CHAPTER 4

EVALUATION OF RISK MANAGEMENT STRATEGIES

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Risk Management Strategy alignment with Business Strategy
- Internal Control environment and linkages with Risk Management
- Risk Culture and attitudes to Risk Management
- Integrated Risk Reporting and Stakeholder responsibilities
- IT Risk Management – Disaster Recovery

1. RISK MANAGEMENT STRATEGY ALIGNMENT WITH BUSINESS STRATEGY

Primary goals and objectives of successful businesses are to make profits in an ethical and fair manner, fulfill social responsibilities, tax obligations and sustain the business for a longer duration. Organizations may have short, medium- and long-term strategic objectives. Business strategies are crafted keeping in mind the risk and opportunities, competitive landscape, regulatory regime, consumer preferences and business differentiators to meet such goals and objectives. Enterprise Risk Management (ERM) is a tool that assists organizations in meeting its business objectives. ERM is initiated by the Board of directors in a strategic context and implemented by senior executives of the organisation. Strategic context is Strategic objectives together with the strategies to achieve them. The strategic objectives of the organisation drive the risk management objectives. One of the key strategic objective and outcome of ERM is to improve the performance of the

organisation. The term "strategic context" is relevant as it indicates alignment with business strategy. Further, as ERM deals with risk mitigation it is natural that any event that prevents an organisation from meeting its objectives would be managed effectively through an Internal Control (IC) measure designed for this purpose; thereby improving the performance of the organisation. ERM is closely linked to business strategy and performance of the organisation. ERM and IC are also inter-connected subjects that compliment each other.

Empires or Businesses that survived over 100 years practiced risk management effectively by anticipating events that could threaten their very existence. Over the years the art of anticipation has been mastered through use of smart risk management strategies that are aligned to business objectives. These smart risk management strategies have revolved around –

- Collecting signals for potential events,
- Acquiring data to learn more about such potential events,
- Detecting patterns of change in the environment and acquired data,
- Imagining event outcomes, using intuition and taking precautionary actions such as designing internal controls.

Whether it is the golden era of India or the current digital era; substance or core of risk management strategies remain the same. The primary design of any risk management strategy is focused on de-risking the organisation from sudden surprise, emerging crisis, ability to adapt to changing consumer needs, altered circumstances, rare large shock events such as natural disasters, terrorism, collapse risk of business model and insulating from a contagion risk.

Contemporary Risk management strategies that are linked to business strategy and performance outline the ERM vision on "how risks can be effectively managed" in addition to "what risks need to be managed". Further, risk management strategies focus on how to identify "Key Risk Indicators" by describing "what measures need to be tracked or monitored" for monitoring emergence of a risk factor.

For example: -

Risk Factor - Threat of a disaster at an off-shore service centre

Key Risk Indicator - Tracking the threat levels from emergency response teams/ weather bureaus

1.1 Alignment of risk with strategy

Global statistics suggest that 80% of companies suffered business losses as a result of strategic blunders. Such strategic blunders are often caused on account of inability of the businesses to learn from history or past events, lack of sufficient planning for the short and long term, ignoring customer needs, pre-mature scaling, on-boarding costly capital, etc. Entrepreneurs end up with wrong strategic choices leading to strategic blunders or business failures. On the other hand, successful Companies incorporate Enterprise Risk Management into strategy setting sessions to a large, or very large extent foster a growth and performance-oriented culture. Involves appropriate levels of management;

For example

Strategic Objective	Strategic Measure	Risk Factor	Control Measure
Flawless Operations Provide flawless implementation and operations at competitive cost	Reliability (number of faults/ unit time) Serviceability (mean time to repair)	Machine break down	Use of specified material (quality and quantity) Preventive inspection (daily) and maintenance (scheduled)

Boards and entrepreneurs should understand the Risk Profile of the "Strategic Choice" that they are making and also the "Strategy Execution Risks" involved.

For example: -

Strategic Objective	Strategic Measure	Risk Factor	Control Measure
Product development Reduce product introduction cycle time	Product development cycle time	Delay in legal clearances	Planned product filings that are comprehensive, pre-audited for accuracy and complete. Product acceptance testing by retired or ex-regulators to incorporate improvements at test stage.

Boards foster an environment of performance, outcome orientation and quick risk responses to manage emerging risk events. In emerging risk situations responses are "action oriented" rather than focused on analyzing the "reason" of occurrence. Reasons and root causes are either pre or post analyzed for preventive actions.

In order to align risk with strategy a goal alignment must exist from top to bottom. This is possible by creating education and awareness of the significance of ERM in achieving strategic objectives, open communication about strategic business objectives and events that could prevent achievement of strategic business objectives, employee empowerment towards positive contributions/ suggestions on introducing control measures that could prevent risk event occurrences and finally linking employee compensation to risk management outcomes.

To align risk to business strategies – Corporate Boards invest time and resources in ERM implementation exercises. Such exercises are a combination of top down and bottom up approach where the Boards are setting the strategic context and executive management are identifying, assessing and reporting risks. Regulators such as SEBI, RBI, IRDA in India are issuing enhanced prescriptions to companies to develop robust ERM models and prepare their organisations to address emerging challenges and opportunities. Indian companies that have evolved risk monitoring practices are using Dashboards, Business Intelligence tools and enterprise wide pictorial maps to monitor risk indicators on a real-time basis and take corrective action to prevent

crisis and resultant losses. The financial services industry in India is heading towards a risk-based supervision regime involving real-time risk monitoring through automatic data transfer to the regulator with respect to key risk indicator position for the purpose of centralised risk monitoring.

1.2 Case Example – Risk Management at core of Business Strategy – Unilever Code of Business Principles

Risk management is integral to Unilever's strategy and to the achievement of Unilever's long-term goals. Our success as an organisation depends on our ability to identify and exploit the opportunities generated by our business and the markets Unilever operates in.

Unilever takes an embedded approach to risk management which puts risk and opportunity assessment at the core of the leadership team agenda. Unilever defines risks as actions or events that have the potential to impact our ability to achieve our objectives. Unilever identifies and mitigates downside risks such as loss of money, reputation or talent as well as upside risks such as failure to deliver strategy if it does not strengthen brand equities or growth in growing channels.

Unilever's Risk Management approach is embedded in the normal course of business. Its structural elements include: -

- Governance of Unilever, organizational structure and delegation of authority
- Vision, Strategy and Objectives
- Risk and Control Frameworks
- Performance management and operational processes execution
- Compliance and assurance activities.

1.3 Integrating Risk in the Strategic Planning Process

Strategic risks impact an organization's ability to deliver its goal - that is generally articulated in the strategic plan or intent document of the organisation. At the annual or early stage of strategic planning organization can identify and respond to strategic risks. Given the velocity with which threats and risk events strike organizations find it useful to integrate significant risk factors in the strategic planning process.

For example: -

- An organisation with an on-line selling business model may identify a cyber-attack threat at the stage of business plan preparation and respond by investing in a suitable internal control such as a best in class Firewall device.
- Strategic risks affect the organizations' s strategic plan can arise from internal operations or external factors. More often from external forces that shape its business environment such as - political, demographic, economic—and the dynamics of the industries where the organisation plays a role.

- New legislation that curtails the selling price of a medical device. This would significantly curtail the margins of the company.
- Company's strategic objective may require launch of a new sophisticated product, however, a specific set of skills required for installing the product may not be available with the company
- A new strategic initiative to implement cloud computing solutions may make the company more vulnerable to information security breaches

The strategy of an organisation should make it clear as to how it intends to mitigate or manage risks and maximize opportunities. It should develop objectives and the strategies to fulfil them. Further, these can be implemented through resource allocation plans.

1.4 Integrating Risk with Performance

Organisations can evaluate the level of risk they are exposed to while they pursue their growth goals. Knowledge of the level of risks that the organisation can take or accept at each stage of progression or growth enables the organisation to make informed decisions while pursuing their growth/ performance goals. Management's confidence enhances with risk awareness, understanding the risk profile of a strategic choice, risks associated with a desired performance. Existence of Internal controls and internal control assurance programs such as internal control evaluations or internal audits provide confidence to the management that they are ready to accept greater risks in pursuing their growth/ performance goals.

Certain business performance indicators may also disclose the associated risk profile –

Examples: -

- % of Customer attrition (loss of customer is a risk event for the company)
- % of Employee turnover (loss of employee is a risk event for the company)
- Profitability of customer by regional segments (unprofitable customers in certain regions may be a risk for the company)
- % of mission critical business processes with tested contingency plans (lack of contingency testing for mission critical processes represents a risk for the company)

2. INTERNAL CONTROL ENVIRONMENT AND LINKAGES WITH RISK MANAGEMENT

The subject of ERM is a sub-set of Corporate Governance. ERM is mandatory under the Companies Act, 2013 for large and listed entities therefore a matter of compliance as well. IC is a sub-set of ERM, basically internal control is the strategy or tool for the purpose of managing or mitigating the identified risk factor under the ERM. Internal Control Environment (ICE) is an intangible concept that represents the ethical, moral and governance climate of the organisation. It is difficult to measure the effectiveness of the ICE in simplistic terms, however, it can be assessed by surveying the culture of

the organisation. Such surveys to ascertain the ICE effectiveness are referred to as "Ethical Climate Surveys" or "Culture Monitoring Surveys". ICE can be evaluated through company-wide or entity level controls as well. These are high level controls that set the direction for other operating controls, example policy for financial closure or budgeting. We can observe a clear linkage between the concepts of ERM, IC and ICE as they have similar objectives of: -

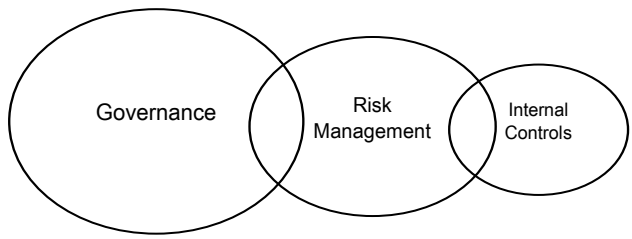
- Ensuring reliable financial reporting
- Efficient use of resources
- Compliance with the laws
- Improving performance

ERM is business strategy aligned whereas IC is operational and transactional driven. ERM is generally driven by the highest level whereas IC is implemented by the operating management.

ERM exercise requires the risk teams to study the business environment, eco-system of the company in terms of vendors, customers, employees, etc to identify relevant business risks and develop risk response action plans.

ICE and IC exercises requires the executive management to develop entity and process specific control strategies say for example internal control checklists, authorisation matrix, compliance procedures, standard operating procedures, etc.

Risk Management is a larger concept and internal control is a sub-set of Risk Management. Both subjects fall under the mega-concept of Governance. The pictorial depiction of the three concepts is as under: -



Generally, organizations face a wide range of uncertain internal and external uncertainties that may affect achievement of their objectives which can be strategic, operational, financial or otherwise and effect of these uncertainties on their objectives can be a Positive or a Negative Risks. While Positive Risks are opportunities the Negative Risks are threats to the achievement of objectives.

Both Risk Management and IC works together as on one hand the Risk Management mainly focuses on identification of threats and opportunities, on the other hand IC assist in countering threats and taking advantage of opportunities.

Proper Risk Management and IC hand in hand assist organizations in to effectively pursue their objectives by making informed decisions about the level of risk that they want to take and

implementing the necessary controls.

Accordingly, it can be said that both Risk management and IC are important pillars for governance, management, and operations of an organization's. Further to be a successful organization it is essential to integrate effective governance structures and processes along with performance-focused risk management and internal control at every level as well as across all operations of an organization.

It should be noted that though both Risk Management and IC should always be considered when setting and achieving organizational objectives and creating, enhancing, and protecting stakeholder value but are not objectives in themselves.

Since Risk Management and IC form an integral part of an organization's governance system with an integrated, organization-wide approach Risk Manager can treat risks in a more holistic, comprehensive way, ensuring that all business decisions are based on proper risk assessment and management considering the overall effect of uncertainties on the organization's objectives.

It is pertinent from above that internal control is an important sub-set of ERM. ERM is applied by the Board or highest executive from strategy through execution, while placing reliance on internal control at various stages. The two concepts of ERM and IC are interconnected, but not interchangeable. Both are used together, as powerful complementary tools in supporting management.

The task of IC is to help organisations achieve compliance, reporting and operations goals and objectives. So, IC is basically a component of risk management. And, internal control complements ERM. The ERM is basically a top down approach to Risk Management. It's focus is broader and aims at reducing risks that affect the entire enterprise. On the other hand, internal control provides a bottom up approach and it complements ERM by doing an in-depth assessment of agency's business processes, its specific risks, and how those risks are being controlled.

IC includes activities designed to help organizations achieve compliance, reporting and operations goals and objectives. Part of doing so requires that management consider the risk to those objectives – so it is inherently a component of risk management. But IC complements ERM; each raises the value of the other. For example, ERM helps in developing the objective used as a basis for developing controls, while IC makes ERM more effective when control activities are in place over risk responses and other ERM processes.

3. RISK CULTURE AND ATTITUDES TO RISK MANAGEMENT

3.1 Risk Culture

People are the cornerstone for effective Risk Management in any organisation or society. Risk aware culture and pro-active attitude ensure quick risk responses and containment of damages. Risk culture means that all levels of the organisation from the junior most to the Chief Executive understand and appreciate the positive and negative results that a risk event can bring.

Risk culture takes a long time to evolve, it requires continuous efforts of communication, building of corporate memory so that people can learn from previous mistakes, shaping the right risk actions, etc.

Basel's Principles for the Sound Management of Operational Risk defines Risk culture as "the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of Operational Risk Management."

Organisations are integrating Risk management into strategic planning, performance measurement, budgeting, projects and operational activities to create Risk Culture and reap benefits of sustainable business practices.

Various definitions of risk culture are available. The 2009 International Institute of Finance report "Reform in the financial services industry: Strengthening Practices for a More Stable System" defines Risk culture as the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify and understand, openly discuss and act on the organisations current and future risk.

Guidance on Supervisory Interaction with Financial Institutions on Risk Culture - A Framework for Assessing Risk Culture (April 2014) states that: -

A sound risk culture should emphasise throughout the institution the importance of ensuring that:

(i) an appropriate risk-reward balance consistent with the institution's risk appetite is achieved when taking on risks;

(ii) an effective system of controls commensurate with the scale and complexity of the financial institution is properly put in place;

(iii) the quality of risk models, data accuracy, capability of available tools to accurately measure risks, and justifications for risk taking can be challenged, and

(iv) all limit breaches, deviations from established policies, and operational incidents are thoroughly followed up with proportionate disciplinary actions when necessary.

3.2 Case Example – Risk Culture Development – Risk Focus Integrity

One of the leading Corporates operating in the Energy Sector has disclosed its policy on "Supporting our Culture of Integrity". Let us study the policy disclosure for prevention of improper payments: -

3.2.1 Supporting our Culture of Integrity

CNOOC International's culture and processes support our commitment to integrity. Our Prevention of Improper Payments Standard requires that all employees comply with applicable laws everywhere we operate. This Standard is periodically reviewed for best practices, vetted by external counsel and reviewed by our Compliance Committee.

The Compliance Committee is comprised of members of our executive management team and provides oversight on potential high-risk payments. Approvals required under the Prevention of Improper Payments Standard are dealt with by this Committee, which also receives a report on high risk payments. As an additional control, our internal audit department assesses corruption risk on a periodic basis and conducts investigations if necessary.

Risk-based Prevention of Improper Payments training has been developed that provides employees in high risk positions with guidance on avoiding improper payments.

3.2.2 Integrity Leaders

A network of Integrity Leaders has been established to promote the organization's culture of integrity, facilitate integrity education and awareness, as well as act as a divisional resource for employees and internal stakeholders faced with an ethical dilemma or seeking guidance. Integrity Leaders regularly liaise between the Integrity and Compliance group in Calgary, Canada and employees working in our global locations.

4. INTEGRATED RISK REPORTING AND STAKEHOLDER RESPONSIBILITIES

Business models are being constantly challenged with volatile economic cycles, wide fluctuations in fuel and commodity prices, ballooning of debts; as a result, instances of business failures are rising. There is a growing demand for better and comprehensive risk disclosures. Stakeholders, investors, societies, communities and special interest groups believe that existing risk management disclosures are not enough, and they lack:

- Transparency
- Timeliness
- Depth
- Quality

They also believe that the disclosures are Strait jacketed.

Regulators have realised that corporates are reporting risks in a standardised manner as they do not like to disclose the true risk and opportunities. Therefore, regulators are deepening the risk disclosure norms applicable to listed and regulated entities.

Globally, there is a movement that has been initiated by the International Integrated Reporting Council (IIRC) on Integrated Reporting. IIRC is a global coalition of regulators, investors, companies, standard setters, the accounting profession and NGOs. The coalition is promoting communication about value creation as the next step in the evolution of corporate reporting. IIRC has promoted the concept of Integrated thinking and integrated report. The IIRC's vision is to align capital allocation and corporate behaviour to wider goals of financial stability and sustainable

development through the cycle of integrated reporting and thinking.

The main aim of an Integrated Report is to highlight by way of explaining to the investors who have contributed financial capital about the organisation's value creation over time. Further, an integrated report proves advantageous to all the stakeholders of the company including employees, customers, suppliers, business partners, regulators, policy makers etc.

An Integrated Report's primary purpose is to explain to providers of financial capital how an organization creates value over time. An integrated report benefits all stakeholders interested in an organization's ability to create value over time, including employees, customers, suppliers, business partners, local communities, legislators, regulators and policy-makers.

An integrated report includes the eight Content Elements. The Content Elements are fundamentally linked to each other and are not mutually exclusive. The order of the Content Elements is not the only way they could be sequenced.

The Content Elements are not intended to serve as a standard structure for an integrated report with information about them appearing in a set sequence or as isolated, standalone sections. Rather, information in an integrated report is presented in a way that makes the connections between the Content Elements apparent.

The content of an organization's integrated report will depend on the individual circumstances of the organization. The Content Elements are therefore stated in the form of questions rather than as checklists of specific disclosures. Accordingly, judgement needs to be exercised in applying the Guiding Principles to determine what information is reported, as well as how it is reported.

There are eight content elements of Integrated Report suggested by the Framework which include answering the Questions raised.

4.1 Organisational Overview and External Environment

Question: "What does the organisation do and what are the circumstances under which it operates?"

(I) Organisational Overview

An integrated report identifies the organization's mission and vision, and provides essential context by identifying matters such as:

(a) The organization's:

- Culture, ethics and values
- Ownership and operating structure
- Principal activities and markets

- Competitive landscape and market positioning (considering factors such as the threat of new competition and substitute products or services, the bargaining power of customers and suppliers, and the intensity of competitive rivalry)
- Position within the value chain

(b) Key Quantitative Information (KQI)

- Number of employees
- Revenue
- Number of countries in which the organization operates
- Highlighting, in particular, significant changes from prior periods

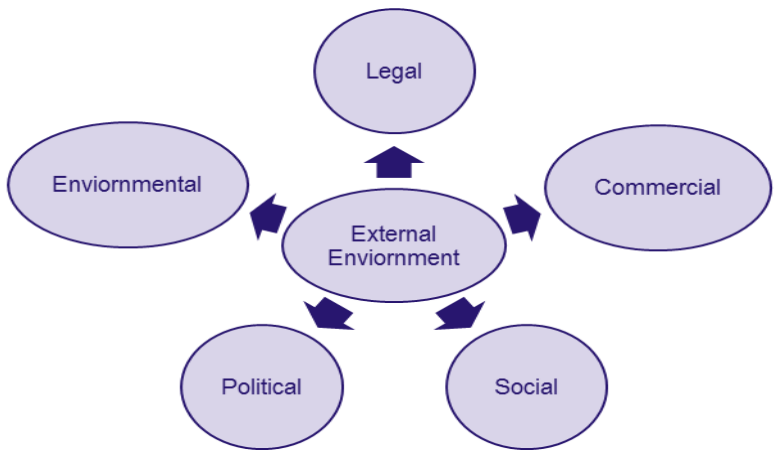
(c) Significant factors

- Significant factors affecting the external environment and the organization's response

(II) External Environment

External Environment can affect the organization directly or indirectly (e.g., by influencing the availability, quality and affordability of a capital that the organization uses or affects). Significant factors affecting the external environment that affects the organization's ability to create value in the short, medium or long term include aspects of:

- Legal
- Commercial
- Social
- Environmental
- Political context



4.2 Governance

Question: "How does the organisation's governance structure support its ability to create value in the short, medium and long term?"

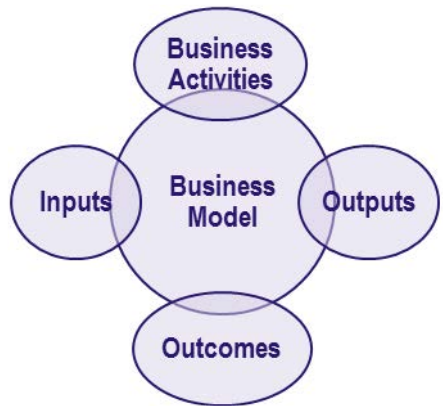
An integrated report provides insight about how such matters as the following are linked to its **ability to create value:**

- The **organization's leadership structure**, including the skills and diversity (e.g., range of backgrounds, gender, competence and experience) of those charged with governance and whether regulatory requirements influence the design of the governance structure.
- **Specific processes** used to make strategic decisions and to establish and monitor the culture of the organization, including its attitude to risk and mechanisms for addressing integrity and ethical issues
- **Particular actions** those charged with governance have taken to influence and monitor the strategic direction of the organization and its approach to risk management
- How the **organization's culture, ethics and values** are reflected in its use of and effects on the capitals, including its relationships with key stakeholders
- Whether the organization is **implementing governance practices** that exceed legal requirements
- The **responsibility** those charged with governance take for promoting and enabling innovation
- How **remuneration and incentives are linked to value creation** in the short, medium and long term, including how they are linked to the organization's use of and effects on the capitals.

4.3 Business Model

Question: "What is the organisation's business model?"

Basically Business Model is a system of transforming inputs into output or outcomes using business activities that fulfil organization's strategic purposes and creating value.



(I) **Inputs:** An integrated report shows how key inputs relate to the capitals on which the organization depends, or that provide a source of differentiation for the organization, to the extent they are material to understanding the robustness and resilience of the business model.

(II) **Business Activities:** An integrated report describes key business activities. This can include:

- How the organization differentiates itself in the market place? – For example through product differentiation, market segmentation, delivery channels and marketing
- The extent to which the business model relies on revenue generation after the initial point of sale – For example extended warranty arrangements or network usage charges
- How the organization approaches the need to innovate? – For example, growing demand less pollutant vehicles.
- How the business model has been designed to adapt to change – For example, producing electric vehicles.

(III) **Outputs:** An integrated report identifies an organization's key products and services. There might be other outputs, such as by-products and waste (including emissions), that need to be discussed within the business model disclosure depending on their materiality.

(IV) **Outcomes:** An integrated report describes key outcomes, including:

- Both internal outcomes (e.g., employee morale, organizational reputation, revenue and cash flows) and external outcomes (e.g., customer satisfaction, tax payments, brand loyalty, and social and environmental effects)
- Both positive outcomes (i.e., those that result in a net increase in the capitals and thereby create value) and negative outcomes (i.e., those that result in a net decrease in the capitals and thereby diminish value).

4.4 Risks and Opportunities

Question to be answered through this element in the integrated reporting is "What are the specific risks and opportunities that affect the organisation's ability to create value over the short, medium and long-term, and how is the organisation dealing with them?"

An integrated report identifies the key risks and opportunities that are specific to the organization, including those that relate to the organization's effects on, and the continued availability, quality and affordability of, relevant capitals in the short, medium and long term.

This can include identifying:

- The specific source of risks and opportunities, which can be internal, external or, commonly, a mix of the two. External sources include those stemming from the external environment. Internal sources include those stemming from the organization's business activities.
- The organization's assessment of the likelihood that the risk or opportunity will come to

fruition and the magnitude of its effect if it does. This includes consideration of the specific circumstances that would cause the risk or opportunity to come to fruition. Such disclosure will invariably involve a degree of uncertainty such as:

- ♦ an explanation of the uncertainty
- ♦ the range of possible outcomes, associated assumptions, and how the
- ♦ information could change if the assumptions do not occur as described
- ♦ the volatility, certainty range or confidence interval associated with the information provided

- The specific steps being taken to mitigate or manage key risks or to create value from key opportunities, including the identification of the associated strategic objectives, strategies, policies, targets and KPIs.

4.5 Strategy and Resource Allocation

Question: "Where does the organisation want to go and how does it intend to get there?"

An integrated report ordinarily identifies:

- The organization's short, medium and long term strategic objectives
- The strategies it has in place, or intends to implement, to achieve those strategic objectives
- The resource allocation plans it has to implement its strategy
- How it will measure achievements and target outcomes for the short, medium and long term.

This can include describing:

- The linkage between the organization's strategy and resource allocation plans, and the information covered by other Content Elements, including how its strategy and resource allocation plans.
- What differentiates the organization to give it competitive advantage and enable it to create value.
- Key features and findings of stakeholder engagement that were used in formulating its strategy and resource allocation plans.

4.6 Performance

Question: "To what extent has the organisation achieved its strategic objectives for the period and what are its outcomes in terms of effects on the capitals?"

An integrated report contains qualitative and quantitative information about performance that may include matters such as:

- **Quantitative indicators** with respect to targets and risks and opportunities, explaining their significance, their implications, and the methods and assumptions used in compiling them

- The **organization's effects (both positive and negative) on the capitals**, including material effects on capitals up and down the value chain
- The **state of key stakeholder relationships** and how the organization has responded to key stakeholders' legitimate needs and interests
- The **linkages between past and current performance**, and between current performance and the organization's outlook

4.7 Outlook

Question: "What challenges and uncertainties is the organisation likely to encounter in pursuing its strategy, and what are the potential implications for its business model and future performance?"

An integrated report ordinarily highlights anticipated changes over time and provides information, built on sound and transparent analysis, about:

- The **organization's expectations** about the external environment the organization is likely to face in the short, medium and long term
- How that will **affect** the organization
- How the **organization is currently equipped** to respond to the critical challenges and uncertainties that are likely to arise.

4.8 Basis of Preparation and Presentation

Question: "How does the organization determine what matters to include in the integrated report and how are such matters quantified or evaluated?"

An integrated report describes its basis of preparation and presentation, including:

- A summary of the organization's Materiality determination process
- A description of Reporting boundary and how it has been determined
- A summary of Significant frameworks and methods used to quantify or evaluate material matters

[Source: International <IR> Framework, The International Integrated Reporting Council (IIRC)]

5. RISK & OPPORTUNITY REPORTING

As per the IIRC - Continuous monitoring and analysis of the external environment in the context of the organization's mission and vision identifies risks and opportunities relevant to the organization, its strategy and its business model.

Most of the guidance and regulatory requirements for risk reporting were developed after the global financial crisis of 2007-08, but few nations have a better record than others, historically, of

mandating or encouraging companies to report on risk. The US, for example, has required companies listed with the Securities and Exchange Commission (SEC) to describe the risks faced by the business (in some form or another) since the 1970s. The EU Accounts Modernisation Directive of 2003 said that companies should describe the risks they face, in both annual and interim reports.

Two countries have gone further than the Europe-wide requirements – Germany has its own Risk Reporting Standard (GAS 5), while the UK's Corporate Governance Code states that companies should report at least annually on the effectiveness of their risk-management procedures. The UK's Corporate Governance Code still goes further where a more integrated approach to risk reporting, linking risk management to internal controls and going concern.

The Management Discussions & Analysis (MD & A) section that is popular in Annual Report disclosures was prescribed by the US Securities & Exchange Commission in the 1980s to meet the growing demand of enhanced risk disclosures. The MD & A section requires has specific disclosures on the trends, economic uncertainties that the business is exposed to and the likely positive or negative impact of such trends and economic uncertainties on the revenues of the company. In the US, large unexpected losses on derivatives incurred by several firms in the early to mid-1990s reinforced demands that had already begun to emerge for better information on firms' derivative positions and market risks. This led to risk disclosure requirements in Disclosures about Derivative Financial Instruments and Fair Value of Financial Instruments and Accounting for Derivative Instruments and Hedging Activities, and Disclosure of Accounting Policies for Derivative Financial Instruments etc. These include Germany's requirement for companies to disclose all material risks, subsequently supplemented by an accounting standard on risk reporting, and the EU's requirement that a company's annual report to include description of principal risks and uncertainties that it is exposed to.

Global developments about risk reporting encompass following contemporary aspects to provide a holistic risk reporting disclosure to stakeholders and investors: -

- Reporting of principal or material risk factors and responsibility for mitigating such risk factors
- Clear categorisation of risks into company specific or general/ industry related
- Ordering or numbering the risks so that investor understand the risk priorities
- Movement of risks from previous reporting periods showing the context and cause for such changes
- Risk linkages to financial statements, other important parts of the Annual Report
- Impact of risks on financial and non-financial matters
- Indictive risk appetite of the company as it may be difficult to quantify
- Short term Liquidity and Long-term Business Viability reporting
- Stress and Sensitivity analysis with specific scenarios linking back to principal risk factors

In India, as per the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015: -

(i) Under responsibility of Directors - Ensuring the integrity of the listed entity's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.

(ii) The Board of Directors shall ensure that, while rightly encouraging positive thinking, these do not result in over-optimism that either leads to significant risks not being recognised or exposes the listed entity to excessive risk.

(iii) The Board of Directors shall have ability to "step back" to assist executive management by challenging the assumptions underlying: strategy, strategic initiatives (such as acquisitions), risk appetite, exposures and the key areas of the listed entity's focus.

(iv) The listed entity shall lay down procedures to inform members of board of directors about risk assessment and minimization procedures.

(v) The Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.

(vi) Risk Management Committee: - The board of directors shall constitute a Risk Management Committee. Majority members of Risk Management Committee shall consist of members of the board of directors. The Chairperson of the Risk management committee shall be a member of the board of directors and senior executives of the listed entity may be members of the committee.

The board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit. The provisions of this regulation shall be applicable to top 100 listed entities, determined based on market capitalisation, as at the end of the immediately preceding financial year.

(vii) Under minimum information to be placed before the Board on a quarterly basis- Quarterly details of foreign exchange exposures and the steps taken by management to limit the risks of adverse exchange rate movement, if material.

(viii) Under disclosures in Annual Reports applicable to all listed entities except banks - Management Discussion and Analysis: This section shall include discussion on the following matters within the limits set by the listed entity's competitive position:

(a) Industry structure and developments

(b) Opportunities and Threats

(c) Segment–wise or product-wise performance

(d) Outlook, (e) Risks and concerns,

(f) Internal control systems and their adequacy

(g) Discussion on financial performance with respect to operational performance,

(h) Material developments in Human Resources / Industrial Relations front, including number of people employed and General information to shareholders: Commodity price risk or foreign exchange risk and hedging activities.

6. IT RISK MANAGEMENT – DISASTER RECOVERY

6.1 Disaster Recovery Plan

Information is said to be the currency of the 21st century and it is considered the most valuable asset of an organisation. This is more so in case of organisations which use and are heavily dependent on Information Technology (IT). Organisations in this modern era run their business based on information which are processed using Information and Communication Technology (ICT). The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. There is a heavy dependence on real time information from information technology assets for conducting business. Information is a critical factor for continued success of the business. This dependence on Information is more explicit in the most organisations which are now dependent on IT for performing their regular business operations. We can understand the criticality of IT by imagining impact of failure or non-availability of IT in case of following types of organisations:

(i) Bank using Core banking solution with a million accounts, credit cards, loans and customers.

(ii) Companies using centralised ERP software having operations in multiple locations.

(iii) An airline serving customers on flights daily using IT for all operations.

(iv) Pharmacy system filling millions of prescriptions per year (some of the prescriptions are life-saving).

(v) Automobile factory producing/manufacturing hundreds of vehicles daily using automated solution.

(vi) Railways managing thousands of train routes and passengers through automated ticketing and reservation.

The above situations clearly demonstrate the heavy dependence on IT systems. IT can fail due to multiple factors. Hence, organisations should have appropriate disaster recovery and/ or contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen manmade or natural disaster and this may lead to loss of productivity, revenue and market share among many other impacts. Hence, organisations have to take necessary steps to ensure that the impact from such disasters is minimised and build resilience which ensures continuity of critical operation in the event of disruptions. Modern organisations

cannot think of running their business operations without IT. IT is prone to increased risks which can lead to failure of IT thus impacting operations. Hence, it is becoming increasingly important for organisations to have a business contingency plan for their Information Systems. The criticality of the plan can be determined based on the level of impact on critical business operations due to failure or non-availability of IT impacting service delivery. The failure of IT could be caused due to any or more of the following: -

(i) Server or network failure

(ii) Disk system failure

(iii) Hacker break-in

(iv) Denial of Service attack

(v) Electrical or extended power failure

(vi) Snow storm, earthquake, tornado, tsunami or fire

(vii) Spyware, malevolent virus or worm

(viii) Employee error or revenge

(ix) Sabotage or theft

(x) Terrorist cyber attack

(xi) Communication link break down

(xii) Civil disturbance

Disaster is a physical event which interrupts business processes sufficiently to threaten the viability of the organisation. The basic objective of a Disaster Recovery Plan (DRP) is to document a set of procedures which can be used to protect a business IT infrastructure if any disaster takes place. DRP includes tasks like plan for disaster recovery, crisis management, recovery operations etc. Disaster Recovery Plan is the set of plans which are to be executed initially at the moment of crisis. These plans include measures to control the disaster, mitigate them and to initiate the recovery of the resources that is needed for the continuity of business. These plans are targeted to initiate/recover the resources that have been affected by a disaster. These are the first plans that would be executed at the time of disaster. There are three basic strategies that encompass a disaster recovery plan:

- preventive measures,
- detective measures, and
- corrective measures.

As the name indicates, the job of preventive measures is to prevent a disaster from taking place. The purpose of these measures is proper identification and reduction of risks. They are designed to mitigate or prevent an event from turning into a disaster.

These measures may include keeping data backed up and off site, using surge protectors, installing generators and conducting routine inspections. Further, these measures may be bifurcate into Detective or Corrective measures. For example: -

- Installing Fire alarms – detective
- Employee DR related trainings – detective
- Insurance Policies – Corrective
- Restoring systems post disaster - Corrective

A disaster can be defined as an unplanned interruption of normal business process. It can be said to be a disruption of business operations that stops an organisation from providing critical services caused by the absence of critical resources. An occurrence of disaster cannot always be foreseen; hence we need to be prepared for all the types of disasters that can arise, handle them effectively in the shortest time.

Business Continuity Plan (BCP) includes tasks like establishing continuity strategies, planning for continuity of critical operations, continuity management etc. BCP is a plan that contains the steps that would be taken by an entity to resume its business functions during its period of disruption. These plans are executed in parallel with the disaster recovery plans depending on the impact of the disaster. BCPs on a whole is about re-establishing existing business processes and functions, communications with the business contacts and resuming business processes at the primary business location.

6.2 Testing the Disaster Recovery Plan

The Disaster Recovery Co-ordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. Special Disaster Recovery testing is undertaken whenever there are changes in the software and technology or business environments. Objectives of testing the Disaster Recovery plan/ procedures are outlined under: -

(i) To simulate the conditions of an actual Business recovery situation

(ii) Determine the time consumed and feasibility of the recovery process

(iii) Identify deficiencies in the existing procedures for improvement and take note of the physical / practical constraints

(iv) Test the completeness of the business recovery information stored at the Offsite Storage Location.

(v) Train members of the Disaster Recovery teams the initial test of the plan will be in the form of a structured walk-through and should occur within two months of the Disaster Recovery plan's acceptance. Subsequent tests should be to the extent determined by the Business continuity co-ordinator that are cost effective and meet the benefits and objectives desired.

(vi) Test the state of resilience of the organisation and associated service providers

(vii) Provide assurance to the Board and regulators that Disaster Recovery plan is operational and effective