CHAPTER 7

RISK ASSOCIATED WITH CORPORATE GOVERNANCE

LEARNING OUTCOMES

After going through the chapter student shall be able to understand

- Evaluation of Risk Associated with Governance
- Description and evaluation of framework for Board level consideration of risk
- OECD Guidelines for Corporate Governance

1. EVALUATION OF RISK ASSOCIATED WITH GOVERNANCE

Governance risks mean significant deficiencies that can impact the reputation, existence and continuity of the organisation. These arise on account of failure of the Board to direct and control the organisation or inappropriate practices adopted by the Board or collusion of management to override significant internal control mechanism causing financial losses or inability of the Board to identify principal risk factors that can impact business continuity.

May 18 MCQ

Often these failures are facilitated by corporate governance failures, where boards do not fully appreciate the risks that the companies are taking (if they are not engaging in reckless risk-taking themselves), and/or deficient risk management systems.

Governance Risks Nov 18 MTP MCQ - twice

- Absence of effective corporate governance framework and documented governance policies
- The rights of shareholders and key ownership functions are not defined and communicated
- There is no equitable treatment of shareholders

- The role of stakeholders in corporate governance is not defined, communicated and monitored
- Disclosure and transparency norms are not articulated
- The responsibilities of the Board of directors are not defined, documented and reviewed annually
- Board has not defined risk capacity, appetite and risk response strategies
- Risk not managed on an enterprise basis and not adjusted to corporate strategy.
- Risk managers separated from management and not regarded as an essential part of implementing the company's strategy. Most important of all, boards were in a number of cases ignorant of the risk facing the company.
- Risk management and control functions be independent of profit centres and the "Chief Risk Officer" (CRO) or equivalent should report directly to the board of directors along the lines
- Corporations developing their risk management and oversight practices face challenges, such as linking risks to strategy; better defining risks; developing corporate responses to risks that manage to address all five key dimensions (strategy, people, detail, tasks, and drivers); effectively considering stakeholders' and gatekeepers' concerns; and addressing all these issues from a whole-enterprise perspective. These challenges are faced by both financial and non-financial companies.
- Boards simply review and approve management's proposed strategies.
- Insignificant Board time spent on business risk management
- Boards have incomplete understanding of the risks faced by the company.
- Boards receive information that is short-term.
- The process of risk management and the results of risk assessments should be appropriately disclosed. Disclosure of risk factors should be focused on those identified as more relevant and/or should rank material risk factors in order of importance on the basis of a qualitative selection whose criteria should also be disclosed.
- Whistle blower matters
- Negative media reports
- Shareholder activism
- Unauthorised related party transactions
- Ownership /Shareholder disputes

To evaluate and assess Governance Risks it is highly recommended to study the **Sound Risk Governance Practices recommended by the Financial Stability Board in 2013**. The list extracts some of the better practices exemplified by national authorities and firms. The sound practices also build on some of the principles and recommendations published by other organisations and standard setters, drawing together those that are relevant for risk governance.

This integrated and coherent list of sound practices aims to help national authorities and firms continue to improve their risk governance. This list is summarized as below:

(i) The Board of Directors Nov 18 MTP CS - 3

a) avoids conflicts of interest arising from the concentration of power at the board (e.g., by having separate persons as board chairman and CEO or having a lead independent director where the board chairman and CEO are the same person);

b) comprises members who collectively bring a balance of expertise (e.g., risk management and financial industry expertise), skills, experience and perspectives;

c) comprises largely independent directors and there is a clear definition of independence that distinguishes between independent directors and non-executive directors;

d) sets out clear terms of references for itself and its sub-committees (including tenure limits for committee members and the chairs), and establishes a regular and transparent communication mechanism to ensure continuous and robust dialogue and information sharing between the board and its sub-committees;

e) conducts periodic reviews of performance of the board and its sub-committees (by the board nomination or governance committee, the board themselves, or an external party); this includes reviewing, at a minimum annually, the qualifications of directors and their collective skills (including financial and risk expertise), their time commitment and capacity to review information and understand the firm's business model, and the specialised training required to identify desired skills for the board or for director recruitment or renewal;

f) sets the tone from the top, and seeks to effectively inculcate an appropriate risk culture throughout the firm;

g) is responsible for overseeing management's effective implementation of a firm-wide risk management framework and policies within the firm;

h) approves the risk appetite framework and ensures it is directly linked to the business strategy, capital plan, financial plan and compensation;

i) has access to any information requested and receives information from its committees at least quarterly;

j) meets with national authorities, at least quarterly, either individually or as a group.

(ii) The risk committee May 20 MTP - I CS - 4 MCQ

a) is required to be a stand-alone committee, distinct from the audit committee;

b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

Also, Risk Management Committee
Page 2.30

c) includes members who are independent;

d) includes members who have experience with regard to risk management issues and practices;

e) discusses all risk strategies on both an aggregated basis and by type of risk;

f) is required to review and approve the firm's risk policies at least annually;

g) oversees that management has in place processes to ensure the firm's adherence to the approved risk policies.

(iii) The audit committee

a) is required to be a stand-alone committee, distinct from the risk committee;

b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

c) includes members who are independent;

d) includes members who have experience with regard to audit practices and financial literacy at a financial institution;

e) reviews the audits of internal controls over the risk governance framework established by management to confirm that they operate as intended;

f) reviews the third party opinion of the design and effectiveness of the overall risk governance framework on an annual basis.

May 19 MTP

(iv) The CRO CRO = Head of RM Functions

a) has the organisational stature, skill set, authority, and character needed to oversee and monitor the firm's risk management and related processes and to ensure that key management and board constituents are apprised of the firm's risk profile and relevant risk issues on a timely and regular basis; the CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities as well as a direct reporting line to the board and/or risk committee;

b) meets periodically with the board and risk committee without executive directors or management present; ✓

c) is appointed and dismissed with input or approval from the risk committee or the board and such appointments and dismissals are disclosed publicly;

d) is independent of business lines and has the appropriate stature in the firm as his/her performance, compensation and budget is reviewed and approved by the risk committee; ✓

e) is responsible for ensuring that the risk management function is adequately resourced,

taking into account the complexity and risks of the firm as well as its Risk Assessment Framework (RAF) and strategic business plans;

f) is actively involved in key decision-making processes from a risk perspective (e.g., the review of the business strategy/strategic planning, new product approvals, stress testing, recovery and resolution planning, mergers and acquisitions, funding and liquidity management planning) and can challenge management's decisions and recommendations;

g) is involved in the setting of risk-related performance indicators for business units;

h) meets, at a minimum quarterly, with the firm's supervisor to discuss the scope and coverage of the work of the risk management function.

Asked in Nov 18 exam : Functions of Rm
Head of RM functions = CRO

2. THE RISK MANAGEMENT FUNCTION

a) It is independent of business lines (i.e., is not involved in revenue generation) and reports to the CRO;

b) It has authority to influence decisions that affect the firm's risk exposures;

c) It is responsible for establishing and periodically reviewing the enterprise risk governance framework which incorporates the Risk Appetite Framework (RAF), Risk Appetite Statement (RAS) and risk limits.

May 18 exam MCQ

i) The RAF incorporates an RAS that is forward-looking as well as information on the types of risks that the firm is willing or not willing to undertake and under what circumstances. It contains an outline of the roles and responsibilities of the parties involved, the risk limits established to ensure that the framework is adhered to, and the escalation process where breaches occur.

ii) The RAS is linked to the firm's strategic, capital, and financial plans and includes both qualitative and quantitative measures that can be aggregated and disaggregated such as measures of loss or negative events (e.g., earnings, capital, and liquidity) that the board and senior management are willing to accept in normal and stressed scenarios.

iii) Risk limits are linked to the firm's RAS and allocated by risk types, business units, business lines or product level. Risk limits are used by management to control the risk profile and linked to compensation programmes and assessment.

d) It has access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis; risk-bearing affiliates and subsidiaries are captured by the firm wide risk management system and are a part of the overall risk governance framework;

e) It provides risk information to the board and senior management that is accurate and reliable and periodically reviewed by a third party (internal audit) to ensure completeness and integrity;

f) It conducts stress tests (including reverse stress tests) periodically and by demand. Stress test programs and results (group-wide stress tests, risk categories and stress test metrics) are adequately reviewed and updated to the board or risk committee. Where stress limits are breached or unexpected losses are incurred, proposed management actions are discussed at the board or risk committee. Results of stress tests are incorporated in the review of budgets, RAF and ICAAP processes, and in the establishment of contingency plans against stressed conditions.

3. INDEPENDENT ASSESSMENT OF THE RISK GOVERNANCE FRAMEWORK

A Risk Management Framework (RMF) sets the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management capability. Undertaking a periodic review to assess the effectiveness of an entity's risk management framework is necessary to ensure that the framework continues to evolve and meet the needs of the entity. The RMF should define a policy statement on the following matters:-

ICAI Case Study 2

(i) Determining when to review the RMF and the frequency for undertaking the review.

(ii) Deciding who is responsible for the review. The RMF is generally reviewed by the Audit Committee or a team of Directors. Once in few years the RMF can be reviewed with external facilitation this would provide fresh insights and benchmarking information to the Board.

(iii) Selecting the scope and method for a review. The scope and boundary of the RMF review can be clearly set out along with the most suited method for review.

(iv) Manner of circulation of results.

The Board requires a periodic independent assessment of the firm's overall risk governance framework and provides direct oversight to the process.

The Board should assess whether the organisation has the required stature, talent, and character needed to provide a reliable independent assessment of the firm's risk governance framework and internal controls and not be unduly influenced by the CEO and other members of management;

Organisations may develop an entity level control framework on the basis of the Sound Risk Governance Principles prescribed by the Financial Stability Board for evaluating Governance Risks. The results and findings from the said entity level control assessment may be submitted to the Board of the company on an annual basis and suitably disclosed as part of its risk disclosures.

3.1 Entity's Risk Assessment Process with respect to Financial Reporting

The **ICAI Guidance note on Internal Financial Controls** over financial reporting states that for financial reporting purposes, the entity's risk assessment process includes how management

identifies business risks relevant to the preparation of financial statements in accordance with the entity's applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to respond to and manage them and the results thereof.

For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyses significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting include external and internal events, transactions or circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations.

Risks can arise or change due to the following circumstances: May 18 MTP MCQ + Nov 20 MTP

a) **Changes in operating environment.** Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.

b) **New personnel.** New personnel may have a different focus on or understanding of internal control.

c) **New or revamped information systems.** Significant and rapid changes in information systems can change the risk relating to internal control.

d) **Rapid growth.** Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.

e) **New technology.** Incorporating new technologies into production processes or information systems may change the risk associated with internal control.

f) **New business models, products, or activities.** Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.

g) **Corporate restructurings.** Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with internal control.

h) **Expanded foreign operations.** The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.

i) **New accounting pronouncements.** Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

3.2 Role of Risk Assessment with respect to Financial Reporting

Risk assessment underlines the entire audit process described by the ICAI guidance note, including the determination of significant accounts and disclosures and relevant assertions, the selection of controls to test, and the determination of the evidence necessary for a given control. A direct relationship exists between the degrees of risk that a significant deficiency or material weakness could exist in a particular area of the company's internal financial controls over financial

reporting and the amount of audit attention that should be devoted to that area. In addition, the risk that a company's internal financial controls over financial reporting will fail to prevent or detect a misstatement caused by fraud usually is higher than the risk of failure to prevent or detect error. The auditor should focus more of his or her attention on the areas of highest risk. On the other hand, it is not necessary to test controls that, even if deficient, would not present a reasonable possibility of material misstatement to the financial statements. The complexity of the organisation, business unit, or process, will play an important role in the auditor's risk assessment and the determination of the necessary procedures.

3.3 Risk Based Internal Auditing (RBIA)

Internal Audit

The definition of internal audit, as described in the Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India, amply reflects the current thinking as to what is an internal audit: Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system.

Internal auditors can carry out their job in a more focused manner by directing their efforts in the areas where there is a greater risk, thereby enhancing the overall efficiency of the process and adding greater value with the same set of resources.

Internal audit is a management function, thus, it has the high-level objective of serving management's needs through constructive recommendations in areas such as, internal control, risk, utilisation of resources, compliance with laws, management information system, etc.

Risk management enables management to effectively deal with risk, associated uncertainty and enhancing the capacity to build value to the entity or enterprise and its stakeholders. Internal auditor plays an important role in providing assurance to management on the effectiveness of risk management.

Boards of Directors are increasingly becoming risk aware and risk focused. Expectations from internal auditors are increasing from providing an assurance on the adequacy and effectiveness of internal controls to an assurance on whether risks are being managed within acceptable limits as defined by the Board of Directors. This has given to birth Risk Based Audit Methodologies that are pursued by Auditors.

The business environment is increasingly throwing up newer challenges and opportunities with globalisation, disruptive technologies and rules being continuously rewritten. New risks are hence coming up frequently. Risk management is the process of measuring or assessing risk and developing strategies to manage it. The 21st century internal auditors have the following vital areas of responsibility in the field of risk management:

- Review operations, policies, and procedures.
- Help ensure that goals and objectives are met.

- Understanding the "big picture" and diverse operations.
- Make recommendations to improve economy and efficiency.

Therefore, the internal audit report is on the management of significant risks of the organisation and the assurance is on these risks being managed within the acceptable limits as laid down by the Board of Directors. To give this assurance, the internal auditor conducts a process audit on risk management processes at all levels of the organisation, viz., corporate, divisional, business unit, business process level, etc., put in place by line management so as to assess the adequacy of their design and compliance

3.4 Audit Risk & Sampling

Some degree of uncertainty is implicit in the concept of "a reasonable basis for an auditor's opinion". The justification for accepting some uncertainty arises from the relationship between factors such as cost and time required for examining all of the data and the adverse consequences of possible erroneous decisions based on the conclusions resulting from examining only a sample of the data.

Audit risk includes both uncertainties due to sampling and uncertainties due to factors other than sampling. These aspects of audit risk are sampling risk and non-sampling risk, respectively. Sampling risk arises from the possibility that, when a test of controls or a substantive test is restricted to a sample, the auditor's conclusions may be different from the conclusions he would reach if the test were applied in the same way to all items in the account balance or class of transactions. That is, a particular sample may contain proportionately more or less monetary misstatements or deviations from prescribed controls than exist in the balance or class as a whole. For a sample of a specific design, sampling risk varies inversely with sample size: the smaller the sample size, the greater the sampling risk.

Non-sampling risk includes all the aspects of audit risk that are not due to sampling. An auditor may apply a procedure to all transactions or balances and still fail to detect a material misstatement. Non-sampling risk includes the possibility of selecting audit procedures that are not appropriate to achieve the specific objective. For example, confirming recorded receivables cannot be relied on to reveal unrecorded receivables. Non-sampling risk also arises because the auditor may fail to recognize misstatements included in documents that he examines, which would make that procedure ineffective even if he were to examine all items. Non-sampling risk can be reduced to a negligible level through such factors as adequate planning and supervision and proper conduct of a firm's audit practice.

4. RISK MANAGEMENT DISCLOSURES IN INDIA See page no. 9.2

4.1 Indian Scenario

Nov 2020 MTP CS - 4

4.1.1 Provisions of the Indian Companies Act, 2013

In recognition of the risk realities, the Indian Companies Act, 2013 has mandated provisions that

MCQ May 18

the Annual Report of the Board of Directors must include a statement indicating the development and implementation of a risk management policy for the company. This should include the identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.

The audit committee is directed to act in accordance with the terms of reference specified in writing by the Board, which shall, inter alia, include evaluation of risk management systems. The code of conduct prescribes that the Independent Directors should satisfy themselves that systems of risk management are robust and defensible.

4.1.2 Provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015

SEBI Listing Requirements as applicable to listed entities in India is a comprehensive set of guidelines that are prepared on the lines of international practices. As per SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015 following risk management disclosures are mandatory for listed entities in India.

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) The board of directors shall constitute a Risk Management Committee.

The majority of 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 on the basis of market capitalisation, as at the end of the immediate previous 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.

(i) Details of significant changes (i.e. change of 25% or more as compared to the immediately previous financial year) in key financial ratios, along with detailed explanations therefor, including:

(i) Debtors Turnover

(ii) Inventory Turnover

(iii) Interest Coverage Ratio

(iv) Current Ratio

(v) Debt Equity Ratio

(vi) Operating Profit Margin (%)

(vii) Net Profit Margin (%) or sector-specific equivalent ratios, as applicable.

(j) Details of any change in Return on Net Worth as compared to the immediately previous financial year along with a detailed explanation thereof.]

General information to shareholders: Under this head the information related to Commodity Price Risk or Foreign Exchange Risk and related Hedging activities are covered.

May 20 MTP - I MCQ

4.2 Risk Management Disclosures – Global Scenario

In US, the Companies listed with the Securities and Exchange Commission (SEC), have to describe the risks faced by the business (in some form or another) since the 1970s. In Europe, 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 says 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 is included.

The first important attempt to meet the demand for increased risk disclosures was the 1980 remodelling of the rules of the US securities and Exchange Commission (SEC) for a management discussion and analysis (MD&A). The MD&A rules include a requirement to 'Describe any known trends or uncertainties that the company reasonably expects will have a material favourable or unfavourable impact on net sales or revenues or income from continuing operations', and similar requirements in relation to capital and liquidity.

In many jurisdictions, risk management principles are dealt with (in one way or another) in national corporate governance codes, as is the case with the New York Stock Exchange (NYSE) listed company rules, the UK's combined code, the French AFEP-MEDEF code and several other county regimes. Internationally, professional institutes and associations also offer their prescriptions. In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an internal control – integrated framework guide, and in 2004 an enterprise risk management (ERM) – integrated framework guide. A report prepared for the OECD in 2010 concluded, however, "none of the existing guidance on risk management is adequate for the purpose. Most of the guidance is extremely high-level, is process-oriented and gives scant guidance on how to create an effective risk management and assurance framework." More recently, COSO published guidance on risk assessments and on risk appetite (2012), which provides more specific guidance on certain issues. In 2009, the International Organization for Standardization issued its standard for implementation of risk management principles, ISO 31000, which has de facto become the world standard. The purpose of ISO 31000 is to provide principles and generic guidelines on risk management that could achieve convergence from a variety of standards, methodologies and procedures that differ between industries, subject matters, and countries. In 2016 (year-end), the revised ERM standard of COSO has been released.

Enhancing Organizational Reporting: Integrated Reporting Key

There is emergence of Integrated Reporting Framework (IRF) on the global landscape. It is fast emerging as holistic framework of corporate reporting that goes beyond the traditional financial reporting frameworks. The key objective of the IRF 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.

International Federation of Accountants (IFAC) states that Integrated Reporting is the way to achieve a more coherent corporate reporting system, fulfilling a need for a single report that provides a fuller picture of organizations' ability to create value. Integrated reporting can be used as an "umbrella" report for an organization's broad suite of reports and communications, enabling greater interconnectedness between different reports. IFAC also strongly supports the International Integrated Reporting Council and the implementation of its Framework.

IFAC's position paper No. 8 addresses reporting that provides decision-useful information to organizational stakeholders beyond that which is provided in traditional financial reporting and financial statements, and may provide important links between that financial reporting and other organizational reporting.

Risk & Opportunity Reporting (ROR) is a key component in the IRF. The details of the ROR as part of the IRF are as under:-

a. Key risks impacting ability to create value in short term, medium term and long term- these could be from:-

   i) Internal sources – business related risks

   ii) External sources-from external environment

b. Key opportunities like those related to process improvement, employee training and relationships management.

c. Organisation assessment of likelihood that the risk or opportunity will fructify and probability or certainty of same.

d. Steps taken to mitigate or manage key risks or create value from key opportunities including identification of associated strategic objectives, policies, targets and KPIs.

4.3 Risk Management Disclosures – A Global Case Study

Let us study the annual report of Global major operating in the retail sector in 2016; Principal Risk and Uncertainties Disclosure in a summarised manner describes all the Principal Risk Factors covering Customer Proposition, Transformation of economic model, Liquidity, Competition and Markets, Brand, Reputation and Trust, Technology, Data Security and Privacy, Regulatory and Compliance, Safety, People, etc. Further, the Board discloses that three scenarios have been modelled, considered severe but plausible, that encompass these identified risks. None of these scenarios individually threaten the viability of the Company; therefore the compound impact of these scenarios has been evaluated as the most severe stress scenario.

Scenario	*Associated principal risks*	*Description*
Competitive pressure	• Brand, reputation and trust • Competition and markets • Customer	Failure to respond to fierce competition and changes in the retail market drives sustained significant like-for-like volume

		decline in core food categories with no offsetting price inflation, putting pressure on margins.
Data security or regulatory breach	• Brand, reputation and trust • Data security and data privacy • Political, regulatory and compliance	A serious data security or regulatory breach results in a significant monetary penalty and a loss of reputation among customers.
Brexit impact	• Competition and markets • Political, regulatory and compliance	Brexit continues to drive high UK domestic inflation and increased import costs from a weaker Sterling, compounded by new import duties and tariffs, with a consequential economic impact.

These scenarios assumed that external debt is repaid as it becomes due and also considered the results with and without the proposed Booker merger which is still subject to regulatory and shareholder approval and other conditions to a merger. The scenarios above are hypothetical and purposefully severe for the purpose of creating outcomes that have the ability to threaten the viability of the Group. In the case of these scenarios arising, various options are available to the Group in order to maintain liquidity so as to continue in operation such as: accessing new external funding early; more radical short-term cost reduction actions; and reducing capital expenditure. None of these actions are assumed in our current scenario modelling. Based on these severe but plausible scenarios, the Directors have a reasonable expectation that the Company will continue in operation and meet its liabilities as they fall due over the three-year period considered.

4.4 Risk & Opportunity Disclosures – An Indian Example

Let us study the annual report of a leading manufacturing company in India operating in the steel sector;

Risk & Opportunity Disclosure in the Annual Report (2017) is as under:

Risks and Opportunities

Risks

We are exposed to risks arising out of the dynamic macroeconomic environment as well as from internal business environment. These could adversely affect our ability to create value for our stakeholders.

Macroeconomic

- Over capacity and over-supply in steel industry
- High levels of imports
- Consolidation among competitors

- Local circumstances of geographies we operate in

Financial

- Volatility in financial markets and fluctuations in exchange rates
- Downgrading of credit rating of Company's securities
- Substantial amount of debt
- Restrictive covenants in financing agreements

Regulatory

- Predatory pricing
- Non-renewal of mining leases
- Non-availability of protective trade measures
- Regulatory and judicial actions

Climate Change

- International and domestic regulations relating to Green House Gas emissions

Operational

- Highly cyclical industry
- Inability to implement growth strategies
- Inherently hazardous industry
- Volatility in raw material prices
- Hostilities, terrorist attack or social unrest
- Failure of Information Technology Systems

Market Related

- Competition from alternate materials
- Product liability claims

People

- Continued services of Senior Management
- Unanticipated labour unrest

Opportunities

Setting benchmarks in the sector, we monitor and leverage opportunities presented by the external and internal environment.

- Capitalising the demand growth, due to urbanisation and needs of a young demography in

India, and developmental needs of other emerging economies

- Leveraging Supportive schemes of the Government such as the "Make in India" initiative
- Securing raw-material supplies by investing in mines which are in close proximity
- Innovating and adopting new technologies through Company-wide mobilisation of resources, implementation of pilots and capacity development
- Value realisation of by-products by exploring new areas of application, collaboration and potential customers
- Creating differentiation through acceleration of new product development, growing revenue from services & solutions and the B2C segment

5. DESCRIPTION AND EVALUATION OF FRAMEWORK FOR BOARD LEVEL CONSIDERATION OF RISK

Directors and boards need to ensure that policies, frameworks and governance arrangements are in place to ensue ethical conduct and decision making and effective risk governance and management. They must also make sure that their own conduct and the vision, mission, values, goals, objectives and priorities they set are conducive of them and do not undermine them.

The failure to address certain risks can prove catastrophic. Yet the taking of reasonable and calculated risks is at the heart of entrepreneurship. The courage to venture and explore is necessary for innovation if a company wants to progress. Hence, in relation to risk governance, directors need to achieve a balance between contending factors and there may be difficult choices to be made.

The following are some of the issues that directors may have to consider and the questions they should ask:

A degree of risk is inevitable in business operations. To obtain higher returns, innovate and secure market leadership one may need to adopt a higher risk strategy. Not innovating and being risk averse can result in the stagnation of the enterprise. A Board should establish and communicate its risk appetite and agree to the level of risk it is prepared to accept in different areas of corporate operation. Which stakeholder should be involved and how should they be engaged? Does the risk culture of the board match to that of the organization and its aspirations? If not, what changes are required and how might they be brought about?

What are the risk oversight functions of the board and how effectively are they being discharged? For example, is annual reporting of risk to shareholders fair and balanced? Would confidence accounting present a clearer picture? Within the governance structure, what arrangements have been made for risk governance which involves setting a strategy and policies for the management of risks and monitoring the performance of those to whom risk and security responsibilities are delegated?

Policies could cover the transfer of risk, such as whether or not to hedge or insure against certain risks, depending upon the costs and practicalities involved. They could establish criteria and thresholds for reporting and guiding management responses. Directors need to ensure effective processes and practices are in place for the identification and management of risks. How complex and comprehensive do these needs to be once the most likely and significant risks have been addressed?

Assumptions and business models should be periodically challenged. An assessment of the implications, consequences and dependencies of certain corporate strategies, policies and projects might reveal exposure and vulnerability. Corporate systems and processes need to be sufficiently resilient to be able to withstand the simultaneous materialization of multiple risks.

For example,

- Should an interruption in certain supplies occur, might just in time approaches result in shortages?
- What external and objective advice does the board receive in relation to risk?
- Overall, from the board perspective, what more needs to be done to build a risk resilient enterprise?

5.1 Corporate Risk Management

Are people within the organization and its supply chain aware of the diversity, incidence and severity of some categories of risk? For example, while overall relationships with customers might seem acceptable, what about particular relationships with key customers that are especially at risk? When addressing questions read the road ahead. A small account might have growth potential and could become strategically significant in the future.

Directors need to make sure that a management team and executives are not so focused upon listing and addressing individual risks that they overlook the interrelationship of different risk factors. An incident or development in one area can often have consequences elsewhere. For example, too many errors and exceptions can lead to overload and may bring down a system.

How well positioned is a company in respect of certain risks? Is the risk culture of the organization appropriate in relation to its activities, its operations and the opportunities it faces? A degree of balance is required. An excessively risk averse culture could prevent progress, but a step change increase in risk might be unsettling for some investors. High risk in certain areas can sometimes be balanced within a portfolio of activities and products by other items with lower risk profiles.

Processes and systems need to be adaptive as well as resilient. The nature and source of risks can change. As old ones are addressed so new ones may emerge. Are risk registers and management reports relating to risk over generalized? How realistic are they in relation to assessments of risk and planned corporate responses? Do they provide sufficient evidence and explanation to inform the board's own reporting of risk to shareholders?

5.2 Risk Management Frameworks, Approaches and Techniques

The following are the points to be considered by the Board :

- Has the management team established an effective risk prevention, management and control framework?
- Are people equipped with the skills, tools, techniques and other support they need to effectively operate it?
- Are the techniques used adequate in the situation and circumstances? How outward looking and inclusive does risk management need to be?
- Are the risks of major and strategic customers and business partners understood?
- Are business opportunities being identified for how the company might use its capabilities to help customers and others to mitigate, prevent or manage the risks they face? Does the company's risk management framework, policies and practices extend to its supply chain? In particular, are supplier risks and the risks of activities such as outsourcing and joint ventures assessed and managed? Does this involve collaborative action where relevant?
- Is the risk registering a living document? Are the prioritization of risks, mitigation measures, responsibilities and residual risks regularly reviewed? Are risk reports color coded to reflect likelihood of occurrence and impact?
- Is the direction of travel given?
- Are movements in relation to high priority "red rated" risks monitored by the board? Are there trigger points at which additional advice is sought and/or further resources deployed or other action taken? Are risk factors understood, appropriately categorized and mapped? Are the risk assessment criteria used reasonably and fair in the circumstances? Do the results of risk analysis inform business and management decisions? Are they inhibiting or supporting innovation and entrepreneurship?
- To whom should risk management responsibilities be delegated? Is there a Chief Risk Officer (CRO)? If so, how is the role of the CRO changing? What skills and experience are required by risk management professionals? What steps are taken to ensure that other people do not abdicate their responsibilities in relation to risk by leaving too much to the CRO and his or her team?
- Responsibilities for risk prevention, mitigation and management need to be delegated with care. Allocating them to particular individuals can sometimes led to others assuming that risks are "taken care of "and not themselves being alert to risks. A healthier approach may be to both delegate and ensure all staff reflect upon and help to address risks inherent in their roles and any corporate operations they are involved in. Any risk concerns they might have should be reported.
- What should be done to ensure that adopted approaches to risk management are current and that knowledge of changing risks and how they might best be addressed is up-to-date? Within the governance structure, how does the CRO relate to and collaborate with the audit, compliance, finance and legal teams? Are regular formal and/or informal meetings held to identify and discuss patterns, trends and common root causes?

Some boards regularly review schedules of risks notified by management, but rarely consider less predictable and external risks such as natural disasters, an act of terrorism or political instability. Does issue monitoring and management involve identifying and ranking developments in the eternal business environment and assessing their impact upon a company and its customers and supply chain? Do the results feed into risk management processes? Is the risk management team involved in deciding what action a company needs to take in response?

Certain unpredictable events might potentially have huge implications for companies and their activities. Corporations have had their assets and operations nationalized as a result of regime change. How resistant would offices and plants be to gales, floods or a tsunami or earthquake? How should a company cope with a terrorist attack, a pandemic, a sudden interruption to its supply chain, the loss of key staff, or a breakdown of law and order? Are contingency arrangements and backup and recovery plan in place? How resilient area company's finances and business model?

Companies that operate internationally sometimes find that the risk profiles of their local activities vary significantly. Particular involvements might expose them to geopolitical, economic, trade and other risks. These could range from a repudiation of debts to the sudden devaluation of currencies.

Some risks might be insurable at a cost, while others may need to be borne. How does a company assess unpredictable and/or uninsurable risks? Are these spread across a range of activities, or is there disproportionate exposure in certain markets? Are such risks and a distinctive risk management perspective taken into account in related and strategic decision making? For example, a strategy of focusing upon a core business has resulted in many companies being less diversified and having "more of their eggs in a single basket."

The continuing operation of many businesses as going concerns is dependent upon the effective operation of the utilities, the banking and financial system and the activities of governments, regulators and the legal system in the major markets within which they operate even in advanced countries, one cannot assume a banking and financial system will remain free of the challenges and loss of confidence that occurred in the period 2008-09 and which led to bank failures and bailouts.

A company's defenses are only as strong as the weakest link across the various networks to which its people and operations are connected. The internet of things is a frontier of opportunity for hackers. The issue is not whether a breach will occur, but how to limit the damage and recover quickly when a breach occurs.

Monitoring of emerging and mutating threats in relation to cyber security and fraud, is important., such as sharing of information about identified threats, breaches and responses with other organizations, regular review of cyber security and information governance policies, testing of threat scenarios and planned responses and contingency arrangements.

Checks to avoid money laundering, to avoid the loss of strategically significant intellectual property and unapproved access to personal information when data thefts occur/ means of information when in case of corporate data breach and compensation to those who suffer losses.

The speed with which defensive and anti-malware software, and data and system security, can be updated quickly as and when the need arises, is also a key question.

Further, whether adequate security, measures to a company's supply chain, corporate data that is held externally and corporate systems that are operated by thief parties? How secure are "working from home" equipment, customer support facilities and portable devices? What advice and assistance is given to staff and business partners in these areas?

The management/Board should also consider and review the usefulness of International frameworks and standards such as COSO's ERM framework, ISO 31000 standards, in enterprise risk management, in effective internal control and fraud deterrence and prevention, mitigation and management of risk.

5.3 Striking the Right Balance in Action and Reaction

Today, companies operate in an uncertain world. Management and Boards face multiple challenges and confront sensitive issues. Circumstances demand difficult decisions.

An organization that is prepared is able to respond quickly and aptly when unwelcome risks materialize. Having a moral compass and reacting in a proportionate, fair and responsible way can help a company and its board to restore confidence, maintain trust and build relationships with stakeholders. This can be achieved by listening to peers and learning, thereby building resilience and a balanced perspective. It is important to both recover and move forward while responding to incidents.

In a globally competitive market transition and with intense digitization taking place in the country, it is but necessary that risk appetite and risk mitigation measures are fully integrated with the business plans and policies so that the companies can benefit by correctly assessing their risk appetite and identifying and mitigating risk in time. Cyber Security has taken a new dimension and is important not only for the financial sector but for all sectors of the society. The majority of the cases reported so far under cyber security refer to financial institutions, alone, whereas cyber security for infrastructure sectors is equally important.

Today, Companies from different sectors of activities are seriously trying to put the risk management system in place as per the international standard. What is now needed is an emphasis on the effective implementation, thereby ensuring maximum benefits to the companies and "Enterprise risk management" emerging as the "Business differentiator".

May 20
MTP I
CS - 4

6. OECD GUIDELINES (PRINCIPLES) FOR CORPORATE GOVERNANCE

OECD

The Organization for Economic Corporation and Development (OECD) emphasized the importance of corporate governance and has developed set of principles for better corporate governance. The principles are intended to assist and improve the overall economic efficiency and bring more stability to the markets.

6. Principles

6.1 Ensuring the basis for an effective corporate governance framework

The corporate governance framework should be developed keeping in mind the macroeconomic changes, market situation and legislation requirements. Companies implementing corporate governance need to have a method of regularly reviewing and monitoring the objectives set as part of the framework. It should be ensured there is proper distribution of responsibilities among the authorities and it is clearly articulated. The management along with the responsibilities should be vested with the powers to take timely, transparent and correct decisions which are in line with the strategy defined by the company.

6.2 The rights and equitable treatment of shareholders and key ownership functions

Under the Companies Act, shareholders are classified under different categories like equity shareholders, preference shareholders etc. Shareholders can influence an organization's core functioning as they have right to participate and vote in general shareholders meeting, elect the board member, make amendments to company's organic documents, approval of extraordinary transactions, etc.

The Corporate governance framework ensures the equitable treatment of all the minority and foreign shareholders. Also, shareholders should have the appropriate redressal mechanism for any violation of their rights.

The acquisition of corporate control in the capital markets, mergers, and sales of substantial portions of corporate assets, should be clearly articulated and disclosed so that investors understand their rights and recourse.

6.3 Institutional investors, stock markets, and other intermediaries

The corporate governance framework should provide sound incentives throughout the investment chain and provide for stock markets to function in a way that contributes to good corporate governance.

6.4 The role of stakeholders in corporate governance

The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises. Further, the mechanism for employee participation should be encouraged. Also, stakeholders should have access to regular flow of information.

6.5 Disclosures and Transparency

May 18 Exam MCQ

An organization should have adequate disclosures regarding the following:

- The financial and operating results of the company.

- Company objectives and non-financial information.
- Major share ownership, including beneficial owners, and voting rights.
- Remuneration of members of the board and key executives, Information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board.
- Related party transactions.
- Foreseeable risk factors.
- Issues regarding employees and other stakeholders.
- Governance structures and policies, including the content of any corporate governance code or policy and the process by which it is implemented.

A strong disclosure regime can help to attract capital and maintain confidence in the capital markets.

An annual audit should be conducted by an independent, competent and qualified auditor in order to provide an external and objective assurance to the board and shareholders that the financial statements fairly represent the financial position and performance of the company in all material respects.

6.6 The responsibilities of the board

+ See page 3.3 - BOD responsibilities in risk appetite etc.

- The Board members should act in good faith, diligently and in the best interest of the company and the shareholders.
- The Board should also adopt high ethical standards.
- The Board should also review and guide corporate strategy, action plans, management policies and procedures etc.
- The Board should also monitor the company's governing practices and make required changes as and when required.
- Monitoring and executing the selection, remuneration and replacement of key executives.
- Ensuring a formal and transparent board nomination and election process.
- Monitor and manage conflicts of interest of management, misuse of corporate assets and abuse in related party transactions.
- Ensure the integrity of the company's accounting and financial reporting systems and make sure that appropriate systems are in place for risk management, financial and operating control.
- The Board should oversee the process of disclosure and communications.

(Source : OECD Website)