organizational business hierarchy; record risks and their underlying causes and controls; and associate risks, cause and controls to business lines/ processes/products.
- Loss Event Management: A 'Loss Event' is an instance of operational risk event. Continuous collection of loss events is extremely important as loss events form the backbone of risk measurement. The loss events can be internal exposures or external events outside the bank. So an ideal loss event management necessitates an extraction of loss events from internal and external sources and cleansing and loading loss events.
- Risk Measurement: Measuring risk using a combination of qualitative/quantitative models as:
 - Simulating operational value-at-risk using techniques such as Monte Carlo simulation
 - Performing qualitative assessments using the RCSA (Risk Controls and Self Assessments) framework
 - Combining the quantitative and qualitative approaches to report an aggregated risk measure.
- Risk Mitigation: This requires the banks to assess quality of controls and identify issues, in addition to establishing action plans to address identified issues.

Decentralize ORM

A successful implementation of lifecycle approach requires an involvement from various groups. The roles and responsibilities in the hierarchy need to be properly defined to ensure an efficient operation of the approach. The Basel II Accord also recommends an 8*7 matrix of business line and event type categories and expects regulatory reporting to conform to this matrix ^[1].

While banks are recommended to follow the matrix suggested by Basel II, internally the banks may decide to adopt their own hierarchies, based on their strategic goals and day-to-day operations.

The hierarchy may be based on lines of business, geographies, legal structures and cost centers. In case of lines of business, there could exist further levels and sub levels which can again be categorised into activity groups. These activity groups quintessentially form the primary source for all types of risks associated with a particular business line [Fig. 2].

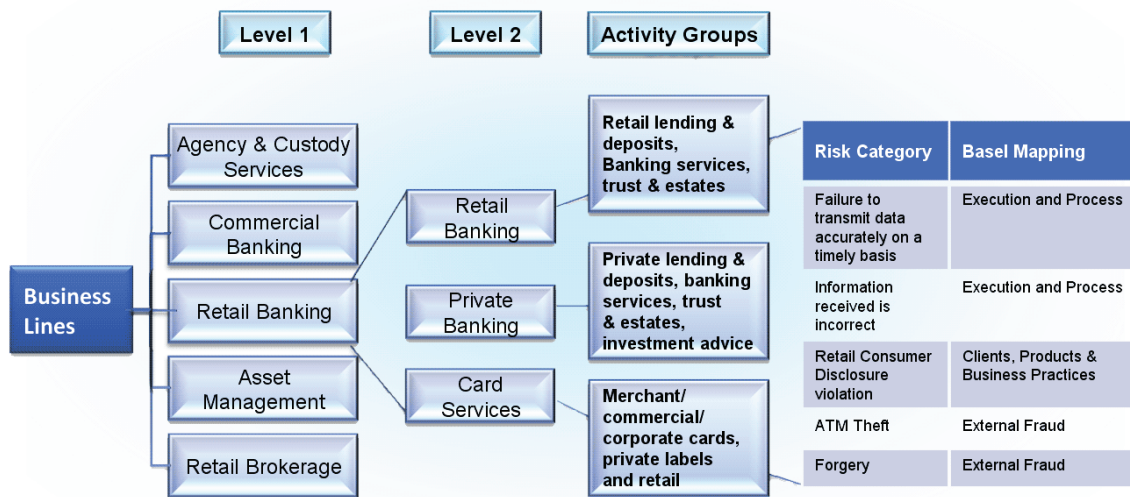


Figure 2: Internal Hierarchy vis-à-vis Basel II Hierarchy
Source: Infosys Experience

While the main idea of having an independent risk management function, apart from business functions, is to ensure that the integrity of risk functions is not compromised, it is clear that without the buy-in and active participation of the business lines, the ORM initiative may not succeed. It is imperative that the business lines and the associate personnel are actively engaged in core ORM activities.

More often than not, the ORM function in a bank is a part of the central risk function. But to have an effective ORM system, the central risk function needs to work closely with the business groups by de-centralizing some of the core ORM functions and at the same time preserve the goal of independence of its function. [Fig. 3]. The goal should be to empower the individual business groups with the responsibility for operational risk management. Business groups at a local level manage

operational risk most effectively, so it is vital that these groups are entrusted with the responsibility, accountability and power to manage their own operational risks.

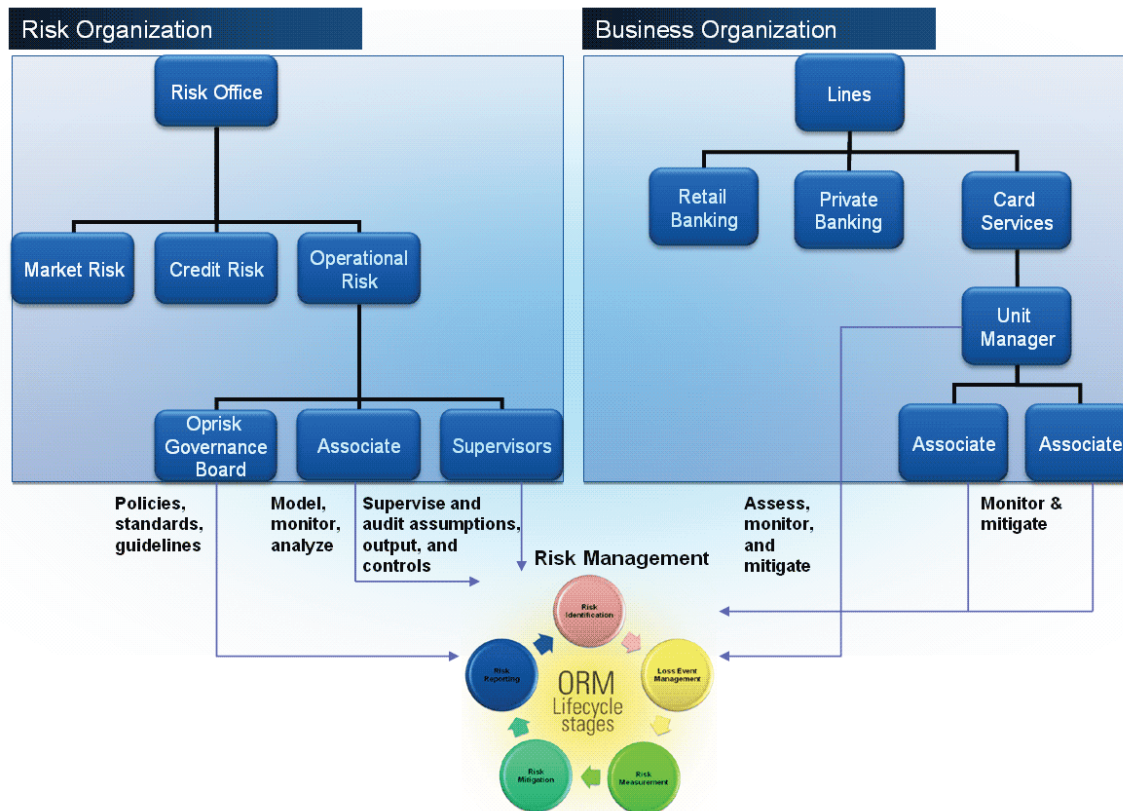


Figure 3: Interplay between risk and business functions
Source: Infosys Experience

On the other hand, the risk office can focus on regulatory requirements and work with the business groups in closing the gap between the business processes and their readiness from a compliance perspective. This would help in bridging organization gaps, mandate roles and responsibilities between the two groups, viz., the central risk office and business groups.

While the central risk office should focus on defining operational losses like financial, provisional, direct, indirect etc; resolving boundary issues that prevent multiple counting of losses under different risks; defining home/host country considerations, the business group should take ownership of (i) validation of financial losses within an LOB; (ii) definition of policies and procedures specific to line of business (LOB) requirements, and (iii) definition of threshold violation for loss events (risk appetite) and associated workflows.

To ensure compliance to regulations, reporting should conform to the Basel II mandated hierarchy. The IT system in place supporting the ORM platform should be flexible enough to translate the internal hierarchy information into the regulatory structure and also to incorporate changes in internal structure and future regulatory changes.

By de-centralizing ORM activities, the ‘risk culture’ can spread beyond core risk functions in an organization.

Integrated ORM

Risk management should be seen as a part of the holistic compliance platform of a bank and to achieve the desired holistic platform, decentralizing risk management function ensures effective participation from stakeholders with different goals.

In the wake of the dynamic business scenario of the banks and their ever-changing products, it is difficult for them to comply with the multitude of regulatory requirements and compliance needs. Few examples of regulatory requirements are Anti Money Laundering (AML), GLBA, SOX etc. Many of these requirements are applicable across the organization and some of them are applicable to one or two business lines or even more.

Most regulations have stringent deadlines. Many banks have either adopted or are adopting tactical means of addressing the regulation requirements. In many cases, the violations of regulatory requirements are due to operational risks. For example, in an AML scenario, large wire transfers need to be investigated for legitimacy. The inability of detecting a large wire transfer could be due to inefficient processes and system failures -- which are operational risks. Repeated instances could cause large operational losses and reputation losses.

One often cited example for the need for prudent risk management is the Bank of Credit & Commerce International (BCCI) scandal which came into light in the early 1990s [8][9]. The problem essentially stemmed from general internal fraud, a subset of the People risk category in operational risk. The bank's unsustainable loan strategy and practice of hiding losses compounded by dubious trading strategies contributed to its ultimate downfall. The case also involved several instances of relationship risks and money laundering activities. What began as a minor operational loss event spiraled into a vortex of regulatory violations, each more grave in nature than the previous ones.

Number of business lines involved	Number of Loss Events	Percentage of Loss Events
2	450	87.40%
3	52	10.10%
4	2	0.40%
5	4	0.80%
6	5	1.00%
8	2	0.40%
Total	515	100%

Table 1: Losses across Business Lines. A survey done by Basel Committee on Banking Supervision, Loss Data Collection Exercise for Operational Risk, (2003)

A Survey [Table 1] clearly highlighted the fact that individual losses often cut across business lines and event types. A couple of loss events affected, up to 8 different business lines.

Hence, there is a case for banks taking a holistic view of their compliance programs. There is a need for integrating other compliance silos with the common ORM platform to derive the benefits it can provide and move the company towards a culture of compliance.

Common practices of compliance managements can be consolidated on an ORM platform to have greater return on the compliance spend.

- Case Management and Risk Catalogue: A 'case' is a suspected violation of regulatory requirement. A case typically is an instance of an operational risk. By having a centralized unified case management dashboard which is workflow driven, the underlying operational risks can be consolidated bank wide. While regulatory specific case management can be handled by appropriate personnel, this approach will ensure that all operational risks are at one place and would thus help creating a 'risk catalogue.' The business line owners are responsible for operational efficiency of their business functions along with the mandate of ensuring the compliance of business processes to regulations. This approach will ensure that they do not have to worry about duplicate risks and other associated problems of compliance silos.
- Process Repository: The ORM platform can act as a common repository to store all business process related information across the enterprise.
- Consolidation of IT Infrastructure: Having an integrated ORM platform, the IT spends can be considerably reduced as many features can be aggregated on a common ORM platform
 - Data Management
 - Meta data configuration for source systems, infrastructure, connectivity
 - Administration and reporting
 - Common utilities such as access control, user alerts, audit trail, search, workflow and business rules management.

A scalable and flexible ORM platform will ensure integration of compliance programs resulting in a one-stop place for process, products, risk elements and their management. This will further ensure a comprehensive approach to compliance with reduced total cost of compliance.

Conclusion

Banks are now approaching ORM with risk capital measurement being the focal point. They can use this opportunity to take a holistic view of compliance programs by having ORM as the fulcrum for their compliance initiatives. They can look beyond Basel II by shifting the focus on re-designing vulnerable processes. They can also develop and propagate cultures of 'risk and compliance' on top of the ORM platform and ensure a greater return on their compliance investment.

A different version of this article, with the title "*Integrated Operational Risk Management: A Look Within and Beyond Basel II*" has been published earlier in SETLabs Briefings' BFSI Bulletin, 2008, pp.13-20

References

1. Consultative Document, Operational Risk, BIS, January 2001. Available at <http://www.bis.org/publ/bcbsca07.pdf>
Accessed on Nov 2007
2. Working Paper on the Regulatory Treatment of Operational Risk, BIS, September 2001. Available at http://www.bis.org/publ/bcbs_wp8.pdf
3. Sound Practices for the Management and Supervision of Operational Risk, BIS, July 2002. Available at <http://www.bis.org/publ/bcbs91.pdf>
4. Sound Practices for the Management and Supervision of Operational Risk, BIS, February 2003. Available at <http://www.bis.org/publ/bcbs96.pdf>
5. OCC Website at <http://www.occ.gov/ftp/release/2007-123.htm>
6. Observed Range of Practice in Key Elements of Advanced Measurement Approaches (AMA), October 2006. Available at <http://www.bis.org/publ/bcbs131.pdf>
7. Dr. Dayanath Pandey, University Of Wollongong In Dubai, Dubai, UAE, Operational Risk: Measurement Issues, Basel-II and UAE banks, 2006
8. http://en.wikipedia.org/wiki/Bank_of_Credit_and_Commerce_International
9. Douglas G Hoffman, "Managing Operational Risk: 20 Firmwide Best Practice Strategies", John Wiley & Sons Inc, 2002 p.107

About the Authors

Navin Shankar Patel is a Senior Project Manager with the Banking and Capital Markets Unit of Infosys. He has several years of experience in developing and implementing solutions in risk and compliance area.

Godwin George is a Business Analyst with the Banking and Capital Markets Unit of Infosys. He has experience in developing and implementing solutions in risk and compliance area.



For more information, contact askus@infosys.com

About Infosys

Many of the world's most successful organizations rely on Infosys to deliver measurable business value. Infosys provides business consulting, technology, engineering and outsourcing services to help clients in over 30 countries build tomorrow's enterprise.

For more information about Infosys (NASDAQ:INFY), visit www.infosys.com.