LTIMindtree

Whitepaper

Operation Risk Management Efficacy - The Litmus Test

Author

Raji Daniel

Introduction

Operational risk management is at a crucial juncture in its development. The urgency for a deeper understanding of operational risk is driven primarily by the following factors - the increasing sophistication of financial technology, the rapid globalization of the financial industry, regulatory compliance, geo-political incidents and cyber security, among others. These factors contribute to the increasing complexity of banking activities and therefore, heighten the operational risk profile of the financial services industry.

History is replete with incidents of high-impact and high profile losses, a few leading to the unwinding of once revered, bellwether institutions, all of them consistently pointing to total failures in the management of operational risk. This seemingly sudden awareness of operational risk management is quite ironic, considering that operational risk has always been an integral part of the risk associated with conducting business – occupational hazard.

'Operational risk is as old as the banking industry itself', the rating agency Fitch reports, and yet, the industry has only recently arrived at a definition of what it actually is. The report further, goes on to say that in its rating analysis of banks, Fitch will be looking for evidence of a clearly articulated definition of operational risk, examining the quality of an organization's structure and operational risk culture, the development of its approach to the identification and assessment of key risks, data collection efforts, and overall approach to operational risk quantification and management.

Operational Risk Landscape

Basel norms under the aegis of BIS attempted to articulate a qualitative identification and measurement of risk. The subsequent versions beginning with Basel 1 laid down the three pillars for banks to collate data and aggregate their exposures, against which minimum capital requirements were to be established.

That might have been the case, from a purely Basel reporting perspective; however, dwelling deeper, one would encounter subtleties in the risk components that form part of the whole, in terms of reporting namely, those that dealt with Credit Risk, Market Risk and Operational Risk. Each of these components existed in silos and was treated, accordingly. Correlation between each component was largely ignored. The serial crisis that occurred despite toughening capital adequacy norms, failed to prevent many financial institutions from the loss. Regulators and banks worldwide have realized that credit risk, market risk, liquidity risk, and all its collective components were interrelated and ought to be seen and treated together.

BIS defines Operation Risk as the `risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.' In other words, any risk arising due to people and their actions involving all hardware, software, communication/ decisions/ thought process or management, and the losses/gains incurred as a result of manmade or force majeure, now comes under the ubiquitous ORM. While it is true that ORM rolls into Governance, Risk and Compliance (GRC), which in turn rolls up to Enterprise Risk Management (ERM), its role cannot be understated.

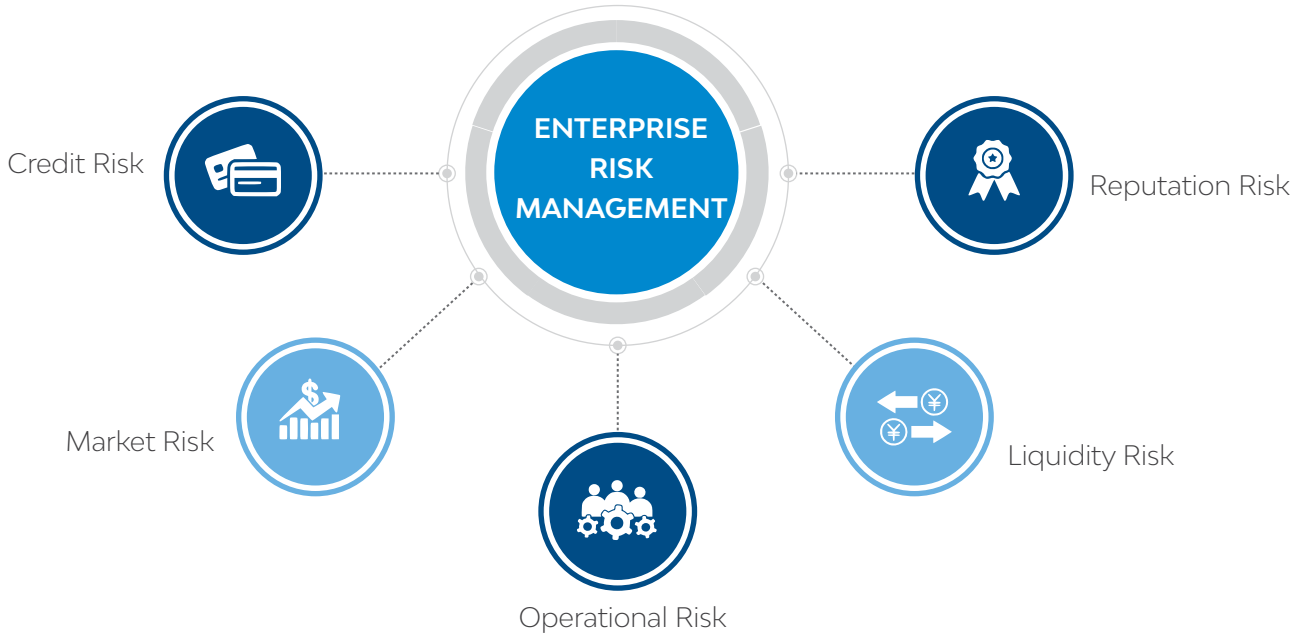

Figure 1 : Risk viewed in silo

While Regulators and risk practitioners were contemplating measures to avoid the pitfalls in implementation, and at the same time, deploying scalable models to correctly estimate risks based on macro- economic factors (CCAR ORM testing, scenario testing, what-if analysis, tail loss, etc.), certain events/incidents redefined and rewrote the ORM approach, further.

As part of ORM preparedness, Business Continuity and Disaster Recovery plans were seen as components woven from the same cloth; however, the ingenuity of the human mind, both noble as well as nefarious ushered in a new level of technology and ulterior motives – fraud, manipulation and cybercrime, coupled with geo-political events and natural calamities, further muddied the pond.

CCAR and the yet to be announced `Cyber security regulation act' are components/exercise being fed into, the now, ubiquitous Operational Risk Management.

The effectiveness of a target state operational risk management has been impeded by the failure to embed operational risk into the overall Governance, Risk and Compliance (GRC) Framework. Group risk functions must demonstrate to business units the full potential of using operational risk processes, developed under the group risk framework to manage the actual risks in the business. In the absence of this exercise, business units resort to developing their own ad hoc processes for managing operational risk and control irrespective of stated internal compliance processes.

The reasons are multi-fold, irrespective of the risk assessment approach (top down/bottoms up), such as:

- Linkages between risk indicators and risk assessment are vaguely or insufficiently mapped to provide effective risk monitoring.

- Loss data collection often provides one way feed into a group model, rather than being used by the business, to identify areas of control weakness/inadequacy.
- Advanced Technology comes with the added risk of erroneous system errors; (algorithmic trading/mispricing) automated algorithmic trading software has led to fears of new forms of unauthorized trading, the growth in automated customer advisory systems known as 'robo-advisers' has led at least one regulator, the US Securities and Exchange Commission, to lay out guidelines on how these algorithms can avoid misleading customers – and how human overseers should be held accountable if they do.
- New forms of risk has emerged (Cyber fraud, denial of service, blackmail, hacking, terrorism) both by individual/s and/or state player/s.
- Business Continuity Programme (BCP) doesn't always work and are linked to the Disaster Management Process. The latter is viewed more as a salvage operation that can contain the damage, and not as a mitigation or prevention option.
- Management of operational risk is not a data-driven process, given nature of operational risk, always been viewed more of a management issue than a measurement issue.
- Operational risk quantification is often viewed as irrelevant to the day-to-day management of risk. Having identified some issues in the effective implementation of a robust ORM framework, it bears mention that the changing face of ORM has been largely influenced by some of the following incidents:

2005 - 2018 Fraud cases reported (a few)

Case Study

A GSIB entity' BCP/Disaster Recovery Programme throws its Operational Risk Management to the winds:

The bank follows a process-centric risk management framework, where all critical processes are identified and mandated to have a pair of disaster recovery locations -one primary and one back-up, to ensure business continuity and sustenance. As per the policy, the bank was mandated to evaluate the efficacy of these location pairs to ensure DR (Disaster Recovery) standards are met based on 13 pre-identified risk factors. The Risk Factors were evaluated based on a set of pre-defined questionnaire for which responses were collated at the time of assessment. The assessment frequency was annual or semi-annual depending on the geographic location of the pair.

The proposed solution was to leverage a third-party vendor's Business Process Management (BPM) product capability compounded with (RPA) Robotics Process Automation for data collation and response automation. The risk scoring calculation and interpretations were to be created as configurable parameters within a custom extension of the BPM platform and were independent of the RPA service vendors.

Though the solution addressed the risk assessment procedures, the challenges in actual interpretation and execution of this data in times of crisis was not in purview of the solution. For example, when NY was affected by the snow storm, the bank HQ had to shut down critical operations due to employee mobility challenges. Mexico which was the primary DRL for the NY

location was activated and BCP sustained, based on the efficacy of the risk assessments performed in the past. However, when the US eastern sea-board was impacted due to a cyclone and Mexico was simultaneously impacted by an earthquake, all relevant locations were simultaneously impacted causing disarray in the DRL plans.

1) IT Disruption – Distributed Denial of Service (DDoS)

In a DDoS attack, large amounts of data traffic is sent to a particular website, overloading its server and thereby, crashing the site. Dutch banks ABN Amro and ING were both hit by DDoS attacks over one weekend, leaving customers unable to use their mobile- or online banking for hours at a time.

2) Data Compromise

Credit checking agency Equifax, compromised the personal information of an estimated 145 million individuals. It was attributed to the firm's failure to apply an update to a critical piece of software. Equifax didn't report the breach until September 2017, four months after it had taken place. Under the European Union's General Data Protection Regulation, which comes into effect from May 25, 2018, will severely penalise companies that fail to notify their regulator within 72 hours of a data breach, inducing fines of up to 4% of global turnover.

3) Fraud

Old-fashioned frauds made up a substantial portion of the largest risk losses for 2017, however – not least the USD 2.5 billion that fraudulent loans are said to have cost Brazilian development bank BNDES. Two of last year's top 10 losses – one involving Agricultural Bank of China and the other a group of eight Indian banks – also came from commercial loan fraud. Indian banks alone experienced 37 cases of commercial loan fraud totalling more than USD 2.57 billion.

4) Geopolitical risk – Brexit

Britain's exit from the Eurozone entails several banks shifting their important location elsewhere. Market access and contract certainty are the main issues, for mainstream business it is supply chains, and the fact that components and raw materials might attract tariffs every time they move across a border, causing anxiety to several firms.

Operational Risk Management

Evolving risk - Given the evolution of ORM, and in wake of several developments, any ORM framework/approach should encompass identifying all risks (apart from the traditional ones such as credit risk, market risk) to now include, Disaster recovery, cybercrime, BCP, manmade and natural calamities.

The former, a tangible, much mapped activity/process requires no further introduction/ innovation. The second category of risk though, warrants a closer examination which may arise from force majeure/natural disasters, strikes and economic disruptions, from acts of vested interests/agents, including terrorism and/or state players/rogue nations.

Figure 2 : ORM in Investment Banking

OTC market volumes by the end December 2017 was over USD 267 billion plus, in spite, of increased regulation and the move to have OTC derivatives executed on swap execution facilities and if not, at least, reported onto a swap execution facility/ trade repository. Regulatory arbitrage too, diminishing, with the G20 now slowly getting on-board, signifying the evolution of a globalfinancial regime. However, along with the bulk of the trade now shifting to electronic platforms and all things digital, the rise and dominance of the algorithm and robotics/AI isn't far. Closer connectedness and speed of processes also means cascading of individual actions into proportions of unimaginable magnitude, as witnessed during erroneous trade orders disrupting the entire financial system. Such incidents aren't just isolated, but part of a larger malaise, both fraudulent and unintended.

Additionally, with the migration of technology/s across multiple domains, coupled with the creation of several technological innovations, the disintermediation or breakup of the traditional sentinels/controls that authorities have relied on and regulated for investor protection, and market integrity have long been compromised/ignored giving rise to a new kind of operational risk.

Financial firms also face a variety of risks associated with their over dependence on service providers. The risk of theft, the inadvertent release of client data or dissemination of intellectual property, such as on strategy or trades, cartelization (LIBOR rate manipulation) and regulatory breaches, leading to substantial fines.

To ring-fence critical operations and to stem contagion, some investment management firms are working to gain a more holistic view of their extended enterprise by evaluating the risk profile for each service provider. They are also establishing a service provider oversight framework that aligns with their overall risk profile. Regulations such as MREL/TLAC have mandated reports that compartmentalize each firms risk vis-a-vis the other. Considering a part of the local/national economy in terms of impact of resolution or restructuring, banks need to identify their critical services to third parties, the percentage of exposures, and the likely impact on the economy, should such service providers be rendered non-performing.

- With macro-economic factors linked to the Risk assessment of firms, the parameters governing modelable and non-modelable risk models have reached a new level of complexity and the risk associated with its output. The TRIM Regulation (Targeted Review of the Internal Model) aims to do just that.

Figure 3 : Changing landscape of ORM

- Effective securities regulation will thus have to be upgraded to account for a computerized and often virtual market microstructure that is subject to increasing change.

Two key sources of disruptive innovation are:

1) The automated financial services that are transforming the meaning and operation of market liquidity.

2) The private markets, specifically the dark pools (iceberg trading) electronic communication networks, 144A trading platforms, and crowd funding websites—that are creating an ever-expanding plethora of alternatives for both securities issuances and trading.

- Data and technology: Investment management firms face significant system, Infrastructure and data challenges, which are compounded by the investment manager's fund and account structures, as well as its reliance upon service providers for technology and data. Data quality is clearly affecting the organizations' abilities to assess, monitor and mitigate risk.

CCAR and Operation Risk

Efforts of developing validated models for projecting operational losses under the Federal General's specific Comprehensive Capital Analysis and Review (CCAR) stress scenarios looks daunting and may pose multiple challenges to banks. CCAR requires correlating operational risk loss events to the Fed's macroeconomic stress scenarios and projecting them over nine quarters. The overall methodology must definitely demonstrate reliable statistical correlations between operational loss frequency and severity curves and specific macroeconomic variables.

In developing and validating operational risk models, there are several areas that require robust solutions:

1) Lack of detailed operational loss datasets be addressed by augmenting internal data with external industry experience.

2) Haphazard time assignment to operational events that tend to occur over time (e.g. litigation, and regulatory fines).

3) Correct modelling of idiosyncratic operational risk characteristics of a bank's unique profile.

4) Fitting operational risk models to specific macro-economic variables over nine quarters across Fed stress scenarios and estimating loss magnitude.

5) Careful examination and inclusion of all significant historical operational losses and linking them to relevant macro factors.

6) Inclusion of reserved as well as potential future provisioning for litigation and regulatory fines, including pending and threatened claims.

Given the somewhat unstable and unreliable correlation of historical operational risk data, thoughtful analytical methods should be devised. These include full use of specific scenario analysis and sensitivity. Often, the approach requires determination of loss frequency and severe probability of distribution curves. Different methods and distributions are used to build out operational loss frequency and severity curves.

CCAR operational loss projections might seem to many as stochastic and unreliable, however regulators emphasized the use of a highly disciplined compliance framework with documenting model development, implementation, validation, governance and proper controls of the data gathering and process.

Bibliography

https://www.sciencedirect.com/science/article/pii/S0925527316302857
https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018
https://www.fitchratings.com/site/search?groupId=80089104&type=entity&content=research
https://www.prnewswire.com/news-releases/otc-markets-group-reports-2017-trading-statistics-and-highlights-300592580.html

About the Author

Raji Daniel is a Senior Consultant within LTIMindtree Consulting. He holds a post-graduate management degree from the University of Pune.

Having worked with several investment banks such as Lehman Brothers, Morgan Stanley, Knight Trading, VPS (Norway), RBS, Barclays, Nomura, UBS, etc. Raji has been involved in business consulting within the investment banking domain in credit risk, market risk management, and governance risk and compliance. He can be reached at raji.daniel@lntinfotech.com.