Implementation of ERM under COSO Framework

By Muhammad Mubashir Nazir, FCCA, CISA, CIA

Concern for risk management is increasing in recent years. A series of high-profile business scandals and failures in United States and other countries around the globe prompted a need for a robust framework to effectively identify, assess and manage risks. In 2001, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project, and engaged PriceWaterhouseCoopers (PWC) to develop a framework which can be used by the management of companies to evaluate their risk management function.

In the foreword of "**Enterprise Risk Management – Integrated Framework**" issued by COSO, the framework is introduced as follows:

> "This Enterprise Risk Management – Integrated Framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.
>
> Among the most critical challenges for managements is determining how much risk the entity is prepared to and does accept as it strives to create value. This report will better enable them to meet this challenge."[1]

ERM is defined by COSO as "a process, affected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity goals."[2]

All business organizations focus on maximizing their shareholder value. Uncertainty is a threat to this objective. It is a great challenge for the management to determine different aspects of uncertainty and effectively manage the risk.

COSO explains the ERM in three dimensions which are depicted in Figure I:

- Organization's objectives (from ERM perspective)
- Components of ERM
- Levels of Business Organization

The goal of ERM Framework is to help the organization achieve its objectives. The horizontal dimension divides the organization's objectives into four types:

- **Strategic:** High-level goals of an organization which support it in achieving its mission e.g. acquisition of another company, launching a new product, installing a new factory etc.
- **Operations:** Effective and efficient use of its resources e.g. delivering the product to the customer at the right time, effectively marketing the product, financing at reasonable rates, arranging human resources etc.

- **Reporting:** Reliability of reporting e.g. preparation of financial reports in a reliable manner, environmental reporting, compliance reporting etc.
- **Compliance:** Compliance with applicable laws and regulations e.g. company law, tax law, securities and exchange laws, environmental regulations etc.

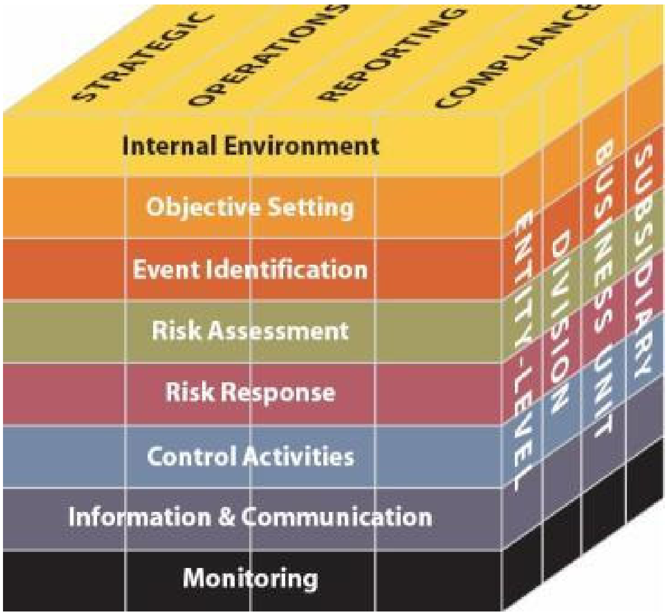


Figure I: COSO Framework for Risk Management

These four categories if organization's objectives expose the organization to certain risks. Strategic risks include competitors entry, increase in intensity of competition, technological developments in the industry, adverse legislation, changes in demographics and social structure of the society which may have an adverse impact on the organization. Operational risks include supply chain problems, employee fraud, production breakdowns, physical safety and security etc. Some authors include natural hazards e.g. hurricanes, earthquakes etc. also in operational risk.

Recent developments in regulatory framework in aftermath of high-profile business scandals like Enron and World Com has posed the organization to reporting and compliance risks. Among the outgrowths in the United States is the Sarbanes Oxley Act of 2002, and similar legislation has been enacted or is being considered in other countries. Sarbanes Oxley Act has imposed significant penalties on non compliance of various sections. Certain reporting requirements are imposed on the companies in order to provide reliable information to the investors. These developments have exposed the organizations to reporting and compliance risks. A dimension of these risks is called "Information Risk" which is the risk of incorrect information available in company's information systems. Unauthorized access to confidential information, malicious attacks on information systems, unavailability of required information and the loss of claims and lawsuits by the parties whom confidential information is disclosed, are different risks which are classified under information risk.

The third dimension of the COSO Framework depicts the level of implementation of ERM. ERM can be implemented at the level of a business unit, division, subsidiary or entire organization. The vertical dimension describes the components of ERM as discussed in rest of this article.

ERM consists of eight interrelated components as depicted on vertical dimension of ERM Framework. These are derived from the way management runs and enterprise and are integrated with the management process of the business. These components are:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communication
- Monitoring

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another. In this article, we will discuss these components of ERM from the perspective of an ERM implementer.

Internal Environment

The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.[3]

The Casualty Actuarial Society describes this process as the first step in ERM Process. According to their ERM Framework, it is described as "Establishing Context".[4] This step includes the following areas:

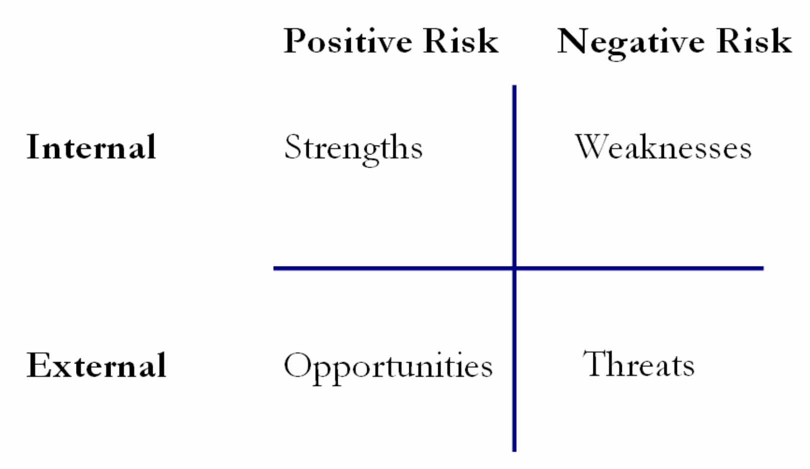
- Define the relationship of organization with its external and internal environment
- Perform SWOT Analysis
- Identify stakeholders
- Understand organization's objectives and strategies
- Identify Key Performance Indicators (KPIs)
- Identify relevant key risk categories
- Identify existing risk management practices
- Determine the "Risk Appetite" of management
- Determine Integrity and Ethical Values of the organization

Relationship of an organization with its internal and external environment

Relationship of an organization can be defined with its external environment by identifying the political, legal, sociological, economic and technological factors which can affect the organization. Factors in immediate environment of the organization are suppliers, customers, competitors, intermediaries, trade organizations and all those parties directly related with a company. Internal factors include the management, employees, financing methods, marketing techniques, information systems and company's internal processes.

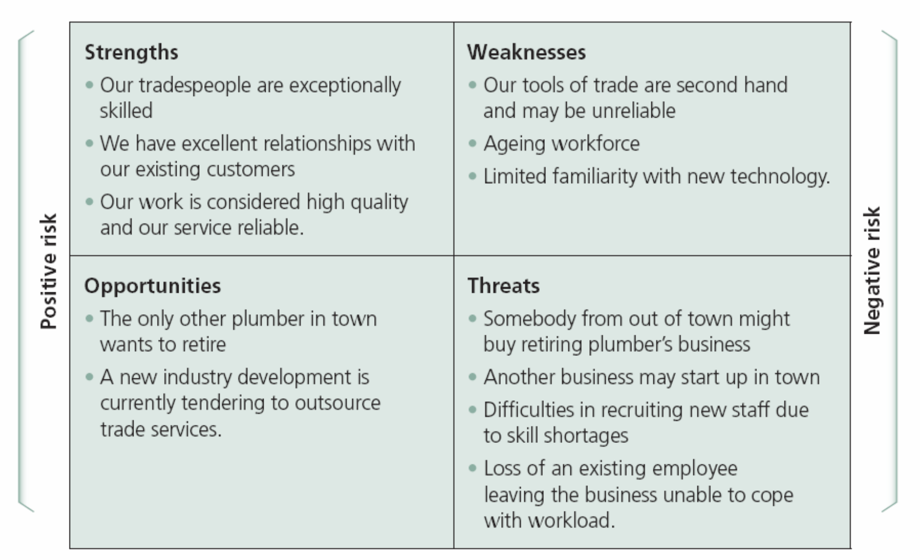
SWOT Analysis

SWOT Analysis includes the analyzing the strengths and weaknesses of, and opportunities and threats to the organization. Although this analysis is also performed in strategic planning process but in ERM, it is performed from the perspective of risk management. Figure II depicts the SWOT Analysis whereas Figure III provides an example of SWOT Analysis.



	Positive Risk	Negative Risk
Internal	Strengths	Weaknesses
External	Opportunities	Threats

Figure II: SWOT Analysis



Positive risk	**Strengths** • Our tradespeople are exceptionally skilled • We have excellent relationships with our existing customers • Our work is considered high quality and our service reliable.	**Weaknesses** • Our tools of trade are second hand and may be unreliable • Ageing workforce • Limited familiarity with new technology.	Negative risk
	Opportunities • The only other plumber in town wants to retire • A new industry development is currently tendering to outsource trade services.	**Threats** • Somebody from out of town might buy retiring plumber's business • Another business may start up in town • Difficulties in recruiting new staff due to skill shortages • Loss of an existing employee leaving the business unable to cope with workload.	

Figure III: An example for SWOT Analysis for a plumbing company.[5]

Stakeholders Analysis

Stakeholders are defined as the parties interested in the business and activities of the company. They include:

- Shareholders
- Potential Investors

- Management
- Employees
- Creditors / Bankers
- Government
- General Public
- Competitors

Requirements of all stakeholder groups with respect to risk management will be identified at this stage.

Understand organization’s objectives and key strategies

Vision Statement, Mission Statement and key strategic planning documents will be reviewed in order to understand the organization’s objectives and key strategies related to marketing, operations, finance, human resources and information systems.

Identify Key Performance Indicators (KPIs)

KPIs are used by organizations to measure their performance in different areas. Examples of KPIs include the following:

- Return on Capital Employed
- Net Profit of each division
- Customer Satisfaction Index
- % of Sales Returns
- Current Ratio
- Financial and Operating Leverage
- HR Training Hours

KPIs are identified in the ERM process because in latter stages, impact of each risk on KPIs will be measured.

Identify relevant risk categories

At this step, the risk categories relevant to the organization are identified. Following risk categories are common to all organizations:

- **Natural hazards** e.g. fire, earthquakes, hurricanes etc.
- **Man-made hazards** e.g. wars, terrorism
- **Financial risk** e.g. credit risk, liquidity risk, bankruptcy risk, adverse movement in exchange rates, interest rates, prices, costs etc.
- **Operational risk** e.g. production breakdowns, supply chain issues, distribution issues, product quality problems, physical safety and security etc.
- **Strategic risk** e.g. fluctuations in demand, technological advances, economic cycles, adverse legislation etc.
- **Information risk** e.g. incorrect information, access to confidential information by unauthorized persons, cyber crime, malicious attacks
- **Compliance risk** e.g. penalties and fines due to non-compliance, law suits, reputation losses, losing patents etc.

Some risk categories will be more important for one organization while other risk categories will be more important for other ones. For example, liquidity and credit risk are the most important ones for a bank whereas fire risk is the most important risk for an oil refinery.

Identify existing risk management practices

Even before implementation of ERM, organizations manage their risks. In most of cases, it is managed by individual department in silos without an integrated framework. Credit Department may be managing the credit risk whereas Finance Department may be managing the exchange rate and liquidity risks. Objective of identifying the existing practices is to integrate them into a centralized risk management function.

Determine the Risk Appetite of the Management

Risk Appetite of the organization management is dependent on two elements i.e. risk preferences and risk affordability. Some executives accept risk at high level whereas some executives do accept risks. Risk appetite will be a major determinant in selecting risk response strategies.

Determine the Integrity & Ethical Values of the Organization

Organization's ethical climate is directly related to managing risks. Organizations having weak ethical and integrity values are exposed to a large number of risks like employee frauds, legal penalties and lawsuits.

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.[6]

Event Identification

Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.[7]

As discussed above, common risk categories for an organization include natural- and man-made hazards, financial risk, operational risk, strategic risk, information risk and compliance risk. All risks related to each category must be identified during the process of event identification. Risks can be identified by following methods:

- Perform brainstorming sessions
- Perform risk surveys
- Conduct risk workshops
- Review and discuss internal audit reports
- Review and discuss reports of other assurance groups e.g. health & safety, quality assurance, security management etc

A detailed list of risks will be developed as a result of this process. Relationships between risks can be depicted in the form of the risk universe.

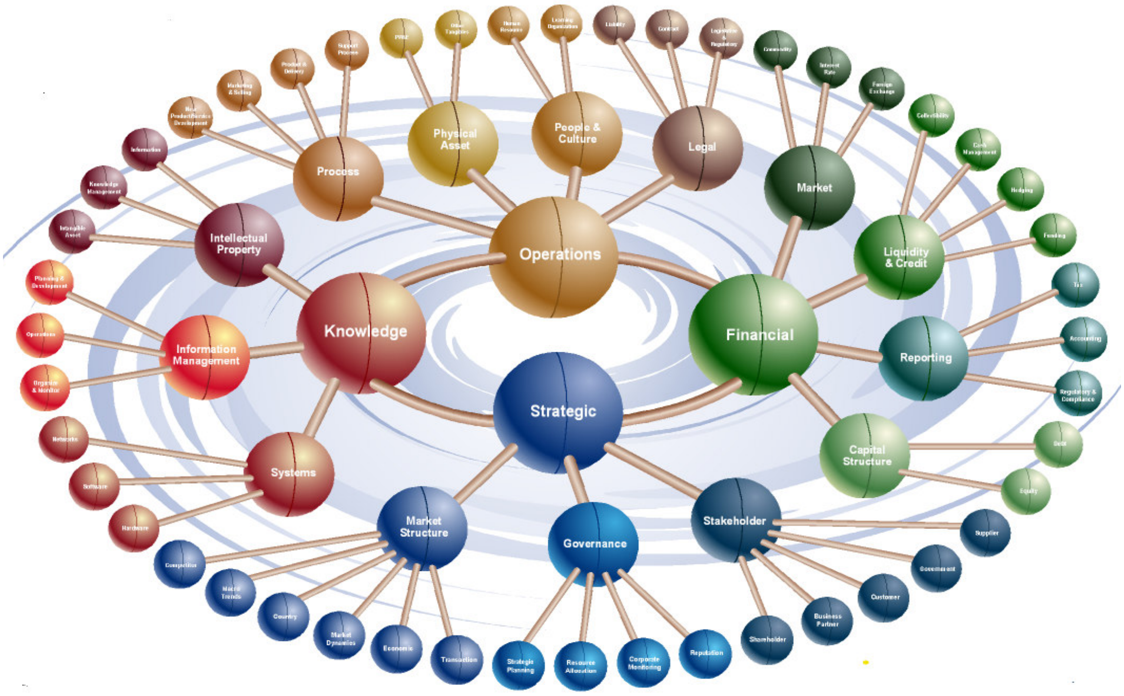


Figure IV: The Risk Universe[8]

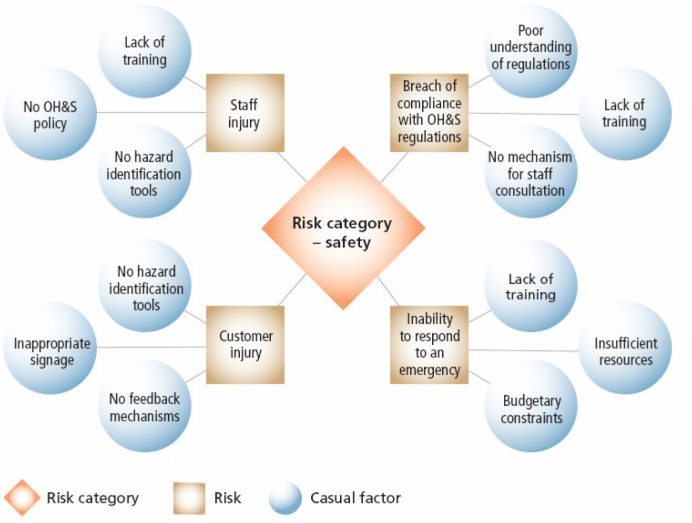
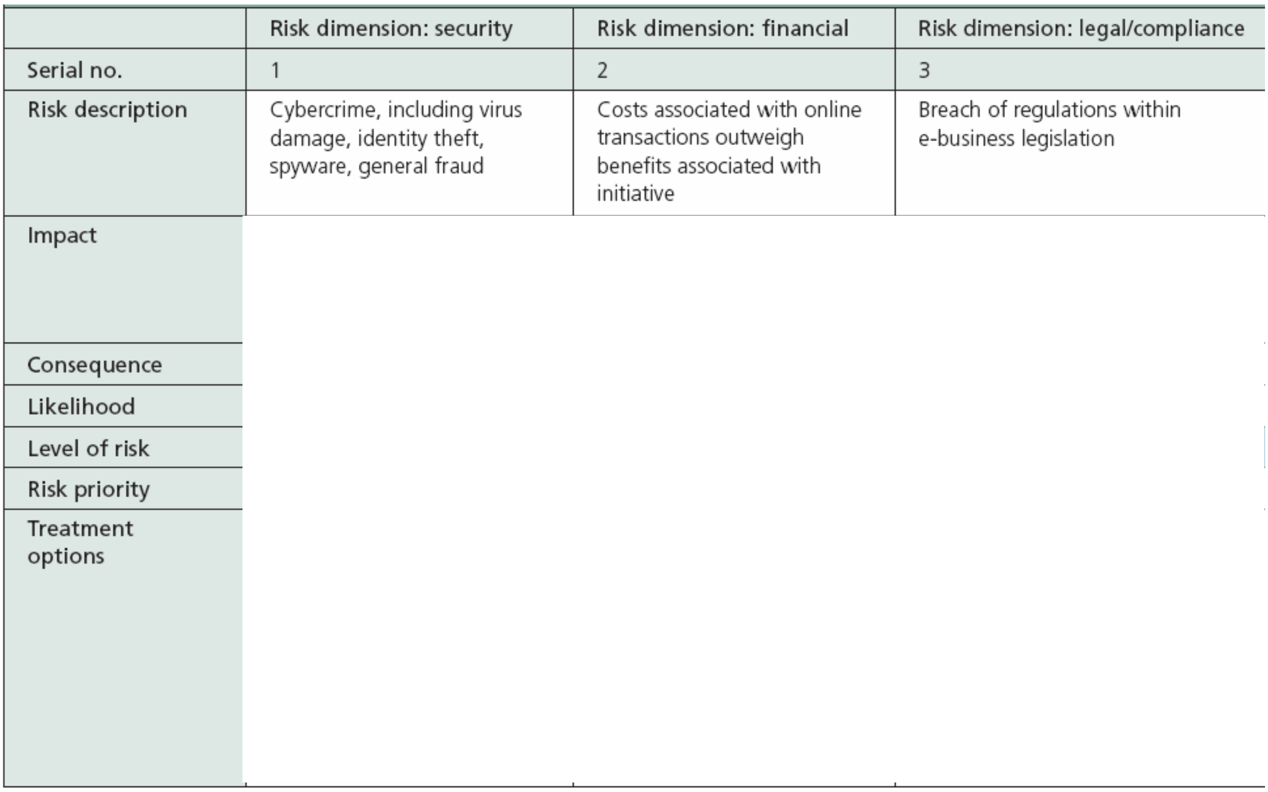


Figure V: Developing the Risk Universe



	Risk dimension: security	Risk dimension: financial	Risk dimension: legal/compliance
Serial no.	1	2	3
Risk description	Cybercrime, including virus damage, identity theft, spyware, general fraud	Costs associated with online transactions outweigh benefits associated with initiative	Breach of regulations within e-business legislation
Impact			
Consequence			
Likelihood			
Level of risk			
Risk priority			
Treatment options			

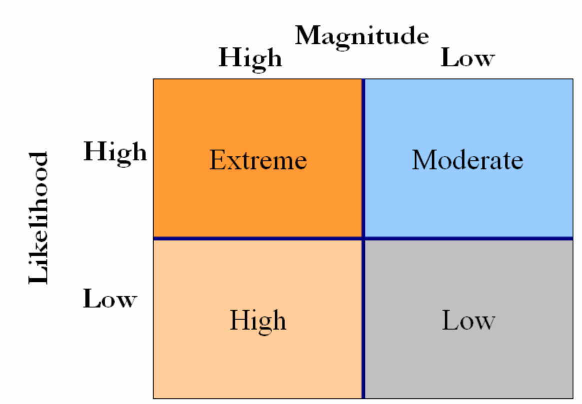
Figure VI: Initial Risk Register

As described above, product of Events Identification Process will be the initial risk register which will be completed in next stages of ERM Implementation Process.

Risk Assessment

Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.[9]

Risk is the product of likelihood and magnitude (impact). Risk Assessment is the process of determination of likelihood and impact after identification of risk events. After calculating these two elements of risk, overall risk rating will be determined as Figure VII.



		Magnitude	
		High	Low
Likelihood	High	Extreme	Moderate
	Low	High	Low

Figure VII: Risk Assessment Matrix

Various tools can be used to determine the impact of the risk e.g. Qualitative Risk Analysis, Fault Tree Analysis, Maximum Loss Estimation etc. To determine likelihood, probability distribution tables are used.

In most of the companies, qualitative risk analysis is used for determining impact and likelihood. After assessing the risk, it is essential to develop "Risk & Control Matrix" to map the existing internal controls with the risks. Risks will be prioritized according to their overall risk rating as depicted in Figure VIII.

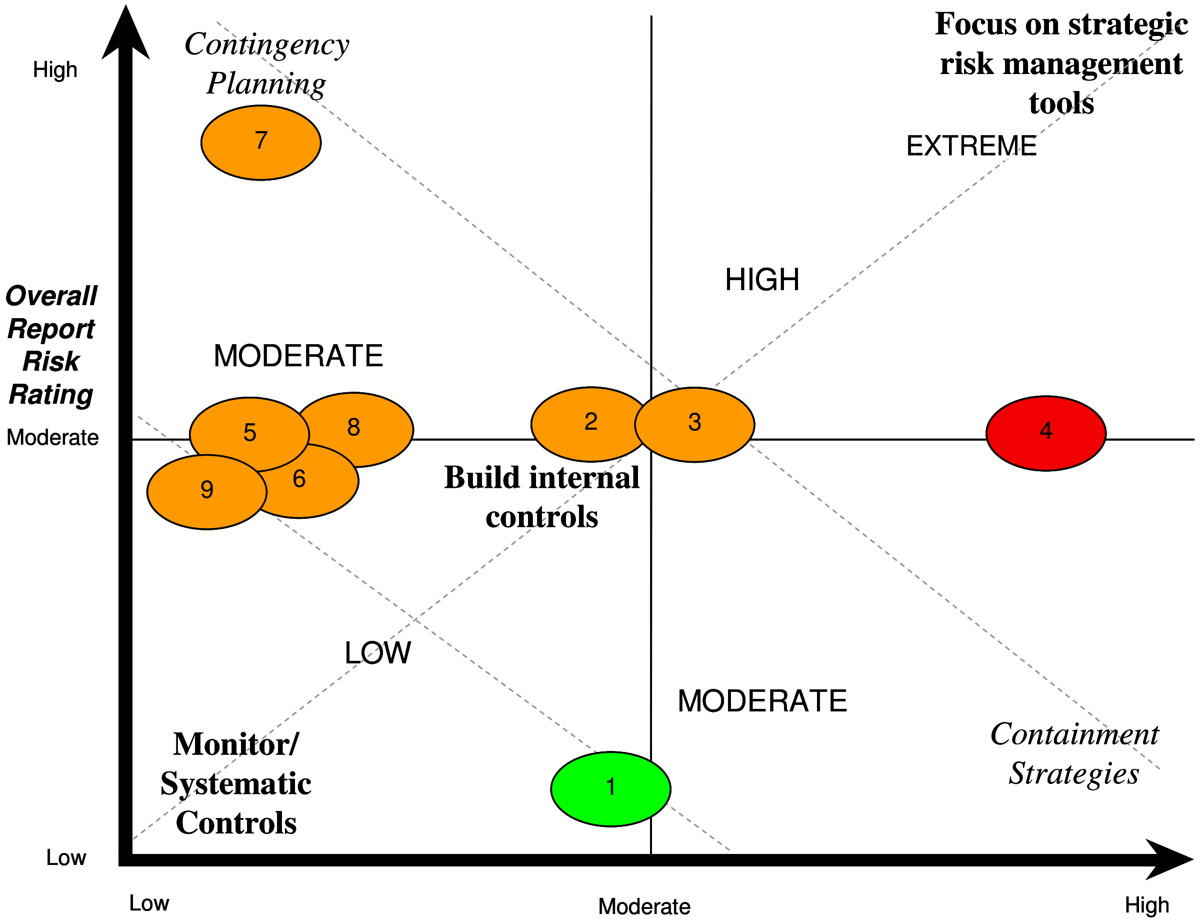


Figure VIII: Risk Prioritization

Risk Response

Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.[10] These strategies are described in Figure IX.

Some risks can be avoided. For example, risk of cash theft can be avoided by simply not dealing in cash. Risk of malicious attacks from the internet can be avoided by disconnecting the company's network from the internet.

All risks cannot be avoided. Some risks can be transferred to or shared with other parties. For example, risk for fire, theft and health can be transferred to insurance companies. Risk of doubtful debts can be transferred to a factoring company. With avoidance and transfer, overall exposure of the company can be reduced. Other risks can be mitigated by implementing internal and external controls. The risks that cannot be mitigated will be accepted by the management. These accepted risks are also called "Residual Risk".

The company must perform cost-benefit analysis of each risk strategy and select the ideal strategy for each risk.

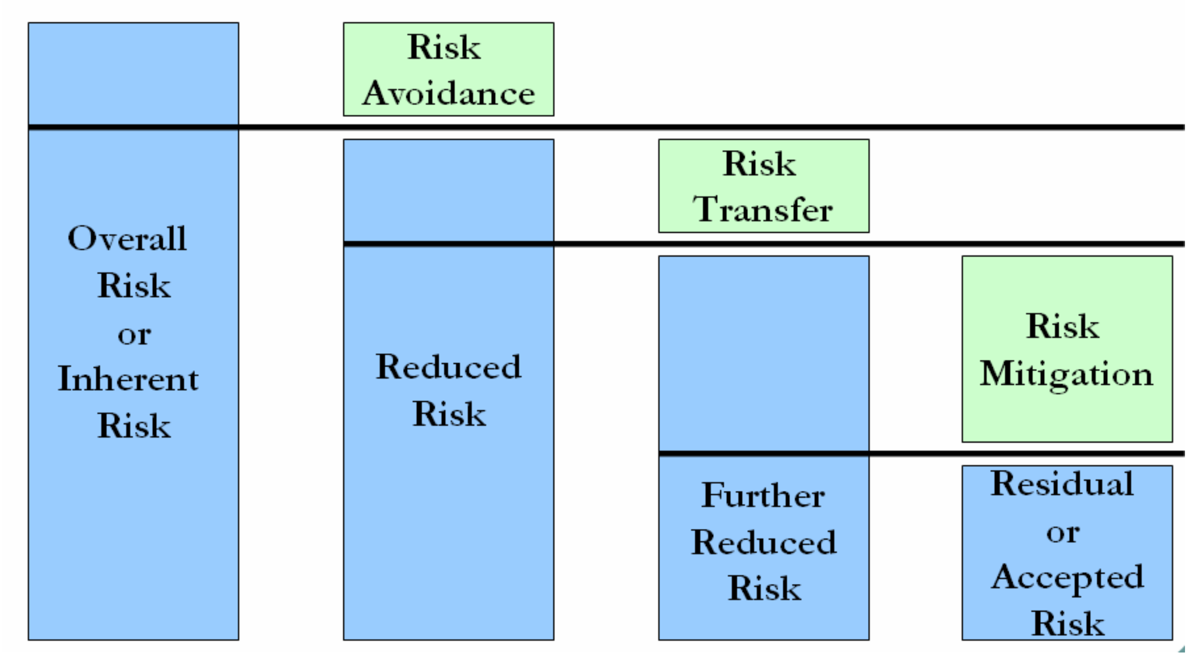
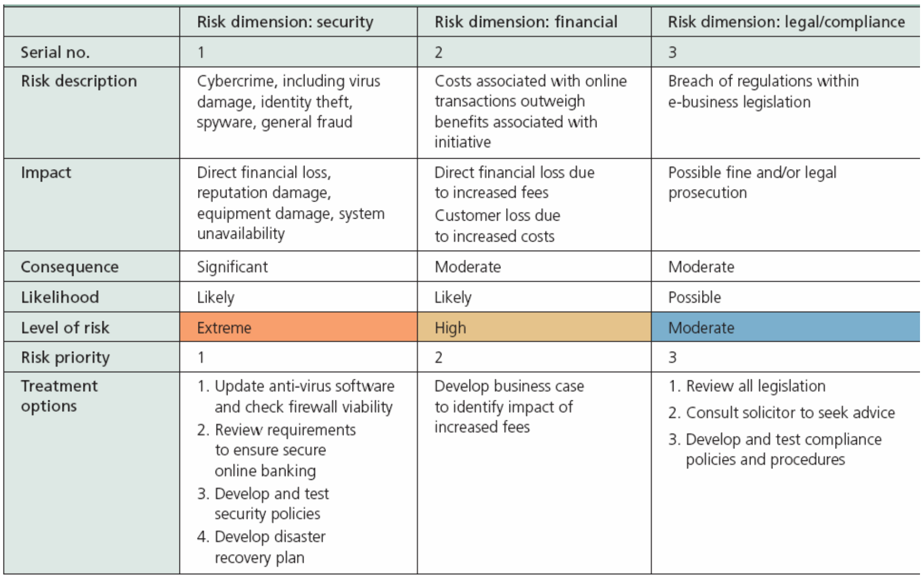


Figure IX: Risk Treatment

At this stage, risk register of the company will be complete as depicted in Figure X. This register will be used as a tool to track and monitor the company controls.



	Risk dimension: security	Risk dimension: financial	Risk dimension: legal/compliance
Serial no.	1	2	3
Risk description	Cybercrime, including virus damage, identity theft, spyware, general fraud	Costs associated with online transactions outweigh benefits associated with initiative	Breach of regulations within e-business legislation
Impact	Direct financial loss, reputation damage, equipment damage, system unavailability	Direct financial loss due to increased fees Customer loss due to increased costs	Possible fine and/or legal prosecution
Consequence	Significant	Moderate	Moderate
Likelihood	Likely	Likely	Possible
Level of risk	Extreme	High	Moderate
Risk priority	1	2	3
Treatment options	1. Update anti-virus software and check firewall viability 2. Review requirements to ensure secure online banking 3. Develop and test security policies 4. Develop disaster recovery plan	Develop business case to identify impact of increased fees	1. Review all legislation 2. Consult solicitor to seek advice 3. Develop and test compliance policies and procedures

Figure X: Complete Risk Register

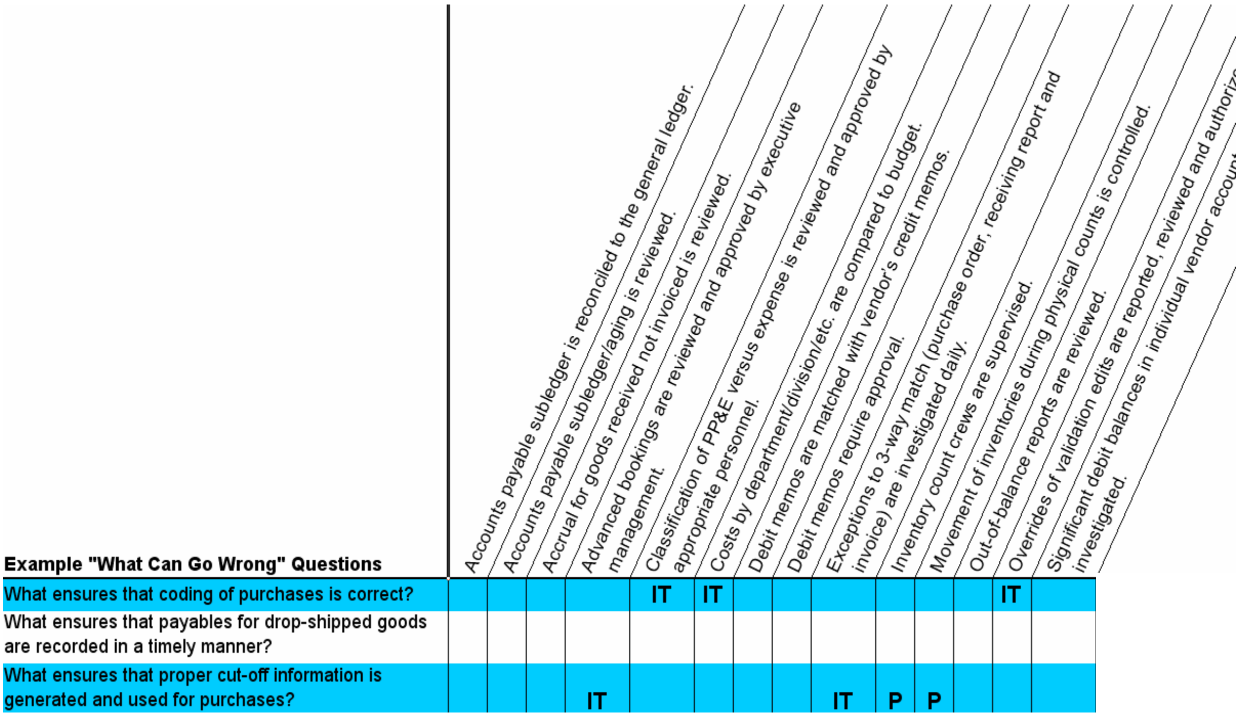
Control Activities

Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.[11] Controls can be preventive, detective, directive or deterrent. Controls can be exercised manually or through computer systems. A few examples of control activities are as follows:

- Credit policies and credit authorizations by appropriate level of authority are preventive controls for credit risk.

- Marketing research is a detective control for risks related to market e.g. entry of a new competitor.
- Workflow management is an automatic preventive and detective control for authorization of transactions mitigating the risks of errors and frauds in routine business transactions.
- Three-way matching of invoice, purchase order and goods receiving note (GRN) is a preventive control to the operational risk of receipt of and payment for unwanted goods.
- Review of activity logs is a detective control to mitigate the risk of unauthorized / incorrect transactions performed in computer systems.
- Planning an activity is a directive control to mitigate the operational risks.
- Penalties and fines are deterrent controls to mitigate the risk of fraud.

The company must develop "Risk & Control Matrix" to map all the risks with relevant controls as shown in Figure XI. This matrix should be regularly updated and reviewed.



Example "What Can Go Wrong" Questions	Accounts payable subledger is reconciled to the general ledger.	Accounts payable subledger/aging is reviewed.	Accrual for goods received not invoiced is reviewed.	Advanced bookings are reviewed and approved by executive management.	Classification of PP&E versus expense is reviewed and approved by appropriate personnel.	Costs by department/division/etc. are compared to budget.	Debit memos are matched with vendor's credit memos.	Debit memos require approval.	Exceptions to 3-way match (purchase order, receiving report and invoice) are investigated daily.	Inventory count crews are supervised.	Movement of inventories during physical counts is controlled.	Out-of-balance reports are reviewed.	Overrides of validation edits are reported, reviewed and authoriz	Significant debit balances in individual vendor accoun investigated.
What ensures that coding of purchases is correct?					IT	IT							IT	
What ensures that payables for drop-shipped goods are recorded in a timely manner?														
What ensures that proper cut-off information is generated and used for purchases?				IT					IT	P	P			

Figure XI: Risk & Control Matrix

Information and Communication

Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.[12] Information about the risks can be disseminated in a number of ways e.g. risk reports, internal audit reports, newsletters, notice boards, electronic mail, internet and intranet websites etc.

Monitoring

The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.[13] Tools for monitoring risks include the following:

- Key Risk Indicators (KRIs)
- Risk Governance, Policies & Procedures
- Establishing the Risk Management Department
- Risk Register
- Risk Reporting
- Internal Audit

Key Risk Indicators

A large number of KRIs and Risk Scorecards can be developed to monitor different types of risks. A few examples are as follows:

- Market share (for market risk)
- Number of direct competitors (for market risk)
- Loss caused by frauds during the period (for fraud risk)
- Total exposure to foreign exchange risk (for exchange rate risk)
- Number of significant internal control weaknesses reported (for operational risk)
- % of price fluctuation (for price risk)
- Bad debts written off (for credit risk)
- Avoidable losses during the period (for all risks)
- Number of cyber attacks (for information risk)

Success of an ERM Implementation Project

An ERM Implementation project will help a company in reducing losses, enhancing business processes, improving reputation, enhancing control over the business, reducing penalties and securing information. On the basis of my experience of ERM Implementation projects, following factors are essential for the success of an ERM Implementation.

- **Agreed risk strategy:** The audit committee and management must provide guidance on the appropriate strategy and approach to risk management aligned to the organizational structure.

- **Clear governance framework:** The audit committee will usually delegate day-to-day governance through an oversight structure that includes a Chief Risk Officer.

- **Efficient risk management processes:** The organization needs firm procedures for assessing and continuously monitoring risks on an enterprise wide basis.

- **Appropriate technology:** Effective systems providing access to information about risk identification, assessment and solutions to support the risk management process.

- **Co-ordination of risk management functions:** Integrated risk functions embedded within the business to leverage expertise across the entire organization.

- **The right culture and capability:** Everyone in organization must be attuned to the risk culture and performance measurements must be risk based.

[1] COSO, Enterprise Risk Management, Integrated Framework, Executive Summary, P V
[2] Ibid, P 2
[3] Ibid, P 3
[4] Casualty Actuarial Society, ERM Committee, Overview of ERM Process", P 8, May 2003
[5] NSW Department of State and Regional Development, Risk Management for Small Businesses, P 52
[6] COSO, Enterprise Risk Management, Integrated Framework, Executive Summary, P 3
[7] Ibid, P 4
[8] Ernst & Young, Developing the Risk Universe
[9] COSO, Enterprise Risk Management, Integrated Framework, Executive Summary, P 4
[10] Ibid, P 4
[11] Ibid, P 4
[12] Ibid, P 4
[13] Ibid, P 4