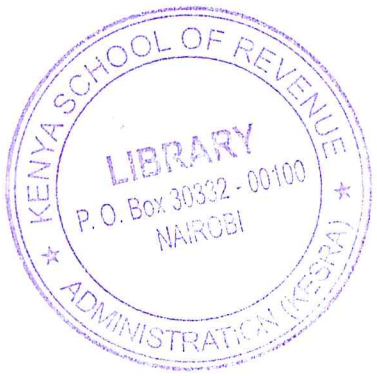
CORPORATE GOVERNANCE,RISK MANAGEMENT AND COMPLIANCE TRAINING MANUAL

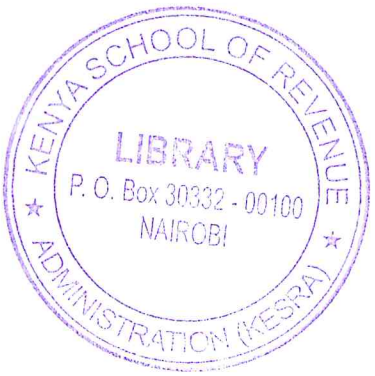


BY-DR. OLWENY TOBIAS, PhD

Contents

CHAPTER ONE

INTRODUCTION TO GOVERNANCE,RISK MANAGEMENT AND COMPLIANCE



1.0 INTRODUCTION TO GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

1.1 WHAT IS GRC?

GRC originated in the management consulting world several years ago. Technology firms and others quickly picked it up and used it to describe available services and software solutions. And while sometimes the term is used by compliance officers, risk officers, or internal auditors, it is rarely used by line executives or board members.

As for what it means, GRC is a combination of related although somewhat disparate concepts. The term governance traditionally has been used in the context of a company's board of directors. A definition of governance is the allocation of power among the board, management, and shareholders. But today the term is used also to encompass an array of actions taken by management in running a company, from senior levels down throughout the management ranks.

The R is for risk management. This term is used in many different ways, from a simple risk assessment to a full-blown enterprise risk management process. The C stands for compliance, initially meaning adherence to applicable laws and regulations, though many users now include adherence to internal company policies as well.

These pieces as "disparate" because GRC isn't really one end-to-end process that companies employ. While the elements of GRC relate to a company's strategic and other business objectives, they also pertain to activities and processes at different levels of an organization. Indeed, there's significant overlap, in that risk management can and should be designed to address compliance as well as other categories of a company's objectives.

1.2 GLOBAL FIRMS GLIMPSE ON WHY GRC MATTERS

Johnson & Johnson, for example. Back in the 1980s when the Tylenol scandal hit, J&J's culture of integrity and ethics drove a quick decision—to pull every last unit of Tylenol off drugstore shelves. The action was costly, but it positioned the company extremely well in the consumer marketplace, providing tangible dividends for decades to come. But the recent travails of J&J have been quite different. When Tylenol, Motrin, and other products of its McNeil Consumer Healthcare Products unit were found to make people sick, the company was accused of failing to report and investigate the matter, and its reputation has taken a hit.

Another company suffering charges of not doing the right thing is Toyota, which has had numerous recalls due to vehicle safety issues and allegations of failing to inform regulators. Toyota has lost market share to competitors, and we can surmise that while some customers simply are concerned about safety, others have stayed away due to anger at the company's failure to be forth-coming in reporting the dangers.

1.3 WHY CORPORATE GOVERNANCE?

Corporate or a Corporation is derived from the Latin term "corpus" which means a "body". Governance means administering the processes and systems placed for satisfying stakeholder expectation. The root of the word Governance is from 'gubernate', which means to steer. When combined, Corporate Governance means a set of systems, procedures, policies, practices, standards put in place by a corporate to ensure that relationship with various stakeholders is maintained in transparent and honest manner.

The phrase "corporate governance" describes "the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled within corporations. It encompasses the mechanisms by which companies, and those in control, are held to account."

Corporate governance is the broad term used to describe the processes, customs, policies, laws and institutions that direct the organizations and corporations in the way they act or administer and control their operations. It works to achieve the goal of the organization and manages the relationship among the stakeholders including the board of directors and the shareholders.

Corporate governance means to steer an organization in the desired direction by determining ways to take effective strategic decisions. It also deals with the accountability of the individuals through a mechanism which reduces the principal-agent problem in the organization.

Corporate Governance has a broad scope. It includes both social and institutional aspects. Corporate Governance encourages a trustworthy, moral, as well as ethical environment. In other words, the heart of corporate governance is transparency, disclosure, accountability and integrity. It is to be borne in mind that mere legislation does not ensure good governance. Good governance flows from ethical business practices even when there is no legislation.

Good corporate governance promotes investor confidence, which is crucial to the ability of entities listed to compete for capital. Good corporate governance is essential to develop added value to the stakeholders as it ensures transparency which ensures strong and balanced economic development. This also ensures that the interests of all shareholders (majority as well as minority shareholders) are safeguarded. It ensures that all shareholders fully exercise their rights and that the organization fully recognizes their rights.

1.4 SOME OF THE SALIENT ADVANTAGES OF CORPORATE GOVERNANCE ARE STATED HEREUNDER:

- ⇨ Good corporate governance ensures corporate success and economic growth.
- ⇨ Strong corporate governance maintains investors' confidence, as a result of which, company can raise capital efficiently and effectively.

- ⇨ There is a positive impact on the share price.
- ⇨ It provides proper inducement to the owners as well as managers to achieve objectives that are in interests of the shareholders and the organization.
- ⇨ Good corporate governance also minimizes wastages, corruption, risks and mismanagement.
- ⇨ It helps in brand formation and development.
- ⇨ It ensures organization in managed in a manner that fits the best interests of all.

1.5 NEED FOR CORPORATE GOVERNANCE

Corporate Governance is integral to the existence of the company. Corporate Governance is needed to create a corporate culture of transparency, accountability and disclosure.

(a) Corporate Performance

Improved governance structures and processes ensure quality decision-making, encourage effective succession planning for senior management and enhance the long-term prosperity of companies, independent of the type of company and its sources of finance. This can be linked with improved corporate performance- either in terms of share price or profitability.

(b) Enhanced Investor Trust

As individuals and institutions invest capital directly or through intermediary funds, they look to see if well-governed corporate boards are there to protect their interests. Investors who are provided with high levels of disclosure and transparency such as relating to data on matters such as pay governance, pay components, performance goals, and the rationale for pay

decisions etc. are likely to invest openly in those companies. On Apple's investor relations site, for example, the firm outlines its leadership and governance, including its executive team, its board of directors and also the firm's committee charters and governance documents, such as bylaws, stock ownership guidelines etc.

The consulting firm McKinsey surveyed and determined that global institutional investors are prepared to pay a premium of upto 40 percent for shares in companies with superior corporate governance practices.

(c) Better Access to Global Market

Good corporate governance systems attract investment from global investors, which subsequently leads to greater efficiencies in the financial sector. The relation between corporate governance practices and the increasing international character of investment is very important. International flows of capital enable companies to access financing from a much larger pool of investors. In order to reap the full benefits of the global capital market and attract long-term capital, corporate governance arrangements must be credible, well understood across borders and should adhere to internationally accepted principles. On the other hand, even if corporations do not rely primarily on foreign sources of capital, adherence to good corporate governance practices helps improve the confidence of domestic investors, reduces the cost of capital, enables good functioning of financial markets and ultimately leads to more stable sources of finance.

(d) Combating Corruption

Companies that are transparent, and have sound system that provide full disclosure of accounting and auditing procedures, allow transparency in all business transactions, provide environment where corruption would certainly fade out. Corporate Governance enables a corporation to -compete more efficiently and prevent fraud and malpractices within the organization.

(e) Easy Finance from Institutions

Several structural changes like increased role of financial intermediaries and institutional investors, size of the enterprises, investment choices available to investors, increased competition, and increased risk exposure have made monitoring the use of capital more complex thereby increasing the need of Good Corporate Governance. Evidences indicate that well-governed companies receive higher market valuations. The credit worthiness of a company can be trusted on the basis of corporate governance practiced in the company.

(f) Enhancing Enterprise Valuation

Improved management accountability and operational transparency fulfill investors' expectations and confidence on management and corporations, and in return, increase the value of corporations.

(g) Reduced Risk of Corporate Crisis and Scandals

Effective Corporate Governance ensures efficient risk mitigation system in place. A transparent and accountable system makes the Board of a company aware of the majority of the mask risks involved in a* particular strategy, thereby, placing various control systems in place to facilitate the monitoring of the related issues.

(h) Accountability

Investor relations are essential part of good corporate governance. Investors directly/ indirectly entrust management of the company to create enhanced value for their investment. The company is hence obliged to make timely disclosures on regular basis to all its shareholders in order to maintain good investor relation. Good Corporate Governance practices create the environment whereby Boards cannot ignore their accountability to these stakeholders.

CHAPTER TWO

GRC AND CULTURE

2.0 GRC AND CULTURE

The dictionary says culture is the professional atmosphere of a company, along with its values, customs, and traditions. A well-recognized risk management report adds substance and context:

An entity's strategy and objectives and the way they are implemented are based on preferences, value judgments, and management styles. Management's integrity and commitment to ethical values influence these preferences and judgments, which are translated into standards of behavior. Because an entity's good reputation is so valuable, the standards of behavior must go beyond mere compliance with law. Managers of well-run enterprises increasingly have accepted the view that ethics pays and ethical behavior is good business. . . .

Ethical behavior and management integrity are by-products of the corporate culture, which encompasses ethical and behavioral standards and how they are communicated and reinforced. Official policies specify what the board and management want to happen.

Corporate culture determines what actually happens, and which rules are obeyed, bent, or ignored. Top management starting with the CEO plays a key role in determining the corporate culture. As the dominant personality in an entity, the CEO often sets the ethical tone.

The effect of culture can be seen in any company, and German engineering company Siemens is worth a look. Reports say corruption at the company was far reaching, driven by a culture where employees believed bribes were not only acceptable, but implicitly encouraged. Reflecting on Siemens' reaction to the bribery scandal, a founder of Transparency International says: "There are new processes, new people, and new procedures, but that does not make a difference in the world unless there is a change in culture." An executive brought in from General Electric as the company's new anticorruption cop understood the challenges inherent in his new role, saying, "Healthy compliance cultures depend on a more values-based leadership, where people don't need to look at the rule book, where they know intuitively what the right thing to do is."

Johnson & Johnson, clearly a company that knew the right thing to do when the Tylenol package tampering scandal hit in 1982. Because the company's culture put the customer first regardless of short-term profit pressures management pulled the product from shelves and maintained and strengthened its positive reputation in the marketplace. Because of the shared values within the organization, the decision was a no brainer: There was no choice but to do the right thing for customers.

Critical to a corporate culture founded in integrity and ethical values is how people within the organization communicate with one another as well as with external parties. We all know there's a significant difference in providing technically accurate information versus communicating in a way that provides a true picture of what's really relevant.

2.1 HOW TO HANDLE CULTURE

First, all evidence points to flawed cultures, with tainted tone at the top set by the actions of senior executives. What may be surprising is that this occurred at brand-name institutions. Clearly, if it can happen there—as looks to be the case—it can happen anywhere.

Second, experience shows that how an organization reacts, in the form of public statements, can actually exacerbate a cultural problem. We understand that spin doctors—some well-meaning PR and legal professionals—try to keep the names of their companies from being further tarnished. But the truth is that few people, inside or outside the business, believe such statements. Perhaps most damaging is how company personnel react, with some thinking, "Well, management says this wasn't so bad, and things are fine now, so it's business as usual."

Top management must set the right tone not only with words, but also with its actions—before a crisis hits, and also when it does—along with sound organization and management processes. And second, spin is seen for what it is: It doesn't fool anyone, sends the wrong message, and is counterproductive both within and outside the organization.

The governance, risk, and compliance realm is not exempt from lousy communication, and indeed seems to lend itself to misunderstandings both inside a company and outside. This is about saying what we mean and meaning what we say. Using the right words is not about precision for its own sake, but about ensuring that we're communicating effectively. Because we need to be sure we're getting our messages across as intended, words really do matter.

CHAPTER THREE

FRAMEWORK OF CORPORATE GOVERNANCE

3.0 FRAMEWORK OF CORPORATE GOVERNANCE

Some of the important elements of good corporate governance are discussed as under:

1. Role and powers of Board

Good governance is decisively the manifestation of personal beliefs and values which configure the organizational values, beliefs and actions of its Board. The board is the primary direct stakeholder influencing corporate governance.

Directors are elected by shareholders or appointed by other board members and are tasked with making important decisions, such as corporate officer appointments, executive compensation and dividend policy. In some instances, board obligations stretch beyond financial optimization, when shareholder resolutions call for certain social or environmental concerns to be prioritized.

The Board as a main functionary is primary responsible to ensure value creation for its stakeholders. The absence of clearly designated role and powers of Board weakens accountability mechanism and threatens the achievement of organizational goals. Therefore, the foremost requirement of good governance is the clear identification of powers, roles, responsibilities and accountability of the Board, CEO, and the Chairman of the Board. The role of the Board should be clearly documented in a Board Charter.

2. Legislation

Clear and unambiguous legislation and regulations are fundamental to effective corporate governance. Legislation that requires continuing legal interpretation or is difficult to interpret on a d.ay-to-day basis can be subject to deliberate manipulation or inadvertent misinterpretation.

3. Management environment

Management environment includes setting-up of clear objectives and appropriate ethical framework, establishing due processes, providing for transparency and clear enunciation of responsibility and accountability, implementing sound business planning, encouraging business risk assessment, having right people and right skill for the jobs, establishing clear boundaries for acceptable behaviour, establishing performance evaluation measures and evaluating performance and sufficiently recognizing individual and group contribution.

4. Board skills

To be able to undertake its functions efficiently and effectively, the Board must possess the necessary blend of qualities, skills, knowledge and experience. Each of the directors should

make quality contribution. A Board should have a mix of the following skills, knowledge and experience:

- ⇨ Operational or technical expertise, commitment to establish leadership;
- ⇨ Financial skills;
- ⇨ Legal skills; and
- ⇨ Knowledge of Government and regulatory requirement.

5. Board appointments

To ensure that the most competent people are appointed on the Board, the Board positions should be filled through the process of extensive search. A well-defined and open procedure must be in place for reappointments as well as for appointment of new directors. Appointment mechanism should satisfy all statutory and administrative requirements. High on the priority should be an understanding of skill requirements of the Board particularly at the time of making a choice for appointing a new director. All new directors should be provided with a letter of appointment setting out in detail their duties and responsibilities.

The role of the board of directors was summarized by the King Report (a South African report on corporate governance) as:

- ⇨ to define the purpose of the company
- ⇨ to define the values by which the company will perform its

  daily duties to identify the stakeholders relevant to the

  company to develop a strategy combining these factors
- ⇨ to ensure implementation of this strategy.

6. Board induction and training

Directors must have a broad understanding of the area of operation of the company's business, corporate strategy and challenges being faced by the Board. Attendance at continuing education and professional development programmes is essential to ensure that directors remain abreast of all developments, which are or may impact on their corporate governance and other related duties.

7. Board independence

Independent Board is essential for sound corporate governance. This goal may be achieved by associating sufficient number of independent directors with the Board. Independence of directors would ensure that there are no actual or perceived conflicts of interest. It also ensures that the Board is effective in supervising and, where necessary, challenging the activities of management. The Board needs to be capable of assessing the performance of

managers with an objective perspective. Accordingly, the majority of Board members should be independent of both the management team and any commercial dealings with the company.

8. Board meetings

Directors must devote sufficient time and give due attention to meet their obligations. Attending Board meetings regularly and preparing thoroughly before entering the Boardroom increases the quality of interaction at Board meetings. Board meetings are the forums for Board decision-making. These meetings enable directors to discharge their responsibilities. The effectiveness of Board meetings is dependent on carefully planned agendas and providing relevant papers and material to directors sufficiently prior to Board meetings.

9. Code of conduct

It is essential that the organization's explicitly prescribed norms of ethical practices and code of conduct are communicated to all stakeholders and are clearly understood and followed by each member of the organization. Systems should be in place to periodically measure, evaluate and if possible recognise the adherence to code of conduct.

10. Strategy setting

The objectives of the company must be clearly documented in a long-term corporate strategy including an annual business plan together with achievable and measurable performance targets and milestones.

11. Business and community obligations

Though basic activity of a business entity is inherently commercial yet it must also take care of community's obligations. Commercial objectives and community service obligations should be clearly documented after approval by the Board. The stakeholders must be informed about the proposed and ongoing initiatives taken to meet the community obligations.

12. Financial and operational reporting

The Board requires comprehensive, regular, reliable, timely, correct and relevant information in a form and of a quality that is appropriate to discharge its function of monitoring corporate performance. For this purpose, clearly defined performance measures - financial and non-financial should be prescribed which would add to the efficiency and effectiveness of the organization.

The reports and information provided by the management must be comprehensive but not so extensive and detailed as to hamper comprehension of the key issues. The reports should be available to Board members well in advance to allow informed decision-making. Reporting should include status report about the state of implementation to facilitate the monitoring of the progress of all significant Board approved initiatives.

13. Monitoring the Board performance

The Board must monitor and evaluate its combined performance and also that of individual directors at periodic intervals, using key performance indicators besides peer review. The Board should establish an appropriate mechanism for reporting the results of Board's performance evaluation results.

14. Audit Committees

The Audit Committee is inter alia responsible for liaison with the management; internal and statutory auditors, reviewing the adequacy of internal control and compliance with significant policies and procedures, reporting to the Board on the key issues. The quality of Audit Committee significantly contributes to the governance of the company.

15. Risk management

Risk is an important element of corporate functioning and governance. There should be a clearly established process of identifying, analyzing and treating risks, which could prevent the company from effectively achieving its objectives. It also involves establishing a link between risk-return and resourcing priorities. Appropriate control procedures in the form of a risk management plan must be put in place to manage risk throughout the organization. The plan should cover activities as diverse as review of operating performance, effective use of information technology, contracting out and outsourcing.

3.2 EVOLUTION OF CORPORATE GOVERNANCE

The following theories elucidate the basis of evolution of corporate governance:

- ⇨ Agency Theory
- ⇨ Shareholder Theory
- ⇨ Stake Holder Theory
- ⇨ Stewardship Theory

a) Agency Theory

According to this theory, managers act as 'Agents' of the corporation. The owners set the central objectives of the corporation. Managers are responsible for carrying out these objectives in day-to-day work of the company. Corporate Governance is control of management through designing the structures and processes.

In agency theory, the owners are the principals. But principals may not have knowledge or skill for getting the objectives executed. Thus, principal authorizes the mangers to act as 'Agents' and a contract between principal and agent is made. Under the contract of agency, the agent

should act in good faith. He should protect the interest of the principal and should remain faithful to the goals.

In modern corporations, the shareholdings are widely spread. The management (the agent) directly or indirectly selected by the shareholders (the Principals), pursue the objectives set out by the shareholders. The main thrust of the Agency Theory is that the actions of the management differ from those required by the shareholders to maximize their return.

The principals who are widely scattered may not be able to counter this in the absence of proper systems in place as regards timely disclosures, monitoring and oversight. Corporate Governance puts in place such systems of oversight.

b) Stockholder/shareholder Theory

According to this theory, it is the corporation which is considered as the property of shareholders/ stockholders. They can dispose off this property, as they like. They want to get maximum return from this property.

The owners seek a return on their investment and that is why they invest in a corporation. But this narrow role has been expanded into overseeing the operations of the corporations and its mangers to ensure that the corporation is in compliance with ethical and legal standards set by the government. So the directors are responsible for any damage or harm done to their property i.e., the corporation. The role of managers is to maximise the wealth of the shareholders. They, therefore should exercise due diligence, care and avoid conflict of interest and should not violate the confidence reposed in them. The agents must be faithful to shareholders.

c) Stakeholder Theory

According to this theory, the company is seen as an input-output model and all the interest groups which include creditors, employees, customers, suppliers, local-community and the government are to be considered. From their point of view, a corporation exists for them and not the shareholders alone.

The different stakeholders also have a self interest. The interests of these different stakeholders are at times conflicting. The managers and the corporation are responsible to mediate between these different stakeholders interest. The stake holders have solidarity with each other. This theory assumes that stakeholders are capable and willing to negotiate and bargain with one another. This results in long term self interest.

The role of shareholders is reduced in the corporation. But they should also work to make their interest compatible with the other stake holders. This requires integrity and managers play an important role here. They are faithful agents but of all stakeholders, not just stockholders.

d) Stewardship Theory

The word 'steward' means a person who manages another's property or estate. Here, the word is used in the sense of guardian in relation to a corporation, this theory is value based. The managers and employees are to safeguard the resources of corporation and its property and interest when the owner is absent. They are like a caretaker. They have to take utmost care of the corporation. They should not use the property for their selfish ends. This theory thus makes use of the social approach to human nature.

The managers should manage the corporation as if it is their own corporation. They are not agents as such but occupy a position of stewards. The managers are motivated by the principal's objective and the behavior pattern is collective, pro-organizational and trustworthy. Thus, under this theory, first of all values as standards are identified and formulated. Second step is to develop training programmes that help to achieve excellence. Thirdly, moral support is important to fill any gaps in values.

3.3 CONCEPT OF MANAGEMENT VS. OWNERSHIP

The shareholders vest control of the business in the board of directors, who employ specialist management to run the business and return the profits of the business back to the shareholders.

Company law's central dilemma has been the separation of ownership and control in companies. On one side are shareholders, the ostensible owners; on the other side are corporate officers, the shareholders' ostensible fiduciaries. Between them is the board of directors.

Theoretically, shareholders own the company and hence the company ought to be work according to the dictates of the shareholders. However, it is not practically possible for each shareholder to participate in the decision making process on a day-to-day basis. Further shareholders generally cannot know and manage the full details of a corporation's business (nor do many wish to), they elect a board of directors to make broad corporate policy.

Companies allow for the separation of ownership and management. That means that owners do not need to be managers and managers do not need to be owners. In most small corporations, the owners typically manage

3.4 OECD PRINCIPLES OF CORPORATE GOVERNANCE

Good corporate governance is not an end in itself. It is a means to create market confidence and business integrity, which in turn is essential for companies that need access to equity capital for long term investment. Access to equity capital is particularly important for future oriented growth companies and to balance any increase in leveraging. The updated G20/OECD Principles of Corporate Governance (the Principles) therefore provide a very timely and

tangible contribution to the G20 priority in 2015 to support investment as a powerful driver of growth.

The Principles are also about inclusiveness. Today, millions of households around the world have their savings in the stock market, directly or indirectly. And publicly listed companies provide for more than 200 million jobs. The Principles also address the rights of these stakeholders and their ability to participate in corporate wealth creation.

The Principles were originally developed by the OECD in 1999 and further updated in 2004. Following the request by the G20 Finance Ministers and Central Bank Governors at their meeting on 9-10 February 2015 in Istanbul, a draft of the revised Principles was presented and discussed at the G20/OECD Corporate Governance Forum in Istanbul on 10 April 2015 where they found broad support among participants. The Principles were subsequently presented at the May and August 2015 meetings of the G20 Investment and Infrastructure Working Group. The OECD Council adopted the Principles on 8 July 2015. The Principles are now submitted to the G20 Finance Ministers and Central Bank Governors meeting in Ankara 4-5 September for endorsement as joint G20/OECD Principles and transmission to the G20 Leaders Summit in November 2015.

3.5 THE PRINCIPLES PROVIDE GUIDANCE THROUGH RECOMMENDATIONS AND ANNOTATIONS ACROSS SIX CHAPTERS.

3.5.1 Ensuring the basis for an effective corporate governance framework:

The corporate governance framework should promote transparent and fair markets, and the efficient allocation of resources. It should be consistent with the rule of law and support effective supervision and enforcement:

- ⇨ The corporate governance framework should be developed with a view to its impact on overall economic performance, market integrity and the incentives it creates for market participants and the promotion of transparent and well-functioning markets.
- ⇨ The legal and regulatory requirements that affect corporate governance practices should be consistent with the rule of law, transparent and enforceable.
- ⇨ The division of responsibilities among different authorities should be clearly articulated and designed to serve the public interest.
- ⇨ Stock market regulation should support effective corporate governance
- ⇨ Supervisory, regulatory and enforcement authorities should have the authority, integrity and resources to fulfill their duties in a professional and objective manner. Moreover, their rulings should be timely, transparent and fully explained.
- ⇨ Cross-border co-operation should be enhanced, including through bilateral and multilateral arrangements for exchange of information.

3.5.2 The rights and equitable treatment of shareholders and key ownership functions:

The corporate governance framework should protect and facilitate the exercise of shareholders' rights and ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights:

- Basic shareholder rights should include the right to:
- secure methods of ownership registration, convey or transfer shares;
- obtain relevant and material information on the corporation on a timely and regular basis;
- participate and vote in general shareholder meetings;
- elect and remove members of the board; and 6) share in the profits of the corporation.

Shareholders should be sufficiently informed about, and have the right to approve or participate in, decisions concerning fundamental corporate changes such as:

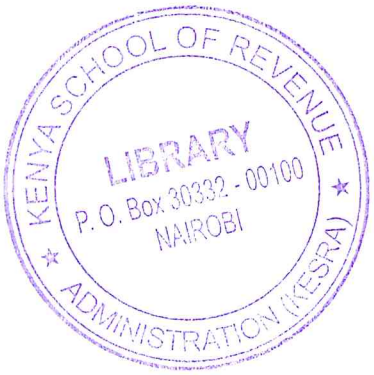
- amendments to the statutes, or articles of incorporation or similar governing documents of the company;
- the authorization of additional shares; and
- extraordinary transactions, including the transfer of all or substantially all assets, that in effect result in the sale of the company.

Shareholders should have the opportunity to participate effectively and vote in general shareholder meetings and should be informed of the rules, including voting procedures, that govern general shareholder meetings:

- Shareholders should be furnished with sufficient and timely information concerning the date, location and agenda of general meetings, as well as full and timely information regarding the issues to be decided at the meeting.
- Processes and procedures for general shareholder meetings should allow for equitable treatment of all shareholders. Company procedures should not make it unduly difficult or expensive to cast votes.
- Shareholders should have the opportunity to ask questions to the board, including questions relating to the annual external audit, to place items on the agenda of general meetings, and to propose resolutions, subject to reasonable limitations.
- Effective shareholder participation in key corporate governance decisions, such as the nomination and election of board members, should be facilitated. Shareholders should be able to make their views known, including through votes at shareholder meetings, on the remuneration of board members and/or key executives, as

applicable. The equity component of compensation schemes for board members and employees should be subject to shareholder approval.

- Shareholders should be able to vote in person or in absentia, and equal effect should be given to votes whether cast in person or in absentia.
- Impediments to cross border voting should be eliminated.
- Shareholders, including institutional shareholders, should be allowed to consult with each other on issues concerning their basic shareholder rights as defined in the Principles, subject to exceptions to prevent abuse.
- All shareholders of the same series of a class should be treated equally. Capital structures and arrangements that enable certain shareholders to obtain a degree of influence or control disproportionate to their equity ownership should be disclosed.
- Within any series of a class, all shares should carry the same rights. All investors should be able to obtain information about the rights attached to all series and classes of shares before they purchase. Any changes in economic or voting rights should be subject to approval by those classes of shares which are negatively affected.
- The disclosure of capital structures and control arrangements should be required.
- Related-party transactions should be approved and conducted in a manner that ensures proper management of conflict of interest and protects the interest of the company and its shareholders.
- Conflicts of interest inherent in related-party transactions should be addressed.



- Members of the board and key executives should be required to disclose to the board whether they, directly, indirectly or on behalf of third parties, have a material interest in any transaction or matter directly affecting the corporation.
- Minority shareholders should be protected from abusive actions by, or in the interest of, controlling shareholders acting either directly or indirectly, and should have effective means of redress.
- Abusive self dealing should be prohibited.
- Markets for corporate control should be allowed to function in an efficient and transparent manner.
- The rules and procedures governing the acquisition of corporate control in the capital markets, and extraordinary transactions such as mergers, and sales of substantial portions of corporate assets, should be clearly articulated and disclosed so that investors understand their rights and recourse. Transactions should occur at transparent prices and under fair conditions that protect the rights of all shareholders according to their class.
- Anti-take-over devices should not be used to shield management and the board from accountability.

3.5.3 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:

- Institutional investors acting in a fiduciary capacity should disclose their corporate governance and voting policies with respect to their investments, including the procedures that they have in place for deciding on the use of their voting rights.
- Votes should be cast by custodians or nominees in line with the directions of the beneficial owner of the shares.
- Institutional investors acting in a fiduciary capacity should disclose how they manage material conflicts of interest that may affect the exercise of key ownership rights regarding their investments.
- The corporate governance framework should require that proxy advisors, analysts, brokers, rating agencies and others that provide analysis or advice relevant to decisions by investors, disclose and minimise conflicts of interest that might compromise the integrity of their analysis or advice.

- Insider trading and market manipulation should be prohibited and the applicable rules enforced.
- For companies who are listed in a jurisdiction other than their jurisdiction of incorporation, the applicable corporate governance laws and regulations should be clearly disclosed. In the case of cross listings, the criteria and procedure for recognizing the listing requirements of the primary listing should be transparent and documented.
- Stock markets should provide fair and efficient price discovery as a means to help promote effective corporate governance.

3.5.4 The role of stakeholders in corporate governance:

The corporate governance framework should recognise 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:

- The rights of stakeholders that are established by law or through mutual agreements are to be respected.
- Where stakeholder interests are protected by law, stakeholders should have the opportunity to obtain effective redress for violation of their rights.
- Mechanisms for employee participation should be permitted to develop.
- Where stakeholders participate in the corporate governance process, they should have access to relevant, sufficient and reliable information on a timely and regular basis.
- Stakeholders, including individual employees and their representative bodies, should be able to freely communicate their concerns about illegal or unethical practices to the board and to the competent public authorities and their rights should not be compromised for doing this.
- The corporate governance framework should be complemented by an effective, efficient insolvency framework and by effective enforcement of creditor rights.

3.5.5 Disclosure and transparency:

The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company:

Disclosure should include, but not be limited to, material information on:

- 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.
- Information should be prepared and disclosed in accordance with high quality standards of accounting and financial and non-financial reporting.
- An annual audit should be conducted by an independent, competent and qualified, auditor in accordance with high-quality auditing standards 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.
- External auditors should be accountable to the shareholders and owe a duty to the company to exercise due professional care in the conduct of the audit.
- Channels for disseminating information should provide for equal, timely and cost-efficient access to relevant information by users.

3.5.6 The responsibilities of the board:

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders:

- Board members should act on a fully informed basis, in good faith, with due diligence and care, and in the best interest of the company and the shareholders.
- Where board decisions may affect different shareholder groups differently, the board should treat all shareholders fairly.
- The board should apply high ethical standards. It should take into account the interests of stakeholders.
- The board should fulfill certain key functions, including:

- Reviewing and guiding corporate strategy, major plans of action, risk management policies and procedures, annual budgets and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions and divestitures.
- Monitoring the effectiveness of the company's governance practices and making changes as needed.
- Selecting, compensating, monitoring and, when necessary, replacing key executives and overseeing succession planning.
- Aligning key executive and board remuneration with the longer term interests of the company and its shareholders.
- Ensuring a formal and transparent board nomination and election process.
- Monitoring and managing potential conflicts of interest of management, board members and shareholders, including misuse of corporate assets and abuse in related party transactions.
- Ensuring the integrity of the corporation'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.
- Overseeing the process of disclosure and communications.

- The board should be able to exercise objective independent judgment on corporate affairs.
  - Boards should consider assigning a sufficient number of nonexecutive board members capable of exercising independent judgment to tasks where there is a potential for conflict of interest. Examples of such key responsibilities are ensuring the integrity of financial and non-financial reporting, the review of related party transactions, nomination of board members and key executives, and board remuneration.
  - Boards should consider setting up specialised committees to support the full board in performing its functions, particularly in respect to audit, and, depending upon the company's size and risk profile, also in respect to risk management and remuneration. When committees of the board are established, their mandate, composition and working procedures should be well defined and disclosed by the board.

- Board members should be able to commit themselves effectively to their responsibilities.
- Boards should regularly carry out evaluations to appraise their performance and assess whether they possess the right mix of background and competences.

- In order to fulfill their responsibilities, board members should have access to accurate, relevant and timely information.
- When employee representation on the board is mandated, mechanisms should be developed to facilitate access to information and training for employee representatives, so that this representation is exercised effectively and best contributes to the enhancement of board skills, information and independence.

CHAPTER FOUR

CORPORATE GOVERNANCE IN KENYA

4.0 CORPORATE GOVERNANCE IN KENYA

4.1AUTHORITY AND DUTIES OF SHAREHOLDERS

Shareholders of the company shall jointly and severally protect, preserve and actively exercise the supreme authority of the company in general meetings. They have a duty, jointly and severally, **to exercise that supreme authority to:**

- ⇨ Ensure that only competent and reliable persons who can add value to the company are elected or appointed to the Board of Directors;
- ⇨ Ensure that the Board of Directors is constantly held accountable and responsible for the efficient and effective governance of the company.
- ⇨ Change the composition of a Board of Directors that does not perform to expectation or in accordance with the mandate of the corporation.

4.2 LEADERSHIP OF THE COMPANY

The Board of Directors shall exercise leadership, enterprise, integrity and sagacious judgment in directing the company so as to achieve continuing prosperity for the company and shall always act in the best interests of the company.

4.3 ROLE AND FUNCTIONS OF THE BOARD

The Board of Directors shall exercise all the powers of the company subject only to the limitations contained in the law and the memorandum and articles of incorporation.

In this regard, it is expected that the Board of Directors shall fulfill the following functions:

- ⇨ Exercise leadership, enterprise, integrity and sound judgments in directing the corporation so as to achieve continuing prosperity and to act in the best interest of the enterprise while respecting the principles of transparency and accountability;
- ⇨ Ensure that through a managed and effective process, board appointments are made that provide a mix of proficient directors, each of whom is able to add value and bring independent judgment to bear on the decision-making process;
- ⇨ **Determine the corporation's purpose and values, determine the strategy to achieve its** purpose and to implement its values in order to ensure it survives and thrives, and ensure that procedures and practices are in place that protect **the corporation's assets and** reputation;
- ⇨ Monitor and evaluate the implementation of strategies, policies, management performance criteria and business plans;
- ⇨ Ensure that the corporation complies with all relevant laws, regulations and codes of best business practice;

- ⇨ Ensure that the corporation communicates with shareholders and other stakeholders effectively;
- ⇨ Serve the legitimate interest of the shareholders and the corporation and account to them fully;
- ⇨ Identify the corporation's internal and external stakeholders and agree on a policy, or policies determining how the corporation should relate to them;
- ⇨ Ensure that no one person or a block of persons has unfettered power and that there is an appropriate balance of power and authority on the board which is, inter alia, usually reflected by separating the roles of the Chief Executive Officer and Chairman, and by having a balance between executive and non-executive directors;
- ⇨ Regularly review processes and procedures to ensure the effectiveness of its internal systems of control, so that its decision-making capability and the accuracy of its reporting and financial results are maintained at a high level at all times;
- ⇨ Regularly assess its performance and effectiveness as a whole, and that of the individual directors, including the Chief Executive Officer;
- ⇨ Appoint the Chief Executive Officer and at least participate in the appointment of senior management, ensure the motivation and protection of intellectual capital intrinsic to the corporation, ensure that there is adequate training in the corporation for management and employees, and a succession plan for senior management;

- ⇨ Ensure that all technology and systems used in the corporation are adequate to properly run the business and for it to remain effectively competitive;
- ⇨ Identify key risk areas and key performance indicators of the business and monitor these factors;
- ⇨ Ensure annually that the corporation will survive, thrive and continue as a viable going concern.

In Order to fulfill these functions, the Board of Directors shall:

- ⇨ Meet regularly and retain full and effective control over the company.
- ⇨ Evolve procedures for the selection and removal of individual directors (including the chairman and chief executive) to facilitate regular alteration of the mix and composition of the Board ensuring relevant rejuvenation.
- ⇨ Define the limits of authority of the Chief Executive and other top executives.
- ⇨ Compile and communicate company policies, strategies etc. covering style of operation; external and internal relationships; markets and business; required rates of return and performance standards; growth and change policies; planning and budgetary procedures.
- ⇨ Review and approve strategic plans and arrange that meaningful plans are produced at all levels on an on-going basis covering the longest realistic time-scale.

- ⇨ Determine the (actual and potential) total resources of the company in terms of men, money, methods, equipment etc. and market position, and allocate these by unit and time-scale, defining closely what returns are expected and when.
- ⇨ Devote sufficient time to their responsibilities.
- ⇨ Structure and organize the company.
- ⇨ Monitor management performance.
- ⇨ Map out the mechanisms for internal and external liaison and communications.
- ⇨ **Define how the Board will operate including:**
    - What information or reports it requires on a monthly or quarterly basis.
    - How, with what data, and by what means, it will constantly monitor management performance and the financial progress of the company.
    - How it will evaluate its own performance at least once every year.
- ⇨ Ensure that the company is properly managed and for the attainment of lawful objectives.
- ⇨ Ensure that the company's affairs are not managed or conducted in a manner oppressive to any of its shareholders or for fraudulent purposes.
- ⇨ Ensure that the company complies with all statutory requirements.

4.3.1 Composition of the Board

The Board shall include a balance of executive and non-executive directors (including independent non-executive directors) such that no individual or group of individuals or interests can dominate its decision taking.

The Board shall be chaired by an independent director who is not managing the company.

There are two key tasks at the top of the company, that of running the Board and that of the Chief Executive responsible for running the company. Therefore as a general rule, there is a clear division of these roles to ensure that a balance of power and authority is maintained, and that no one individual has unfettered powers of decision. Where these roles are combined, the reasons thereof shall be publicly explained.

The roles of the Chairman are:

To lead the Board;
To chair meetings of the Board and members, ensuring order, proper conduct of meetings, affording participants a reasonable opportunity to speak, ensuring decisions are fairly made, deciding on technicalities and to cast the deciding vote in case of ties;
To organize and facilitate a balance of internal and external relationships, and
To facilitate effective Board management.

Independent non- executive directors shall be independent of management, and free from any business or other relationship which would interfere with the exercise of their ability to bring an independent judgment to bear on issues of strategy, performance, resources, key appointments and standards of conduct. Independent non-executive directors shall be relied upon in matters where there is potential for conflict of interest e.g.:

- ⇨ Financial reporting (Audit Committee)
- ⇨ Nomination and remuneration of directors
- ⇨ Evaluation of Board performance

It is suggested that:

- ⇨ The company must contain at least one third of its members as non-executive directors.
- ⇨ Persons with full time employment in any company or organization should not hold many non-executive directorships elsewhere [indicatively, not more that two.
- ⇨ Persons without full-time employment in one organization (professional directors, consultants etc.) should not hold more than ten non-executive directorships.
- ⇨ Executives from subsidiaries, the parent company or any other of its acquisitions cannot become non-executive directors on the parent company.
- ⇨ Suppliers, direct customers or other trading associates of the company cannot become non-executive directors of the company.
- ⇨ Persons with prior professional or social relationships with directors of the company cannot become non-executives directors in the company.

The company must always have a qualified, competent, fit and proper company secretary who must have the requisite knowledge and experience necessary to undertake the statutory duties and responsibilities of the post and advise the Board. The Company Secretary should have responsibility for ensuring that the company adheres to this code of best practice for corporate governance.

4.3.2 Appointments to the Board

There will be formal and transparent procedures for nomination and appointment of new directors to the Board.

In this regard:

- ⇨ There shall be set up a search and nominations committee of the Board.
- ⇨ The Board of Directors will formally review its composition and performance at least once every year to ensure that:
  - The mix of membership is appropriate and compatible with the needs of the Board and company.
  - Every non-executive director commits adequate time to his responsibilities and contributes effectively. *[Each non-executive director should commit at least two*

days per month to his duties as a director and the actual time spent shall be recorded and reflected in the annual report].

- ⇨ Based on the priority needs of the Board and the Company, the nominations committee will recommend to the Board qualified, competent fit and proper persons to be nominated for election to the Board.
- ⇨ All directors shall be required to submit themselves for re-election at regular intervals and at least once every three years.
- ⇨ Service contracts of Executive Directors shall not exceed three years but these are renewable with the approval of shareholders on the recommendation of the Board.

4.3.3 Directors' Remuneration

In order to avoid potential conflict of interest, the Board of directors shall set up independent remuneration committee to determine the remuneration of respective individual executive directors. The committee shall make a report to the shareholders every year.

The Committee shall:

- ⇨ Establish a formal and transparent procedure for developing policy on executive remuneration and for fixing the remuneration packages of individual executive directors.
- ⇨ Ensure that the level of remuneration shall be sufficient to attract and retain the quality and calibre of directors needed to run the company successfully while the make up should be so structured as to link corporate and individual performance.
- ⇨ **Ensure that the company's annual report contains a statement of the remuneration** policy and details of the remuneration and benefits of each director, including family-related benefits.

4.3.4 Disclosures of Information by Directors

On first appointment and at regular intervals (at least once every year), or at any time when circumstances change, all directors shall, in good faith, disclose to the Board for recording and disclosure to the external auditors, **any business or other interests that are likely to create a potential conflict of interest, including:**

- ⇨ All business interests (direct or indirect) in any other company, partnership or other business venture.
- ⇨ Membership in trade, business or other economic organizations.
- ⇨ Their shareholding, share options and/or other interest in the company.
- ⇨ Any interest (direct or indirect) in any transaction with the company.
- ⇨ Any gifts, monies, commissions, benefits or other favours extended or received from whatsoever party in respect of or in relation to any business dealings with the company.

At any time when a director resigns or is removed from office before the expiry of his term, he shall disclose to the company's external auditors and if necessary to the shareholders (if the reason for removal or resignation is refusal to compound fraud, corruption or other activities or behaviour incompatible with the shareholders' interests) the reasons for his resignation or removal.

4.3.5 Supply of Information to Directors

For Board members to exercise informed, intelligent, objective and independent judgments on corporate affairs, they shall have access to accurate, relevant and timely information. In this regard:

- ⇨ There shall be established a formal procedure to enable independent directors to take professional advice on any matter pertinent to their functions if and where they deem it necessary and at the company's expense but subject always to the limitations, restrictions and conditions stipulated by the Board.
- ⇨ All directors shall have unlimited access to the advice and services of the Company Secretary who has a statutory duty to advice the Board on maters of procedures, rules and regulations, and to any other professional officer of the company.
- ⇨ It is the duty of every director to demand and obtain any information he deems critical to the performance of his duties as a director.

4.3.6 Directors' Training and Development

The weighty responsibilities placed upon a director, the level of commitment called for and the fast-changing corporate environment dictates that the company must now increasingly prepare those expected to assume these roles.

It is therefore recommended that all directors shall receive some formal training on their role, duties, responsibilities and obligations as well as Board practices and procedures on first appointment. This is particularly critical for those with no previous Board experience.

It is desirable that all company directors are exposed, at least once every three years, on matters relevant to legal reforms, corporate governance, changing corporate environment, business/commercial risks and other matters that may be of interest in the execution of their role.

It is currently suggested that initial training of directors shall cover, inter alia:

- ⇨ Role, duties and responsibilities of the Board and directors.

- ⇨ Rights and obligations of a director.
- ⇨ Statutory liabilities and duties of a director under criminal and company law.
- ⇨ Board practices and procedures.
- ⇨ Corporate strategy and organization.
- ⇨ Disclosure and communication policies.
- ⇨ Financial management systems, internal control procedures and internal audit.
- ⇨ External Audit and the Board.
- ⇨ The Corporate Environment.
- ⇨ Performance targeting, monitoring and evaluation.
- ⇨ Risk management.
- ⇨ Information Technology and information to the Board.
- ⇨ Any other matters of interest to the Board.

4.3.7 Accounts: Audit and Disclosure

It is the statutory duty of directors, jointly and severally, to cause to be kept proper and accurate books of accounts in respect to all sums of money received and expended by the company, and the matters in respect of which receipt or expenditure takes place; all sales and purchases by the company; and of all the assets and liabilities of the company, as necessary to give with reasonable accuracy at anytime, the financial position of the company at that time; and to lay before the company's annual general meeting, a profit and loss account and a balance sheet reflecting a true and fair view of the profit or loss of the company and of the state of affairs of the company.

4.3.8 Consequently the Board of Directors is responsible for:

- ⇨ Maintaining adequate systems of financial management and internal control over the company, including procedures designed to minimize the risk of fraud.
- ⇨ Ensuring the integrity and adequacy of the accounting and financial systems.
- ⇨ Ensuring that qualified, competent, fit and proper persons are employed to undertake accounting and financial responsibilities.
- ⇨ Ensuring that the company complies with the accounting standards applicable.
- ⇨ The Board shall present to the shareholders balanced and understandable assessment of the company's position and prospects at least once a every year and preferably every six months.
- ⇨ It shall also establish formal and transparent arrangements for maintaining an "arm's length" relationship with the external auditors, and ensure that there is timely and

accurate disclosure to the shareholders of any information that would materially affect either the value or worth of their investment or earnings there-from including:

- ⇨ Material changes in ownership structures, take over bids, shareholders arrangements, acquisitions, mergers, script splits and consolidations, or other arrangements.
- ⇨ Material information on:
    - Company objectives
    - Financial and operating results
    - Material issues relevant to governance structures and policies
    - Changes or factors affecting members of the Board or key executives.
    - **Directors' remuneration and benefits.**
    - Government policies or legislative amendments
    - Technological or other material issues affecting sources of raw materials, suppliers etc.

All information affecting the shareholders shall be prepared, audited, [where appropriate] and disclosed in accordance with high quality standards of financial and non-financial disclosure and objectivity.

4.4 EXTENSION OF SCOPE AND DUTIES OF AUDITORS

The Board of Directors shall ensure that persons who are qualified, reliable and independent of the Board and management are appointed as auditors. In light of developments elsewhere, the Board shall endeavour to:

- ⇨ **Extend the definition and scope of audit to cover:-**

"To provide an independent opinion to those with interest in the company that they have received from those responsible for the direction and management of the company an adequate account of:

- **The proper conduct of the company's affairs;**
- **The company's financial performance and position;**
- Future risks.

- ⇨ Facilitate an extension of Auditors duties in regard to:
    - Reporting on whether the company has financial and other risk management controls
    - Evaluating and reporting on aspects of propriety and efficiency
    - Reporting directly to the Board, regulatory authorities and shareholders as appropriate, when illegal acts are discovered and to monitor basic ethical behaviour particularly in regard to the public interest
- ⇨ Enhance the independence of the auditor from the Board and management;
- ⇨ Extend the liability of Auditors to third parties.

4.5 THE ROLE OF AUDIT COMMITTEES

A separate audit committee enables a Board to delegate to a sub-committee the responsibility for a thorough and detailed review of Audit matters, enables the non-executive directors to contribute an independent judgment and play a positive role in an area for which they are particularly fitted, and offers the auditors a direct link with the non-executive directors. The appointment of a properly constituted Audit Committee shall therefore be an important step in raising standards of corporate governance.

- ⇨ The Board shall establish an Audit Committee composed of independent non-executive directors to keep under review the scope and results of audit, its effectiveness and the independence and objectivity of the auditors.

- ⇨ The Audit Committee shall be given written terms of reference which deal adequately with their membership, authority and duties and shall meet at least twice a year.
- ⇨ The Audit Committee will:
- ⇨ **Review the half year and annual financial statements before submission to the Board focusing particularly on:-**
    - Changes in accounting policies
    - Significant adjustments arising from the audit
    - Major judgmental areas
    - Compliance with accounting standards, disclosure and legal requirements, and
    - Subject the financial statements to independent critical appraisal
- ⇨ Consider appointment, remuneration and the resignation or dismissal of external auditors.
- ⇨ Discuss and agree on the scope, nature and priorities of audit.
- ⇨ Discuss with external auditors any reservations and problems arising in the course of audit and any audit management letters and management responses prior to the issuance of the audit certificate.
- ⇨ Review and discuss with the external auditors aspects relevant to internal control procedures, risk management and internal audit.
- ⇨ Review major findings on internal audit and investigations and consider management response or actions thereto.
- ⇨ Undertake such other duties or function as may be assigned by the Board which are relevant to audit and investigations.

4.6 OTHER ASPECTS RELEVANT TO THE COLLECTIVE AND INDIVIDUAL ROLES OF DIRECTORS

In order to enable every director to be more clearly aware of their collective and individual accountability and liability in regard to their acts of commission and omission, the company shall provide every director with a detailed manual covering, *inter alia,* the following:

Accountability of Directors jointly and severally to ensure that:

- ⇨ They provide direction to the company.
- ⇨ They put in place independent and viable mechanisms to evaluate performance of the company and management.
- ⇨ They appoint competent, qualified and able executives.
- ⇨ They evaluate and manage risk.
- ⇨ They manage effectively and efficiently all stakeholder relationships and reconcile any potential conflict of interest.
- ⇨ They account for stewardship [efficient and effective use of entrusted resources] for the maximum benefit of shareholders.
- ⇨ They ensure that the Company operates within the law and the legality of transactions.
- ⇨ They ensure that the company operates within ethical guidelines that enhance integrity, social accountability and the reputation and credibility of the company.

Liability of directors jointly and severally in the context of:

- ⇨ Criminal and penal laws relevant to companies.
- ⇨ Fiduciary trust and agency.
- ⇨ Fraudulent trading with an insolvent company.
- ⇨ Fraudulent promotion or misrepresentation in the promotion of the company.
- ⇨ Personal liability for fraud, secret profits, corruption and bribery.

4.7 RIGHTS OF SHAREHOLDERS

All shareholder rights shall be recognized, respected and protected.

Basic shareholder rights include:

- ⇨ To secure methods of ownership registration;
- ⇨ To convey or transfer shares;
- ⇨ To obtain relevant information on the corporation on a timely and regular basis;
- ⇨ To participate and vote in general shareholder meetings;
- ⇨ To elect members of the Board; and

- ⇨ To share in the residual profits of the company.

Shareholders have the right to participate in, and to be sufficiently informed on, decisions concerning fundamental corporate changes such as:

- ⇨ Amendments to the statutes, or articles of incorporation or similar governing documents of the company;
- ⇨ The authorization of additional shares; and
- ⇨ Extra-ordinary transactions that in effect result in the sale of the company

Shareholders shall have the opportunity to participate effectively and vote in general shareholder meetings and shall be informed of the rules, including voting procedures that govern general shareholder meetings:

- ⇨ Shareholders shall be furnished with sufficient and timely information concerning the date, location and agenda of general meetings, as well as full and timely information regarding the issues to be decided at the meetings.
- ⇨ Opportunity shall be provided for shareholders to ask questions of the Board and to place items on the agenda at general meetings, subject to reasonable limitations.
- ⇨ Shareholders shall be able to vote in person or in absentia, and equal effect shall be given to votes whether cast in person or in absentia.
- ⇨ Shareholders shall be provided with adequate information on competencies required on the Board and given options to elect directors from amongst a range of qualified, competent, fit and proper persons.

Capital structures and arrangements that enable certain shareholders to obtain a degree of control disproportionate to their equity ownership shall be disclosed.

The Board shall endeavour to ensure that markets for corporate control are allowed to function in an efficient and transparent manner. In this regard, the Board shall always seek to ensure that:

- ⇨ The rules and procedures governing the acquisition of corporate control in the capital market, and extraordinary transactions such as mergers and sales of substantial portions of corporate assets shall be clearly articulated and disclosed so that investors understand their rights and recourse.
- ⇨ Transactions shall occur at transparent prices and under fair conditions that protect the rights of all shareholders according to their class.
- ⇨ Anti-take-over devices shall not be used to shield management from accountability.
- ⇨ Shareholders, including corporate investors, consider the costs and benefits of using their voting rights.

The Board of Directors shall ensure that there is equitable treatment of all shareholders. In particular the Board shall ensure that:

- ⇨ All shareholders of the same class are treated equally.
- ⇨ Equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders shall have the opportunity to obtain effective redress for violation to their rights.
- ⇨ Within any class, all shareholders should have the same voting rights. All investors should be able to obtain information about voting rights affiliated with all classes of shares before they purchase them. Any changes in voting rights within or between classes of shares should be subject to shareholder vote.
- ⇨ Votes shall be cast by custodians or nominees in a manner agreed upon with the beneficial owner of the shares.
- ⇨ Processes and procedures for general shareholder meetings shall allow for equitable treatment of all shareholders.
- ⇨ Company procedures do not make it unduly difficult or expensive to cast votes.
- ⇨ Self-dealing and insider trading are prohibited.
- ⇨ Members of the Board and managers disclose their material interests in transactions on matters affecting the corporation.

The Shareholders in turn have a duty and are well advised to exercise the supreme authority of the company in general meetings to hold the Board accountable for stewardship of the company.

4.8 RESPONSIBILITIES TO OTHER STAKEHOLDERS

The Board of Directors and the company recognize the rights of stakeholders as established by law and shall encourage active co-operation between the company and its stakeholders in creating wealth, jobs and the sustainability of financially sound enterprises. **In this regard, the Board of Directors shall:**

- ⇨ Ensure that the rights of stakeholders that are protected by law are respected.
- ⇨ Where stakeholder interests are protected by law, ensure that stakeholders have the opportunity to seek effective redress for any violation of their rights.
- ⇨ Permit and facilitate performance-enhancing mechanisms for stakeholder participation.
- ⇨ Ensure that where stakeholders participate in performance-enhancing mechanisms, they have access to all relevant information.

4.9 CODE OF ETHICS

The Board of Directors shall develop and put in place a code of ethics outlining the values, ethics and beliefs that guide the policy and behaviour of the company and define the ethical standards applicable to it and to all who deal with it.

4.9.1 Social Responsibilities

The Board of Directors will monitor the social responsibilities of the company and promulgate **policies consistent with the company's legitimate interests and good business practices. In** particular, **the Board of Directors shall:**

- ⇨ Promote fair, just and equitable employment policies;
- ⇨ Promote and be sensitive to the preservation and protection of the natural environment;
- ⇨ Be sensitive to and conscious of gender interests and concerns;
- ⇨ Promote and protect the rights of children and other vulnerable groups;
- ⇨ Enhance and promote the rights and participation of host co

4.9.2 General

The Board of Directors shall, conscious of its responsibilities to investors, suppliers, creditors, employees and the society:

- ⇨ Issue a certificate at the end of every year confirming that it has complied with the law, conducted its affairs in accordance with the best principles and practices of corporate governance and that to the best of the knowledge of the Board and management, no person, employee or agent acting on behalf of the company with the knowledge or authority of the Board or management, committed any offence under the Prevention of **Corruption Act or indulged in any unethical behaviour in the conduct of the company's** business, or been involved in money laundering or any practice or activity contrary to national laws or international conventions.

- ⇨ Publish a Social Responsibility report every year indicating how it has dealt with its social and environmental responsibilities.

4.9.3 Corporate Governance Reports

CHAPTER FIVE

BOARD EFFECTIVENESS

5.0 BOARD EFFECTIVENESS

5.1 INTRODUCTION

The institution of board of directors was based on the premise that a group of trustworthy and respectable people should look after the interests of the large number of shareholders who are not directly involved in the management of the company. The position of the board of directors is that of trust as the board is entrusted with the responsibility to act in the best interests of the company.

The contribution of board of directors of companies is critical for ensuring appropriate directions with regard to leadership, vision, strategy, policies, monitoring, supervision, accountability to shareholders and other stakeholders, and to achieving greater levels of performance on a sustained basis as well as adherence to the best practices of corporate governance.

An effective board defines the company's purpose and then sets a strategy to deliver it, shapes its culture and the way it conducts its business. It sets the main trends and factors affecting the long-term success and future viability of the company – for example technological change or environmental impacts – and how these and the company's principal risks and uncertainties have been addressed.

The board should have sound understanding of how value is created over time, key strategies and business models towards a sustainable future. This is not limited to value that is found in the financial statements. An understanding of how value for intangible sources are developed, managed and sustained – for example a highly trained workforce, intellectual property or brand recognition – is increasingly relevant to an understanding of the company's performance and the impact of its activity. These are important considerations for boards when setting corporate strategy.

Boards have a responsibility for the health of the company and need to take a long-term view. This is in contrast to the priorities of some investors, not all of whom will be aligned with the pursuit of success over the long-term. An effective board will manage the conflict between short-term interests and the long-term impacts of its decisions; it will assess shareholder and stakeholder interests from the perspective of the long-term sustainable success of the company.

The board's role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed. An effective

board develops and promotes its collective vision of the company's purpose, its culture, its values and the behaviors it wishes to promote in conducting its business.

It's becoming increasingly clear that the landscape has changed permanently. That means it won't go back to the way it was. In other words, ensuring compliance with the letter and spirit of the new requirements will continue to require attention going forward.

Experienced directors and senior executives recognize that the requirements, for the most part, deal with issues of form, not function. Yes, they are important because they're now legal or regulatory mandates, and also can serve as enablers to effective board performance. But as noted, some boards that have always done these things still have not been very effective, while others had few of the now-mandated practices in place yet have been highly effective.

What makes a board truly effective is something else entirely. Experienced directors having spent a disproportionate amount of time on the new mandates that deal for the most part with additional disclosures to and empowering shareholders and imposing checks and balances on management—want to get back to the business of providing the chief executive and senior management team with value-added advice, counsel, and direction on critical issues facing the business.

So where is board attention needed? That will depend on each company, of course. But based on experience, there are eight principal areas of responsibility where the value-add takes place, **outlined here in high-level summary:**

1. Strategy. Making sure the company gets strategy right is absolutely critical. Effective boards carefully analyze proposed strategy plans and management's rationale for its recommendation. These directors bring experience and insight into the constructive debate, focusing on markets, competitors, risks, resources, and interdependencies. It is of critical importance that resource allocation, business processes, and senior executives' buy-in all are positioned to drive successful strategy execution.
2. Risk management. The board must be comfortable that management is identifying and appropriately responding to risk, and that the board itself is apprised of the most significant risks facing the company. To reach this comfort level, effective boards ensure that management has in place an effective risk-management process, and the directors assess whether risks are undertaken and managed consistent with the established risk appetite.

3. Tone at the top. Management establishes the corporate culture, but effective boards ensure that the desired integrity and ethical values are present. Of course, that includes a robust code of conduct, a whistleblower channel, feedback protocols, and related elements comprising a cohesive program, and also means the board must ensure the culture is driven not only by the words of management, but their actions as well.
4. Measuring and monitoring performance. The board must ensure that performance measures are linked to strategy, tactics, and the real value drivers. Metrics should

balance financial performance with forward-looking, non-financial information. And performance awards should be aligned with company goals.

5. Transformational transactions. Directors must be truly comfortable with the business justifications for a proposed deal, whether it be a merger, acquisition, alliance partnership, or joint venture. Effective directors critically evaluate management's data, projections, and assumptions particularly when it comes to "synergy" and integration assumptions. The board should apply lessons learned from past transactions, and should have the courage to walk away from a bad deal.
6. Management evaluation, compensation, and succession planning. Effective boards and compensation committees, especially under the current governance spotlight, ensure that performance criteria and targets for management are linked to strategic goals and desired behavior. Compensation should be crafted to retain the best talent while paying for performance. The best boards don't wait for signs of a departure before having succession plans in place.
7. External communications. Corporate boards particularly their audit committees continue to struggle to understand what entails "appropriate oversight" of financial reporting and related processes. Effective audit committees ensure they have requisite information from management and auditors, and the committee members gain sufficient understanding and insight and challenge critical judgments, resulting in the necessary comfort with the reliability of financial reports, internal control, and related matters.

8. Board dynamics. This involves the ways in which the board itself operates. The most effective boards forge the right relationships, processes, and constructive engagement to carry out the above responsibilities effectively

5.3 DIRECTORS TRAINING, DEVELOPMENT AND FAMILARISATION

Director's Training: An important aspect of Board effectiveness would be appropriate attention to development and training of directors. Director orientation/induction should be seen as the first step of the board's continuing improvement. Since the Board composition is getting more diverse a system of formal training and evaluation is very important to foster trust, cohesion and communication among board members. Investing in board development strengthens the board and individual directors. As the Board of Directors is primarily responsible for good governance practices, which is quite different from management, it calls for new areas of knowledge and different skills.

Training should encompass both a thorough induction programme and an ongoing training and development opportunities for the board members. Training should focus on improving the knowledge and skills of the board and individual members and on overall board performance. Training should be required for each board member and compliance with the requirement used

to assess individual board member performance for reappointment to additional terms of board service. Requirements should be set forth in a board policy that describes the focus and type of education available.

Director Induction: Induction procedures should be in place to allow new directors to participate fully and actively in board decision-making at the earliest opportunity. To be effective, new directors need to have a good deal of knowledge about the company and the industry within which it operates. It involves introducing the new directors to the people with whom they will be working and explaining how the board operates. It involves building up rapport, trust, and credibility with the other directors so that the new director is accepted by and can work with fellow directors. **Common methods of induction include:**

- ⇨ Briefing papers
- ⇨ Internal visits
- ⇨ Introductions

An induction programme should be available to enable new directors to gain an understanding of:

- ⇨ **the company's financial, strategic, operational and risk management position**
- ⇨ the rights, duties and responsibilities of the directors
- ⇨ the roles and responsibilities of senior executives
- ⇨ the role of board committees.

An induction kit should be given to new directors which should contain the following:

- ⇨ Memorandum and Articles of Association with a summary of most important provisions
- ⇨ Brief history of the company
- ⇨ Current business plan, market analysis and budgets
- ⇨ All relevant policies and procedures, such as a policy for obtaining independent professional advice for directors;
- ⇨ Protocol, procedures and dress code for Board meetings, general meetings, , staff social events, site visits etc including the involvement of partners;
- ⇨ Press releases in the last one year
- ⇨ copies of recent press cuttings and articles concerning the company
- ⇨ Annual report for last three years
- ⇨ Notes on agenda and Minutes of last six Board meetings
- ⇨ **Board's meeting schedule and Board committee meeting schedule**
- ⇨ Description of Board procedures.

Director's Development: Professional development should not be treated as merely another training schedule rather it must be more structured so as to sharpen the existing skills and knowledge of directors. It is a good practice for boards to arrange for an ongoing updation of their members with changes in governance, technologies, markets, products, and so on through:

- ⇨ Ongoing education
- ⇨ Site visits
- ⇨ Seminars; and
- ⇨ Various short term and long term Courses

5.4 PERFORMANCE EVALUATION OF THE BOARD AND MANAGEMENT

Board evaluation is a key means by which boards can recognize and correct corporate governance problems and add real value to their organizations. A properly conducted board evaluation can contribute significantly to performance improvements on organizational; board and individual member level. Board evaluation typically examines the roles of the Board and the entailing responsibilities, and assesses how effectively these are fulfilled by the Board. The stakeholders and investors are interested to know whether the members of Board are effectively functioning individually and collectively. The Board at many times requires new skills for promptly responding to the dynamic changing business environment. Performance measurement, against the set benchmarks, in the form of Board evaluation has the potential to significantly enhance Board effectiveness, maximize strengths, tackle weaknesses and improve corporate relationships. Annual assessment is a powerful tool to convert good boards into great boards.

Evaluation provides the board and its committees with the opportunity to consider how group culture, cohesiveness, composition, leadership, meetings information processes and governance policies influence performance. Board Evaluation helps to identify areas for potential adjustment and provides an opportunity to remind directors of the importance of group dynamics and effective board and committee processes in fulfilling board and committee responsibilities.

Thus, Board evaluation contributes significantly to improved performance at three levels - organizational, Board and individual Board member level. It also improves the leadership, teamwork, accountability, decision-making, communication and efficiency of the board. A commitment to annual evaluation is powerful change agent.

The Board evaluation sets the standards of performance and improves the culture of collective action by Board. Evaluation also improves teamwork by creating better understating of Board dynamics, board-management relations and thinking as a group within the board. It helps to maximize board/ director contribution by encouraging participation in meetings and highlighting the skill gaps on the Board and those of individual members. Directors demonstrate commitment to improvement, based on the feedback provided on individual and collective skill gaps.

The purposes of the Board evaluation may be enumerated as under:

- ⇨ Improving the performance of Board towards corporate goals and objectives.
- ⇨ Assessing the balance of skills, knowledge and experience on the Board.
- ⇨ Identifying the areas of concern and areas to be focused for improvement.
- ⇨ Identifying and creating awareness about the role of Directors individually and collectively as Board.
- ⇨ Building Team work among Board members.

5.5 EVALUATION OF THE COMMITTEES

The Board is responsible for the evaluation of the performance of the Committees of the Board. The performance of the committees may be evaluated by the Directors, on the basis of the terms of reference of the committee being evaluated. The evaluation may be externally facilitated. The broad parameters of reviewing the performance of the Committees, inter alia, are:

- ⇨ Discharge of its functions and duties as per its terms of reference;
- ⇨ Process and procedures followed for discharging its functions;
- ⇨ Effectiveness of suggestions and recommendations received;
- ⇨ Size, structure and expertise of the Committee; and
- ⇨ Conduct of its meetings and procedures followed in this regard.

5.6 EVALUATION OF INDIVIDUAL DIRECTOR(s)

5.6.1 Evaluation of Managing Director / Whole time Director / Executive Director

The performance evaluation of Managing Director, Executive Director of the Company may be done by all the directors. The external facilitation may also serve as the efficient tool for evaluation. As per the Code for Independent Directors also provides that Independent Directors should review the performance of non-independent Directors, which include Managing Director / Whole time Director/ Executive Director. The broad parameters for reviewing the performance of Managing Director/ Executive Director are:

- ⇨ Achievement of financial/business targets prescribed by the Board;
- ⇨ Developing and managing / executing business plans, operational plans, risk management, and financial affairs of the organization;
- ⇨ Display of leadership qualities i.e. correctly anticipating business trends, opportunities, and priorities affecting the Company's prosperity and operations;
- ⇨ Development of policies, and strategic plans aligned with the vision and mission of Company and which harmoniously balance the needs of shareholders, clients, employees, and other stakeholders;
- ⇨ Establishment of an effective organization structure to ensure that there is management focus on key functions necessary for the organization to align with its mission; and
- ⇨ Managing relationships with the Board, management team, regulators, bankers, industry representatives and other stakeholders.

5.6.2 Evaluation of Independent Directors:

The performance evaluation of independent directors should be done by the entire Board of Directors, excluding the director being evaluated. On the basis of the report of performance evaluation, it shall be determined whether to extend or continue the term of appointment of the independent director.

The Nomination Committee shall lay down the evaluation criteria for performance evaluation of independent directors. The company should disclose the criteria for performance evaluation, as laid down by the Nomination Committee, in its Annual Report.

5.6.3 Major Factors for Evaluation

- ⇨ The quality of the issues that get raised, discussed and debated at the meetings of the Board and its Committees.
- ⇨ The guidance provided by the Board in the light of changing market conditions and their impact on the organisation.
- ⇨ The methodology adopted by the Board to solve issues referred to them
- ⇨ The effectiveness of the directions provided by the Board on the issues discussed in meetings.

Parameters: In addition to the parameters laid down for Directors, which shall be common for evaluation to both Independent and Non- executive directors, an Independent director shall also be evaluated on the following parameters:

- ⇨ Exercise of objective independent judgment in the best interest of Company;

- ⇨ Ability to contribute to and monitor corporate governance practice; and
- ⇨ Adherence to the code of conduct for independent directors.
- ⇨ Performance of the Board against the benchmark performance set.
- ⇨ Overall value addition by the discussions taking place at the Board meetings.
- ⇨ The regularity and quality of participation in the deliberations of the Board and its Committees.
- ⇨ The answerability of the top management to the Board on performance related matters.

5.6.4 Evaluation of Non-Executive Directors

In terms of the Code for Independent Directors, the Independent director(s) on the Board of the Company should evaluate the performance of Non-independent director(s) which include non-executive director(s). Peer Review method or external evaluation may also facilitate the purpose of evaluating Non-executive directors. The broad parameters for reviewing the performance of Non-executive

Directors are:

- ⇨ Participation at the Board / Committee meetings;
- ⇨ Commitment (including guidance provided to senior management outside of Board/ Committee meetings);
- ⇨ Effective deployment of knowledge and expertise;
- ⇨ Effective management of relationship with stakeholders;
- ⇨ Integrity and maintaining of confidentiality;
- ⇨ Independence of behaviour and judgment; and
- ⇨ Impact and influence.

5.6.5 Evaluation of Chairperson of the Board

The performance of the Chairperson is linked to both the functioning of the Board as a whole as well as the performance of each director. The Code for Independent Directors provides that the Independent Director should review the performance of the Chairperson of the company taking into account the views of the executive directors and non-executive directors.

Therefore, all the directors of the Board of the company thereof contribute in evaluating the performance of the Chairperson of the Board. External agencies may also be involved in evaluating the Chairperson.

The broad parameters for reviewing the performance of Chairperson of the Board are:

- ⇨ Managing relationship with the members of the Board and management;

- ⇨ Demonstration of leadership qualities;
- ⇨ Relationship and communication within the Board;
- ⇨ Providing ease of raising of issues and concerns by the Board members; and
- ⇨ Promoting constructive debate and effective decision making at the board;
- ⇨ Relationship and effectiveness of communication with the shareholders and other stakeholders;
- ⇨ Promoting shareholder confidence in the Board and
- ⇨ Personal attributes i.e. Integrity, Honesty, Knowledge,etc.

5.7 GUIDANCE ON BOARD EFFECTIVENESS

(Issued by FRC, UK – July 2018)

The primary purpose of the Guidance on Board Effectiveness (the Guidance) is to stimulate **boards' thinking on how they can carry out their role and encourage them to focus on** continually improving their effectiveness. The Guidance on Board Effectiveness is includes commentary on areas such as culture, relations with the workforce and wider shareholders and diversity. It also incorporates new sections on the workings of board committees, notably the remuneration committee. Helpfully, the Guidance includes questions for boards to ask themselves or, in some cases, to ask management, about effectiveness in key areas.

The Guidance is not mandatory and is not prescriptive. It contains suggestions of good practice to support directors and their advisors in applying the Code.

The Guidance also includes some of the procedural aspects of governance and is intended to act as a reminder to boards and their support teams that good practice and procedure should continue to be followed. The tools and techniques for board effectiveness are suggested in the Guidance to assist companies in applying the Principles of good corporate governance.

5.8 BOARD EFFECTIVENESS INDICATORS

Sample questions which can be used as a quick check for board effectiveness in any organization. Are the majority of your board members independent from the organization?

- ⇨ Do you have a set of required competencies articulated for your board (and committees), and do your current board members as a whole display the entire set of required competencies?
- ⇨ Do you have a board manual that articulates terms of reference for the board, board committees, individual directors, and the code of conduct? Does it have a forward list of topics for the year?

- ⇨ Does at least one member of the board have extensive experience in the industry of your organization?
- ⇨ Does each director get a comprehensive orientation on the business of the organization and meet key senior staff before the first board meeting?
- ⇨ Are directors offered continuing education in governance or a program of director certification?
- ⇨ Does each director display a keen interest or passion in the undertaking of the organization?
- ⇨ Do directors regularly attend both board and committee meetings?
- ⇨ Are directors encouraged and supported when asking difficult or awkward questions of management?
- ⇨ Does the Chairman solicit views from each director specifically?
- ⇨ Does the Chairman ask board members to refrain from expressing their personal views at the outset of a discussion?
- ⇨ Does the Chair manage the timing of the board meetings to ensure there is sufficient time for discussion after each topic addressed by management?
- ⇨ Does the board regularly have outside experts attend to present on specific topics?
- ⇨ Does the board have an in-camera meeting both before and after each board meeting?
- ⇨ Does the board retain an independent consultant to help evaluate director and board performance?
- ⇨ At the beginning of a board meeting, do the committee chairs have an opportunity to summarize (verbally or in writing) the issues addressed and decisions taken at prior committee meetings?
- ⇨ Does the board have an effective system to provide board members with timely, relevant and reliable financial and strategic information about the organization?
- ⇨ Does the board review the risk identification and management system of the organization?
- ⇨ Does the board approve the business plan and major expenditures?
- ⇨ Does the board work with the CEO and senior staff to develop and review the strategic plan?

5.9 BOARD COMMITTEES

A board committee is a small working group identified by the board, consisting of board members, for the purpose of supporting the board's work. Committees are generally formed to perform some expertise work. Members of the committee are expected to have expertise in the specified field.

Committees are usually formed as a means of improving board effectiveness and efficiency, in areas where more focused, specialized and technical discussions are required. These committees prepare the groundwork for decision-making and report at the subsequent board meeting. Committees enable better management of full board's time and allow in-depth scrutiny and focused attention.

However, the Board of Directors is ultimately responsible for the acts of the committee. Board is responsible for defining the committee role and structure.

The structure of a board and the planning of the board's work are key elements to effective governance. Establishing committees is one way of managing the work of the board, thereby strengthening the board's governance role. Boards should regularly review its own structure and performance and whether it has the right committee structure and an appropriate scheme of delegation from the board.

Committees may be formed for a range of purposes, including:

- **Selection Committee/Nomination Committee**: To select Board members, to select a CEO, to select key managerial and senior management personnel
- **Board development or Governance Committee**: To look after/ administer/support Board members and committee members and other executive positions
- **Investment Committee**: For advising to the board for investments
- **Risk Management Committee**: To report to the board about potential risks factor and to suggest action point for risk mitigation.
- **Safety, Health & Environment Committee**: To take care of the safety mearsures, prevention and effective disposal of the hazardous materials during the course of manufacturing and taking of care of sustainability development.
- **Committee of Inquiry**: To inquire into particular questions (disciplinary, technical, etc.)
- **Finance or Budget Committees**: To be responsible for financial reporting, organising audits, etc.
- **Marketing and Public Relations Committees**: To identify new markets; build relationship with media and public, etc.

5.10 RATIONAL BEHIND BOARD COMMITTEES

- ⇨ To improve Board effectiveness and efficiency
- ⇨ Minor details needs to be evaluated/ analysed to arrive at a logical conclusion- This requires body having expertise in subject matter, a Board Committee shall in such cases assist the Board and give well considered recommendations to the Board. e.g. Audit Committee go through minor details of internal audit reports which is not possible and give suitable recommendations, this is not possible for entire Board to consider.
- ⇨ Insulate Board from potential undue influence of controlling shareholders and managers
- ⇨ Committees prepare groundwork for decision making and submit their recommendations to the Board for decision making
- ⇨ **Enables better management of Board's time and allows in**-depth scrutiny of proposals
- ⇨ Establishing committees is one way of managing the work of the Board and **strengthening the Board's governance role.**

5.11 SELECTION OF COMMITTEE MEMBERS

Specific committee members may be appointed by either the Board or the committee Chairman. Area of knowledge and expertise domain and time commitment of the Board member should be considered as the criteria for the selection on any specific committee. The committee members should be selected with following questions in mind: What tasks are the committee responsible for and who among the members possess the skills and experience needed to complete those tasks. Every effort should be made to match the needs and requirements of the committee and the skills, knowledge and interests of prospective committee members.

It is very important that members have a clear view of the committee's goals and the chairman should have flair to utilize the committee member's knowledge exponentially well to achieve those goals.

5.12 APPOINTMENT OF THE COMMITTEE CHAIRMAN

The Board may appoint the committee chairman or the committee members can choose/elect the chairman. The committee chairman is the key to an effective committee, he sets the tone, **pace and strategies of the committees' functioning, hence chairman selected should have** motivational and leadership skills and time commitment expected of him.

In seeking an effective chairman, most important things are knowledge and experience relevant to the work of the committee, proven leadership and behavioral skills that will be essential if the committee is to work effectively. The role of committee chairman requires extra work, time for communication with committee members and senior management so that he remains informed about the developments and a willingness to resolve conflicts among members.

Suggested Content of the Terms of References of Committees

- ⇨ Objectives
- ⇨ Composition
- ⇨ Secretary
- ⇨ Quorum
- ⇨ Meetings
- ⇨ Annual General Meeting
- ⇨ Authority
- ⇨ General Responsibilities
- ⇨ Specific Responsibilities
- ⇨ Reporting
- ⇨ Evaluation
- ⇨ Review of Committee

(a) Common Board Committees

Audit Committee is one of the main pillars of the corporate governance mechanism in any company. The Committee is charged with the principal oversight of financial reporting and disclosure and aims to enhance the confidence in the integrity of the company's financial reporting, the internal control processes and procedures and the risk management systems.

(b) Nomination and Remuneration Committee

Concerns nomination or remuneration of a director. However, there was a provision where public companies having no profits or inadequate profits and would like to remunerate the directors has to constitute a remuneration committee and such committee shall approve such remuneration to directors.

(c) Shareholder Relations Committee

The main function of the committee is to consider and resolve the grievances of security holders of the company. The role of the Stakeholders Relationship Committee shall be to consider and resolve the grievances of the security holders of the listed entity including complaints related to transfer of shares, non-receipt of annual report and non-receipt of declared dividends.

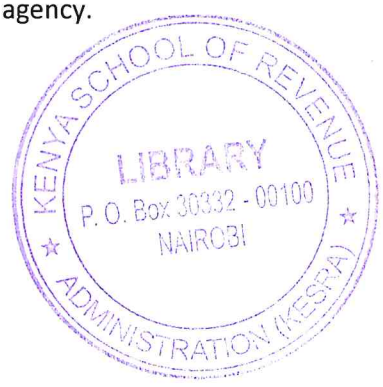
(d) Corporate Governance Committee

The Corporate Governance Committee is responsible for considering and making recommendations to the Board concerning the appropriate size, functions and needs of the Board. The Corporate Governance Committee may, at its sole discretion, engage director search firms and has the sole authority to approve the fees and other retention terms with respect to any such firms. The Corporate Governance Committee also has the authority, as necessary and appropriate, to consult with other outside advisors to assist in its duties to the Company. A company may constitute this Committee to develop and recommend the board a set of corporate governance guidelines applicable to the company, implement policies and processes relating to corporate governance, to review, periodically, the corporate governance guidelines of the company. Many companies give the mandate of corporate governance to nomination committee and is given the nomenclature Nomination and Corporate Governance Committee.

(e) Regulatory, Compliance & Government Affairs Committee

The primary objective of the Compliance Committee is to review, oversee, and monitor:

- **the Company's compliance with applicable legal and regulatory requirements,**
- **the Company's policies, programmes, and procedures to ensure compliance with** relevant laws, the Company's Code of Conduct, and other relevant standards;
- **the Company's efforts to implement legal obligations arising from settlement** agreements and other similar documents; and
- perform any other duties as are directed by the Board of Directors of the company.
- **The committee oversees the Company's** non-financial compliance programmes and systems with respect to legal and regulatory requirements. Besides, it also oversees compliance with any ongoing Corporate Integrity Agreements or any similar undertakings by the Company with a government agency.



(f) Science, Technology & Sustainability Committee

Science, Technology & Sustainability Committee may be constituted to:

- ⇨ Monitor and review the overall strategy, direction and effectiveness of the Company's research and development.
- ⇨ Serve as a resource and provide input, as needed, regarding the scientific and technological aspects of product safety matters.
- ⇨ Review the Company's policies, programmes and practices on environment, health, safety and sustainability.
- ⇨ Assist the Board in identifying and comprehending significant emerging science and technology policy and public health issues and trends that may impact the Company's overall business strategy.
- ⇨ Assist the Board in its oversight of the Company's major acquisitions and business development activities as they relate to the acquisition or development of new science or technology

(g) Customer Service Committee / Customer Grievance Committee

Some service oriented companies may have separate Board Committee on customer service matters. Grievance committee may look after the complaints (if any) received from the customer and the steps taken to resolve it.

(h) Fraud Monitoring Commitee

Although the fraud related aspects may be taken care of by the Audit Committee, but in some companies which are in field of financial services, there may be need of the separate fraud monitioring committee, which may take care of the checks and balances and preventive measures in order to discourage the employees in their modus operandi.

(i) Information Technology Committee

Information Technology is need of hour. This committee may look after the present and future need of the induction of Information Technology and also takes care of need of providing the training to the existing as well new incumbents.

(j) Performance Appraisal Review Committee

This committee periodically (say annually) reviews the performance to Top Executives/ Key Managerial Person of the company as well as the Directors of the company. It is just like the performance review of the each and every employee, which happens in most of the organizations. By this annual exercise, the persons sitting at helm of the affairs of the company comes under the scanner of this committee.

5.13 BOARD STRUCTURE IN KENYA

The CMA corporate governance code 2015 provides that:
The Board shall comprise a balance of executive and non-executive directors, with a majority of non-executive directors. Independent non-executive directors shall be at least one third of the total number of Board members.

(a) The structure of the Board shall comprise a number of directors, which fairly reflects the company's shareholding structure. The composition of the Board shall not be biased towards representation by a substantial shareholder but shall reflect the company's broad shareholding structure. The composition of the Board shall provide a mechanism for representation of the minority shareholders without undermining the collective responsibility of the directors.

(b) In instances where there is no major shareholder but there is a substantial shareholder, the Board shall exercise judgment in determining the representation on the Board of such shareholder and of the other shareholders that effectively reflects the shareholding structure of the Company.

(c) Executive members of the Board shall manage the conflict that arises between their management role and their role in the Board.

The Board shall be of such a number that enables the requirements of the company's business to be met. The size of the Board shall not be too large to undermine an interactive discussion during Board meetings or too small such that the inclusion of wider expertise and skills to improve the effectiveness of the Board and the formation of its committees is compromised.

Each Board shall consider whether its size, diversity and demographics make it effective. Diversity applies to academic qualifications, technical expertise, relevant industry knowledge, experience, nationality, age, race and gender. The appointment of Board members shall be gender sensitive and shall not be perceived to represent a single or narrow constituency interest. Where companies establish a diversity policy, the companies shall introduce appropriate measures to ensure that the policy is implemented

5.14 MULTIPLE DIRECTORSHIPS

There shall be a limit to the number of directorships a member of the Board holds at any given time. A director of a listed company except a corporate director shall not hold such position in more than three public listed companies at any one time. This is to ensure effective participation by such directors in the Board. In a case where the corporate director has appointed an alternate director, the appointment of such alternate director shall be restricted to two public listed companies at any one time. An executive director of a listed company shall be restricted to one other directorship of another listed company. A chairperson of a public

listed company shall not hold such position in more than two public listed companies at any one time, in order to allow the chairperson to devote sufficient time to steering the Board.

5.15 Alternate Board members

An alternate director shall be nominated by the substantive director but subjected to vetting by the nomination committee.

CHAPTER SIX

CORPORATE GOVERNANCE AND SHAREHOLDERS RIGHTS

6.0 CORPORATE GOVERNANCE AND SHAREHOLDERS RIGHTS

6.1 INTRODUCTION

Protection of shareholder rights is sacrosanct for good corporate governance. It is one of the pillars of corporate governance. For the efficient functioning of the capital market, the fundamental requirement is that the investor rights are well protected. The central element in corporate governance is the challenges arising out of separation of ownership and control.

Shareholder rights and investor protection are key factors to consider when determining the ability of companies to raise the capital they need to grow, innovate, diversify and compete effectively. If the legal and governance framework does not provide such protection, investors may be reluctant to invest unless they become the controlling shareholders. It is critical that the governance framework ensures the equitable treatment of all shareholders, including the minority.

The shareholders are the true owners of a corporate and the governance function controls the operations of the corporate. There is a strong likelihood that there is a mismatch between the expectations of the shareholders and the actions of the management. Therefore there is a need to lay down clearly the rights of the shareholders and that of the management.

6.2 SHAREHOLDERS RIGHTS IN KENYA

- **All shareholders shall receive relevant information on the company's performance** through the distribution of annual reports and accounts, and half-yearly results as a matter of best practice. Such reports shall be availed across multiple communication **channels suitable to shareholders' different media consumption habits. These include** websites, postal mail and newspapers.
- All shareholders have a right to receive relevant sufficient and timely information concerning the date, location and agenda of the Annual General Meeting as well as full and timely information regarding issues to be decided during the Annual General Meeting. Such information shall be received at least 21 calendar days before the Annual General Meeting.
- The Board shall make shareholders expenses and convenience a primary criterion when selecting the venue and location of Annual General Meeting.
- The shareholders have a right to a secure method of transfer and registration of ownership of their shares.
- Every shareholder has the right to participate and vote at the general shareholders meeting including the election of directors.
- The shareholders are encouraged to participate in the Annual General Meetings and to exercise their votes.
- **The Board shall ensure that shareholders' right to full participation at Annual General**

Meetings are protected by giving shareholders—

- ⇨ Sufficient information on each subject to be discussed at the Annual General Meeting.
- ⇨ sufficient information on voting rules or procedures;
- ⇨ proxy models with different voting options:
- ⇨ the opportunity to question the management;
- ⇨ the opportunity to place items on the agenda at Annual General Meetings;
- ⇨ the opportunity to vote in absentia; and
- ⇨ sufficient information to enable them to consider the costs and benefits of their votes.
- ⇨ Every shareholder shall be **entitled to ask questions, seek clarification on the company's** performance as reflected in the annual reports and accounts or on any matter that may **be relevant to the company's performance or promotion of shareholders' interests and** to receive explanation from the directors and/or management. This right shall be exercised in such a way as not to disrupt the business of an Annual General Meeting.
- ⇨ Every shareholder is entitled to distributed profit, in form of dividends, and other rights for bonus shares, script dividend or rights issue, as applicable and in the proportion of its shareholding in the company.
- ⇨ The Board shall maintain an effective communication policy that enables both management and the Board to communicate effectively with its shareholders, stakeholders and the public in general.
- ⇨ The annual report and accounts to the shareholders must include highlights of the operations of the company, financial performance and status of application of this Code.
- ⇨ Companies shall employ modern communication techniques including the use of teleconferencing, videoconferencing, websites, and emails to communicate with shareholders.
- ⇨ Companies, as a matter of best practice, are encouraged to organize regular investor briefings and in particular when the half-yearly and annual results are declared or as may be necessary to explain their performance and promote interaction with investors.
- ⇨ **The Board shall encourage the establishment and use of the company's website by** shareholders to speed up communication and interaction among shareholders and the company.

6.3 SHAREHOLDER ACTIVISM

The term activism often accompanies notions of unrest. On the contrary, activism isn't always a bad thing. It's a process that can often lead to long-term meaningful change. Shareholders can be instrumental as change agents through private meetings, public votes, media debates and other avenues to drive better corporate governance practices. Corporations will almost surely

pay a price for not paying attention to issues that lead to shareholder activism. Some of the big topics related to activism are executive pay, succession planning, diversity and board director independence.

Shareholders are looking for assurance that executive pay increases are aligned with performance. Taking it a step further, shareholders are also interested in understanding how boards come up with their guidelines for executive pay structures. Shareholders are also seeking assurance that boards have the experience, skills and diversity to protect their investments and to enable the company to make steady long-term progress. The current climate encourages shareholders to scrutinize all new board director appointments and evaluate them based on how their talents and abilities enhance the board.

Board directors need to be aware of other issues that can lead to shareholder activism, including taking a closer look at the board's strategy and use of capital. Another hot topic for shareholders is how corporations factor social, ethical and environmental matters into their strategies and general decision making.

6.4 THE ROLE OF COMMUNICATIONS IN PREVENTING SHAREHOLDER ACTIVISM

Enhanced communications between board directors, executives and shareholders can often reduce the possibility of shareholder activism. Shareholders desire assurance that boards are practicing good oversight to prevent risks and other issues that could lead to a downturn in performance.

Boards that are willing to listen to shareholder concerns on a regular basis and to communicate with shareholders to address their concerns may reduce incidences of shareholder activism. Communication that takes place early and often between boards and shareholders will alert boards to times when the board is taking a direction that shareholders feel isn't in their best interests. Shareholders can be instrumental in giving boards a heads-up about serious issues early enough to prevent the perception of decreased value.

Boards also need to be aware of shareholder activism styles. In the recent past in the United Kingdom, shareholders generally adopted a more communicative, cooperative style with

boards. By contrast, shareholders in the United States were more likely to take a hostile, aggressive stance. In the current climate, the tides seem to be changing, as some U.K. shareholders have been taking the more aggressive U.S. approach to activism under certain circumstances. At the same time, U.S. shareholders are starting to adopt the more private, communicative activism approach that U.K. shareholders have traditionally taken.

6.4.1 Shareholder Activism in Kenya

The Companies Act 2015, the Capital Markets Authority (CMA) Guidelines and the Code of Corporate Governance for Listed Companies 2016, offer greater opportunities for shareholder activism through specific provisions that allow shareholders to not only sanction certain actions by directors before they are taken, but also to speak out against actions taken contrary to their interests.

The CMA Governance Code provides for a number of recommendations and guidelines intended to form best practice for various sectors and industries. The Code provides or a 'call to action' for shareholder activists and potential shareholder activists to create equitable treatment of all shareholders. The Code recommends that institutional investors take up a stewardship role as representatives of their clients in listed companies and this has seen greater engagement with the company's management and board with the aim of enhancing company performance and best practice in corporate governance. The CMA gazetted a Stewardship code for Institutional Investors in 2017, giving reinforcement to the provisions of the CMA Governance Code by requiring responsible investment policies, active and informed voting practices, engagement and collaboration with other institutional investors, monitoring companies held in investment portfolios and public disclosures and reporting.

The Companies Act 2015, also provides for a number of opportunities for shareholder activism through derivative actions under Part 11, protection against oppression and unfair prejudice under Part 29, rights to information about the company, inspection of company records, general and specific duties of directors, mandatory shareholder approval prior to certain transactions being undertaken, etc.

Overall, there has been some progress made in the shareholder perception from passive shareholders to more aggressive investors aware of their role in using activist strategies to

demand for change across a broad spectrum of issues ranging from company strategy, performance, executive compensation, corporate governance and profit distribution etc.

6.4.2 Level of Shareholder Activism in Kenya

Shareholder activism has not been very prevalent in Kenya due to a general lack of interest by investors, particularly minority shareholders. Nonetheless, the recent past has witnessed an increase in shareholder activism, especially in cases of threatened collapse of various companies. In these instances, there has been heightened shareholder activism demanding for accountability from management with the aim of rallying government action to resuscitate such entities. One example of shareholder activism is the minority shareholders demand for accountability from the management of Uchumi Supermarkets, one of Kenya's former leading supermarket chains, on what led to the collapse of the entity sometime in the year 2006. This resulted in government action to resuscitate Uchumi. Shareholder activism has also been witnessed in other public companies, such as Kenya Airways Limited and Mumias Sugar Company Limited, effectively resulting in government financial bailout.

Shareholder activism has also gained traction in profitable companies in which large institutional investors and government have a stake, such as Safaricom PLC, a leading mobile network operator, which has, over the years, responded by increasing timely and accurate financial information to shareholders including explaining their business model and strategy, updates on management expectations regarding changes in the economic environment, changes in regulatory landscapes, consistent financial performance and strong corporate governance practices. Safaricom PLC has, however, not been insulated from some effects of increased shareholder activism, such as attempts to influence the appointment of top executives and board members due to various stakeholder interests such as government, regulators, majority shareholders, etc.

The increase in shareholder activism can be attributed to an expanded space for press freedom and greater proactive investor engagement by management, which in turn has fuelled greater awareness among investors on their various investment portfolio companies.

Regulatory changes and jurisprudence created from corporate and commercial disputes have also heightened public awareness and emboldened investors by disrupting the traditional balance of power between management and shareholders. The transfer of a significant part of

an organisations' control of information to investors, due to digital information accessibility, has also contributed to greater shareholder activism as investors can access information and communicate their demands at any time rather than waiting to receive reports on the company by post prior to general meetings being convened. Transparent disclosure practices by companies and their management, required by legislation, have also helped to fuel greater shareholder activism in areas such as executive compensation.

6.4.3 Shareholder Activist Strategies

Shareholder activism strategies are largely influenced by the short-term and long-term goals and objectives of different investor classes. Some strategies commonly employed by activist shareholders include collaboration with other investors by stating their view of a company's prospects and making recommendations with minimal publicity, grievance letters to the Board of Directors and seeking election to the Board of Directors.

Other, more aggressive, strategies include leveraging the media through publicity campaigns focused on arguments in favour of activist positions, such as altering the structure of the board, replacing senior executives and divesting specific investment projects etc.

Key agendas typically pursued by activist shareholders include boosting performance, selling under-performing assets, diversifying investments, altering the composition of the board, competence of the management and controlling or influencing executive compensation etc.

6.5 HOW SHAREHOLDER ACTIVISM DRIVES BETTER CORPORATE GOVERNANCE

Shareholder activism drives better corporate governance because it ensures strong governance and approaches to investment styles that produce value for shareholders. Good corporate governance takes for granted that boards will continuously work toward board compositions that support the necessary skills and experience that will net long-term success for the company.

The principles of good corporate governance also place a heavy focus on the fiduciary responsibilities of board directors in managing the corporation's assets. The focus on duty of care creates an environment in which shareholders are more apt to ask more questions about how the board and managers approach strategic planning, risk management and operations.

7.0 CORPORATE GOVERNANCE AND COMPLIANCE TO RISK

7.1 INTRODUCTION

"Governance is the culture, values, mission, structure, layers of policies, processes and measures by which organizations are directed and controlled". Governance defines how the organization should perform, describing through policies what is acceptable and unacceptable and compliance is the area responsible for inspecting and proving that they are adequate, being implemented and followed.

Governance is also responsible for risk and compliance oversight, as well as evaluating performance against enterprise objectives. The board acts as an active monitor for shareholders' and stakeholders' benefit, with the goal of Board oversight to make management accountable, and thus more effective. Accordingly, governance should be able to understand and foresee the organization's vulnerabilities and, hence make decisions to reduce them. Also, governance should distribute power to provide insight and intelligence, at the right time, so that the right people in the management can make risk-aware decisions in accordance with key business objectives. Risk-awareness is possible through the close proximity that governance should have with risk management, which may provide very useful information in strategy setting and decision making. Governance needs to touch every part of the organization. It needs to be at the heart of corporate culture when in today's complex global ecosystems, risks are becoming more interconnected.

In the current globalised world, economies and business networks are so deeply interconnected that a single risk event can cause widespread disruption. Risks themselves are becoming more interconnected. The World Economic Forum's report on the top risks of 2017 emphasized how deep the links are between risks such as unemployment and social instability. Even regulatory enforcement risks are crossing boundaries, as is evident through corporations being fined by cross-jurisdictional regulators. Today, compliance risks are not just compliance risks; they are also reputational risks, strategic risks, and financial risks. It is crucial to understand these interconnections to build risk maturity.

With the advent of a younger workforce and technologies such as the cloud and mobility, the emphasis is on the consumerisation. People want simple and contextual information and accessibility available to them anywhere, anytime. Efficiency is also becoming important. Today, companies need to know less about what happened, and more about what is happening, what is likely to happen, and what needs to be done – the possible scenarios, decisions, and constraints. They also need to be able to tie all this information back to their core business performance.

Today, corporations and government agencies are facing an unprecedented wave of regulatory obligations and increased penalties for non-compliance. The financial services sector, as an example, needs to comply with a myriad of prudential regulations, RBI laws, AML compliances, consumer credit and protection laws to name a few. If companies want to move up the risk maturity curve, they need to find ways of tying various Governance and Compliance elements together with risks.

Compliance with law and regulation must be managed as an integral part of any corporate strategy. The board of directors and management must recognize the scope and implications of laws and regulations that apply to the company. They must establish a compliance management system as a supporting system of risk management system as it reduces compliance risk to a great extent. To ensure an effective approach to compliance, the participation of senior management in the development and maintenance of a compliance program is necessary. They should review the effectiveness of its compliance management system at periodic intervals, so as to ensure that it remains updated and relevant in terms of modifications/ changes in regulatory regime including acts, rules, regulations etc. and business environment.

Every organization has a responsibility to identify existing and emerging legislation relevant to its business and ensure that risks that may arise from the compliance requirements are well understood by the board and management. The risks that may stem from non-compliance with key legislative requirements can be very costly and damaging to an organization and the custodians of governance within the organization.

The consequences of non-compliance range from penalties and fines, to imprisonment, withdrawal of licenses, lawsuits and reputational risk which may individually and or collectively have a fundamental impact on the organisation's sustainability as a going concern; as well as the impact that a lack of good corporate governance at board and business levels can have on the business. The impact and probability of the risks that the legislation represents depend on the attention paid to the legislation and how well risk and compliance management is entrenched within the organisation. It is therefore critical that an organisation implements relevant structures and processes to effectively manage and monitor the compliance process to ensure that these are entrenched in a way that compliance becomes "second nature". The residual risk will also be high until the organisation is able to implement measures or controls that effectively mitigate the new risks arising out of compliance requirements for the new legislation.

7.2 COMPLIANCE RISK

Compliance risk is exposure to legal penalties, financial forfeiture and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices. Compliance risk is also sometimes known as integrity risk. Many compliance regulations are enacted to ensure that organizations operate fairly and ethically. For that reason, compliance risk is also known as integrity risk. This risk is closely interconnected with the operational risk, legal and reputation, so that from one follows the other.

Compliance risk is the threat posed to a company's earnings or capital as a result of violation or non conformance with laws, regulations, or prescribed practices. Companies that fail to comply with the necessary standards may be subjected to fines, payment of damages, and voided contracts. This, in turn, can lead to diminished reputation and limited business opportunities as the company finds its franchises reduced in value and its potential for expansion curtailed. In extreme cases, the company may find it is no longer capable of enforcing its contracts.

7.3 COMPLIANCE RISK MANAGEMENT

Compliance risk management is the process of managing corporate compliance to meet regulations within a workable timeframe and budget. Compliance Risk management is part of the collective governance, risk management and compliance discipline. The three fields

frequently overlap in the areas of incident management, internal auditing, operational risk assessment, and compliance with various regulations.

In recent years, perception of compliance has undergone a sea change. The traditional and narrow outlook that compliance is limited to statutory filings, required to run a business, has widened considerably. Compliance practices are now a cross-functional responsibility. They need to be integrated in the policies and procedures of various functions like HR, quality, risk, facilities, finance, delivery, sales, marketing, procurement, security and more.

Further, laws and regulations in different countries at the national, state and local levels have made compliance more complicated. Therefore, a culture must be instilled in an enterprise to ensure minimum statutory compliance and compliance to other commitments such as social, industry, client consumer etc. This calls for a systematic approach towards compliance management.

As compliance risk continues to be a focal point for regulators, compliance officers are encouraged to take steps to ensure that compliance risk is adequately managed. Best practices for compliance management ensure that compliance risk is adequately managed. On a periodic basis, management should identify and assess the primary compliance risk issues applicable to all business activities including the related control mechanisms utilized to identify measure, monitor and control the relevant risks as ccompliance challenges will only increase with time.

7.4 STEPS IN COMPLIANCE RISK MANAGEMENT

1. **Understand compliance obligations:** The primary element to manage compliance is to understand compliance obligation in the light of strategic goals and objectives. Compliance obligations stem from: Laws and regulations, industry or generic standards, internal policies, processes and procedures and contracts executed with clients and other stakeholders.

   It is important to understand that obligations are either requirements or commitments. Obligations that an enterprise has no control over are termed as compliance requirements, for example, one resulting from new laws and regulations.

While obligations that an enterprise may choose to abide by – for example certain industry standards or best practices – are termed as compliance commitments.

Here, a mechanism to ensure compliance obligations are kept up-to-date must be established. An enterprise may choose to restrict the scope of compliance management to compliance requirement but for a higher assurance, it may include compliance commitments, too.

2. **Assess risks:** Once compliance obligations are established, a compliance risk assessment exercise should be undertaken to identify risks, causes, the areas they impact and the consequences thereof. A risk analysis to have better understanding of the risks should follow. Such an analysis should consider the factors affecting the consequences and likelihood of these consequences occurring as well as the controls in place. Looking at the level of risk arrived at from the analysis exercise; a compliance risk evaluation should be done to take appropriate decisions on treatment. This exercise is to priorities the treatment; it should be used as a tool to accept compliance risks. Compliance risks analyzed as low should also be monitored and subjected to corrective action.
3. **Address all compliance risks:** An enterprise should ensure an effective action plan to address all compliance risks with clear ownership, responsibility, accountability and closure timelines. This can be driven with ease, if the enterprise ensures a documented compliance policy, objectives, processes and procedures. Further, compliance responsibilities must be clearly identified, assigned and established as part of the job descriptions at different levels.

   To ensure risks are addressed effectively, the management should ensure that all employees with compliance obligation are competent. Periodic training and awareness must be carried out and any other medium to communicate assigned responsibilities should be explored. A continuous communication mechanism is required to ensure all employees understand compliance and contribute to it by reporting risks and discharging their responsibilities effectively.
4. **Evaluate performance:** A mechanism to measure and monitor the performance of the compliance practices and its impact on strategic goals and objectives must be developed. Developing compliance performance indicators is one of the tools. It can be as simple as the number of employees trained on compliance practices to mature indicators such as risks of non-compliance and trends. Feedbacks from clients, stakeholders, suppliers, vendors, employees and government agencies are a good source of data to ascertain compliance performance. Governance mechanisms in the form of management reviews, internal audits and periodic compliance reporting give great insights on the performance of compliance practices.

7.5 COMPLIANCE RISK MITIGATION

New ethics, compliance, and reputational risks appear each day. At the same time, the recent global recession has forced many organizational functions to closely examine their budgets and resources. Together, these factors have created a tension between growing regulatory obligations and the pressure to do more with less. To help resolve this situation and continue to add value to their organizations, ethics and compliance professionals need to be sure they understand the full spectrum of compliance risks lurking in each part of the organization. They then need to assess which risks have the greatest potential for legal, financial, operational, or reputational damage and allocate limited resources to mitigate those risks. There are a number of critical questions organizations should ask related to compliance risks and the program(s) in place to mitigate those risks:

- ⇨ What kinds of compliance failures would create significant brand risk or reputational damage? Could the failures arise internally, in the supply chain, or with regard to third parties operating on the organization's behalf?
- ⇨ What is the likely impact of that damage on the organization's market value, sales, profit, customer loyalty, or ability to operate?
- ⇨ What kinds of compliance missteps could cause the organization to lose the ability to sell or deliver products/services for a period of time?
- ⇨ How should the compliance program design, technology, processes, and resource requirements change in light of growth plans, acquisitions, or product/category/ service expansions?
- ⇨ Is the organization doing enough to inform customers, investors, third parties, and other stakeholders about its vision and values?
- ⇨ Is it making the most of ethics, compliance, and risk management investments as potential competitive differentiators?
- ⇨ What are the total compliance costs—beyond salaries and benefits at the centralized level—and how are costs aligned with the most significant compliance risks that could impact the brand or result in significant fines, penalties, and/ or litigation?
- ⇨ How well-positioned is the compliance function? Does it have a seat "at the table" in assessing and influencing strategic decisions?
- ⇨ What are the personal and professional exposures of executive management and the board of directors with respect to compliance?

While it is impossible to eliminate all of an organization's risk exposure, the risk framework and methodology help the organization prioritize which risks it wants to more actively manage. Developing a framework and methodology helps organizations determine the extent to which

the organization's existing risk-mitigation activities (for example, testing and monitoring or employee training programs) are able to reduce risk.

Effective risk mitigation activities may reduce the likelihood of the risk event occurring, as well as the potential severity of impact to the organization. When an organization evaluates inherent risk in light of its existing control environment and activities, the degree of risk that results is known as the "residual risk." If existing risk mitigation strategies are insufficient at reducing residual risk to an acceptable level, this is an indication that additional measures are in order.

Embedding compliance with all key legislation in the organisation is a function of certain critical activities and stems from collaboration across key functions such as Legal, Compliance, Risk Management, Business and Internal Audit. These functions all form part of the "three lines of defence". The success of any compliance management and monitoring programme depends on the existence, functioning and integration of these lines of defence in the performance of their duties.

Management Assurance	✓ Assists in setting and executing strategies. ✓ Provides direction, guidance and oversight ✓ Promotes a strong risk culture & sustainable risk return thinking ✓ Promotes a strong compliance culture and management of risk ✓ exposure. ✓ Ongoing monitoring and management of risks.
Risk Management, Legal & Compliance	✓ Formal, robust and effective risk management within which the ✓ organization's policies and minimum standards are set. ✓ Objective oversight and the ongoing challenge of risk mitigation, ✓ management and performance while reporting is achieved across the ✓ business units. ✓ Overarching risk oversight across all risk types. ✓ Compile and maintain a legislative universe for the organisation. ✓ Facilitate the risk prioritization of all pieces of legislation in the regulatory ✓ universe. ✓ Initiate new legislative requirements within the organisation. ✓ Analyse and send out alerts on the new law to inform the organisation ✓ of the new requirements.

	✓ Facilitate an executive review of the legislation by Legal analysts. ✓ Facilitate the completion of the Compliance Risk Management Plan ✓ ("CRMP") ✓ Update compliance monitoring plans on the CRMP. ✓ Escalate compliance matters to management. ✓ Undertake quarterly compliance reporting. ✓
Internal Audit & other **Independent Assurance Providers**	✓ Independent and objective assurance of overall adequacy and ✓ effectiveness of governance, risk management and internal controls ✓ within the organisation ✓ Ability to link business risks with established processes and provide ✓ assurance on the effectiveness of mitigation plans to effectively ✓ manage organisational risks.

The Risk Management function should support the Compliance Office with the risk rating of the relevant legislation once such legislation becomes operational in the business. A compliance risk register for the regulatory universe, showing both the inherent and residual ratings of each piece of legislation, based on impact and likelihood, should be the product of this process. The penalties - financial, imprisonment, etc - and other business risks associated with key provisions of the legislation should be identified and captured on the compliance risk register for the regulatory universe as management should know if a piece of legislation will affect shareholder value.

Business should also have its own Business Operational Compliance Officer / Champion who, upon receipt from the Legal / Compliance Officer, the information containing the executive review, compliance alert, CRMP and presentation material, will commence the operational monitoring of the compliance of business processes to the legislative requirements. Again, depending on the size and maturity of the organization, the roles of Legal / Compliance Officer can be combined with that of the Business Operational Compliance Officer, even that of the Risk Officer. This, of course, should be with due consideration of the nature and magnitude of business operations, the risk profiles as well as the cost and benefits of combining or separating the functions. Business should readily be able to provide Internal Audit with the legislative universe of the organisation for the commencement of a compliance audit.

Internal Audit, as the assurance provider, is responsible for reviewing the adequacy and effectiveness of the functioning of controls implemented by management to ensure compliance with legislative requirements.

In conducting a review of compliance within the organisation, Internal Audit should ask the following questions:

- ⇨ What are the pieces of legislation that should be reviewed?
- ⇨ What new processes are being put in place as a result of compliance requirements?
- ⇨ What new systems are being put in place to support and monitor compliance?

The span of the internal audit review will be: Legislation – Policy – Procedures – Systems / Processes.

Internal Auditors should be able to map the legislation to the existence of a policy and a risk map. They need to substantiate and audit compliance risk ratings that have changed, especially where residual ratings show improved controls. For example, if the organization has had many complaints escalated to an ombudsman, it is a likely indication of non-compliance and hence the applicable residual rating cannot be acceptable (green); it should probably be yellow or red.

From their review, Internal Auditors should be able to validate or provide the following inputs to the CRMP:

- ⇨ Impacted Areas – processes, systems and policies
- ⇨ Existing Controls
- ⇨ Additional Controls – arising from amendments to, or new legislation
- ⇨ Risk Exposure – High, Medium, Low
- ⇨ Responsible Party – Affected Parties
- ⇨ Monitoring Plan – Business Unit Compliance

Thus the compliance framework needs to be comprehensive, dynamic, and customizable, allowing the organization to identify and assess the categories of compliance risk to which it may be exposed. Some compliance risks are specific to an industry or organization—for example, worker safety regulations for manufacturers or rules governing the behavior of sales representatives in the pharmaceutical industry. Other compliance risks transcend industries or geographies, such as conflicts of interest, harassment, privacy, and document retention.

Essentials Of A Successful Compliance-Risk Management Program

Active board and senior management oversight	An effective board and senior management oversight is the cornerstone of an effective compliance
Effective policies and procedures	risk management process
Compliance risk analysis and comprehensive controls	Compliance risk management policies and procedures should be clearly defined and consistent with the nature and complexity of an institution's activities.
	Organizations should use appropriate tools in compliance risk analysis like self-assessment, risk maps, process flows, key indicators and audit reports; which enables establishing an effective system of i internal controls.
Effective compliance monitoring and reporting	Organizations should ensure that they have adequate management information systems that provide management with timely reports on compliance like training, effective complaint system and certifications.
Testing	Independent testing should be conducted to verify that compliance-risk mitigation activities are in place and functioning as intended throughout the organization.

7.6 NEW DEVELOPMENTS- GOVERNANCE AND RISK COMPLIANCE (GRC)

Until fairly recently, compliance was seen as a separate business practice, along with governance and risk management. However, over the past decade, these three disciplines have developed a considerable number of overlapping activities, such as internal audits, incident management, operational risk assessment, or compliance with regulatory programs. Today, many companies take an integrated approach to these three areas, referring to them collectively as Governance, Risk Management and Compliance (GRC).

GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity. Governance, risk and compliance (GRC) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. GRC is a set of processes and practices that runs across departments and functions. GRC might be enabled by a dedicated platform and other tools, although this is not mandatory. While organizations generally don't need to maintain a separate GRC department, most organizations have a team in place to manage the GRC platform and tools. The scope of GRC doesn't end with just governance, risk, and compliance management, but also includes assurance and performance management, information security management, quality management, ethics and values management, and business continuity management.

Effective GRC implementation helps the organization to reduce risk and improve control effectiveness, security and compliance through an integrated and unified approach that reduces the ill effects of organizational silos and redundancies.

As the world becomes more complex, enterprises need a range of GRC skills and capabilities that may not all be present with a single provider or a single business function. Some may lie with a consulting firm, others with a data or content firm, and still others with a technology platform provider or a system integrator. Going forward, the emphasis will be on how we can bring more of these companies and their capabilities together in a single, comprehensive GRC community – one that fosters open and transparent communication, and enables people to learn from each other's best practices and mistakes.

GRC professionals are increasingly being given a seat at the company strategy table, the revenue generating side. Decision-makers need them to interpret risk profiles and data, and provide intelligence on how to increase revenue and sales.

Soon, operating controls will not only help mitigate operational risk, but also enable faster go-to-market opportunities. Similarly, vendor risk management won't just be about calculating vendor risks, but also tying those metrics to vendor performance and charge backs. The emphasis, more and more, will be on linking GRC to business performance.

CHAPTER EIGHT

RISK MANAGEMENT

8.0 RISK MANAGEMENT

8.1 INTRODUCTION

Managing risk has become a critical element within most companies. The management of risk, though, can be structured differently within companies even for those within the same sector. So what is risk? In the business world, the word risk has come to mean an impediment to the achievement of an organization's objectives. As per the Oxford Dictionary- "Risk is Exposure to the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility'.

While some risk is inherent in every business, organizations and entrepreneurship need to be willing to take risks as without risk there can be no meaningful gain. Like stress one has to live with risk and it cannot be avoided. At best risk can be managed or mitigated. This does not imply taking risk for the sake of taking it rather at every step the risk need to be understood and managed to realize the ultimate gains. However, the cost of risk management failures is still often underestimated, both externally and internally, including the cost in terms of management time needed to rectify a situation where the risks were not understood and managed well. It may be appropriate to say that without "risk management" there is no sustainable gain possible.

Well governed firms ensure that risks are understood, managed, and appropriately communicated and shared. Organizations that manage risks effectively are more likely to protect themselves and succeed in growing their business on a sustainable and long term basis. The challenge in achieving a strong risk management culture for any business is that risk management does not remain outside the mainstream rather that it is fully integrated as good and necessary practice into the day-to-day and every operation and function and therefore covers the organizational practices comprehensively and intrinsically.

8.2 STEPS IN RISK MANAGEMENT PROCESS

The process of risk management consists of the following logical and sequential steps:

i. Risk Identification

Risk identification is the first stage of the risk management strategy. The origin/source of the risk is identified. For example a risk may be due to transport of hazardous raw material to the factory. So the source of the risk origin is utmost important and from this point the journey start to manage the risks.

By risk identification the organization is able to study the activities and places where its resources are placed to risk. Correct risk identification ensures effective risk management. If risk managers do not succeed in identifying all possible losses or gains that challenge the organization, then these non-identified risks will become non manageable. The first task of the risk management is to classify the corporate risks according to their different types. The first step in organizing the implementation of the risk management function is to establish the crucial observation areas inside and outside the corporation. Then, the departments and the employees must be assigned with responsibilities to identify specific risks.

The results of risk identification are normally documented in a risk register, which includes a list of identified risks along with their sources, potential risk responses and risk categories. This information is used for risk analysis, which in turn will support creating risk responses. Identified risks can also be represented in a risk breakdown structure - a hierarchical structure used to categorize potential project risks by source.

Though the major work on risk identification is usually done in the beginning of a project, it is important to remember that risk identification is an iterative process; new risks can be identified throughout the project life cycle as the result of internal or external changes to a project.

Objective : The objective of the risk identification process is to ensure that all potential project risks are identified. The ultimate purpose of risk identification is to minimize the negative impact of project hiccups and threats, and to maximize the positive impact of project opportunities. Awareness of potential project risks reduces the number of surprises during the

project delivery and, thus, improves the chances of project success, allowing the team to meet the time, schedule and quality objectives of the project. Finally, the purpose of risk identification is to provide information for the next step of the risk management process.

Process of Risk Identification : The process for risk identification starts by taking inventory of the potential project risks that can affect the project delivery. This step is crucial for efficient risk management throughout the project. The outputs of the risk identification are used as an **input for risk analysis, and they reduce a project manager's uncertainty. It is an iterative** process that needs to be continuously repeated throughout the duration of a project. The process needs to be rigorous to make sure that all possible risks are identified. An effective risk identification process should include the following steps:

ii. Risk Analysis

After identification of the risk parameters, the second stage is of analyzing the risk which helps to identify and manage potential problems that could undermine key business initiatives or projects.

To carry out a Risk Analysis, first identify the possible threats and then estimate the likelihood that these threats will materialize. The analysis should be objective and should be industry specific. Within the industry, the scenario based analysis may be adopted taking into consideration of possible events that may occur and its alternative ways to achieve the given target.

Risk Analysis can be complex, as it requires to draw on detailed information such as project plans, financial data, security protocols, marketing forecasts and other relevant information. **However, it's an essential planning tool, and one that could save time, money, and reputations.**

Risk analysis is useful in many situations like:

- ⇨ While planning projects, to help in anticipating and neutralizing possible problems.
- ⇨ While deciding whether or not to move forward with a project.
- ⇨ While improving safety and managing potential risks in the workplace.
- ⇨ While preparing for events such as equipment or technology failure, theft, staff sickness, or natural disasters.
- ⇨ While planning for changes in environment, such as new competitors coming into the market, or changes to government policy.
- ⇨ When all the permutations-combinations of possible events/ threats are listed while analyzing the risk parameters and the steps taken to manage such risks, the risk matrix is designed / popped-up before the decision making and implementing authority.

Process of Risk Analysis

Identify Threats: The first step in Risk Analysis is to identify the existing and possible threats that one might face. These can come from many different sources. For instance, they could be:

- ⇨ Human – Illness, death, injury, or other loss of a key individual.
- ⇨ Operational – Disruption to supplies and operations, loss of access to essential assets, or failures in distribution.
- ⇨ Reputational – Loss of customer or employee confidence, or damage to market reputation.
- ⇨ Procedural – Failures of accountability, internal systems, or controls, or from fraud.
- ⇨ Project – Going over budget, taking too long on key tasks, or experiencing issues with product or service quality.
- ⇨ Financial – Business failure, stock market fluctuations, interest rate changes, or non-availability of funding.
- ⇨ Technical – Advances in technology, or from technical failure.
- ⇨ Natural – Weather, natural disasters, or disease.
- ⇨ Political – Changes in tax, public opinion, government policy, or foreign influence.
- ⇨ Structural – Dangerous chemicals, poor lighting, falling boxes, or any situation where staff, products, or technology can be harmed.

A number of different approaches can be used to carry out a thorough analysis:

- Run through a list such as the one above to see if any of these threats are relevant.
- Think about the systems, processes, or structures used and analyze risks to any part of these.
- Ask others who might have different perspectives. Ask for input from team members and consult others in the organization, or those who run similar projects.
- Tools such as SWOT Analysis and Failure Mode and Effects Analysis can also help to uncover threats, while Scenario Analysis helps to explore possible future threats.

Estimate Risk: Once the threats are identified, it is required to calculate both the likelihood of these threats being realized, and their possible impact. One way of doing this is to make best estimate of the probability of the event occurring, and then to multiply this by the amount it will cost to set things on the right track. This gives a value for the risk:

- ⇨ Risk Value = Probability of Event × Cost of Even

- ⇨ You can also use a Risk Impact/Probability Chart to assess risk. This will help you to identify which risks you need to focus on.

iii. RISK ASSESSMENT

Risk assessment is the way in which enterprises get a handle on how significant each risk is to the achievement of their overall goals. To accomplish this, enterprises require a risk assessment process that is practical, sustainable, and easy to understand. The process must proceed in a structured and disciplined fashion. It must be correctly sized to the enterprise's size, complexity, and geographic reach.

When assessing risks, it's important to determine whether the risk is - inherent risk, residual risk, or both. Inherent risk as the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk remaining after management's response to the risk. **Some entities interpret:**

- ⇨ inherent risk to be level of risk assuming responses currently in place fail, and
- ⇨ residual risk to be the level of risk assuming existing responses operate according to design.

Some other entities interpret inherent risk to be the current level of risk assuming existing responses operate according to design and residual to be the estimated risk after responses under consideration are put into place. The first approach is focused more on controls effectiveness of the current environment and the second approach on evaluating risk response options. There is no one right answer and either approach may be useful depending upon the purpose of the assessment and the nature of the risks being considered.

Process of Risk Analysis

a) **Develop assessment criteria**: The first activity within the risk assessment process is to develop a common set of assessment criteria to be deployed across business units, corporate functions, and large capital projects. Risks and opportunities are typically assessed in terms of impact and likelihood. Many enterprises recognize the utility of evaluating risk along additional dimensions such as vulnerability and speed of onset.

b) **Assess risks**: Assessing risks consists of assigning values to each risk and opportunity using the defined criteria. An initial screening of the risks and opportunities is performed using qualitative techniques followed by a more quantitative treatment of the most important risks and opportunities lending themselves to quantification (not all risks are meaningfully quantifiable). Qualitative assessment consists of assessing each risk and opportunity according to descriptive scales as described in the previous section. Quantitative analysis requires numerical values for both impact and likelihood using data from a variety of sources.

- The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used. Model assumptions and uncertainty should be clearly communicated and evaluated using techniques such as sensitivity analysis. Both qualitative and quantitative techniques have advantages and disadvantages. Most enterprises begin with qualitative assessments and develop quantitative capabilities over time as their decision-making needs dictate.
- For qualitative assessments, the most commonly used assessment techniques are interviews, cross-functional workshops, surveys, benchmarking, and scenario analysis. Quantitative techniques range from benchmarking and scenario analysis to generating forward looking point estimates (deterministic models) and then to generating forward looking distributions (probabilistic models). Some of the most powerful probabilistic models from an enterprise-wide standpoint include causal at-risk models used to estimate gross profit margins, cash flows, or earnings over a given time horizon at given confidence levels.

c) **Assess risk interactions**: Risks do not exist in isolation. Enterprises have come to recognize the importance of managing risk interactions. Even seemingly insignificant risks on their own have the potential, as they interact with other events and conditions, to cause great damage or create significant opportunity. Therefore, enterprises are gravitating toward an integrated or holistic view of risks using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions.

d) **Prioritize risks: Once the risks have been assessed and their interactions documented, it's** time to view the risks as a comprehensive portfolio to enable the next step – prioritizing for risk response and reporting to different stakeholders. Risk prioritization is the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. While each risk captured may be important to management at the function and business unit level, the prioritization helps provide focus to senior management and board in addressing and giving attention to key risks. Ranking and prioritizing is often done in a two-step process.

- First, the risks are ranked according to one, two, or more criteria such as impact rating multiplied by likelihood rating or impact multiplied by vulnerability.
- Second, the ranked risk order is reviewed in light of additional considerations such as impact alone, speed of onset, or the size of the gap between current and desired risk level (risk tolerance threshold). If the initial ranking is done by multiplying financial loss by likelihood, then the final prioritization should take qualitative factors into consideration.

e) **Response to Risks**: The results of the risk assessment process then serve as the primary input to risk responses whereby response options are examined (accept, reduce, share,

or avoid), cost-benefit analyses performed, a response strategy formulated, and risk response plans developed.

f) **Effective and sustainable risk assessment process**: To be effective and sustainable, the risk assessment process needs to be simple, practical, and easy to understand. People aren't enough. To be efficient, they must be supported by the right technology.

iv. Handling of Risk

The ownership of risk should be allocated. Responsibilities and accountabilities of the persons handling risks need to be identified and assigned. The persons concerned when the risk arises, should document it and report it to the higher ups in order to have the early measures to get it minimized. Risk may be handled in the following ways:

a) **Risk Avoidance**: Risk Avoidance means to avoid taking or choosing of less risky business/project. For example one may avoid investing in stock market due to price volatility in stock prices and may prefer to invest in debt instruments.

b) **Risk Retention/absorption**: It is the handling the unavoidable risk internally and the firm bears/ absorbs it due to the fact that either because insurance cannot be purchased of such type of risk or it may be of too expensive to cover the risk and much more cost-effective to handle the risk internally. Usually, retained risks occur with greater frequency, but have a lower severity. An insurance deductible is a common example of risk retention to save money, since a deductible is a limited risk that can save money on insurance premiums for larger. There are two types of retention methods for containing losses as under:

   - ⇨ Active Risk Retention: Where the risk is retained as part of deliberate management strategy after conscious evaluation of possible losses and causes.
   - ⇨ Passive Risk Retention: Where risk retention occurred through negligence. Such type of retaining risk is unknown or because the risk taker either does not know the risk or considers it a lesser risk than it actually is.

c) **Risk Reduction**: In many ways physical risk reduction (or loss prevention, as it is often called) is the best way of dealing with any risk situation and usually it is possible to take steps to reduce the probability of loss. The ideal time to think of risk reduction measures is at the planning stage of any new project when considerable improvement can be achieved at little or no extra cost. The cautionary note regarding risk reduction is that, as far as possible expenditure should be related to potential future savings in losses and other risk costs; in other words, risk prevention generally should be evaluated in the same way as other investment projects.

d) **Risk Transfer**: This refers to legal assignment of cost of certain potential losses to another. The insurance of 'risks' is to occupy an important place, as it deals with those risks that could be transferred to an organization that specialises in accepting them, at a price. **Usually, there are 3 major means of loss transfer viz.,**

- ⇨ By Tort,
- ⇨ By contract other than insurance,
- ⇨ By contract of insurance.
- ⇨ The main method of risk transfer is insurance. The value of the insurance lies in the financial security that a firm can obtain by transferring to an insurer, in return for a premium for the risk of losses arising from the occurrence of a specified peril. Thus, insurance substitutes certainty for uncertainty. Insurance does not protect a firm against all perils but it offers restoration, atleast in part of any resultant economic.

e) **Risk Mitigation**

Risk mitigation is defined as taking steps to reduce adverse effects. Risk mitigation is the process by which an organization introduces specific measures to minimize or eliminate unacceptable risks associated with its operations. Risk mitigation measures can be directed towards reducing the severity of risk consequences,reducing the probability of the risk materializing, or reducing the organizations exposure to the risk. The risk mitigation step involves development of mitigation plans designed to manage, eliminate, or reduce risk to an acceptable level. Once risks have been identified and assessed, the strategies to manage the risk fall into one or more of the following categories:

f) **Transfer Risk**: Normally in projects assignments or multifaceted exercises, execution is fought with risks. Different agencies work together and these agencies take care to transfer risk in their areas to another agency which is better equipped to take care of a risk for a consideration. Here the concept of core competence curves in and whenever a particular agency, individual or a firm finds that it is dealing in an area where it does not have the core competence to deal with it seeks the help of another agency which has the specific core competence to transfer its own risk. The risk may be in the form of loss of reputation or sub quality performance and this risk is taken care of through transfer.

g) **Tolerate Risk or Risk Retention**: It is retention of the risk. It is accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided, reduced or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible.

- ⇨ War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amount of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the

chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

h) **Reduce Risk**: By far the greater number of risks will belong to this category. The purpose of treatment is not necessarily to obviate the risk, but more likely to contain the risk to an acceptable level. Internal controls are actions instigated from within the organization (although their effects may be felt outside of the organization) which are designed to contain risk to acceptable levels.

   ⇨ Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. In this case companies outsource only some of their departmental needs. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process.

   ⇨ Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project.

i) **Avoid Risk**: This method results in complete elimination of exposure to loss due to a specific risk. It can be established by either avoiding to undertake the risky project or discontinuance of an activity to avoid risk. This means that no risky projects are undertaken. Alternatively, a project may be abandoned midway to mitigate the risk while handling a project.

   ⇨ It is not performing an activity which could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the aeroplaneswere to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

j) **Combine Risk**: When the business faces two or three risks the overall risk is reduced by combination. This strategy is suitable mainly in the areas of financial risk. Different financial instruments say, shares and debentures are taken in a single portfolio to reduce the risk.

k) **Sharing Risk**: Insurance is a method of sharing risk for a consideration. For example by paying insurance premium the company shares the risk with companies and the insurance companies themselves share their risk by doing re-insurance.

l) **Hedging Risk**: Exposure of funds to fluctuations in foreign exchange rates, prices etc., bring about financial risks resulting in losses or gain. The downside risk is often taken care.

8.3 CONNECTION BETWEEN RISK MANAGEMENT & CORPORATE GOVERNANCE

Corporate Governance is connected to risk management in that the Board of Directors of a company bear the responsibility to look after the company's assets and protect value of shareholder investments by:

- ⇨ Preventing losses through error, omission, fraud and dishonesty.
- ⇨ Ensuring that known and identified risks are managed properly to mitigate and reduce damage and losses to company assets and investments made into the company business.

- ⇨ Failure to identify, monitor, control and contain risks invariably leads to financial collapses of company businesses.

- ⇨ By way of emphasis the Board of Directors of a company bears the ultimate responsibility for risk management.

Risk Evaluation

- ⇨ After identification, assessment and mapping of risks, a company must have a procedure to rank, categorise and anticipate them.

- ⇨ The ranking of risks is guided by the **risk size** or **its impact** and the **likelihood** or **probability** of its occurrence.

- ⇨ The anticipation of risks as part of risk evaluation is guided by the following characteristics. (***See King III Pages 77 – 78***)

    - **Insight** – the ability to identify the root cause of the risk, where there are multiple causes or root causes that are not immediately obvious.

    - **Information** – comprehensive information about all aspects of risks and risk sources especially of financial risks.

    - **Incentives** – the ability to separate risk origination and risk ownership, ensuring proper due diligence and accountability.

    - **Instinct** – the ability to avoid "following the head" when there are systemic and pervasive risks.

    - **Independence** – the ability to view the company independently from its environment.

    - **Interconnectivity** – the ability to identify and understand how risks are related, especially when their relatedness might exacerbate the risk.

The ranking and anticipation of risks can yield the following possible broad **types of risks**:

- ⇨ **Strategic risks** – those associated with the planning of the business and its future strategy.

- ⇨ **Operational risks** – those concerned with the day to day management of the company, e.g. customer spend being over or lower than expected, the risk of obsolescence, i.e. producing a product with no market, and the risk of damage to material and human resources of the business, etc.

- ⇨ **Financial risk – the possibility that the company's financial situation might turn** out to be different from what was expected, e.g.

- ⇨ **Credit risks** – bad debt losses for companies in the lending business.
- ⇨ **Foreign exchange risk** – losses associated with volatile currency rate exchanges.

- ⇨ **Interest rate risk** – losses associated with the rise and fall of interest rates more pronounced in the banking sector.

- ⇨ **Business continuity risk** – i.e. insolvency and associated risks.

- ⇨ **Non-Financial Risk** – e.g. sustainability risks focusing on health, social and environmental issues relevant to the business.

- ⇨ **Compliance risk** – associated with complying with laws, regulations, and codes of best practices.

- ⇨ **Fraud Risk**- Fraud is a deliberate action to deceive another person with the intention of gaining some things. Fraud can loosely be defined as "any behavior by which one person intends to gain a dishonest advantage over another". In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise.

    - For prevention of the fraud, there should be in existence a robust internal check and control systems. For example in banking there is a concept of 'maker' and 'checker'. The day today transactions are entered by the maker and another person validates the transactions. So it is a self balancing system. Further the internal/ concurrent audit also helps in early detection of the frauds. The management should be pro-active in fraud related matter. A fraud is usually not detected until and unless it is unearthed.

- Fraud Risk Management Policy should be incorporated, aligned to its internal control and risk management. Such policy/plan protects the company from any kind of uncertain happening which leads the company to a huge loss or damage (brand reputation, financial loss, assets). The Fraud Risk Management Policy will help to strengthen the existing anti-fraud controls by raising the awareness across the Company and (i) Promote an open and transparent communication culture (ii) Promote zero tolerance to fraud/misconduct (iii) Encourage employees to report suspicious cases of fraud/misconduct. (iv) Spread awareness amongst employees and educate them on risks faced by the company. Such a policy may include the following:

Defining fraud: This shall cover activities which the company would consider as fraudulent.

⇨ Defining Role & responsibilities: The policy may define the responsibilities of the officers who shall be involved in effective prevention, detection, monitoring & investigation of fraud. The company may also consider constituting a committee or operational structure that shall ensure an effective implementation of anti-fraud strategy of the company. This shall ensure effective investigation in fraud cases and prompt as well as accurate reporting of fraud cases to appropriate regulatory and law enforcement authorities.

⇨ Communication channel: Encourage employees to report suspicious cases of fraud/misconduct. Any person with knowledge of suspected or confirmed incident of fraud/misconduct must report the case immediately through effective and efficient communication channel or mechanism.

⇨ Disciplinary action: After due investigations disciplinary action against the fraudster may be considered as per the company's policy.

⇨ Reviewing the policy: The employees should educate their team members on the importance of complying with Company's policies & procedures and identifying/ reporting of suspicious activity, where a situation arises. Based on the developments, the policy should be reviewed on periodical basis.

Reputation Risk -the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (eg through the interbank or securitization markets).

Loss of Reputation has long lasting damages like:

- ⇨ It destroys the Brand Value
- ⇨ Steep downtrend in share value.
- ⇨ Ruined of Strategic Relationship
- ⇨ Regulatory relationship is damaged which leads to stringent norms.
- ⇨ Recruitment to fetch qualified staff as well the retention of the old employees becomes difficult. **For managing the reputation risk, the following principles are worth noting:**
    - Integration of risk while formulating business strategy.
    - Effective board oversight.
    - Image building through effective communication.
    - Promoting compliance culture to have good governance.
    - Persistently following up the Corporate Values.
    - Due care, interaction and feedback from the stakeholders.
    - Strong internal checks and controls
    - **Peer review and evaluating the company's performance.**
    - Quality report/ newsletter publications
    - Cultural alignments

8.4 ENTERPRISE RISK MANAGEMENT

The Enterprise Risk Management – Integrated Framework which is one of the most widely recognized and applied enterprise risk management frameworks in the world. It provides a principles-based approach to help organizations design and implement enterprise-wide approaches to risk management.

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows:

- ⇨ **Enterprise risk management is a process, effected by an entity's board of directors,** management and otherpersonnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations,

industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives.

Enterprise risk management encompasses:

- *Aligning risk appetite and strategy* – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- *Enhancing risk response decisions* – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- *Reducing operational surprises and losses* – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- *Identifying and managing multiple and cross-enterprise risks* – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- *Seizing opportunities* – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- *Improving deployment of capital* – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

8.4.1 Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process.

These components are:

- *Internal Environment* – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

- ⇨ *Event Identification* – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities.
- ⇨ Opportunities are channeled back to management's strategy or objective-setting processes.
- ⇨ *Risk Assessment* – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- ⇨ *Risk Response* – Management selects risk responses – avoiding, accepting, reducing, or sharing risk
  - developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- ⇨ *Control Activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- ⇨ *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- ⇨ *Monitoring* – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

8.4.2 Limitations

While enterprise risk management provides important benefits, limitations exist. In addition to factors discussed above, limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions.

These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

8.4.3 Roles and Responsibilities

Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership. Other managers support the entity's risk management philosophy, promote compliance with its risk appetite,

and manage risks within their spheres of responsibility consistent with risk tolerances. A risk officer, financial officer, internal auditor, and others usually have key support responsibilities.

Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols. The board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite. A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management.

8.4.4 International Standards on Risk Management

ISO 31000 is the international standard for risk management. This standard is published on the 13th of November 2009. By providing comprehensive principles and guidelines, this standard helps organizations with their risk analysis and risk assessments. ISO 31000 applies to most business activities including planning, management operations and communication processes. Whilst all organizations manage risk to some extent, this international standard's best-practice recommendations were developed to improve management techniques and ensure safety and security in the workplace at all times.

By implementing the principles and guidelines of ISO 31000 in organization, the organisation is able to improve operational efficiency, governance and stakeholder confidence, while minimising losses. This international standard also helps to boost health and safety performance, establish a strong foundation for decision making and encourage proactive management in all areas.

8.4.5 Scope

ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization. This approach to formalizing risk management practices will facilitate broader adoption by companies who require an enterprise risk management standard that accommodates multiple 'silo-centric' management systems.

ISO 31000 is not developed for a particular industry group, management system or subject matter field in mind, rather it provides best practice structure and guidance to all operations concerned with risk management. The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes be aligned to a common set of risk management objectives.

Accordingly, ISO 31000:2009 is intended for a broad stakeholder group including:

- ⇨ executive level stakeholders
- ⇨ appointment holders in the enterprise risk management group
- ⇨ risk analysts and management officers

- ⇨ line managers and project managers
- ⇨ compliance and internal auditors
- ⇨ independent practitioners.

8.4.6 Benefits of ISO 31000

ISO 31000 contains 11 key principles that position risk management as a fundamental process in the success of the organization.

ISO 31000 is designed to help organizations:

- ⇨ Increase the likelihood of achieving objectives
- ⇨ Encourage proactive management
- ⇨ Be aware of the need to identify and treat risk throughout the organization
- ⇨ Improve the identification of opportunities and threats
- ⇨ Comply with relevant legal and regulatory requirements and international norms
- ⇨ Improve financial reporting
- ⇨ Improve governance
- ⇨ Improve stakeholder confidence and trust
- ⇨ Establish a reliable basis for decision making and planning
- ⇨ Improve controls
- ⇨ Effectively allocate and use resources for risk treatment
- ⇨ Improve operational effectiveness and efficiency
- ⇨ Enhance health and safety performance, as well as environmental protection
- ⇨ Improve loss prevention and incident management
- ⇨ Minimize losses
- ⇨ Improve organizational learning
- ⇨ Improve organizational resilience.
- ⇨ Proactively improve operational efficiency and governance

8.4.7 Managing risk

ISO 31000:2009 gives a list on how to deal with risk:

- ⇨ Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- ⇨ Accepting or increasing the risk in order to pursue an opportunity
- ⇨ Removing the risk source

- ⇨ Changing the likelihood
- ⇨ Changing the consequences
- ⇨ Sharing the risk with another party or parties (including contracts and risk fiinancing)
- ⇨ Retaining the risk by informed decision

CHAPTER NINE
INTERNAL CONTROLS AND RISK

9.0 INTERNAL CONTROLS AND RISK

9.1 INTRODUCTION

Risk management focuses on identifying threats and opportunities, while internal control helps counter threats and take advantage of opportunities. Proper risk management and internal control assist organizations in making informed decisions about the level of risk that they want to take and implementing the necessary controls to effectively pursue their objectives.

Successful organizations integrate effective governance structures and processes with performance-focused risk management and internal control at every level of an organization and across all operations.

The risk profile of a company may be represented through a Risk Register, a suggestive template of which is illustrated below:

Sl.No	Risk Area	Key risks	Root cause	Mitigation measures
1.	Business Risk	Decreasing market share	Lack of innovation, market survey etc.,	Keeping a vigil on latest developments and continuous monitoring
2.	Financial risk	Leveraging capital structure and the cash flows	Inability to assess the appropriate funding requirements	Adoptiong a Resource planning policy
3.	Regulatory and Compliance Risk	Non compliance of applicable laws	Not keeping abreast of the latest changes in the Regulatory environment	knowledge updation & maintenance of a robust compliance check list

9.2 RISK CONTROL MEASURES AND REVIEW

- After mapping, ranking, anticipating and categorising risks and coming up with an appropriate regime of responses thereto, companies should have **control measures** to monitor and review such identified risks in the context of the distilled responses to the risks.

- Control measures are provided through a system of internal control.

- An internal control system consists of a **control environment** on one hand and **control procedures** on the other.

- A **control environment** encompasses corporate culture, management style and employee and other stakeholder attitude to control procedures – it is a critical stakeholder awareness of and attitude to, internal controls of the company.

- ⇨ **Control procedures and policies** are those devised and enforced to ensure the orderly and efficient conduct of the **company's business such as –**

    - Safeguarding the assets of the business.
    - Preventing and detecting fraud and error.
    - Ensuring the accuracy and completeness of accounting records and timely preparation of reliable information.
    - Compliance with laws, regulations and best practice codes on corporate governance.

- ⇨ Several types of internal control systems exist. An old guideline of the UK Auditing Practices Board can be used to categorise them.

The guidelines are best remembered by the Mnemonic Spamsoap meaning :

- ⇨ **Segregation of duties** – where possible duties should be split between two or more people so that the work done by one person acts as a check on the work done by the other. With segregation of duties, it is more difficult for fraud to take place because several individuals will have to collude in the fraud. It is more difficult for accidental errors to occur because when several people are involved in the task, they act as a check on each other.

- ⇨ **Physical controls** – measures to ensure the physical safety of assets such as putting cash in a safe, banking cash receipts immediately and preventing unauthorized access to computer systems through the use of passwords and internet firewalls.

- ⇨ **Authorisation and approval** – all financial transactions should require the authorization or approval of an appropriate responsible person, and there should be a spending authorization limit that each responsible person can approve.

- ⇨ **Management controls** – management should exercise control over financial systems, e.g. by preparing a budget and then monitoring actual performance by comparing it with the budget. Management controls can also be exercised by reviewing other financial statements such as the balance sheet, profit and loss account, and cashflow statement.

- ⇨ **Supervision** – the day to day work of employees should be properly supervised. Good supervision will reduce the likelihood of errors or fraud.

- ⇨ **Organisation** – everyone should be fully aware of his or her responsibilities and lines of authority, lines of reporting and levels of responsibility should be clear. Errors and fraud are much more likely where it is uncertain who is responsible for what and who should be reporting to whom.

- ⇨ **Arithmetical and accounting controls** – these are procedures in an accounts office to check the accuracy of the records and the numbers. They include the use of control totals and reconciliations.

⇨ **Personnel** – the quality of internal controls is dependent on the quality of the individuals working in the organization and personnel selected to do a job should have the right personal qualities and be properly trained and/or qualified.

⇨ The nature and extent of internal controls in an organization depend on the size of the organization, what controls it can afford and whether the benefits obtained from any particular control measure are sufficient to justify its cost.

⇨ The UK Turnbull Committee Report on internal control is a must read. The committee was set up by the Chartered Accountants of England and Wales after the publication of the combined Code. In addition to the several types of control measures personified by **Spamsoap**, the following minimum control measures need also to be in place to establish and maintain a sound system of internal control.

⇨ **These are :**

- **Internal Auditors**, where appropriate, should be considered depending on the nature and size of the company and the diversity and complexity of its business activities.

- An internal audit is "... an independent appraisal activity within an organization ... a control which functions by examining and evaluating the adequacy and effectiveness of other controls." (***See Coyle Page 161***)

- An internal auditor

  - ✓ Acts independently of executive management. **N.B.** Internal auditor independence is questionable because they are employees of the organization and report to someone on the organizational structure. If the internal auditor reports to a Finance Director, he or she will find it difficult to be critical of the Finance Director himself. Accordingly independence of the internal auditors could be compromised.

  - ✓ Reports to the Board or Audit Committee Chairs on notice to the CEO and Finance Director.

  - ✓ Should be appointed and dismissed only with the approval of the Audit Committee or Board where appropriate.

  - ✓ Should take a risk based approach to planning as opposed to compliance based approach.

  - ✓ Should be informed by the strategy of the company in his planning and approach to the work he has to do.

- **An internal auditor performs various tasks, including:**

  - ✓ **Carrying out checks on the organisation's financial controls to establish** whether such controls exist and if so whether they are properly and effectively applied.

  - ✓ **Conducting special investigations into particular aspects of the organisation's** operations.

  - ✓ Investigating the timeliness of reporting and the accuracy of the information in reports generated and circulated within the organization.

  - ✓ Carrying out value for money audits (VFM) on an operation or activity to establish whether it is economical, efficient and effective.

  - ✓ Revising compliance by the organization with particular laws, regulations and best practice codes.

  - ✓ Investigating aspects of risk management including the adequacy of the mechanisms for identifying, assessing, ranking and controlling significant risks to the organization.

  - ✓ Ensuring that internal audit reporting meets management and Audit Committee requirements.

  - ✓ Acting in terms of the Internal Audit Charter and Plans established and approved by the Board and/or its Audit Committee.

- **Audit Committees** must, where appropriate, be in place, depending on the nature and size of the company and the complexity and diversity of its operations. We have already discussed audit committee composition and who should chair it. We have already discussed some of its roles and functions.

- **In addition, an Audit Committee must**

  - ✓ approve the risk based internal audit plan.

  - ✓ Evaluate the performance of the internal audit function yearly. (***See Page 6 of King III***).

- **The broad purpose of having an audit committee is to:**

  - ✓ Help the Board of Directors to fulfill its obligations in respect of the financial reporting by appointing Board members to consider audit matters.

  - ✓ Strengthen the independence of the external auditors by providing them with another channel of communication with the Board other than the Chairman of the Board, CEO or Finance Director.

- ✓ Indirectly, increase public confidence in the credibility of the company's financial statement.

The Audit Committee functions vary between companies but may include the following:

- ⇨ Recommending the nomination and remuneration of External Auditors.
- ⇨ Reviewing the external audit carried out by auditors.
- ⇨ Discussing with the external auditors any problems that arise in the audit.
- ⇨ Reviewing the company's accounting policies and the need to make changes to these, e.g. when a new accounting standard is issued.
- ⇨ Reviewing the company's internal control procedures.
- ⇨ Reviewing reports from the company's internal audit department providing an independent reporting channel for the internal auditors who would otherwise report to the Finance Director.
- ⇨ Reviewing the half year and annual financial statements prior to the approval of the statements by the Board.
- ⇨ Reviewing the independence and objectivity of the auditors of the company.
- ⇨ Appointing the Chief Financial Officer or Financial Director and reviewing his performance.
- ⇨ Ensuring that the internal control procedures within the company are adequate.
- ⇨ Appointing a new firm of auditors and negotiating the audit fee.
- ⇨ Preparing their terms of reference for adoption by the Board and ensuring that they act within those terms.

External Auditors – these are a necessary party to the establishment and maintenance of a sound internal regime of controls for an organization.

An external auditor or auditors must be independent in that they have no material relationship with the entity whose financial statements are being audited.

The purpose of external auditors is to ensure that financial statements of an organization are objective and can be relied upon.

External auditors prepare an audit report for consumption by shareholders of the company.

The audit report serves two main purposes:

- ⇨ To give and expert and independent opinion about whether the financial statements give a true and fair view of the financial position of the company as at the end of the financial year covered by the report.
- ⇨ To give an expert and independent opinion on whether financial statements comply with the relevant laws, standards and best practice codes.
- ⇨ To give users of company financial statements some reassurance that the information in the statements is believable.

The audit report provides only limited information to shareholders which include:

- ⇨ **An unqualified opinion** – which is given when the auditor believes that the accounts give a true and fair view of the company's financial position and performance. The wording is fairly standard.

- ⇨ **A qualified opinion** – in which the auditor believes the financial statements give a true and fair view except for a particular matter, over which disagreement with company's management is so great as to justify a disclaimer or an adverse opinion.
- ⇨ **Disclaimer of opinion** – which is a refusal by the auditor to give an opinion on a particular item in the financial statement and if appropriate where the auditor has been unable to obtain sufficient audit evidence and the amount involved could be material.
- ⇨ **Adverse opinion** – which is the most negative type of modified audit report and is given when there is a disagreement between the auditors and the company's management and the auditor believes that the financial statements are misleading or incomplete in a material or pervasive way.
    - ✓ External auditors are expected to be independent, ethical and professional. Their conduct must answer into professional quality tests by their regulating board. Unethical conduct by external auditors lead to financial corporate collapses exemplified by the Enron, world.com, etc, etc.
    - ✓ Recent external auditor concerns have revived the debate whether legislation or regulation is necessary to promote auditor independence and professional and ethical conduct on their part.
    - ✓ In the USA the Sarbanes-Oxley Act, which is a corporate accountability legislation was enacted in July 2002.
    - ✓ In the UK at the beginning of 2002, the Accountancy Foundation was established with the sole purpose of ensuring that the accountancy profession operates in the public interests so as to generate public confidence in its impartiality and effectiveness. Also the Ethics Standards Board was established in 2002 to develop ethical standards for the entire accountancy professional and not just for auditors in the UK and the Investigation and Discipline Board was established to provide a scheme for investigating and dealing with cases of special public interests where an element of wrongdoing involving accountancy is suspected.
    - ✓ In Zimbabwe we have the Institute of Chartered Accountants of Zimbabwe which is a body which regulates the conduct of Accountants including Auditors in Zimbabwe.

Risk Control Review- After setting up a system of internal control with all the appropriate checks and balances, that system needs to be subjected to periodic reviews by the Board of Directors represented by the Audit Committee working in conjunction with the Internal Auditor and External Auditors. How soon and what triggers such review will vary from one company to another depending on the size, complexity and diversity of its business operations.

Whistle blowers – as a control measure, is gaining prominence and recognition in the corporate governance discourse.

A whistle blower is an employee who provides information about his or her company, which he or she reasonably believes provides evidence of –

- Violation of law or regulation by the company
- A miscarriage of justice
- Financial malpractice
- A danger to public health and safety

In the government sector, a whistle blower provides evidence of a gross waste of public funds or gross mismanagement.

People blow the whistle because they have been unable to get a response from the company's management through normal lines of reporting and resort to go to someone else with the information for redress.

There is a strong connection between corporate governance and whistle blowing.

Whistle blowing by an employee helps to uncover significant risks and procedures should therefore exist to encourage **honest** whistle blowing whilst at the same time, discouraging malicious and unjustifiable accusations and allegations from employees against their bosses.

Concerns about whistle blowing have grown over the years for three main reasons:

- ⇨ Employees have unofficial access to official information which they use to blow the whistle for malicious reasons.
- ⇨ There is a strong culture of loyalty to the company by employees. Employees who question or criticize actions of management might be considered to be traitors.
- ⇨ Yet whistle played an important role in uncovering information about financial and accounting mismanagement at Enron in 2001 and world.com 2002 and in criticizing the handling of security information by the FBI before the September 11 terrorist attack in New York.
- ⇨ There is a case for retaining whistle blowing as a measure of internal control. Yet whistle blowing can be both malicious as well as honest.
- ⇨ Companies must take measures to manage whistle blowing in terms of procedure and in terms of analysing the reports received and acting on correcting the misconduct reported upon. Companies therefore must have policies and procedures for dealing with people who blow the whistle and these include the following:
- ⇨ A company must have a fair system for dealing with accusations from whistle blowers so that an honest individual does not feel under threat when making an allegation and employees ought to know what these procedures are.
- ⇨ These procedures could include the following arrangements:
- ⇨ The employer should make a formal statement to all employees that it takes seriously any genuine whistle blowing and the allegations of whistle blowers.
- ⇨ The employer should also indicate to employees what it would regard as a failure in the system sufficient to justify whistle blowing.
- ⇨ There should be respect for individuals who blow the whistle.
- ⇨ The company should give an assurance to its employees that it will take every measure to ensure that there is no victimization of a whistle blower.
- ⇨ The system should provide employees with an opportunity to voice their concerns outside the line management structures but still within the organization.
- ⇨ Whistle blowers should be able to take their concerns to the person designated to manage the whistle blowing procedures. The person designated to receive investigate and act upon complaints reported should either be an Internal Auditor or a Company Secretary or the service could be outsourced to a professional body such as a firm of accountants, e.g. the tip offs anonymous managed and supervised by the Delloittes & Touche audit firm.

- ⇨ However, employees making false claims or allegations should be subject to disciplinary measures by the employer and such disciplinary procedures should be made known to the employees in advance.
- ⇨ Such whistle blowing procedure should be documented and a copy given to every employee. It should give examples of the type if misconduct for which employees should use the procedure and set out the level of proof that there should be in an allegation.

9.3 RISK MATRIX

Risk Matrix is a matrix that is used during Risk & Control Self Assessment (RCSA) activity to define the various levels of risk at each stage, activity, process and sub-process. Risk Matrix comprises of :

- ⇨ Impact analysis
- ⇨ Likelihood
- ⇨ Operating Effectiveness
- ⇨ Design Effectiveness

Ratings are assigned to all above categories, pre and post control environment. Based on the ratings a Gross/ Inherent Risk Level and Residual Risk level is determined (HIGH/MEDIUM/LOW), respectively.

In the event where Residual Risk level is HIGH and/ or a particular control environment is weak, these are mitigated with additional controls.

The Inherent and Residual Risks follow the RED-AMBER-GREEN color coding mapped to HIGH-MEDIUM-LOW Risks, respectively.

9.4 MODEL RISK MANAGEMENT POLICY

A risk management policy serves two main purposes: to identify, reduce and prevent undesirable incidents or outcomes and to review past incidents and implement changes to prevent or reduce future incidents. **A risk management policy should include the following sections:**

- ⇨ Risk management and internal control objectives (governance)
- ⇨ Statement of the attitude of the organisation to risk (risk strategy)
- ⇨ Description of the risk aware culture or control environment
- ⇨ Level and nature of risk that is acceptable (risk appetite)
- ⇨ Risk management organisation and arrangements (risk architecture)
- ⇨ Details of procedures for risk recognition and ranking (risk assessment)
- ⇨ List of documentation for analysing and reporting risk (risk protocols)
- ⇨ Risk mitigation requirements and control mechanisms (risk response)

- ⇨ Allocation of risk management roles and responsibilities
- ⇨ Risk management training topics and priorities
- ⇨ Criteria for monitoring and benchmarking of risks
- ⇨ Allocation of appropriate resources to risk management
- ⇨ Risk activities and risk priorities for the coming year

CHAPTER TEN
COMPLIANCE MANAGEMENT

10.0 COMPLIANCE MANAGEMENT

10.1 INTRODUCTION

Historically, boards have been perceived to focus primarily on value creation for shareholders. But with renewed attention to statutory compliance, regulators now also want boards to focus on value management and value protection by doing a formal review of compliance obligations. As a result, corporations are looking to replace informal compliance frameworks with well structured, documented and demonstrable compliance structures that help management monitor and report compliance risk and exposure as well as compliance status to the Board.

The compliance function checks that all relevant laws are being properly complied with. Good corporate governance means -putting the right internal infrastructure to manage the risk that the company faces

Today, there is a growing awareness that if enterprises want to retain their license to operate, and achieve their business objectives, while following regulations and managing risks, they need to have a number of different risk management and compliance groups in place – ranging from the board risk and audit committees, to ethics and governance, safety, security, and compliance.

According to OCEG, "compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary **requirements resulting from contractual obligations and internal policies". Through this** definition, the relation between governance and compliance becomes clearer. Compliant organizations need an effective approach to verify that they are in conformity with external (standards, regulations) and internal (internal policies) rules. This approach is assisted by risk management, which must identify and prioritize risks that are already aligned with corporate objectives defined by governance.

The International Compliance Association has defined the term compliance as the ability to act according to an order, set of rules or request. **Compliance mainly operates at two levels:**

- ⇨ Level 1 - compliance with the external rules that are imposed upon an organisation as a whole.
- ⇨ Level 2 - compliance with internal systems of control that are imposed to achieve compliance with the externally imposed rules.

Thus, Compliance should work to develop a new, forward-thinking and stress-tested approach, and to continuously monitor its situation, evaluating and improving its ability to remain resilient in a financial services landscape that is subject to disruption and overnight change.

Compliance Vs Conformance

- ⇨ Conformance is voluntary adherence to a standard, rule, specification, requirement, design, process or practice.
- ⇨ Compliance is forced adherence to a law, regulation, rule, process or practice.
- ⇨ Conformance applies to strategies and plans that are adopted to be more productive or to improve quality.
- ⇨ Compliance applies to laws and regulations that one has no option but to follow or face penalties. Such regulations may potentially be productive **for society but don't necessarily contribute to an organization's goals.**

10.2 SIGNIFICANCE OF COMPLIANCE

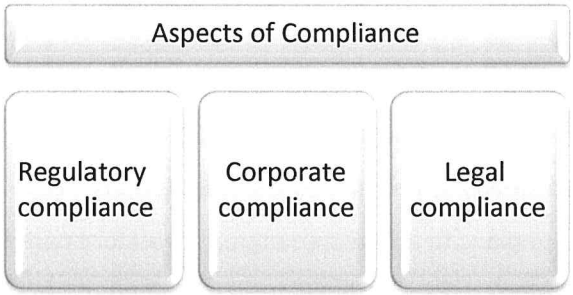
Corporate accountability is on everyone's mind today. Business executive faces significant pressure to comply with a steady stream of complex regulations. Many companies are adopting comprehensive compliance plans to address emerging regulatory paradigm and those that fail to address the new regulations risk losing business, paying hefty fines or incurring punitive restrictions on their operations.

As the organizations face mounting pressures that are driving them towards a structured approach to enterprise-wise compliance management, the key drivers of compliance **management encompass, the complexity of today's business, dependency on IT and hi**-tech processes, growth in business partner relationships. Increased liability and regulatory oversight has amplified risk to a point where it demands continuous evaluation of compliance management systems. Furthermore, the multiplication of compliance requirements that organizations face increases the risk of non-compliance, which may have potential civil and criminal penalties. The following may add to the significance of the corporate compliance management:

- ⇨ Image building of a responsible corporate citizen
- ⇨ Stake holders can trust in the working of the corporate
- ⇨ Prevent improper conduct in the organization
- ⇨ It keeps things running smoothly and minimizes risks
- ⇨ It helps the company in maintaining a good reputation
- ⇨ Real time status of legal/statutory compliances

- ⇨ Prevent unintended non compliances/ prosecutions
- ⇨ Higher Productivity in the Company
- ⇨ Building Positive Reputation
- ⇨ It enhances credibility/creditworthiness being a law abiding company
- ⇨ Proper compliance management avoids the penal provisions
- ⇨ Saves cost in litigation by avoiding penalties/fines
- ⇨ It lays down the foundation for the control environment.
- ⇨ Enjoys healthy returns through employee and customer loyalty
- ⇨ Benefits of compliance program far outweigh its costs

10.3 DIFFERENT ASPECTS OF COMPLIANCES



A. Regulatory Compliance

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including penalties/ fines.

As the number of rules has increased since the turn of the century, regulatory compliance has become more prominent in a variety of organizations. The trend has even led to the creation of corporate, chief and regulatory compliance officer positions to hire employees whose sole focus is to make sure the organization conforms to stringent, complex legal mandates.

Regulatory compliance varies not only by industry but often by location. The financial, research, and regulatory structures in one country, for example, may be similar but with particularly different in another country. These similarities and differences are often a product "of reactions to the changing objectives and requirements in different countries, industries, and policy contexts.

B. Corporate Compliance

A corporate compliance program is generally defined as a formal program specifying an organization's policies, procedures, and actions within a process to help prevent and detect violations of laws and regulations. It goes beyond a corporate code-of-conduct since it is an operational program, not simply a code of expected ethical behavior. Clearly, a code-of-conduct is an important component of a compliance program and ethics remains the heart and soul of all corporate compliance programs.

However, a comprehensive program goes further by applying the code to the specific risks of an organization and integrating measures to address those risks. A more integrated approach also focuses on legal as well as internal compliance to mitigate the risks of fraud, as well as to reach strategic, operational, and financial reporting objectives. A corporate compliance program is a magnet that brings all of a company's compliance efforts together. It is essentially a codification of applicable regulatory and internal compliance requirements, as well as a roadmap to action. A comprehensive program helps position a company to divert disasters, meet objectives, and grow shareholder value.

C. Legal compliance

Legal compliance is the process or procedure to ensure that an organization follows relevant laws, regulations and business rules. The definition of legal compliance, especially in the context of corporate legal departments, has recently been expanded to include understanding and adhering to ethical codes within entire professions, as well.

There are two requirements for an enterprise to be compliant with the law, first its policies need to be consistent with the law. Second, its policies need to be complete with respect to the law. The role of legal compliance has also been expanded to include self-monitoring the non-governed behavior with industries and corporations that could lead to workplace indiscretions. It is important to keep in mind that if a strong legal governance component is in place, risk can be accurately assessed and the monitoring of legal compliance be carried out efficiently.

Companies are challenged to comply with laws and regulations while also increasing shareholder value and protecting their brand. These challenges are acute in highly regulated industries such as financial services, health care, and life sciences where the compliance agenda has evolved beyond mere compliance to include strategic issues such as:

- ⇨ Predicting the impact of emerging regulations on strategic direction, business model and compliance/ risk management processes and systems
- ⇨ Determining the right compliance roles and accountabilities between legal, compliance, audit and business functions
- ⇨ Driving compliance culture change across diverse geographies, functions and teams
- ⇨ Defining and measuring Compliance value and managing performance expectations

- ⇨ Managing through crisis and remediation in more complex and diverse environments
- ⇨ Developing integrated compliance capabilities to better anticipate global trends, increase efficiency and participate in the evolution of the company's core strategies

Thus legal compliance is a must and if the company has entered into formal contracts with customers, the clauses of those contracts also become legal requirements. Without adherence to the letter of the law, the corporates face costly litigation and the potential of untold damage to the business and its reputation.

10.4 CORPORATE COMPLIANCE MANAGEMENT

Corporate compliance management involves a full process of research and analysis as well as investigation and evaluation. Such an exercise is undertaken in order to determine the potential issues and get a realistic view about how the entity is performing and how it is likely to perform in the future. The goals of compliance, a compliance program, sometimes called a corporate compliance program or regulatory compliance program, include:

- ⇨ Compliance with legal and regulatory requirements
- ⇨ Compliance with internal policies and contracts
- ⇨ Management of related compliance risks
- ⇨ Establishment of an ethical culture

10.5 SIGNIFICANCE OF CORPORATE COMPLIANCE MANAGEMENT

Today, business executive faces significant pressure to comply with a steady stream of complex regulations. Many companies are adopting comprehensive compliance plans to address emerging regulatory paradigm and those that fail to address the new regulations risk losing business, paying hefty fines or incurring punitive restrictions on their operations. The following points clarify the significance of the corporate compliance management:

- ⇨ Image building of a responsible corporate citizen
- ⇨ Stake holders can trust in the working of the corporate
- ⇨ Prevent improper conduct in the organization
- ⇨ It keeps things running smoothly and minimizes risks
- ⇨ It helps the company in maintaining a good reputation
- ⇨ Real time status of legal/statutory compliances
- ⇨ Prevent unintended non compliances/ prosecutions
- ⇨ Higher Productivity in the Company
- ⇨ Building Positive Reputation

- ⇨ It enhances credibility/creditworthiness being a law abiding company
- ⇨ Proper compliance management avoids the penal provisions
- ⇨ Saves cost in litigation by avoiding penalties/fines
- ⇨ It lays down the foundation for the control environment.
- ⇨ Enjoys healthy returns through employee and customer loyalty
- ⇨ Benefits of compliance program far outweigh its costs

10.6 ESSENTIALS OF AN EFFECTIVE COMPLIANCE PROGRAM

A corporate compliance program is generally defined as a formal program specifying an **organization's policies, procedures, and actions within a process to help prevent and detect** violations of laws and regulations. The essential of a successful compliance program may be list out as under:

- ⇨ **Development of written Compliance Policies, Procedures and framing of Standards**: The successful implementation of any compliance program needs a well drafted written document of the compliance policy. Until and unless one have a written policy, how the deviation from the set standard will be measured. The policy shall contain the regulatory aspects which in force as on the date of the framing of the policy, based on the such rules and regulations in force, set a Code of Conduct / Standards, action to be taken in case of deviations from the set standards and also the initiation of the disciplinary actions against the erring staff. Further it is also important that the compliance policies and procedures should be designed in such a way that it helps employees remain in compliance while carrying out their job functions.
- ⇨ **Designation of a compliance officer and compliance committee**: The Compliance Policy shall contain a clause of appointment of a designated compliance officer, who shall take care of the regulatory compliance related functions and he shall be responsible to ensure to have the adherence of the compliance policy and put up a note before the Board of Directors periodically for their perusal and directions wherever required. The Board approved note, where ever required be submitted to Regulatory Authorities.
- ⇨ **Developing open lines of communication**: The Compliance Policy shall have a provision to welcome open communication as a product of organizational culture and internal mechanisms for reporting instances of potential fraud and abuse. This concept of whistle blower may prove to be early warning signals and may be effective in prevention thereof. The name and designation of the reporting official shall be kept confidential.

- **Appropriate training and education**: For effective implementation and inculcation of the compliance policy, there is need of proper training and education to the field functionaries and policy implementing officials.
- **Internal monitoring and auditing**: The compliance policy shall contain a clause for having the effective auditing and monitoring plans.
- **Response to detected deficiencies**: Wherever the deficiencies in the prescribed procedure come in the knowledge of the concerned official, there shall be a reporting system to make a report to the designated official.
- **Enforcement of disciplinary standards**: There shall be a clause in the compliance policy to take the disciplinary action against the erring official, who has not adhered to the prescribed set of rules and regulations.
- **Effective use of Information technology**: By using available tools of information technology compliances can be managed effectively. Various compliance management software are available to facilitate compliance management.

10.7 CHALLENGES FOR EFFECTIVE CORPORATE COMPLIANCE MANAGEMENT

- Large number of legislations and multiple regulators
- Multiple business locations attracting state legislations
- lack of ownership /awareness of functional staff about compliance requirements
    - Segmented compliance initiatives
    - Time-consuming and unreliable manual reporting
    - Dynamic legal environment, lack of a robust updation process, frequent changes in process owners and internal processes.

10.8 PROCESS OF CORPORATE COMPLIANCE MANAGEMENT

Installing proper compliance process is a must for the success of compliance programme. Systematic approach helps in chalking out a plan of action in right direction. Installing a process presupposes planning for the activity, identification of desired objective and resources, detailed plan of action with provision for eventualities and continuous monitoring and corrective measures.

Some companies have a streamlined, highly efficient system for managing their compliance requirements. By adopting a unified approach to regulatory management, companies can minimize costs, maximize efficiency and reduce their risk exposure. Such firms, though, are in the minority. More often, there is considerable duplication of cost and effort as organizations attempt to deal with the requirements of multiple regulatory bodies across their operations.

It is desirable that the compliance management process is so designed that it is able to generate a complete

MIS Report for secretarial and legal data providing the key information including company **details, key dates, brief information about company's business, certifications obtained,** addresses of office locations, details of Board of Directors, shareholding pattern, key registration nos. such as company registration no., scrip code, ISIN code etc., contact details of agencies such as auditors, consultant, banker, government agencies, printers, R&T agents etc. Purely for a legal function database of immovable properties, on-going litigations, compliance reports, list of power of attorneys issued etc. prove immensely useful and provide timely information, to take necessary action to correct non-compliance, if any.

It is essential to segregate roles and responsibilities within the function to ensure proper distribution of work, rotation of responsibilities where possible, avoid confusion and set focus for each person within the function.

Considering the multiplicity of laws that are applicable to companies in India, a systematic approach to corporate compliance management is worth doing an exercise to go through a list of laws and identifying those relevant to the industry and business to which the company belongs and categorizing them in future to focus on critical compliances. Critical compliance means the severity of compliance and its impact on business, while it is true that all laws are of equal importance and should be complied with in letter and spirit.

10.9 CHECKLIST TO BE FOLLOWED FOR SETTING UP A GOOD COMPLIANCE PROGRAM

- ⇨ **Understand the Scope**: Identify all regulatory and internal compliance needs and efforts to challenge if organizational responsibilities are properly aligned. This should not be a **"one and done" step, but rather performed periodically as regulatory landscapes and** operational environments are typically changing.
- ⇨ **Gather Internal and External Intelligence**: Tap the collective intelligence of the company by soliciting thoughts from the Board, management and employees. Also look beyond the walls of the organization to understand industry developments and competitor reactions to corporate compliance. This includes researching legal actions to help identify risks.
- ⇨ **Define Objectives**: Define objectives from an enterprise and business unit standpoints. This should be a significant part of the periodic strategic planning process.
- ⇨ **Conduct a Risk Assessment:** Identify risks, probabilities, and the significance in terms of both qualitative and quantitative measures. Consider scenarios from a cause-and-effect standpoint.

- **Align Controls:** Policies, procedures, and actions within a process, should be in place to address the risks to best achieve objectives.
- **Verify /Buy-In and Understandability:** Everyone needs to know their roles. For control owners to be expected to act appropriately, they **need to understand the "why" and "how" of the compliance program. Controls need to be clearly communicated, ideally** with a feedback loop so control owners can voice their insights and concerns.
- **Test Cultural Support:** Many organizations have put in place paper programs that have no real effect on the operations of the organization. Determine if the cultures at headquarters and all relevant business units are supportive of a strong corporate compliance program. This can be accomplished through surveys, independent reviews and entity-level control assessments.
- **Assess On-Going Compliance:** Build monitoring, internal audit and special reviews into the compliance program to help ensure that controls are operating effectively. This effort should also seek to identify the most-efficient alignment of responsibilities and controls.
- **Train, Educate and Communicate:** Deliver periodic targeted training and share compliance information with the business units, global functions, external partners, customers, vendors, and other stakeholder groups.
- **Measure Results and Report to Board:** Develop a reporting dashboard to keep management groups and the Board aware of compliance measures, trends and developments. This should address both internal and external activities.

10.10 INTERNAL COMPLIANCE REPORTING MECHANISM (ICRM)

The Internal Compliance Reporting Mechanism (ICRM) should be sound and fool proof. Deviations in non-reporting should be avoided. In any Compliance Program it is of paramount important that the employees working in the organisation shall feel free in reporting non-compliance related issues either by their own parts or has observed any deficiency on the counter part. **The ICRM may involve the following process:**

- Establish a robust reporting mechanism
- Encourage employees to report the non-compliance in a fear less environment.
- Define the parameters of the compliance issues based on the legal requirements prevailing in force.
- Develop the measures to weigh the variation to the prescribed standards.
- Functional Heads be made responsible to collect such information in a time bound manner.
- Early warning signals should be identified of the possible areas of the non-compliances.

An internal reporting mechanism need not be expensive. It must go far beyond a written policy, however, and it must be designed to reflect the practices, laws and cultures of the countries in which the company is operating. Any broken link in the reporting chain can interrupt the flow of information from the reporter to those who need to hear and act on it. A sound program should include the following elements:

- *Communication* : make the program known to all levels of employees.
- *Accessibility* : make the program available to all employees around the world in various languages.
- *Cultural Appropriateness* : adapt the program to the constraints imposed by local culture, history and practice.
- *Universality* : make the reporting mechanism available to relevant third parties, e.g. suppliers, consultants, customers
- *Confidentiality and Anonymity* : guarantee confidentiality and permit discreet or anonymous reports.
- *Screening* : provide safeguards against frivolous or malicious reports.
- *Collect Data*: monitor reports, track them over time, identify vulnerabilities and take corrective action.
- *Remedial Action and Feedback*: take action and provide feedback to the reporter as appropriate.
- *Management Visibility*: report to the audit committee or board of directors.
- *Employee Protection*: protect reporting employees both during employment and after departure from the company.
- *External Communication*: report to shareholders and other interested parties on actions taken and results achieved.

10.11 USE OF TECHNOLOGY FOR COMPLIANCE MANAGEMENT

A critical component of an effective compliance program is the ability to monitor and audit compliance in a "real time manner." Yet, as companies cross geographical and industry boundaries, it is becoming harder to perform this role in the traditional manner. As a result, companies are increasingly seeking technology solutions.

Technology has become an integral part of day-today corporate compliance systems and procedures. A critical component of an effective compliance program is the ability to monitor and audit compliance in a "real time manner" Yet, as companies cross geographical and industry boundaries, it is becoming harder to perform this role in the traditional manner. As a result, companies are increasingly seeking technology solutions.

Information Technology can play an effective role in implementation of a Corporate Compliance Management Programme across various departments of an organization in terms of real-time compliance reminders, generation of reports, sending warning signals, generation of compliance calendar etc.

Many companies are introducing a comprehensive web-based compliance system that links various offices/ units for better co-ordination and continued compliance. Companies prefer to introduce full-fledged compliance management systems for smooth compliance of multiple laws. Web-based compliance software are available industry-wise and tailor made compliance software can also be made according to company specifications which has to be updated on continuous basis.

A well-designed compliance management programme has abilities to perform the following key functions across the enterprise:

- **Compliance Dashboard**: The compliance programme must provide a single enterprise-wide dashboard for all users to track and trend compliance events. All compliance events should be easily viewed interactively through the enterprise compliance dashboard. External auditors, internal auditors, compliance officers can use the dashboards to make decisions on the compliance status of the organization.
- **Policy and Procedure Management**: A well-designed document management system forms the basis of managing the entire lifecycle of policies and procedures within an enterprise. Ensuring that these policies and procedures are in conformity with the ever-changing rules and regulations is a critical requirement. The creation, review, approval and release process of the policy documents and SOPs (Standard Operating Procedures) should be driven by collaborative tools that provide core document management functionality.
- **Event Management**: The compliance management system must have ability to capture and track events, cases and incidents across the extended enterprise. Compliance officers, call centre personnel, IT departments, QA personnel, ethics hotline should be able to log in any adverse event across the enterprise, upon which the necessary corrective and preventive actions are initiated.
- **Rules and Regulations**: A well-designed compliance management solution must offer capabilities for organization to continuously stay in sync with changing rules and regulations. As soon as there are regulatory changes, the various departments should be notified proactively through "email based" collaboration. This process critically enables the organization to dynamically change their policies and procedures in adherence to the rules and regulations. While tracking a single regulation may be manually feasible, it becomes an error-prone task to track all local, state, and central regulations including those taking place across the globe. A well-designed Compliance management programme offers up-to-date regulatory alerts across the enterprise.

- **Audit Management**: Audits have now become part of the enterprise core infrastructure. Internal audits, financial audits, external audits, vendor audits must be facilitated through a real-time system. Audits are no more an annual activity and corporations offer appropriate audit capabilities. Appropriate evidence of internal audits becomes critical in defending compliance to regulations.
- **Quality Management**: Most organizations have internal operational, plant-level or departmental quality initiatives to industry mandates like Six-sigma or ISO 9000. A well-designed compliance management program incorporates and supports ongoing quality initiatives. Most quality practitioners agree that compliance and quality are two sides of the same coin. Therefore, it is critical to ensure that compliance management solution offers support for enterprise-wide quality initiatives.
- **Training Management**: Most compliance programs often require evidence of employee training. Sarbanes-Oxley Act, stress on employee training. In USA, lack of documented training can lead to fines and penalties. Often the compliance office has to work closely with the HR organization to facilitate employee training. Well-designed compliance program requires a well-integrated approach to training management.
- **Compliance Task Management**: Organizations must plan, manage and report status of all compliance related activities from a centralized solution. Automated updates from the various compliance modules should provide for up-to-the-minute status reporting that could be viewed by the Board, corporate compliance officer, entity compliance coordinators, quality offices and others as designated.

10.12 APPROACH AND PRINCIPLES ON CORPORATE GOVERNANCE COMPLIANCE AND ENFORCEMENT

The Approach – the governance compliance framework

a. Legislated basis or approach for governance compliance

- Governance of corporations can be on statutory basis or on a code of principles and practices or on a combination of both. (***See King III Page 6)***.
- The USA codified a significant part of its governance in the Sarbanes-Oxley Act (2002) ("SOX").
- **The legislated basis for governance operates on "comply or else" basis. Companies** either comply or if they fail, they face legal sanctions for none compliance.
- **The "comply or else" statutory regime to corporate governance has been criticized for –**
- Being too rigid, operating as it does on the one size fits all principle and yet businesses undertaken by companies vary from place to place.

- ⇨ Diverting the Board's attention from improving the economic value of the company to compliance issues.

- ⇨ Being too expensive ***"the total cost to the American economy for complying with the SOX is considered to amount to more than the total right off of Enron, world.com and Tyco combined"***. **(See King III Page 6).**

- ⇨ Stifling innovation and entrepreneual activity. To quote Professor Ribstein of Illinois ***"It is unlikely that hasty, crash induced regulation like SOX can be far sighted enough to protect against future problems, particularly in light of the debatable efficiency of SOX's response to current market problems. Even the best regulators might aim and enact legislation that is so strong that it stifles innovation and entrepreneual activity, and once set in motion, regulation is almost impossible to eliminate. In short, the first three years of SOX were, at best, an over reaction to Enron and related problems and, at worst, ineffective and unnecessary"***. Quoted with approval on Page 6 of King III.

b. Voluntary basis for governance compliance.

- ⇨ Fifty six (56) commonwealth countries including South Africa, and twenty seven (27) states in the European Union including UK, have opted for a code of principles, practices and guidelines on a **"comply or explain"** basis in addition to certain governance issues that are regulated by law.

- ⇨ Under the "comply or explain" approach, directors comply with the governance codes, practices and guidelines and if they cannot, they have to explain and provide reasons.

- ⇨ Debate on the UN Governance Code on whether it should be a "comply or else" or "comply or explain" basis opposed the use of the word **comply** because it implies **adherence** and leave no room for **flexibility**.

- ⇨ The UN Code therefore opted for **"an adopt or explain"** basis for governance compliance.

- ⇨ Under the "adopt or explain" approach, company boards adopt the governance codes, practices and guidelines and if they cannot, they have to explain why. The word "adopt" is used in substitution to the word "comply" as it gives room for flexible application. It moves away from the rigidity implied in the word "comply".

- ⇨ The Netherlands Code on corporate governance opted for yet another terminology, i.e. the **"apply or explain"** approach for governance compliance.

- ⇨ Under the "apply or explain" approach, company boards either apply the governance code, practices and guidelines and if not they explain the reasons why.

- ⇨ The Netherlands Code approach drops the use of the word "adopt" as it was the case in the UN Code and move to the word "apply". The argument advanced is that you apply

rather adopt the governance codes, practices and guidelines. The argument on the use of the word "adopt" or "apply" talks of a **distinction** without a **difference**.

- ⇨ **The "comply or explain" has been criticized for being "... a mindless response to the King Code and its recommendations whereas the "apply or explain" regime shows an** appreciation of the fact that it is often not a case of **whether** to comply or not but rather to consider **how** the principles and recommendations can be applied. (***See King III Page 7***).

- ⇨ **The King III Code therefore opted for the Netherlands Code approach. i.e. the "apply or explain" basis for governance compliance riding on the principle that it is the legal duty** of directors to act in the best interests of the company at all times.

- ⇨ **In following the "apply or explain" approach, the Board of Directors , in its collective** decision making, could conclude that to follow a recommendation would not, in the particular circumstances, be in the best interests of the company. The Board would decide to apply the recommendation differently or apply another practice and still achieve the objective of the over arching Corporate governance principles of fairness, accountability, responsibility and transparency. Explaining how the principles how the principles and recommendations were applied or if not applied, the reasons, results in **compliance. In reality the ultimate compliance officer is not the company's .....** or a bureaucratic compliance with statutory proceedings but the stakeholders. (***See King III Page 7***).

c. The link between governance principles, guidelines and the law

- **Good corporate governance and compliance with the law are linked in that:**

  - ⇨ The starting point of any analysis of corporate governance compliance focuses on the legal duties of directors, the time honoured four (4), i.e. care, skill, diligence and good faith.
  - ⇨ Good corporate governance principles and guidelines, established structures and processes with the appropriate checks and balances that enable directors to discharge their legal responsibilities and oversee compliance with legislation.
  - ⇨ Good corporate governance, practices, codes and guidelines lift the bar of what are regarded as appropriate standards of conduct and courts of law use such corporate codes and guidelines as persuasive materials in determining whether or not a board member or indeed the Board itself is liable at law. Codes therefore become law through judicial precedent.
  - ⇨ Around the world, some principles of good corporate governance are being legislated in addition to being part of voluntary codes.
  - ⇨ What was contained in the common law and in good corporate governance codes and guidelines are being restated in the statutes, e.g. the common law duties for directors and the King II recommendations have been restated in the New South African Companies Act.
  - ⇨ There are other pieces of legislation which create statutory duties on directors, e.g. legislation on public finance and environmental control, state owned companies and not for profit companies, etc.

d. Governance compliance – guiding principles

- ⇨ Boards of companies should establish a compliance framework and ensure adherence to its terms.
- ⇨ Companies must comply with all applicable laws.
- ⇨ Compliance with applicable laws should be understood not only in terms of the obligations that they create, but also for the rights and protection that they afford. Companies and their boards should always aim to achieve a balanced approach in their outlook on compliance. Simply complying with laws without consideration of the rights available in the circumstances cannot be deemed to be acting in the best interests of the company. The duty to act in the best interests of the company includes considering the rights of the company when dealing with compliance.
- ⇨ The Board should consider adherence to applicable non-binding rules, codes and standards if it would constitute good governance and practice. The board should disclose in the integrated report the applicable non-binding rules, codes and standards to which the company adheres on a voluntary basis.
- ⇨ **The Board is responsible for the company's compliance with applicable laws and with** those non-binding rules, codes and standards with which the company elected to comply. One of the important responsibilities of the board is therefore to monitor the **company's compliance with all applicable laws, rules, codes and standards.**
- ⇨ Compliance with applicable laws, rules, codes and standards should be proactively and systematically managed by companies and compliance should be a regular item on the agenda of the Board even if this responsibility is delegated to a separate committee or function within the organisational structure.
- ⇨ The extent of reliance placed by the board on those delegated committees or functions depends on **the board's assessment of their knowledge, effectiveness and experience.**
- ⇨ The board and each individual director should have a working understanding of the effect of the applicable laws, rules, codes and standards on the company and its business.
- ⇨ Compliance **risk should form an integral part of the company's risk management** process.
- ⇨ The board should delegate to management the implementation of an effective compliance framework and processes.

CHAPTER ELEVEN

CURRENT ISSUES IN GRC

11.0 CURRENT ISSUES IN GRC

11.1 DIRECTOR COMPENSATION

While director pay is not as pressing an issue, it nonetheless is a board responsibility and, for a number of reasons, boards need to get this right. We begin here with how one successful company tried a new pay paradigm that raised more than a few eyebrows. As to non-executive director remuneration, the Corporate Governance Principles state that companies may find it useful to consider the **following in relation to non-executive directors**:

- ⇨ non-executive directors should normally be remunerated by way of fees, in the form of cash, non-cash benefits, superannuation contributions or salary sacrifice into equity – they should not normally participate in schemes designed for the remuneration of executives
- ⇨ non-executive directors should not receive options or bonus payments
- ⇨ non-executive directors should not be provided with retirement benefits other than superannuation

As to executive remuneration, the Corporate Governance Principles suggest that executive remuneration will involve a balance between fixed and incentive pay. **Those Principles go on to provide guidance in relation to the following aspects:**

- ⇨ fixed remuneration
- ⇨ performance-based remuneration
- ⇨ equity based remuneration
- ⇨ termination payments

The board must be able to justify its directors' fees to members and shareholders. Suggested considerations include:

- ⇨ Company-specific factors
- ⇨ Size, nature and profitability of the company
- ⇨ Complexity of operations – lines of business, geographic spread of operations
- ⇨ Industry sector – some sectors are paid more than others
- ⇨ Structure and responsibilities of board including the number of board committees
- ⇨ Risks and challenges of the business
- ⇨ **Shareholders' vote on remuneration at annual general meeting**
- ⇨ Director-Specific Factors
- ⇨ Qualifications and experience
- ⇨ Time commitment required
- ⇨ General performance and involvement in value-added decision making
- ⇨ Additional responsibilities, e.g. chair of a committee, other special duties such as at takeover time
- ⇨ External market factors
- ⇨ Business and economic conditions

Supply and demand – the shrinking pool of non-executive directors and the fact that such directors are taking on fewer board positions, increased workloads

11.2 CEO COMPENSATION

There's long been a tug of war between boards of directors and activist shareholders about how boards should be comprised to best carry out their responsibilities. Central to these issues is the relationship with the chief executive officer specifically, how to provide the kind of oversight that enables the CEO to successfully run the business and achieve corporate goals. **There's little doubt that expectations of and pressures on chief executives continue to evolve, and there are real questions as to whether any CEO can satisfy all constituents' demands.**

The board and management need to agree on a compensation paradigm, one that reflects meaningful pay-for-performance metrics. This program should be tied to long-term shareholder interests of growth and return and should be designed to motivate the CEO and senior management to best achieve those objectives.

Directors must ultimately ignore those shareholders who send mixed messages, com-plaining both when CEO compensation tied to stock price rises with broad market upswings and when CEO compensation moves with internally developed benchmarks that might not follow the **company's short**-term stock price. Boards need to take the time to get compensation metrics right.

If CEOs' exorbitant pay packages come at the expense of shareholders, one obvious solution is to make it easier for shareholders to exert control over the pay of CEOs and top management.

As a practical matter, it is difficult to rally shareholders in a say-on-pay vote, just as it is difficult to organize for an election to the the presidency. Organizers must contact a large number of shareholders to have any hope of winning, and there is not much incentive to organize since, **even if the measure succeeds, it's not binding.**

Furthermore, the voting structure is stacked against shareholders unhappy about current managerial pay. A large portion of corporate shares are voted by mutual funds and asset management companies.

Just as directors may view corporate CEOs as their friends rather than their employees, it seems that a similar relationship exists with many of the asset managers who control the bulk of company stock. They have little reason to pick fights with the management on behalf of the people they ostensibly represent.

There are many ways to design contracts that would incentivize directors to restrict CEO pay. From the standpoint of shareholders, directors should be constantly asking whether it is possible to get comparable performance from the CEO and other top executives while paying them less, just as management tries to minimize costs by paying ordinary workers as little as possible given their levels of productivity. Remarkably few, if any, companies design compensation packages for directors along these lines.

It would probably be too much micromanagement for the government to mandate incentive packages that encourage directors to hold down CEO pay. However, it is certainly reasonable for large organizational shareholders such as pension funds, foundations, and universities to ask the companies in which they hold stock why directors have no incentive to limit CEO pay. This is consistent with maximizing returns to shareholders. After all, if a CEO is being paid more than necessary for a person with his or her abilities and performance, then shareholders are throwing away their money.

One argument against giving shareholders more ability to rein in CEO pay is that there is too little at stake for shareholders to be concerned about. The idea is that even salaries in the tens of millions of dollars are not a big deal for companies with billions or tens of billions of dollars of profits each year. It is worth getting a more precise assessment of how much is at stake and whether it is likely to be enough to concern shareholders.

If the concern is to develop policies that benefit workers at the middle and bottom of the income distribution, it might seem peculiar to promote policies that will include the country's very richest people as beneficiaries. But the reality is that shareholders are the group most immediately in a position to effectively rein in CEO pay. And, for reasons noted earlier, we would likely have considerably less inequality in a context in which the ratio of CEO pay to the pay of ordinary workers is closer to its levels of 50 years ago, even if this implies somewhat higher corporate profits.

Empowering shareholders to rein in excessive CEO pay is obviously not sufficient to make for a fairer economy, but it is useful. There are other measures, like more progressive income taxes and a more effective estate tax that can limit the fortunes of the very rich who make a large portion of their earnings off of corporate equities. The concern that these shareholders might become slightly richer if excess CEO pay is reined in should not be a reason for tolerating bloated CEO pay and the inequality and corruption it entails.

11.4 CEO SUCCESSION PLANNING

One thing we know with certainty every company someday will need a new CEO. Unless a CEO's mandated retirement date is approaching, a board seldom knows when that day will arrive, though for many companies it's sooner than expected. Whether performance doesn't meet expectations, a major crisis requires change at the top, or a chief executive suffers a debilitating health issue or departs voluntarily seeking greener pastures, pursuing personal interests, or simply retiring a board may find itself having to identify a new leader for the organization.

If fortunate, a board will have the benefit of sufficient time to go through a comprehensive selection process. But it's not uncommon for a CEO's departure to come with stunning suddenness, requiring quick and decisive action. Despite common knowledge of what's happened at other companies, too many boards simply are not prepared to deal with departure of the company's CEO, especially if it is unexpected.

Where does one begin? Certainly a board will want to consider who should jump into the chief executive's seat should a sudden change be needed, as well as defining a selection process when time is on the board's side. There's the issue of internal versus outside candidates, and how one is groomed and others identified. Let's take a look at what needs to be considered now, before coming face to face with an emergency situation.

Every director knows that at least one individual must be identified as positioned to immediately take over as chief executive. This person might be viewed as a temporary stand-in until a more thorough search is conducted, or as the next generation of leadership.

The common aspects in dealing with succession includes:

The board identifies the skills, knowledge, experience, and personal attributes needed for the company—based on its industry, business, competitive and regulatory demands, consumer markets, strategy, cul-ture, and other factors. A sharp focus is on identifying what's needed not only where the company is today, but where the strategic plan will bring the company tomorrow.

Responsibility rests with the current CEO to identify and groom a cadre of individuals who meet the identified criteria. This includes individual development plans ensuring that managers are given sufficient roles and responsibilities to provide the requisite experience and perspective and develop the needed knowledge and skills, and are exposed to top-level strategic and related issues. Potential candidates are coached, with the sitting CEO, head of HR, and possibly selected directors playing a role, and development progress is tracked.

The process cascades throughout the company, where managers at every level take similar action to recruit, develop, and assess direct reports to ensure individuals with the requisite knowledge and skills are positioned to step up as necessary.

The board gets to know and understand the strengths and weaknesses of potential CEO successors. This should occur naturally at board and committee meetings, dinners preceding meetings, and offline interactions where additional information or insight is obtained. Sometimes overlooked but important is learning first hand whether an individual truly wants the top spot usually but not always the case.

The board's process includes identifying executives outside the company that should be considered. While direct contact typically is neither possible nor appropriate, maintaining an up-to-date list of individuals from the outside provides a useful head start when a search is initiated.

When it comes time to make a decision, the current CEO serves in an advisory role. The point is made well by Richard Koppes, an active director and longtime governance expert, who says that ideally, when it comes time to make decisions, the independent directors meet first with the CEO and then without him or her, because ultimately it's the board's job to decide.

The issue of whether it's best to promote internally or go to the outside has long been debated. Certainly the answer for any company is: It depends on factors too numerous to mention here, including the results of the studies conducted on the same.

Among the advantages to an internal candidate are knowledge of the organization and its business, operations, people, and challenges, and more modest compensation costs. An

outsider brings different knowledge and perspective, and perhaps vision and skills that may be lacking internally. The list goes on, as will the debate.

11.5 PERFORMANCE MEASUREMENT AND REPORTING/DISCLOSURE

Financial reporting is the process of producing statements that disclose an organization's financial status to management, investors and the government. Financial reporting serves two primary purposes. First, it helps management to engage in effective decision-making **concerning the company's objectives and overall strategies. The data disclosed in the reports** can help management discern the strengths and weaknesses of the company, as well as its overall financial health. Second, financial reporting provides vital information about the financial health and activities of the company to its stakeholders including its shareholders, **potential investors, consumers, and government regulators. It's a means of ensuring that the** company is being run appropriately.

Financial Reporting involves the disclosure of financial information to the various stakeholders about the financial performance and financial position of the organisation over a specified period of time. These stakeholders include – investors, creditors, public, debt providers, governments & government agencies. In case of listed companies the frequency of financial reporting is quarterly & annual.

The main components of financial reporting are:

- ⇨ The financial statements – Balance Sheet, Statement of Profit & Loss, Cash flow **statement & Statement of changes in stock holder's equity**
- ⇨ The notes to financial statements
- ⇨ Quarterly & Annual reports (in case of listed companies) which should be made available to the shareholders by the directors.

Shareholders and stakeholders of a company do not run the company. The directors do. The only principal way in which directors make themselves accountable to the shareholders is through communicating and disclosing information about the company and its business performance to them. That process needs a detailed analysis from the perspective of corporate governance.

Investors hold back from investing and share value will drop if there are doubts about the honesty and transparency of how information about the company is collected and disclosed.

Information technology has taken over centre stage on how data and information about companies are recorded, preserved and transmitted. Accordingly companies should have information technology frameworks in place to ensure complete, timely, relevant, accurate and accessible IT reporting firstly from management to the Board and secondly by the Board to shareholders and stakeholders in the integrated report. Accordingly Boards of entities must ensure that there is an IT Governance Charter and policies are established and implemented in terms of that Charter.

The Boards of companies should delegate to their management the responsibility for establishing and implementing the IT Governance framework through charters and plans of action. Effective IT Frameworks and policies as well as the processes, procedures and standards that these evolve, should be implemented with a view to minimizing risk, deliver value, and ensure business continuity and assist the company to manage its IT resources efficiently and cost effectively. .

The Managing Director or CEOs of companies should appoint an individual responsible for the management of IT often referred to as Chief Information officer, whose task would be to establish and implement the IT framework in line with the strategic objectives of the company.

The Board, through management should ensure that company information which is confidential is treated as such.

The Board cannot afford to provide misleading financial statements. There are three ways in which published financial statements can be misleading, namely:

- ⇨ There could be a fraudulent misrepresentation of the affairs of the company where the company's management deliberately presents a false picture of its financial position and performance.

- ⇨ A company might use accounting policies where it presents its reported profits more favourable than would be the case if more conservative accounts policies were used.

- ⇨ The financial statement could be complex and difficult for investors to understand. It is often the practice of accountants to present financial statements in a way that readers will find difficult to comprehend properly.

- ⇨ Board of companies should communicate and disclose certain information about the company performance to all stakeholders of the entity.

What type of information should be communicated and disclosed to the stakeholders?

- ⇨ It should be information which paints a holistic and integrated representation of the company's performance in terms of both its finances and its sustainability.

- ⇨ The information could be communicated in the form of a single or dual reports, emphasis being more on substance over form.

Principles which guide integrated reporting and disclosure are:

- ⇨ Transparency and accountability – the integrated report should be prepared every year and should convey adequate information about –

    - The operations of the company, the sustainability issues pertinent to its business, the financial results and the results of its operations and cash flow.

- The goals and strategies of the company as well as its performance with regard to economic, social and environmental issues.

- How the company's business operations are aligned with legitimate interests and expectations of all its stakeholders.

⇨ Integrated reporting should be focused on substance over form and should disclose information that is complete, timely, relevant, accurate, honest and accessible and comparable with past performance of the company as well as forward looking information.

⇨ The Board should include commentary on the company financial results and this commentary should include information to enable the stakeholder to make an informed assessment of the company's economic value by allowing stakeholders insight into the prospects for future value creation and the Board's assessment of the key risks which may limit those prospects. The Board must disclose whether the company is a going concern and whether it will continue to be a going concern in the financial year ahead.

⇨ Sustainability disclosure – the integrated report should describe how the company made its money hence the need to contextualize financial results by reporting on the positive and negative impact the company's operations had on its stakeholders. Companies must familiarize themselves with the global reporting initiative and G3 Guidelines on sustainability reporting. These provide a number of important innovations since the 2002 guidelines referred to in King II.

⇨ Assurance over all disclosures in the integrated by any entity should be obtained. Formal processes of assurance with regard to integrated reporting should be established.

⇨ Providing assurance is different from verification in that verification confirms the existence of stated facts, it confirms data. Assurance is a broader term that refers to the integrity of certain processes and systems. Verification of certain information may be therefore be necessary to provide assurance.

⇨ Verifications can take the form of representation letters by Management which are part of the annual reports. Assurances can take the form of confirmations by Boards of entities that companies will have adhered to best practice codes and the law.

⇨ . In obtaining assurance, companies should be clear on the scope of the assurance to be provided and this should be disclosed to stakeholders in their annual reports or any other reports. In addition the name of the assurer should be clearly disclosed together with the period under review, the scope of the assurance exercise and the methodology adopted.

⇨ General oversight in reporting disclosure should be delegated by the Board to the Committee.

- ⇨ Risk disclosure – the Board should disclose in the integrated report any undue, unexpected or unusual risks it has taken in pursuit of reward as well as material losses and the causes of the losses. This disclosure should be made with due regard to the company's commercially privileged information.

- ⇨ In addition the Board should disclose any current, imminent and envisaged risk that may threaten the long term sustainability of the company.

- ⇨ The Board should also disclose its views on the effectiveness of the company risk management processes in the integrated report.

11.6 STAKEHOLDER INTERFACE

- ⇨ The overall assessments of stakeholders of companies result in the formation of corporate reputations. Reputation is based on how well a company performs compared with the legitimate interests and expectations of stakeholders. There is an awareness of how important the contribution of reputation is to the economic value of the company.

- ⇨ The gap between stakeholder perceptions and the performance of the company should be managed and measured to enhance or protect corporate reputation and to avoid or destruction by company actions.

- ⇨ The Board should adopt a stakeholder inclusive corporate governance approach and should from time to time rectify important stakeholder groupings as well as their legitimate interests and expectations relevant to the company's strategic objectives and long term sustainability.

- ⇨ The Board should therefore delegate to management to proactively deal with stakeholder relationships.

- ⇨ Management should develop for adoption by the Board a strategy and suitable policies for the management of its relations with stakeholder groupings. Management should strive to strike a balance between the interests of various stakeholders and ensure that they receive equitable treatment at all times. Board and management of companies should engage all stakeholders to the company in a transparent and effective way in order to maintain their trust and confidence.

- ⇨ From the business leadership perspective, we call it networking and netweaving with company stakeholders.