Enterprise Risk Management (ERM) Maturity Model and Challenges for Insurance Companies in the Nepalese Context

Ashish Shrestha,
Head – Risk Management Department, SuryaJyoti Life Insurance Company Limited
Email Address: ashish.shrestha@suryajyotilife.com

Abstract

Enterprise Risk Management (ERM) has advanced considerably since the early 2000s, evolving from a governance-driven, compliance-oriented framework into a strategic, integrated approach informed by COSO and ISO standards. For insurance companies in Nepal, the increasing complexity of the risk environment driven by regulatory reforms, digital transformation, and emerging threats such as cyber, ESG, and operational risks has made structured ERM implementation essential. This paper outlines the core prerequisites for establishing an effective ERM system, including a clear governance structure, systematic risk assessment and quantification, informed risk-based decision-making, and robust monitoring and reporting mechanisms. It further presents the ERM Maturity Model, which encompasses five stages ranging from foundational setup to full integration of ERM into strategic planning and business optimization. Although this model provides a practical roadmap, Nepalese insurers encounter notable challenges, particularly limited modeling expertise, difficulties in validating advanced risk models, and insufficient reliable data for quantifying operational and reputational risks. These constraints underscore the need for capacity enhancement, improved data infrastructure, and strengthened risk culture to support the continued evolution of ERM within the sector.

Keywords: Enterprise Risk Management (ERM), risk assessment, economic capital, risk transfer, maturity model, risk tolerance, risk culture.

1. Introduction

The formal development of the ERM framework began in the early 2000s, shaped largely by the COSO and ISO standards, with an initial focus on governance, organizational culture, and accountability. As the risk landscape evolved, the framework expanded to include strategic risk alignment, stress testing, and increased board-level oversight. Today, ERM continues to evolve, placing greater emphasis on resilience, crisis preparedness, ESG factors, digital risk management, and the integration of AI and real-time analytics.

Traditionally, organizations managed risks in isolation, with each department handling its own exposures separately and minimal coordination or communication across the company.

It was reactive in nature, tactical rather than strategic, and had a limited scope. Unlike ERM offers an integrated approach that is dynamic, flexible, and highly interdependent, enabling organizations to manage a broad portfolio of risks more effectively and align risk management with overall strategy (Lam, 2014).

Before heading toward the ERM Module, the organizations should understand the requirements for implementing the ERM. They are:

- ✓ **Governance structure and policies:** Who is responsible to provide risk oversight and make critical risk management decisions? Boards play a key role in overseeing risk and form a dedicated risk committee. Involving members with risk expertise can strengthen oversight. Board members should be actively engaged in setting risk tolerance, challenging management decisions, and ensuring accountability (Sheedy & Canestrari-Soh, 2023). An ERM policy should support this oversight by clearly outlining governance roles, risk principles, reporting requirements, and defined risk tolerance levels, and promote a strong risk culture.

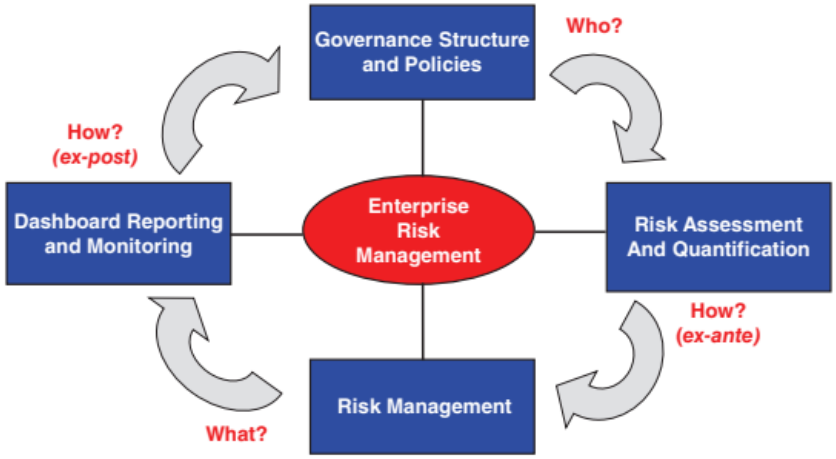
- ✓ **Risk Assessment and Quantification:** How will they make these risk management decisions in terms of analytical input? Risk assessment and quantification tools for ERM include:
    - Risk assessments help identify and evaluate key risks facing the organization, including estimates of their likelihood, potential impact, and how effectively they are controlled.
    - A loss event database records actual losses and risk incidents, helping management learn from past events and identify emerging risks and trends.
    - Key Risk Indicators (KRIs) track risk exposure over time and should ideally be measured against risk tolerance levels and aligned with related Key Performance Indicators (KPIs).
    - Risk analysis models assess specific or organization-wide risks using tools like value-at-risk (VaR), stress testing, and scenario analysis to estimate potential losses based on the organization's risk profile.
    - Economic capital models allocate capital to specific risks based on a set solvency standard (IAA, 2010). They are often used to assess risk-adjusted profitability and support shareholder value analysis.

To avoid a siloed approach, companies should integrate their risk assessment and analysis processes and focus on the relationships between critical risks.

- ✓ **Risk Management:** *What* specific decisions will they make to optimize the risk/return profile of the company? Key decision points include:
    - **Risk acceptance or avoidance:** An organization can choose to increase or reduce specific risks through its core operations or financial activities.

- **Risk mitigation:** This involves implementing controls and strategies to manage a specific risk within the organization's defined risk tolerance.
- **Risk-based pricing:** Every business takes on risks, but the only way to be compensated for them is through the pricing of products or services. Prices should reflect the full cost of the risks involved.
- **Risk transfer:** If a risk is too high or transferring it is cheaper than keeping it, an organization can shift the risk through insurance or capital markets.
- **Resource allocation**: An organization can assign people and funds to activities that offer the highest risk-adjusted returns to maximize its value.

✓ **Reporting and Monitoring:** *How* will the company monitor the performance of risk management decisions (i.e., a feedback loop)? As the saying goes, "what gets measured gets managed." Lam (2014) found that to improve monitoring and reporting, companies should develop forward-looking, role-based dashboards tailored to the needs of the board, executives, or operational teams and these dashboards should combine both qualitative and quantitative data, connect internal risks with external factors, and include key performance and risk indicators. Like other departments, such as sales tracking revenue, customer service measuring satisfaction, or HR monitoring turnover, risk management also needs clear performance metrics and feedback loops to measure success and drive improvement.



2. ERM Maturity Model

As mentioned above, ERM implementation is built on four key building blocks. Companies can view ERM implementation as a step-by-step journey, with each stage creating a stronger foundation. While it typically unfolds over several years, this gradual process allows for thoughtful integration and long-term success. It is helpful for each company to create an ERM roadmap that outlines where they are now, where they want to go, and how they plan to get there (Zhao, Hwang, & Low, 2013). This roadmap should be tailored to the company's current situation, future goals, business needs, regulatory requirements, and available

resources. When developing the roadmap, using an ERM Maturity Model can help assess progress and set key benchmarks. However, an organization may have specific ERM practices from a more advanced stage before completing all of the practices in prior stages (Beasley, Branson, & Pagach, 2015). The 5 stages of ERM maturity Model are:

Stage 1: Laying the Foundation for ERM

In Stage 1, the organization focuses on organizing resources and defining the scope and goals of its ERM program. Key objectives include identifying ERM needs, gaining support from the board and executives, and developing a high-level framework and action plan. Many organizations form a cross-functional task force to help achieve these goals. This stage typically includes the following activities:

- Reviewing regulatory requirements and industry standards
- Providing risk briefings to board members and executives
- Forming or assigning an ERM functional team.
- Establishing a committee in line with NIA's standards.
- Benchmarking against other companies
- Assessing current risk management practices
- Defining the ERM vision, scope, and plan
- Developing an ERM framework, including a risk taxonomy

Stage 2: Preliminary Development

In Stage 2, the ERM program is just getting started. The primary objectives are to formalize roles and responsibilities within an ERM policy, identify key risks through risk assessments, and provide risk education to enhance awareness. This stage includes activities such as:

- Creating an ERM policy that defines roles and responsibilities
- Conducting annual risk assessments across business units
- Coordinating risk identification and controls among risk, audit, and compliance teams
- Offering risk education for the board and training for employees
- Setting up risk functions within business units

Developing the ERM policy is a critical step, as it lays the foundation for advancing through the ERM maturity model. A standard ERM policy typically includes:

- **Executive Summary** – Outlines the purpose, scope, and goals of ERM
- **Risk Philosophy** – Describes the company's approach and guiding principles
- **Governance Structure** – Defines roles, responsibilities, and board/management committees
- **Risk Tolerance** – States the organization's risk appetite and limits for key exposures

- **ERM Framework** – Summarizes the overall risk management process and requirements
- **Risk Categories** – Provides a standard list of risk types and definitions

Setting risk tolerance levels can be challenging. Organizations may use judgment, financial ratios (like a percentage of quarterly earnings or capital), or **advanced models** such as VaR or economic capital. Regardless of the method, tolerances must meet regulatory standards. Benchmarking against peers can also offer helpful insights.

Stage 3: Standard Practice

In Stage 3, the organization focuses on performing more frequent and detailed risk analyses. The main goals are to conduct risk assessments more often and to develop ways to quantify risk. This stage involves:

- Updating risk assessments quarterly or monthly
- Creating risk databases, including information on past losses
- Developing Key Risk Indicators (KRIs) and reporting on company-wide risks monthly
- Combining material risk models and building operational risk models
- Developing risk-adjusted performance measurement methodologies

Stage 4: Business Integration

In Stage 4, the primary goal is to embed Enterprise Risk Management (ERM) directly into the company's daily operations and management processes. This means ERM tools and practices become more widely used across the organization. At this point, the trade-offs between risk and potential returns are more clearly considered in business decisions.

Key objectives for this stage include:

- Quantifying the cost of risk to support pricing and risk transfer decisions
- Assessing business risks up front as part of business and product development
- Developing automated risk reporting and escalation technologies
- Linking risk and compensation

Implementing Stage 4 usually takes two to four years. The actual time can vary based on an organization's existing **risk culture**, how clearly its **objectives** are defined, and other relevant factors. During this stage, organizations will focus on:

- Expanding the scope of ERM to include business risk
- Allocating economic capital to underlying market, credit, operational, and business risks
- Incorporating the cost of risk into product and relationship pricing, as well as portfolio management and risk transfer strategies
- Integrating risk reviews into new business and product approval processes

- Automating ERM reporting through the use of electronic dashboards, including customized queries and real-time escalations
- Establishing trigger points to make timely business decisions, including risk mitigation and exit strategies
- Developing feedback loops on risk management performance

Stage 5: Business Optimization

At this highest maturity stage, ERM is leveraged to optimize business performance and strengthen relationships with key stakeholders. Key objectives in Stage 5 include:

- Integrating ERM into strategy development and execution
- Maximizing organization value by optimizing risk-adjusted profitability
- Providing risk transparency to key stakeholders
- Helping customers manage their risks

This advanced stage focuses on ongoing efforts, including:

- Expanding the scope of ERM to include strategic risk
- Integrating ERM into strategic planning processes
- Maximizing business value by strategically allocating resources
- Providing risk transparency to key stakeholders with respect to current risk exposures and future risk drivers

Depending on the organization's structure and risk culture, the ERM maturity model can be adapted to combine Stages 3 and 4 into a consolidated 4-stage framework. During implementation, organizations may encounter several key challenges:

1. Limited modeling skills and resources require specialized expertise, but most organizations have insufficient in-house capability to effectively use or implement these tools.
2. Validation of such risk modeling will be challenging, as it requires robust governance, regular testing, and expert oversight to ensure accuracy, reliability, and alignment with evolving business risks.
3. Identifying reliable sources to quantify operational and reputational risks in support of sound decision-making.

References

Beasley, M., Branson, B., & Pagach, D. (2015, May-June). An analysis of the maturity and strategic impact of investments in ERM. Journal of Accounting and Public Policy, 34(3), 219-243. doi:https://doi.org/10.1016/j.jaccpubpol.2015.01.001

IAA, S. S. (2010). Note on the use of internal models for risk and capital management purposes by insurers. International Actuarial Association. Retrieved from https://actuaries.org/app/uploads/2025/04/Internal_Models_EN.pdf

Lam, J. (2014). Enterprise risk management: From incentives to controls. (2nd, Ed.) John Wiley & Sons.

Sheedy, E., & Canestrari-Soh, D. (2023, March 30). Does executive accountability enhance risk management and risk culture? Accounting & Finance, 63(4), 4093-4124. Wiley Online Library. doi:https://doi.org/10.1111/acfi.13087

Zhao, X., Hwang, B.-G., & Low, S. (2013, March 1). Developing a Fuzzy Enterprise Risk Management Maturity Model for Construction Firm. Journal of Construction Engineering and Management, 139(9), 1179-1189. doi:https://doi.org/10.1061/(ASCE)CO.1943-7862.0000712