ORACLE
Business Process Services

OPERATIONAL RISK MANAGEMENT

VARYING PARADIGMS IN NON-FINANCIAL RISK MANAGEMENT

MEASURING WHAT MATTERS

Operational Risk is embedded in the fabric of every organization. Its effective management not only increases visibility into material and emerging impacts across business but if leveraged differently can assist in delivering competitive advantage by harnessing risk measures to improve results

RAJIV RAJAGOPALAN
SRIKARTHIC V S

WHITE PAPER / MARCH 8, 2019

ORACLE

DISCLAIMER

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

1.0 INTRODUCTION

The premise of any Banking Organization's business model is to generate profit by taking on Financial Risk. Banks are seasoned to this approach and have developed and devised their strategies over time to measure, accept, transfer or mitigate these Risks. But the broadly categorized Non-Financial Risk (NFR) consisting of Operational, Compliance Failures, Misconduct and Technology challenges pose a significant downside for Banks both from identification and mitigation perspective

The financial cost of Non-Financial Risk is significant. The Conduct Cost Project by the Conduct, Culture, People (CCP) Research Foundation estimates that in the period following the 2007 crisis, the top ten banks globally accepted a financial loss of USD 320 Billion in half a decade for Litigation, Compensation Claims and Operational Losses. Amongst that just 17 incidents accounted for aggregated losses of more than USD 1.6 Billion and another 65 incidents each resulted in losses of above USD 160 Million. The top 6 US banks' Costs and Provisions amounted to USD 228 Billion – a staggering 70% of the participating network.

Though significant, the consequences of NFR are not restricted only to its financial impacts. The reputational damage can pose hard questions on the Bank's operating model from public stakeholders and customers. Also, there is the possible liability for Senior Managers, whom regulators are willing and intending to hold personally accountable for misdemeanors and failures to comply with laws and regulatory guidelines. In addition, the imposition of tighter regulations, like the Basel Committee on Banking Supervisions (BCBS) accord to remove the Advance Measurement Approach (AMA) and replace it with the Standardized Approach (SA) will increase Regulatory Capital thresholds, especially for banks in the EU region, which have traditionally allocated lesser capital for Operational Risk Management. All of this combined with quantitative improvements to Credit & Market Risk nearing saturation, increases the pressure on banks to better manage Non-Financial Risk

Banks are investing heavily to better control Compliance, Fraud and IT Risk by creating new Governance Structures, boosting headcounts and making Compliance awareness and training a Board level priority. Yet operationally, in most banks' mitigation remains elusive. Too much time is spent firefighting Compliance submissions and Audit findings are hardly a precursor to Risk materialization. Topping it all, the periodic Risk Assessment cycles have become more procedural than participative, compounding the qualitative dependency and their respective quantitative extrapolations.

An important factor to this reality is the way Non-Financial Risk management relies heavily on the 'three lines of defense' scheme

2.0 THE THREE LINES-OF-DEFENSE

Today's Risk Management framework for NFR is primarily subsumed under the Operational Risk Management (ORM) guidelines and relies heavily on the 'three lines of defense' scheme with **Business**, **Control Functions** and **Audit** forming the first, second and third line of defense respectively. The concept which is borrowed from the world of the armed forces & military strategy, is based on the premise of intelligence and the ability to gather it. In this the first line owns and manages the Risk, the second line defines control thresholds and monitors adherence, while the third line oversees the implementation practices of the first two from a wider governance perspective

However, in today's world, financial institutions are plagued by the lack of clear responsibilities between the first line of defense (Business) and the second line of defense (Control Function) leading to significant loggerheads in Organizational cooperation. It gets further amplified when first line expands to include central infrastructure areas like IT and Operations and second line expands to accommodate Legal, HR and Accounting

Instances of both the lines of defense being manned by the same Business Function creates the burden for optimizing Business Performance against Compliance, adding to the complexity. In addition, Control Functions have their own Risk Identification procedures and Process Breakage analysis, which are comprehensively exhaustive compared to Business' which focusses on the narrow prism of Performance, Revenue, Balance Sheet and Profit & Loss. All the above could lead

to a complete isolation of the Control Function across Business lines or Processes, having its own Risk Identification procedures, Reporting Structures, Control Frameworks and supporting IT infrastructure as necessary

Such an isolated Control Function running its own dedicated Risk Management procedures could operationally lead to 'ballooning' of the Risk and Control measures, especially at lower hierarchies, disturbing the foundation of any Non-Financial Risk Management Framework

Hence it is imperative for banks to adopt a robust principles-based approach to clearly delineate the first and second line function responsibilities by emphasizing its operational complexity, governance structure and regulatory demands. Ideally the second line should act as a trusted advisor to Business while having independent control over the definition and monitoring of business-critical thresholds. These principles need to emphasize the importance of the first line taking responsibility of Non-Financial Risk Management with support from the second line rather than focusing only on revenue, cost and operational metrices. Furthermore, the second line can no longer only promulgate regulatory guidelines and internal policies on an advisory capacity. It is imperative that the second line starts focusing on active Risk management and mitigation by transforming underlying business risk exposures into management actions

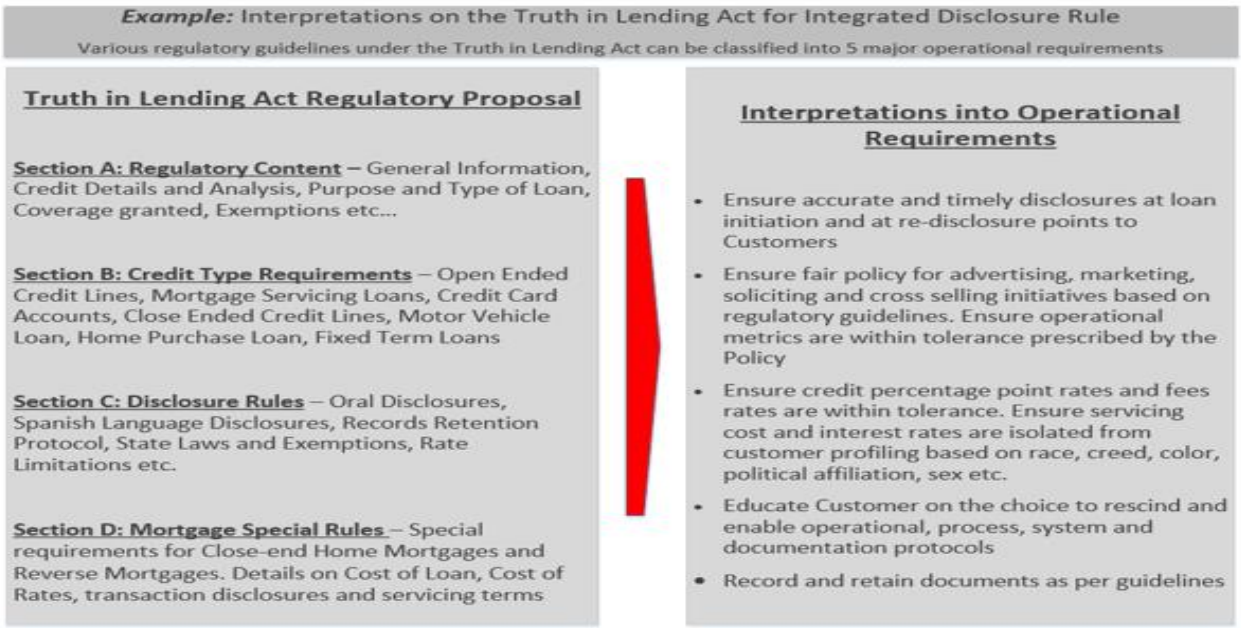
3.0 OWNERSHIP OF OPERATIONAL FRAMEWORK, RISK TAXONOMY AND CONTROL FRAMEWORK

Banks need to transform both their first line and second line functions. The first line needs to internalize responsibility for Non-Financial Risk Management whereas the second line needs to actively look at business Risk management. Both the first and the second lines can work together by expanding their functions to include various aspects of the Risk and Control framework. Some of these include

- Avenues in generating practical perspectives and interpretations on applicability of regulatory guidelines and legal mandates across businesses and processes. They can together define how these will translate into operational requirements and impact current business processes *(example below)*

- Creating standards for defining material risk, tolerance thresholds and risk appetite (Risk Materiality)

- Define and manage risk identification and assessment procedures by creating a comprehensive inventory of Risks based on risk/process centric framework, defining risk measurement methodology and assessment scorecard

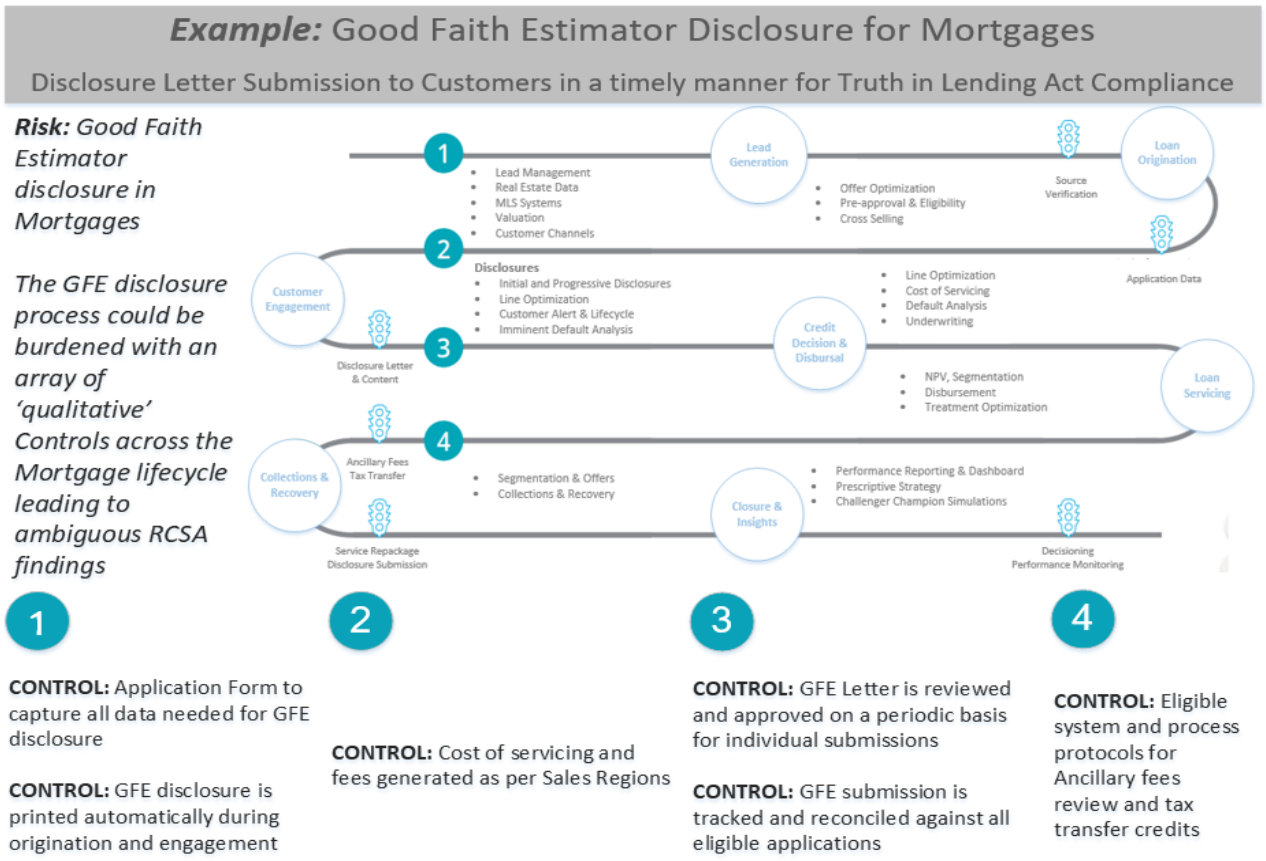


Ideally, the first line which understands the nuances of the Operational challenges should lead the initiative in defining the Risk taxonomy and the second line should define the Controls hierarchy to deal effectively with the identified Risks. The objective of these controls is not only to reduce residual risk, but to prevent Risk materialization. The efficacy of this participation needs to be critically evaluated while conducting the Risk and Control Self-Assessment (RCSA) cycles by analyzing qualitative and quantitative metrics

4.0 GAUGING EFFICACY OF RISK EXPOSURES AND CONTROL EFFECTIVENESS

In the traditional practice of performing RCSA cycles the first and the second lines have had a quasi-symbiotic commensalism relationship. The Business benefits from the activities of the second line to 'tick-the-box' for Organizational mandates enforcing RCSA protocol, while the second line suffices itself with the 'theoretical' completion of the RCSA cycle falling significantly short of both Risk Exposure evaluation and prediction

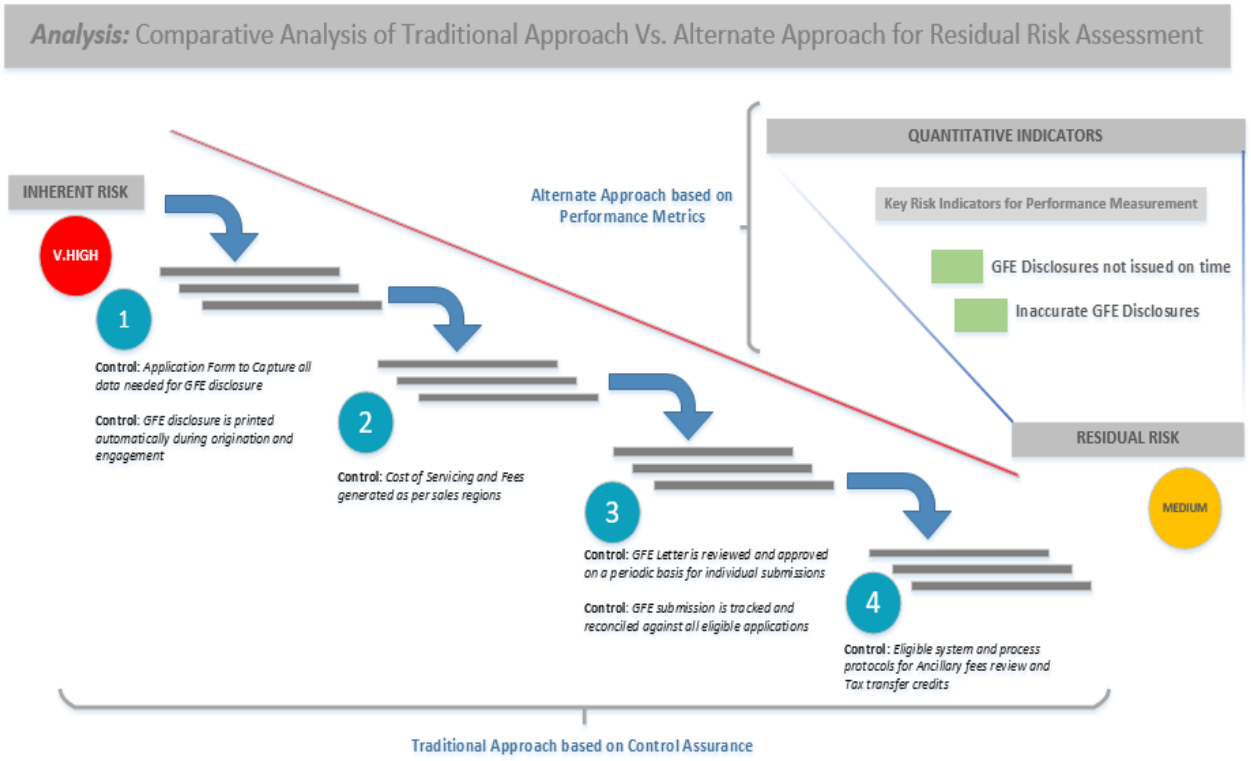
Business generally identifies the 'high-risk processes' or 'key risks' derived either from a Process centric or a Risk centric framework. Autonomy in identifying these processes could lead to possible omissions based on Business priority. For example, a low impact, high volume record to report operational loss (or) near miss could be deemed labor intensive and hence secondary by business, whereas it can be critical for compliance



In turn, the second line engages in identifying the inventory of 'all' the related risks and controls pertaining to the Business defined 'high-risk processes' or 'key risks'. This approach, as mentioned earlier, not only leads to ballooning of the Risk and Control libraries but also falls short of creating transparency into material risk exposures

A better approach would be to conduct a breakpoint analysis for each of the critical Processes and analyze the materiality impact of these breakpoints should any related Risk materialize. This not only ensures that no known material risk is ignored but such break points can be tied to underlying regulatory requirements, process level risks, controls and impacted products, thereby enabling upstream movement of pro-active Controls and monitoring Metrices

As illustrated in the below example the Good Faith Estimate Disclosure for Mortgages could be monitored by the indicated six controls which needs to be tested for their effectiveness each time an RCSA cycle is conducted under the traditional approach.



Traditional Approach: Mandates Control Assurance across all 6 Controls in the Business Process

Alternate Approach: Monitoring KRI's increases specificity of Control Assurance (or) renders it redundant. Focus shift from 6 Controls to 2 KRI's for Residual Risk Assessments

Alternately, by adopting an approach based on Key Risk Measures (Eg: KRI's) the efficacy of Control Assurance can be increased – in our example two KRI's instead of six default Controls. Moreover, these KRI's can also be used for monitoring process performance and efficiency

5.0 QUANTITATIVE MEASUREMENT OF NON-FINANCIAL RISK

Quantification of Non-Financial Risk is a great enabler for improving Risk Management. Unlike Credit and Market Risk, which can be analytically measured at individual and various aggregate levels, measurement of Non-Financial Risk still poses significant challenges for Banks

A direct, straight-forward approach is to identify quantifiable, critical Risk indicators; like GFE disclosures mentioned above; linked to pre-identified top Risks. If identified accurately these could prove to be the real measures not only to quantify NFR exposures but also to evaluate the quality of the Controls thereby providing a robust foundation for Residual Risk Assessments, Scenario Analysis, Risk Indicators Management, Capital Estimations and Projections

In case of instances where it is challenging to define a straightforward approach, advanced analytics combined with leveraging technologies like Robotic Process Automation & Machine Learning can attribute to better NFR management. Leading organizations are adopting various approaches to not only reduce Risk mitigation like instances of rouge trading, but also to consciously evaluate relevancy of Residual Risk Assessments for critical processes like Business Continuity Management (BCM)

6.0 CONCLUSION

As regulatory guidelines around measuring and managing Non-Financial Risk evolve Organizations can achieve tangible benefits by changing the current quasi-symbiotic commensalism relationship between the first and second lines of defense into a mutually symbiotic relationship. The nuances of such a relationship will depend on the complexity of the Organization and the approach designed, with Audit providing an independent view on both its efficiency and effectiveness

Working together, measuring what matters, both Compliance and Business can not only deliver better quality oversight and increased operational efficiency but also guarded protection to Senior Management from personnel liability

ORACLE CORPORATION

Worldwide Headquarters
500 Oracle Parkway, Redwood Shores, CA 94065 USA

Worldwide Inquiries
TELE + 1.650.506.7000 + 1.800.ORACLE1
FAX + 1.650.506.7200
oracle.com

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

White Paper Title
January 2017
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]