Enterprise Risk Management Components

By John Thackeray

This paper gives a summary of all the key elements that make up Enterprise Risk Management and its integration in key organizational business activities.

Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization to minimize the effects of risk on an organization's capital and earnings, reputation and shareholder value. The benefit of ERM is that it aligns organization, people, processes and infrastructure, provides a benchmark for risk/reward, aids risk visibility to operational activities and for the more mature benefit, a competitive advantage. When ERM is sound business management if it becomes an integral part of the organization's DNA. Integration of ERM can occur in the following management activities a) Strategic planning; b) Budgeting; c) Quality control d) Scenario planning; e) Corporate governance; and f) Risk disclosures.

1.BUSINESS OBJECTIVES AND STRATEGY

Risk management must function in the context of business strategy and the first step in this integration is for the organization to determine its goals and objectives. Typical organizational strategic objectives would include market share, earnings stability/growth, investor returns, regulatory standing and capital conservation. From there, the institution assesses the risk implied in that strategy implementation and determines the level of risk, it is willing to assume in executing that strategy, given its internal risk capacity, existing risk profile, vision, mission and capability. Regardless of a specific business strategy, an institution is exposed to the following financial, strategic and operational risks:

- Credit/Market/Operational
- Liquidity
- Technology
- Strategic/Reputation/Business
- Compliance/Legal/Regulatory
- Insurance/Environmental
- Capital

The COSO definition of ERM states that ERM is part of strategy setting. ERM and strategy setting should be viewed as complementing each other and forming the basis for a strategy-risk-focused organization. When formulating the company's strategy, management analyzes its strategic alternatives and identifies events that could threaten their achievement. Strategy formulation is enhanced by ERM because risks are identified, and the strategic alternatives are assessed given the company's risk appetite.

2. RISK APPETITE

Risk direction is defined by the risk appetite which in turn is defined as “the amount of risk (volatility of expected results) an organization is willing to accept in pursuit of a desired financial performance (returns).” A risk appetite statement is the critical link that combines strategy setting, business plans, capital and risk. It reflects the entity’s risk management philosophy and influences the culture and operating style. Considerations affecting the risk appetite, include the following: existing risk profile, attitudes towards risk, risk capacity and risk tolerances. The risk appetite statement is developed by management with Board review and is translated into a written form. The overall risk appetite uses broad risk statements and then is expressed for each major class of organizational objective and for the different categories of risk. An effective risk appetite statement needs to be stated precisely enough so it can be communicated, operationalized and aid decision making. More importantly It needs to be broken down into specific operating metrics so that it can be monitored. The risk appetite is converted into operating/tactical metrics known as risk tolerances which reflect the application of risk appetite to specific objectives. and then the risk tolerances are further distilled into risk thresholds. The key here is moving from a low measurement of quantification i.e. risk appetite to a high measure of granularity i.e. a threshold. The risk appetite is converted into Enterprise High-level KPI’s (Key Performance Indicators) which are defined, acceptable and operationalized, with risk appetite and tolerances established for capital, earnings, credit worthiness, reputation and shareholder returns. Once the risk appetite is set, it needs to be embedded, and then continuously monitored and revised. As strategies and objectives change, it should provide a further discussion of risk appetite.

3. CULTURE, GOVERNANCE, AND POLICIES

The statement of risk appetite is conveyed through culture, governance and policies. These three factors help an organization manage and oversee its risk-taking activities. A strong risk culture set from the top, augmented by comprehensively laid out roles and responsibilities, with collective centralized decision making and clear escalation protocols is a must for successful implementation. Strong well thought out risk management principals, ownership and culture training help promote, reinforce and maintain this strong risk culture. Evidence of this strong risk culture would be seen in open communication, both top down and bottom up in decision making and resolution conflict. Enterprise means that no area of the organization is excluded, it includes all operating and support area both in terms of engagement, training and support. An important instrument in this implementation is the risk management policy which sends an intent by the organization of its commitment to its risk appetite to all stakeholders. The policy states its purpose, application, objectives and policy components including the risk management framework. The policy must be written in a common terminology as this will facilitate clear communication with all stakeholders. ERM ties in closely with corporate governance because it: a) Improves information flows between the company

and the board regarding risks; • b) Enhances discussions of strategy and the related risks between executives and the board; c) Identifies acceptable levels of risks to be taken and assumed; d) Focuses management on the risks identified; and e) Improves disclosures to stakeholders about risks taken and risks yet to be managed.

4. RISK DATA AND DELIVERY

It's all about the data but more importantly the correct data. The risk data and delivery must be robust and scalable so that the information collected, integrated, analyzed, can be translated into cohesive, credible narrative, reports and risk disclosures. Increasingly companies are disclosing more information about the risks and with that, the ERM process could be a valuable source for gathering and reporting the potential implications of this risk information. SEC registrants must disclose risk factors in their annual reports, as specified in Item 503(c) of Regulation S-K, 3 which instructs registrants to present risks that are specific to the company. Furthermore, Form 10-K instructions require registrants to discuss risk factors in "plain English." Good solid governance principals would include

a) Forward looking language assessing the potential effect of the risk to the company Examples would be tax policies affecting profitability and/or corporate expansion plans.

b) References to company efforts to manage or mitigate the risk — Examples include company strategies to address cybersecurity, and policies, practices and training to mitigate culture risk. (employee compliance-related).

c) Language describing risk-related trends and developments Examples includes changes in the likelihood, nature or severity of the risk affecting the company, such as changes in the global competitive landscape, trends in asset allocation and technological changes that affect a company's business model.

d) Level of detail provided in the risk factor disclosure — Examples references to operating units, markets, products, specific individuals, and company-specific developments such as operational improvement programs and restructuring efforts.

5. INTERNAL CONTROL ENVIRONMENT

The internal control environment is one of the most important tools helping senior management reduce the level of inherent risk to an acceptable level known as Residual risk. Residual risk is defined as the level of inherent risks reduced by internal controls. Building an effective internal control environment allows management to control what can be controlled. The system of internal controls incorporates culture, governance, controls, and scenario planning. The system of internal controls can be further supplemented by risk management techniques such as Strategies, Policies, Limits, Guidelines Process, Standards, Diversification and Model measurement. Quality initiatives focus on improving the efficiency and effectiveness of detailed processes. ERM requires clarity of objectives at all levels of the enterprise, and the objectives of specific processes can be addressed by utilizing quality tools and methodologies.

Information can be evaluated within the larger context of the enterprise to identify risks in an ERM implementation, leading to better internal controls. Stronger internal controls can lead to improved stability, reaction time, and increased shareholder value. Furthermore, a risk-based ERM approach can help reduce the number of key controls that companies are testing and documenting, significantly lowering the cost of compliance.

6. MEASUREMENT AND EVALUATION

Measurement and evaluation determines which risks are significant, both individually and collectively and where to invest time, energy, and effort in response. Various risk management techniques and tools will be used to measure and quantify the risks on both an aggregate and portfolio level. In my experience, the most important tool is an open mind, 80% of the material risks based on my experience are strategic and or operational, removing risk bias is essential. To accomplish the goal of measurement and evaluation, an organization may adopt a risk impact rating based on a simple model of color rating (green, yellow, and red), number 1, 2, 3 or high/medium and low scales. In The next stage is for Risk mitigation plans to be put into place to address those areas which pose the greatest threat. The internal controls will be measured and evaluated to determine how well the risks are being managed and whether the risk response is both appropriate and effective. All risks, responses and control effectiveness must be reported and communicated in a format to meet the different stakeholders and oversight/governance bodies. The oversight/governance bodies will be tasked with ensuring that the risk profile is aligning to business and capital plans and that the amount of capital is commensurate with the risk taking. This alignment should be seen in the budgeting process described below. A company’s budget reflects the current-year financial commitment to achieve the organization’s long-term strategy. The annual budget can be integrated with ERM to provide insights on what the strategic leadership sees as the threats, to meeting its financial plan. A risk map presented with the budget provides information to senior management on what the major threats are to meet the financial plan for the year, allowing comparison at both the business and enterprise wide level. Responses could include understanding to what extent the cost of mitigating or accepting a risk has been built into the price of the product or service.

7. SCENARIO PLANNING AND STRESS TESTING

Given that management must address known and unknown risks, tools like scenario planning and stress testing are used both to help shed light on these missing risks and more importantly the interconnection of these risks. Armed with this information, the organization can develop contingency plans too at least counter the effects on the future operational viability and trend/model of these risks. Passing Thoughts Enterprise Risk Management is not a passing fad as it is now instrumental to the survival of an organization. Its importance is both in the maturity of the thinking and the structured planning allowing the organization to navigate with some certainty the risks posed to the

organizations business objectives and strategy. In short, Enterprise Risk Management is good business practice.

John Thackeray is the founder and CEO of RiskSmartInc, https://risksmartinc.com, a consulting firm that specializes in the writing of risk documentation. Over his long career, he has held many risk positions, where he interacted and engaged with US and European regulators. He frequently contributes articles on his risk insights to the Financial Executives Networking Group (FENG).