

Enterprise Risk Management: Observations and Perspectives 2013



People matter, results count.

Table of Contents

1. Introduction & Background	3
2. Enterprise Risk Management Framework	4
3. Internal Environment and Objective Setting	5
4. Event Identification	6
5. Risk Assessment	7
6. Risk Response & Control	8
7. Risk Reporting	9
8. Risk Governance	10
9. Conclusion	11

1. Introduction & Background

The post 2009-era of enhanced regulations like Dodd Frank, Comprehensive Capital Analysis and Review (CCAR) and Basel III has had a significant impact on how financial institutions manage risk. These changes have also highlighted the weaknesses in the structures and processes banks currently rely on to manage risk.

The objective of this paper is to present Capgemini's observations and perspectives with respect to the state of enterprise risk management (ERM) in organizations today. Aside from emphasizing and identifying issues which impede the effectiveness of ERM programs, our focus is on the changes that are transpiring in terms of how banks manage risk and the impact these have on people, processes and technologies.

The Committee of Sponsoring Organizations¹ (COSO) ERM framework provides a comprehensive set of essential components that provide clear direction and guidance for ERM. This framework is leveraged to present our observations in a systematic manner.

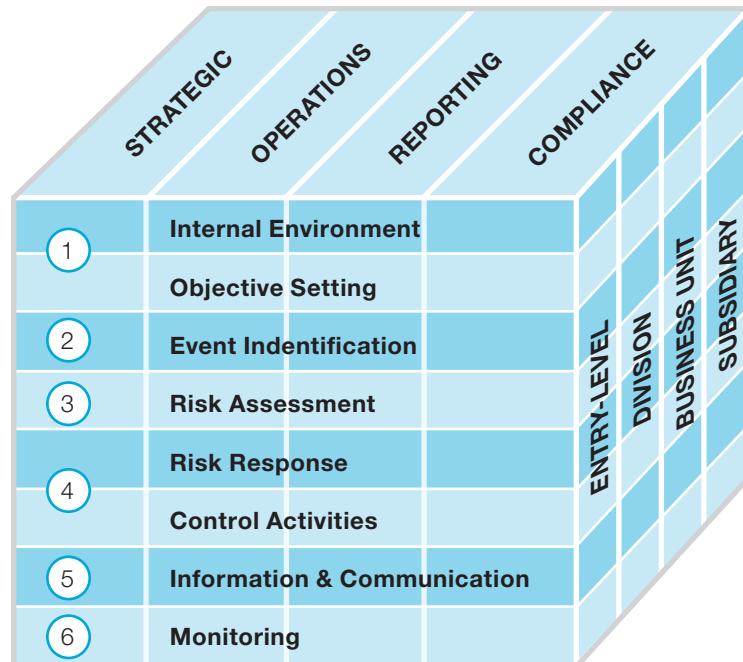


¹ The Committee of Sponsoring Organizations is a joint initiative of five private sector organizations: American Accounting Association, American Institute of CPAs, Financial Executives International, Association of Accountants and Financial Professionals in Business, and the Institute of Internal Auditors. www.coso.org

2. Enterprise Risk Management Framework

The ERM framework from the Committee of Sponsoring Organizations (COSO) gives a comprehensive set of essential components that provide clear direction and guidance for ERM. We leverage this framework to present our observations in a systematic manner. The figure below is called the COSO cube and is the most common depiction of the framework.

Exhibit 1: ERM Integrated Framework from the Committee of Sponsoring Organizations²



Key components of this framework include:

1. **Internal Environment:** Establishes the entity's risk culture
2. **Objective Setting:** Defines the enterprise risk objectives
3. **Event Identification:** Ascertains events that affect entity's objectives
4. **Risk Assessment:** Considers risks based on likelihood and impact
5. **Risk Response:** Evaluates possible responses to risk
6. **Control Activities:** Establishes policies, procedures and controls
7. **Information & Communication:** Enables information exchange
8. **Monitoring:** Evaluates the effectiveness of ERM program

2 <http://www.coso.org/ERM-IntegratedFramework.htm>

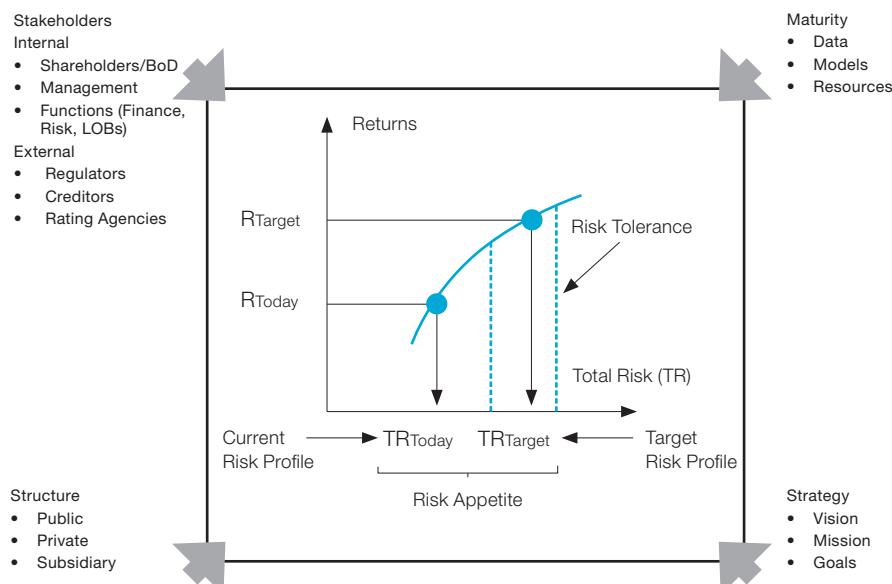
3. Internal Environment and Objective Setting

“ Internal Environment – A financial institution's internal environment reflects the culture of the entity and establishes the basis for how risk is viewed and addressed by its people. It defines the risk management philosophy, risk appetite, integrity and ethical values and most importantly, the environment in which the firm operates.

Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.”

In most banks, this aspect of the framework is addressed via the definition of the risk appetite. The typical components of a risk appetite program are illustrated in the exhibit below.

Exhibit 2: Risk-return Tradeoff, Risk Appetite and Risk Tolerances



3.1. Observations & Perspective

Most banks have defined their risk appetite and tolerances but challenges remain around the following:

- Achieving alignment of risk policies and consistency of roll-ups across the organization.
- Sensitivity of the loss measures to risk drivers and events.
- Understanding interdependencies between risk types e.g. how do credit events impact liquidity.
- Identification of interdependencies between portfolios. E.g. impact of plant closure (C&l) on consumer loans (employees of the plant).
- Relation between finance and risk hierarchies (and mismatch) and its impact on KPIs and loss measures. E.g. regulatory reporting (Y9C/14A) vs. financial reporting vs. business/product vs. modeling segmentation.
- Interrelationship and dependencies between risk and finance data, models and measures.

4. Event Identification



The internal and external events affecting the achievements of an entity's objectives must be identified to distinguish between risks and opportunities. Events that are opportunities are channeled back to management's strategy or to the objective-setting processes."

Event identification is better understood by classifying risks as Known Risks, Unknown Risks and Unknowable Risks.

Known Risks

Known risks are those in which the causes, probability of occurrence and likely impacts are understood and well defined. Some uncertainty may exist around the estimates, but these risk events have occurred previously and can be measured and managed. Examples are credit risk, market risk, operational risk, or liquidity risk.

Unknown Risks

Unknown Risks

There is an emerging interest regarding unknown risks. These are risks where one or more of the risk dimensions—probability, timing, magnitude, or impact—are not known.

Key questions are

- What should be done about unknown risks?
- How to operationalize the monitoring for unknown risks?

Unknown Risks

There are certain risk events which are well defined, but the probabilities as to the occurrence of specific events cannot be assigned. These risks, classified as Unknown risks, have several competing models of how reality might unfold, but no accepted paradigm. They require resilience to be built into risk response models through continuity planning, stockpiling, slack in the system or diversification of sources of vital goods. These are also referred to as "Emerging Risks" and examples include business continuity affected due to terrorism or systemic financial instability.

Unknowable Risks

These risks have not emerged and understanding of the systemic linkages of unknowable risks is speculative. Key consideration is the context of risk conflation, where a large number of possible combinations of risks and vulnerabilities can lead to a vast array of possible outcomes.

4.1. Observations & Perspective

- Most banks have a well defined risk organization to compute and manage traditional risk types like credit, market, liquidity, or operational, but managing and computing the inter-dependencies between risk types remains challenging.
- There is a renewed focus on strategic, business and reputational risk. The data, relevance and quantification process of these risk types remain in a nascent stage of implementation. Sentiment analysis is being done to assess reputational risk.
- There is an emerging interest regarding unknown risks. These are risks where one or more of the risk dimensions—probability, timing, magnitude, or impact—are not known.

5. Risk Assessment

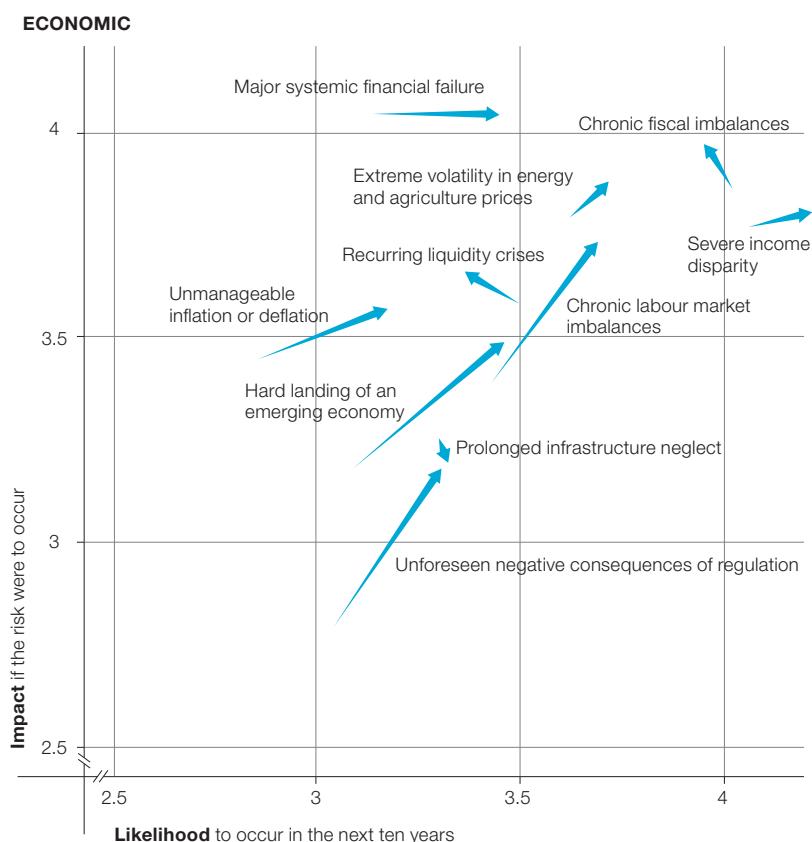
“ Risks are *analyzed*, considering the likelihood and impact as a basis to determine how they should be managed. Risks are *assessed* on an inherent and a residual basis.”

In general:

$$\text{risk level} = \text{likelihood of occurrence} \times \text{impact severity}$$

The exhibit below shows events on these two scales.

Exhibit 3: Risk Assessment: Likelihood and Impact



Source: World Economic Forum 2012³

5.1. Observations & Perspective

- Traditional dimensions of risk assessment have been likelihood and impact. Additional dimensions for risk assessment are now being considered⁴: Vulnerability and speed of onset (velocity) have become critical and need to be assessed as well. The vulnerability aspect is being modeled using stress testing and scenario analysis tools.
- Modeling the velocity component is still in a nascent stage of development; historical analysis is currently being used as a proxy.
- Model driven decision-making is under question and banks are struggling with maintaining the right balance between qualitative and quantitative aspects of risk management.
- Refinements to the estimation of likelihood of occurrence include Bayesian approaches. Key aspects of the Bayesian approach, which makes it applicable here, is the constant updating of posterior probabilities contingent on an event happening.
- The process of translation of losses into capital and liquidity requirements has come into increased scrutiny. This has heightened the need to have better integration between the risk and finance divisions. CCAR programs have exposed banks to the integration challenges from people, process and technology perspectives. Inconsistency of data definitions and lack of data quality are major hindrances for assessing risks.

3 <http://www.weforum.org>

4 ERM Risk Assessment in Practice, COSO, Oct, 2012

6. Risk Response & Control

“ Risk Response – Management selects risk responses to avoid, accept, reduce, or share risk; and develops a set of actions that aligns risks with the entity’s risk tolerance and risk appetite.

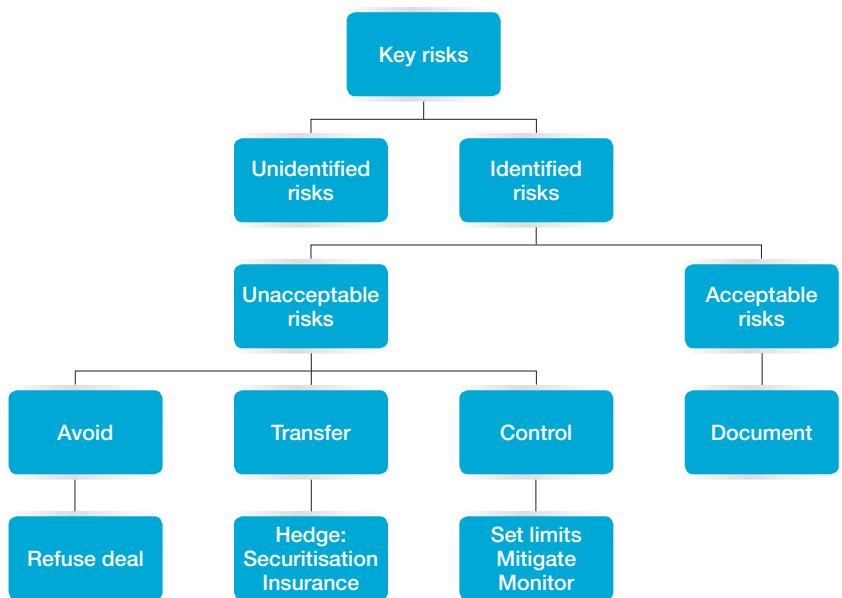
Control Activities – Policies and procedures are established and implemented to help ensure that risk responses are effectively carried out.”

The following exhibit describes a general framework of the risk response and control activities.

Exhibit 4: Risk Response Activities – Avoid / Transfer / Control / Document

Risk Response

Thresholds are being re-evaluated for early flagging.



6.1. Observations & Perspective

- Limit systems are the traditional processes to respond to risk. Challenges remain in using an early flagging system. By the time a limit is breached, it may be too late.
- Traditional measures like risk transfer and hedging (e.g. securitization and insurance) are being re-evaluated for effectiveness. The former is not so effective from a liquidity perspective and the latter from a counterparty perspective.
- “Why did we not sell it at 95?” relates to the timing aspect of taking action against an event.
- Given the complexities of today’s organizations, responses need to be “orchestrated” across business and functional silos. This poses a major challenge to most banks.
- Organization structures are still evolving for how a firm responds to slow moving versus rapidly evolving events. In the absence of this distinction, organizations struggle to monitor and manage such events with their current processes.

7. Risk Reporting

“ Relevant information is identified, captured, and communicated in a form and timeframe that enable people to perform their responsibilities. Effective communication also occurs, in a broader sense, flowing down, across, and up the entity.”

7.1. Observations & Perspective

Data

- Data reconciliation issues have led organizations to re-evaluate their enterprise information strategy.
- There is a move towards platform solutions like Oracle and SAP, away from a best of breed approach which was used in the past.

Reporting

- The variety of different complex platforms within a financial institution makes integrated risk reporting substantially challenging.
- Conventional reporting processes are being complemented by agile/mobile processes.
- Integration of MIS and regulatory reporting is being contemplated to reduce costs.
- Visual and interactive dashboard technologies are being evaluated as opposed to tabular and static reports.
- Reporting processes are being redesigned based on the “response strategy” mentioned earlier.

Technology

- New technologies - especially related to mobile, cloud and big data – are gaining adoption.
- Cyber security is a major concern (unknown risk!) and is an impediment to adoption.

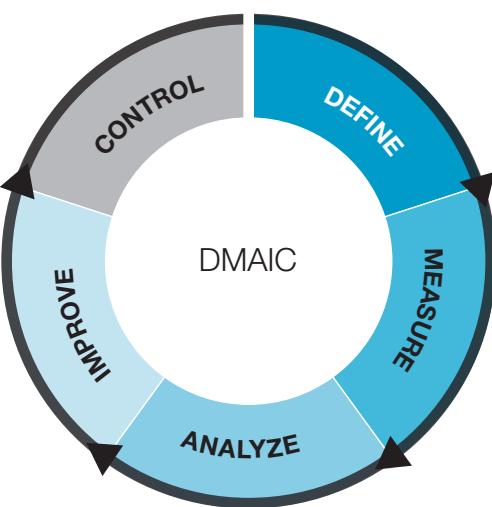
8. Risk Governance

“The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.”

Typically, governance is achieved via a set of tools like:

- Six Sigma (DMAIC)
- COSO (Internal Control Model)
- Regulatory Standards (Basel, Dodd-Frank Act)
- Risk Management Maturity Model
- Performance Metrics (RAROC, EVA)

Exhibit 5: Six Sigma Process for Risk Process Monitoring



8.1. Observations & Perspective

- Internal audit and model validation have gained enhanced visibility internally as well as externally. Model Governance and Model Risk Management are hot topics with scope extending beyond traditional model validation and performance monitoring to an enterprise level.
- The feedback (process) loop from self-assessments is being evaluated and redesigned. Processes from total quality management and Six Sigma approaches are being formalized and evaluated within the context of ERM. NOTE: *Self assessment here refers not only to the Operational Risk RCA but to all aspects of risk management.*
- Governance, Risk and Compliance (GRC) tools are being implemented and also evaluated against expanded requirements. Capturing impact of events on multiple risk types is a key objective.
- Early detection of slow evolving events, especially internal ones, has led banks to evaluate big data and text mining technologies.

9. Conclusion

Enterprise Risk Management has evolved in recent years in response to market and industry demands. In addition, both regulatory trends and technology trends continue to influence the risk management processes in a significant way. For most institutions that have spent a lot of time, effort and money in implementing enterprise risk management, it is worthwhile to make a holistic assessment of their systems and processes in light of recent events.



About the Author

Dr. Samir Kamat is responsible for Capgemini's Business Information Management practice for the Banking industry, leads our Global Risk & Compliance Center of Excellence and is a member of the Global Advanced Analytics Practice Leadership team. He is responsible for the management and growth of the practice with a principal focus on enterprise risk management, customer analytics, data visualization and reporting solutions. He has worked on stress testing and capital management for commercial banks, design and implementation of credit scorecards, economic capital frameworks, RAROC tools, and data quality and governance programs. Additionally, he has defined and implemented strategic and tactical business intelligence plans for large commercial banks.

The author would like to thank **JoEtta Colquitt**, **Rita Melein** and **Suresh Gopalakrishnan** for their contributions to this publication.



About Capgemini

With 125,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2012 global revenues of EUR 10.3 billion.

Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at

www.capgemini.com