A Systematic Approach to Risk Management: Insurance Industry

By Shriram Gokte

Background

Insurance companies are in the business of taking risks. Worldwide these companies write policies that deal with specific risks, and in many cases, even underwrite exotic risks. As a direct corollary, therefore, insurance companies should be good at managing their own risks. However the truth is a little far from that! Most insurance companies are very good at assessing insurance risks but are not very good at setting up structures in their own home to manage their own operating and business risks.

As an emerging need from the credit crisis, IRDA issued a set of guidelines on corporate governance in 2010,1 which contained a reference to the setting up of a mandatory risk management committee (RMC). The RMC has to lay down a risk management strategy across various lines of business, and the operating head must have direct access to the Board. However, IRDA left it to the companies to work out the details of how risk management functions were to be suitably organized by them given the size, nature, and complexity of their business. But that should in no way undermine the operational independence of the risk management head. Because of this leeway, most of the Indian insurance companies have given risk management responsibilities to one of the actuaries, which is not a very strong move toward independence.

Today it is well recognized that sound management of an insurer, as for other financial sector entities, is dependent on how well the various risks are managed across the organization. In this article I have described how ideally should insurance companies manage their various risks.

---

1 IRDA’s guidelines on Corporate Governance for Insurance Companies
Risk Drivers

In an insurance company, the cash flows are organized along two streams: a) Inflows—premiums, investment income, refunds, and so on and b) Outflows—claim payments, reinsurance premium, agent remuneration, salaries, interest and dividends to investors, and so forth. Thus, risks could be considered along these two flows. In addition, insurance products rely on models dealing with longevity/mortality, morbidity, economic conditions, or market conditions. There is a large risk that any of these assumptions or models could be incorrect, leading to first the pricing risk (that price charged was incorrect) and then the solvency risk—risk that arises from inadequate reserves, and company runs out of capital. As many insurance companies have large fixed income holdings or equity position, there is also credit risk and market risk associated with their investment portfolio. Moreover, the processes, people, and systems of an insurance company are also exposed to risks. These are operational risks and are present throughout the company. Additionally, like other corporations, an insurance company is exposed to other strategic risks, such as liquidity, reputation, legal, business planning, and so on.

The time lag between the selling of an insurance coverage and the claim payments can be extremely long. This lag makes insurance a particularly difficult business to manage. There are also a variety of cultural reasons that complicate insurance risk management. For example, there is a perception by some insurance managers that the insurance business is strictly an underwriting game. This essentially means that if an insurance company underwrites “the right risks at the right prices,” the other key insurance activities (i.e., investment, claims handling, reinsurance, and so on) “can take care of themselves.” In this situation risk management obviously takes a back seat.

Risk Framework

A good risk framework should have a strong governance structure so that the board and the management should know how risks are being managed. This involves appointing a chief risk officer (CRO) for risk management and the organizational culture too should support it. In large companies, it is common to form a separate risk management unit, staffed by a multi-disciplinary team. The work of this team is typically facilitated by
designated persons in each of the various departments, such as underwriting, legal/compliance, actuarial, finance, marketing and sales, policy servicing, claims, IT, and so on. The management should always be aware about the dangers of undermining the independence of the department and should ensure that the risk-taking and risk monitoring roles are independent. To ensure this, there are a few well-known frameworks available such as ISO 31000 risk management standard and the COSO ERM. There is another framework used by S&P and A&M Best in their ratings as well. Few of the governance structures are given below.

Figure 1 – An ERM framework (based on COSO, ISO 31000 & S&P frameworks)

A CRO should ensure that risk management in the organization is centralized rather than being carried out from silos. He should functionally report to someone like the risk & audit committee while administratively he could report to a CxO, such as the chief financial officer (CFO). This gives the CRO the independence and ability to ask tough
questions to the top management. Structurally, there are several choices on where the CRO should be placed in the organization.

**Franchise vs Policyholder interest**

To appreciate the risk environment better, a CRO should understand the nuances among the policyholders’ interests, franchisee interests, and other stakeholders’ interests. The policyholder interest represents the objectives behind insurance policy purchases by policy buyers; regulators enforce the protection of policyholder’s interest. Franchisee interests are the objectives of the investors or owners who have provided money to capitalize the company and would want the insurance company to grow and make profits. Mostly policyholder and franchisee interests are not in conflict, but there are times when they can diverge. For example when investors are looking to exit the company, the interests definitely could diverge. What is good for the company may not necessarily be good for existing policyholders. A CRO should understand this difference and should track risks separately if required.

**Three Lines of Defence Model**

The three-line defence model is one of the most popular governance models. It lays down very specific responsibilities for each line of defence while ensuring independence.
Table 1. - Three lines of defence governance model

**First line of defence**
The first line of defence is the primary management responsibility for strategy, performance management, and risk control, which lies with the board, the chief executive officer and the senior management.

**Second line of defence**
The second line of defense is oversight of the risk framework by the risk committee, CRO, and the risk management functionaries working with their counterparts in other areas.

**Third line of defence**
The third line of defence is stringent internal audit that ensures the independence and effectiveness of the group’s risk management systems.

**CRO Role**

Ideally, as CRO is the main risk facilitator of the company, all risk-related decisions should have his inputs. However, at the very least, a CRO should have the following elements in his role:
• Enterprise risk management (ERM)
• View of the key risk control programmes
• Ensuring common risk language across organization
• Managing the risk view through the risk dashboard

**Enterprise Risk Management**

Through enterprise risk management (ERM) risks in a company are understood, managed, and used for decision making. In a robust implementation, a CRO becomes the focal point of the ERM universe.

In the ERM role, a CRO then becomes the owner of the risk management in the company. The following set of accountabilities should become a part of his/her KPIs.

- Ensure that company has the right risk framework
- There is sufficient management buy-in, and the company has provided resources with the right quality and in the quantity.
- There is a process and rigour to risk assessments.
- All key risks are understood and analysed.
- All risk mitigation strategies and tactics are adequate. Wherever there are gaps, a CRO should ensure that there are action plans to fix them up.
- Risk factors become central to all key decisions.
- Ensure that the perceptions about risks in the organization are the same and that there is a common risk language in the organization.
- There are sufficient key risk indicators (KRI) to monitor risks regularly.
Key risks control programmes

The key risks in an insurance company are underwriting risks, market risks, credit risks, operational risks, liquidity risks, and strategic risks (reputation, compliance/legal, agency, and so on). Each of the risks should be typically owned by a department, which will then set up procedures, put systems in place, and have the right people to manage them. But the effectiveness of such a set up has to be independently verified and monitored by the CRO.

Table 3. Risk categories

<table>
<thead>
<tr>
<th>Credit Risk</th>
<th>Market Risk</th>
<th>Insurance Risk</th>
<th>Operational Risk</th>
<th>Strategic Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Credit Officer</td>
<td>Treasury Asset/Liability Manager</td>
<td>Actuaries</td>
<td>Operational Process Risk Management IT Internal Audit Actuaries</td>
<td>Senior Management Compliance Legal</td>
</tr>
</tbody>
</table>

Credit risk is incurred whenever an insurance company is exposed to loss if counterparty fails to perform its contractual obligations including failure to perform them in a timely manner. Credit risk may therefore have an impact upon a company's ability to meet its valid claims as they fall due. Credit risk can also arise from underlying causes that have an impact upon the creditworthiness of all counterparties of

- Business credit risk -. failure of a re-insurer
- Invested asset credit risk - non-performance of invested assets
- Political risk (affecting credit worthiness of securities held by the insurer)
- Sovereign risk (affecting credit worthiness of securities issued by government or government entities)
Market Risk

Market risk is the risk that as a result of market movements a company may be exposed to fluctuations in the value of its assets, the amount of its liabilities, or the income from its assets. Sources of general market risk include movements in interest rates, equities, exchange rates and real estate prices.

- Interest rate risk - losses arising due to change in interest rates
- Equity and property risk - losses arising due to drop in equity prices
- Currency risk - losses arising due to adverse movements in exchange rates
- Basis risk - arising because the yields on instruments of varying risk quality, liquidity and maturity don't move together, affecting the assets and liabilities of the company independently.
- Reinvestment risk – risk that assets will be reinvested at a lower rate.
- Concentration risk – that market risks are concentrated on few intermediaries
- ALM risk – that assets and liabilities are not matched
- Off balance sheet risk - losses arising from assets or liabilities not shown on the balance sheet eg payments required under futures agreements with zero value at the balance sheet date

Operational Risk

The uncertainty arising from events caused by failures in people, process and technology as well as external dependencies.

- Fraud & defalcation
- Sales practices
- People & skills Attrition
- External disruption
- Inadequate employee training
- Computer security
- Processing Errors
- Non-compliance
- Contractual risks
- Changes in laws/regulations

Insurance

The uncertainty due to differences between

- Underwriting process risk - related to
Another risk that Indian insurance companies should consider is the improvements in longevity due to improved living standards, socio-cultural advances, changing lifestyles, improving delivery of health services, breakthroughs in medical treatment, improving diets, and generally healthy living. These improvements may not take place equally in all demographics. A report by Mortality and Morbidity Investigation Centre (MMIC), set up by the Life Insurance Council and the Institute of Actuaries of India, has shown that improvements in Indian longevity has been “spectacular” in the 1970s and 1980s, but slowed in the 1990s and 2000s. Insurance companies should begin building models so that they can price mortality and morbidity risks accurately.

**Operational Risks**

Operational risk has been defined by the Basel Committee on Banking Supervision as the risk of loss resulting from inadequate or failed internal procedures, people, and systems, or from external events. The insurance industry is no different, and same definition is typically used. Thus, this covers management of risks concerning any of the firm’s operations, whether caused by internal or external sources. Examples of operational risk exposures include internal and external fraud; failure to comply with employment law or
meet workplace safety standards; damage to physical assets; business disruptions and system failures; and transaction processing failures.

The various operational risk control programmes are:

1. **Fraud control programmes.** Some insurance companies’ set up fraud control teams to assess and investigate frauds. Due to the nature of the business, several types of policyholder-related frauds are possible, in addition to employee and supplier frauds. Britain's insurers have agreed to pay £9 million ($14.4 million) to fund a new police unit dedicated to combating insurance fraud as the industry grapples with rising bogus claims. It is reported that such bogus claims cause losses of around £2 billion a year².

2. **Information Security programme.** These are implementation of policies, procedures, and controls aimed at avoiding leakages or misuse of information. Insurance companies have several types of information that should be protected. For example personal information, financial and medical information, and claim information. Imagine if the claim data or financial information gets leaked to criminals, they can identify potential victims and perpetrate crimes. The Indian Information Technology Act of 2000 and its amendment in 2008 require companies to implement and maintain reasonable policies and procedures. ISO 27001 certification is one of the commonly used standard to set up a globally recognized information security programme that will assure confidentiality, integrity, and availability of information.

3. **Business continuity programme.** Companies plan their responses and how they will continue their business if they are faced with disasters and disruptions. Companies typically have a business continuity planning (BCP) in place, test it periodically, and evaluate criticalities and recovery times if the office was to be unavailable for a long period. Alternate work area sites should be set up that are far away from the location of the primary operation. The Mumbai flood of 2005

provides an example when an insurance company in Mumbai was able to service its branches because its disaster recovery centre was in Hyderabad. Pandemic flu scare is another scenario where companies have planned their responses. In fact, in a pandemic situation, it is not only the operations that are affected, but the number of claims coming in would increase and the new business could shutdown. Insurance companies should plan for such scenarios during “peacetime.”

4. **Quality programmes.** The transactional nature of insurance company’s new business, claims or policy administration, makes them amenable to processing errors, customer complaints, and loss of quality. Several insurance companies have initiated quality enhancement programmes like E&O (errors & omissions) to track errors as well as 6 sigma or ISO 9001 to improve the quality of processing and services.

5. **Legal/compliance programme.** Insurance companies are exposed to significant legal as well as regulatory risks. Legal risks include incorrect policy wordings, outsourcing service-level agreement (SLA) risks, agency arrangements, and so on. IRDA compliance is ever evolving, and insurance companies typically have a compliance team to manage compliance requirements. Insurance companies also need to record, resolve, and track customer complaints.

### Risk Management Tools

**Risk Appetite**

Risk appetite is the amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time. Risk appetite can provide consistency in decision making. It enables people to take well-calculated risks when opportunities arise that will improve delivery, and conversely, to also identify when a more cautious approach should be taken to mitigate a threat. The CRO should ensure that the risk owners articulate their risk appetite as an effect on capital, so that one can easily understand and monitor.

**Risk Self-Assessments**

Risk assessment is the basic unit of risk identification across the company and typically should be performed by the departments themselves though facilitated and challenged by
the risk management people. A risk self-assessment is a very powerful tool and is based on the premise that those who perform or facilitate a process best know their risks. These exercises can uncover emerging risks. A risk assessment exercise done with top management for articulating the major risks to the company is the entity-level risk assessment. Such risk assessments should throw up the strategic risks for the company in the near and long term. Efficacy of entity-level risk assessment lies in seeing whether there was an emerging risk in the past that caught the management unaware. These could be vulnerable points that require a tightening of risk assessment. Entity-level risk assessments could also be used for making 302 certifications under US SOX. A typical UK insurance company saw its entity level risk assessments as given in Table 4.

<table>
<thead>
<tr>
<th>RISK</th>
<th>Risk ID</th>
<th>Risk Description</th>
<th>Central Description</th>
<th>Controls and Actions</th>
<th>Action Plan</th>
<th>Effective Date</th>
<th>Next Review Date</th>
<th>Risk Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market</td>
<td>1</td>
<td>Shockwave events and tailwinds give rise to market exposure particularly relevant currency for inflation as differences arise in between inflation and inflation rate</td>
<td>Review by Investment Committee and Investment (supervisory) Committee of all activity (market and inflation impacts, duration decisions, etc.)</td>
<td>Monitoring to the credit teams' daily, also by IC at least weekly and IC, challenge every 4 weeks. Consideration of other products related (inter, Review of watch list, review of IC, Set of early warning triggers for monitoring credit spreads over goals.)</td>
<td>Ongoing review by the credit team and the Investment Committee. Early warning triggers reviewed by investment risk Committee. Notify management if any.</td>
<td>10/11/2013 next Risk Committee</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Credit</td>
<td>2</td>
<td>Inherent rates of level default / level recovery rates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit</td>
<td>3</td>
<td>Valuing credit spreads causes a fall in asset values on a mark to market basis</td>
<td>Ongoing review by the credit team and the Investment Committee. Non-trading entities approved by IC, Set of early warning triggers for monitoring credit spreads over goals.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>4</td>
<td>An error in the production of the situation exist or will give rise to incorrect accounts or a false position of our capital</td>
<td>Review by Audit/ control committee, validation of numbers by MI and Audit teams. Process controls implemented on valuation System.</td>
<td>Ensure that variance is updated, ensure that results are incorporated as part of the system review and that systems are improved and tested.</td>
<td>10/11/2013 next Risk Committee</td>
<td>B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Longevity</td>
<td>5</td>
<td>Mortality improves at a faster rate than expected</td>
<td>Ongoing research and external review by Capital, DB, and Nelson Wyatt. Expiration of reserves to pass the on the risk to reinsurers.</td>
<td></td>
<td>10/11/2013 next Risk Committee</td>
<td>B</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4 – Entity level risk map

Entity-level risk assessments should be matched by risk assessments done at departments and function levels. The structure of such risk assessments should mirror the organizational structures. If every manager in a company, including the CxOs, have their top risks to focus on and if these are linked to performance objectives, the tone and level of risk management in the company would be very robust.

Depending on the extent of risk assessments, the process, transactions, and applications could also be covered by risk assessments. Risk assessments should provide inputs for risk registers. Risk registers are the compendium of risks and their controls. A typical risk registers (Figure 5) is a good tool to assess the effectiveness of risk mitigation in the
company. The risk registers could be used by auditors to drive their audit planning and extent of their testing. The top-down risks from entity-level risk assessments have some correlation with some of the down-up risks coming from process-level assessments. For example if attrition is one of the top risks, some of its components can come from process-level risks, such as excessive disciplinary action, or high reliance of a process on few skilled staff. For operational risks, the top-down risks can usually be drilled into bottom-up risks.

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Owner</th>
<th>Risk Description</th>
<th>Severity Gross</th>
<th>Likelihood Gross</th>
<th>Control Description</th>
<th>Control Strength</th>
<th>Severity Net</th>
<th>Likelihood Net</th>
<th>Action Plans</th>
<th>Deadlines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance, Regulatory &amp; Capital Risk</td>
<td>ABC</td>
<td>ABC is in tax payable position due to non-availability of group tax losses</td>
<td>44</td>
<td>34</td>
<td>ABC needs to issue funding bonds and needs to complete implementation with QUB facility to ensure withholding tax payments will not be due.</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>Auditor opinion is in place and issuance of funding bonds and QUB facility needs to be completed before Sep 10</td>
<td>Sept 10</td>
</tr>
</tbody>
</table>

*Figure 5 – Risk register format*

**Risk Registers**

The risk registers are the central repository of risk information. They basically store the risk and control information for a process, department, or entity. Typically, the risk registers contain the risk description, risk category, risk owner, gross risk measure, [severity (impact) and likelihood before controls], control details, and strength of the controls (self assessed as well as assessed by risk management), net risk measure, [severity (impact) and likelihood after controls], action plans, and deadlines to project target risk as impact and likelihood. Control documentation, including end-to-end process maps, key control sheets, and procedures manuals can be attached to the risk register. Use of colours can provide the visual triggers regarding the statuses – which of the risks need attention. Output from the Register can be used in quantitative risk analysis for reserving purpose, management information in the form of Top risk report and an
Internal Audit plan which can be partly driven by the identification of less strong controls within the business.

**Common Risk Language**

A common risk language forms an important part of the overall risk management framework. It enables meaningful comparisons to be drawn between risk information provided by the risk owners, which facilitates an understanding of the risks facing the company. With a common risk language, the management, the risk owners, and interested stakeholders would find it easier to fully understand or effectively communicate the risks that the group faces.

The common risk language is expressed through the common risk framework consisting of standard risk categories, consistent risk identification, scoring and prioritization methodologies, and a common risk-recording mechanism (Figure 6).

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk (sub-category)</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit</td>
<td>Counterparty Risk</td>
<td>The risk of guarantors, reinsurers, borrowers and general insurers failing to meet their financial obligations.</td>
</tr>
<tr>
<td>Market</td>
<td>Equity</td>
<td>The risk of stock price fluctuations.</td>
</tr>
<tr>
<td></td>
<td>Real Estate</td>
<td>The risk of real estate value fluctuations.</td>
</tr>
<tr>
<td></td>
<td>Foreign Exchange</td>
<td>The risk of foreign exchange rate fluctuations.</td>
</tr>
<tr>
<td></td>
<td>Interest Rate</td>
<td>The risk of asset-liability mismatch resulting from interest rate volatility</td>
</tr>
<tr>
<td>Operational</td>
<td>Financial Reporting/Disclosure</td>
<td>The risk of allegedly inaccurate and/or misleading financial statements and/or related disclosures.</td>
</tr>
<tr>
<td></td>
<td>People</td>
<td>The risk arising from the actions or inaction of the company’s employees.</td>
</tr>
<tr>
<td></td>
<td>Systems/Processes</td>
<td>The risk of information, communications or computer systems failing and/or human or system errors within certain process or transaction.</td>
</tr>
<tr>
<td></td>
<td>Legal &amp; Regulatory</td>
<td>The risk arising from inadequate or incorrect knowledge of, and/or non-compliance with, the laws and regulations governing the company’s business operations and contractual agreements.</td>
</tr>
<tr>
<td></td>
<td>Environmental</td>
<td>The risk of pollution events affecting company property and/or the property of others.</td>
</tr>
<tr>
<td></td>
<td>Strategic Risks</td>
<td>The risk arising from choices of strategies, business models or implementation plans.</td>
</tr>
<tr>
<td>Insurance</td>
<td>Mortality</td>
<td>The risk of over-estimating how long policyholders will live resulting in higher-than-expected claims and benefit payments.</td>
</tr>
<tr>
<td></td>
<td>Morbidity</td>
<td>The risk of misestimating the number of times a policyholder will be sick or the length of the illness, resulting in higher-than-expected claims and benefit payments.</td>
</tr>
<tr>
<td></td>
<td>Longevity</td>
<td>The risk of under-estimating how long policyholders will live resulting in higher-than-expected claim and benefit payments.</td>
</tr>
<tr>
<td></td>
<td>Product Design &amp; Pricing</td>
<td>The risk arising from inappropriate or inadequate product design and pricing, including the risk that the policy is not designed to take into account changes in policyholder behaviour and the external environment may also affect the risk exposure.</td>
</tr>
<tr>
<td></td>
<td>Underwriting</td>
<td>The risk arising from the underwriting process resulting in the acceptance of undependable risks.</td>
</tr>
<tr>
<td></td>
<td>Claims</td>
<td>The risk arising from the claims administration process, including the inappropriate payment of claims, fraud, and assertions of bad faith.</td>
</tr>
<tr>
<td></td>
<td>Property/Casualty</td>
<td>The risk of providing property/casualty insurance coverage to third parties.</td>
</tr>
</tbody>
</table>

*Figure 6. Common risk categories in an insurance company*
**Risk Dashboard**

The next step in the risk management cycle is for the CRO to provide sufficient information to the stakeholders about the status of risk management in the company. The inputs for a risk dashboard should come from a variety of sources—qualitative as well as quantitative, internal as well as external. A good risk dashboard should provide the stakeholders with a view of the full risk measures and trends (Figure 7).

**Figure 7 – Risk dashboard**

**Economic Capital**

Finally, the concept of economic capital provides the company management, CRO, and regulators about solvency matters after considering all risk exposures. Economic capital is defined as the capital required to ensure some likelihood (say 99.5%) of economic solvency over a specified time. Typically, economic capital is calculated by determining the capital that the insurer needs to ensure that its realistic balance sheet stays solvent over one year with a pre-specified probability. For example the economic capital may be determined as the minimum capital required to make 99.5% certain that the insurer remains solvent over the next 12 months (Figure 8). It measures risk in economic...
realities rather than regulatory or accounting rules which may have been designed to support non economic principles.

In 2010 IRDA took a major step towards risk-based capital and required life insurers to submit economic capital along with the appointed actuaries’ annual report for the year ending March 2010. \(^3\)

Compared with the statutory capital (or mathematical reserve) economic capital is a much better metric for assessing and quantifying risk within the risk management framework. Economic capital provides for all risks faced by the company. It represents the emerging best practice for measuring and reporting all kinds of risks across an insurance company. It is called "economic" capital because it measures risk in economic realities rather than potentially misleading regulatory or accounting rules. Economic capital calculations require risks to be quantified as downside to the capital. Some risks can be calculated with more certainty than others—market risks and credit risks tend to be more amenable than operating risks. Economic capital offers an enterprise-wide metric for discussing and pricing risks that is related directly to the principal concerns of management and other key stakeholders—institutional solvency and profitability.

![Figure 8. Economic capital as a function of probabilities](image)

\(^3\) Report of the Committee to draw the road map for moving towards Economic Capital and Market Consistent Embedded value for life insurance industry in India – Institute of Actuaries of India
Conclusion

Insurance companies can improve their risk management by implementing framework based approach and governance structure in the company so that all risks are assessed, understood and controlled. A Chief Risk Officer should have a view of all key risks in the company and should ensure that management is aware of state of risks in the company and that all key risks are controlled or priced appropriately.

About the Author

The writer, a former CRO of an insurance company, has extensive global experience in risk management, audit and controls in the insurance sector. He is currently an independent consultant with practice area in risk & controls issues and can be reached at: shriram.gokte@yahoo.com