Instructions to Candidates

- THREE hours are allowed for this examination plus 15 minutes reading time
- Candidates MUST answer FOUR questions from six
- Each question carries equal marks
- Each answer MUST begin on a new page of the answer booklet
- Your answer booklet and this examination paper MUST be handed to the invigilator at the end of the examination

FAILURE TO COMPLY WITH THESE REGULATIONS MAY LEAD TO YOUR ANSWER BOOKLET NOT BEING MARKED
GOVERNANCE PAPER NOVEMBER 2014

QUESTION ONE

a) Define ‘shareholder activism’. 

b) Explain how institutional shareholders’ investment strategies affect their approach to a corporation’s governance.

c) Explain the purpose of the UK Stewardship Code and what institutional investors must do to demonstrate compliance with the Code.

Question 1 Answer

Syllabus Reference
Unit One: The development of Corporate Governance.

Part a) answer
Shareholder activism is a phrase used for the actions of shareholders who attempt to influence a corporation’s behaviour by exercising their rights as owners.

Shareholders don’t control or direct a company but they can influence the board of directors and management. This can range from simple dialogue with management to voice concerns about a particular issue to formal proposals that are voted on by all shareholders at a company’s annual general meeting.

In recent years the term has been used to describe person(s) who attempt to use rights as shareholder(s) of a publicly listed company to bring about social change. Examples include the environment and investments in sensitive parts of the world and workers’ working conditions (sweatshops). Activist interventions may alter or change a company’s approach to corporate governance.

Shareholders do not always have the same common interests or the same holdings of shares in terms of volume. Interests can vary depending on the investment approach (whether long-term or short term) the influence and effectiveness of the level of activity is subject to the amount of shares owned or held. Major shareholders have a large stake in a company and it follows that it is in their interest to keep a close eye on the governance of an organisation.
Part b) answer
With few exceptions, minority shareholders (private individuals and or employees) do not have the level of influence required (and indeed are protected with a mixture of legal mechanisms and stock market regulations). The leverage resides with the larger institutional investors (asset managers, private equity funds and hedge funds).

Long-term shareholders tend to adopt a ‘maintain’ attitude and will attempt to assert control over the actions of management and short-term shareholders in order to gain shareholder value (net present value of future dividends plus capital gains). The governance approach may be one of rigorous oversight at detailed operational level with some control of the board.
Other long-term investors such as asset managers tend to be hands-off or a ‘docile’ activist until something goes wrong.

Other shareholders adopt a short-term horizon and their strategy is to increase shareholder value by boosting the share price as quickly as possible. This can be done in two ways; restructuring the company with a view to selling it on in which case full control of the board is essential

Alternatively short-selling and intraday trading; in the latter case there will be no scope for engaging in direct governance but traders who seek to influence the price of shares may adopt a highly activist strategy in order to meet a trading objective.

Part c) answer
The Stewardship Code is a set of principles published in 2010 following The Walker Report by the Financial Reporting Council (FRC) and is directed at firm who manage assets on behalf of institutional investors who hold voting rights in United Kingdom companies.

The purpose of the Stewardship Code is to improve the quality of corporate governance through promoting better dialogue between shareholders and company boards, and more transparency about the way in which investors oversee the companies they hold shares in.
The Stewardship Code applies on a ‘comply or explain basis’. In reporting terms this means institutional investors should provide a statement which includes:

- a description of how the principles of the Stewardship Code have been applied; and

- disclosure of the specific information listing policy on:
  - how they will discharge their stewardship responsibilities,
  - that they are willing to act collectively with other investors where appropriate
  - have a clear policy on voting and disclosure of voting activity, periodic reporting on stewardship and voting activities or an explanation if these elements of the Stewardship Code have not been complied with.
QUESTION 2

a) Explain the principles that the UK Corporate Governance Code 2012 applies to the role of a ‘unitary board’ and how that role be should be monitored.  

(50 marks)

b) With the aid of a diagram describe the ‘Three Lines of Defence’ model. 

Explain how this model can be of use to a Board as a framework for governance and risk.  

(50 marks)

Question 2 Answer

Syllabus Reference

Unit Four: Governance in the UK/ Mechanisms of Corporate Governance.

Students to consider the role of the Audit Committee

Part a) answer

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.

‘The Board’s overall responsibilities included determining the company’s approach to risk, setting its culture, risk identification, oversight of risk management, and crisis management.

The first Supporting Principle of Main Principle A1 states: ‘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.

C.2 Internal Control Principle: The board should maintain a sound system of internal control to safeguard shareholders investment and the company’s assets.

Code Provision C.2.1: ‘Internal Control The Board should at least annually conduct a review of the effectiveness of the group’s system of internal controls and should report to the shareholders that they have done so. The review should cover all material controls including financial, operational and compliance controls and risk management systems.’

‘The board of directors is responsible for the company’s system of internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. The board must further ensure that the system of internal control is effective in managing risks in the manner which it has approved.’ Turnbull Report Clause (16)
Part b) answer
The board and the CEO are respectively responsible for providing oversight and monitoring risk management strategies and processes. To effectively assume these duties, they seek assurance from various sources within the organisation.

The three lines of defence model has been increasingly used as a framework for corporate governance, and particularly risk management, over recent years. It is a useful tool to explain and demonstrate the different roles in governance and risk management, the interplay between them and how they fit together to provide stronger corporate governance.

It also forms the basis of a recent paper, jointly issued by ECIIA and the Federation of European Risk Management Associations (FERMA) on ‘Guidance for boards and audit committees on the implementation of Art (41) (2) of the 8th Directive’

The model is rapidly gaining universal recognition and can be illustrated as follows:

The Three Lines of Defence

First line of defence: operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks

Second line of defence: the risk management, compliance and similar functions facilitate and monitor the implementation of effective risk management practices by operational management and assist the risk owners in reporting adequate risk related information up and down the organisation.

Third line of defence: the internal auditing function will, through a risk based approach, provide assurance to the organisation's governing body and senior management, on how effective the organization assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an institution's risk management framework: i.e. from risk identification, risk assessment and response to communication of risk
related information (throughout the organisation and to senior management and the governing body).

While the above-mentioned functions operate within the organisation, the external auditor contributes as an outside body, providing assurance regarding the true and fair view of an organisation’s financial statements. However, given the specific scope and objectives of their mission, the risk information gathered by external auditors is limited to financial reporting risks and does not include the manner in which senior management and the governing body are managing/overseeing other (strategic, operational and compliance) risks, and for which the risk management- and internal auditing function provide monitoring, respectively assurance.

QUESTION 3

a) Discuss the link between ‘morality’ and a ‘corporation’. Describe the different ethical stances an organisation may adopt. (40 marks)

b) Define ‘Corporate Social Responsibility’ and explain why it has been described as ‘stakeholder capitalism’. Explain how the concept of ‘Corporate Social Responsibility’ is enshrined in statute in the UK? (60 marks)

Question 3 Answer

Morality and corporate behaviour is concerned with the relationship between the organisation as a juristic person and its actions in relation to society in terms of social, economic and market considerations. To understand the difficulty that society encounters in trying to communicate standards of conduct to corporations is arguably critical to the study of corporate governance.

In essence, the question is: can a company be treated as a ‘person’ in its own right with given ethical and moral standards? If so, can an organisation be capable of behaving in a socially responsible manner?

A key strategic issue within organisations is the ethical stance it adopts defined by Johnson and Scholes as ‘the extent to which an organisation will exceed its minimum obligations to stakeholders and society.’

Johnson and Scholes go on to identify four different ethical stances:
• Short-term shareholder interests: The only responsibility of an organisation is the short-term interests of its shareholders. It is for the legislature to set constraints on business behaviour and the organisation will comply with the standards.

• Long-term shareholder interests: The organisation adopts a proactive approach to managing relationships with other stakeholders.

• Multiple stakeholder obligations: Stakeholder interests and expectations are explicitly incorporated in the organisations purposes and strategies.

• Shaper of society: Organisations with purposes that are concerned with shaping society so that financial considerations are of secondary importance.

Part b) answer
Public and private sector organisations interact with society in general, not just by creating wealth for its owners but by providing employment, producing goods and services and using resources that effect the environment.

Corporate Social Responsibility (CSR) is a concept of organisation’s business operations and integration with its stakeholders on a wider, social and environmental basis.

Definitions of CSR differ between organisations and different industry sectors but most agree that the focus is on how organisations manage their core business to add social, environmental and economic value in order to maintain sustainable for society in general and for the business in particular.

The CSR forum defines it as: ‘Open and transparent business practices that are based on ethical values and respect for employees, communities and the environment. It is designed to deliver sustainable value to society at large, as well as shareholders’.

According to the department for Trade and Industry (now the Business, Enterprise and Regulatory Reform): ‘Corporate Social Responsibility is a wide ranging agenda and it involves businesses looking at how to improve their social, environmental and local economic impact, their influence on society, social cohesion and human rights, fair-trade and on the ways in which fairness can be corrupted. CSR is an issue both for large multinationals and for small locally based businesses’.

Corporate social responsibility goes far beyond the old philanthropy of the past-donating money to good causes at the end of the financial year-and instead an all year round responsibility that companies accept for the environment around them, for the best working practices, for their engagement in their local communities and for their recognition that brand names depend not only on quality, price and uniqueness but on how, cumulatively, they interact with companies’ workforce, community and environment.
Are we moving toward a challenging measure of corporate responsibility, where we judge results not just on input but by their outcomes; the difference we make to the world in which we live, and the contribution we make to poverty reduction?

Describe how the concept of CSR is now enshrined in statute: Section 172 (1) of The Companies Act? states that Directors’ general duties are: ‘to act in the way he/she considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole and in doing so have regard (amongst other matters) to the:

- likely consequences of any decision in the long term,
- interests of the company’s employees,
- need to foster the company’s business relationships with suppliers, customers and others,
- impact of the company’s operations on the community and the environment,
- desirability of the company maintaining a reputation for high standards of business conduct, and
- need to act fairly as between members of the company.

This was referred to by The Companies Act (2006) as ‘the concept of enlightened shareholder value’.

QUESTION 4

a) Describe the main differences between the UK and the US approach to corporate governance. (70 marks)

b) Explain how the corporate governance requirements of the US Sarbanes-Oxley Act differ from the requirements in the UK and Canada. (30 marks)

Question 4 Answer

Unit Nine: International Corporate Governance Students understanding of global board structures, reporting and knowledge of governance issues in relation to family-owned companies.

Part a) answer
The ‘comply or explain’ approach is the trademark of corporate governance in the UK. It has been in operation since the Combined Code’s beginnings following The
Cadbury Report and the foundation of the Code is in its flexibility particularly in terms of organisation size. It is strongly supported by both companies and shareholders and has been widely admired and the model has been imitated internationally.

The Boards of all Premium and Standard Listed Companies registered in the UK should voluntarily comply with the Code of Best Practice and make a statement about the extent of their compliance with the Code in the Annual Report and Accounts or alternatively, give reasons for any areas of noncompliance – known as the concept of comply or explain. The ‘comply or explain’ requirement was added to the Listing Rules of the London Stock Exchange so that companies should report whether they had followed the Cadbury recommendations or, if not, explain why they had not done so.

The Code is not a rigid set of rules. It consists of principles (main and supporting) and provisions. The Listing Rules require companies to apply the Main Principles and report to shareholders on how they have done so. The principles are the core of the Code and the way in which they are applied should be the central question for a board as it determines how it is to operate according to the Code.

Following high-profile scandals of Enron and WorldCom in the United States, Congress passed the Sarbanes–Oxley Act 2002 (known as ‘Sarbox’ or sometimes ‘sox’). It differs from the UK and other European and Commonwealth countries in that compliance is a matter of law rather than a rule of listing, in other words ‘rules based’ as opposed to ‘comply or explain’. Under NYSE listing rules, US companies must comply with a broad range of NYSE corporate governance standards and must annually certify such compliance. The chief executive officer must annually certify that he or she is not aware of any violation by the company of NYSE corporate governance standards. The Company is required to submit annual and interim written affirmations of compliance with applicable NYSE corporate governance standards, similar to the affirmations required of NYSE-listed US companies.

As a consequence, United States listed companies are required to comply in detail with the Sarbox provisions. One of the major criticisms of this approach is that it assumes ‘one size fits all’ to corporate governance provisions. In other words the same (detailed) provisions are required of small and medium-sized companies as of larger companies. These provisions apply to each company listed on Wall Street even though it may be a part of a company listed elsewhere.

**Part b) answer**

Canada initially adopted and to an extent still retains, a ‘principles-based’ approach to Corporate Governance largely due to its historic and commonwealth connections to the United Kingdom.

However, Canadian corporate governance had to undergo significant reform following the Sarbanes-Oxley Act because of a desire of the Canadian Securities Regulators’ (CSA) to maintain investor confidence in the Canadian regulatory system and preserve Canada’s privileged access to the US public markets.
The CSA introduced a series of national instruments and policies which affect the corporate governance of Canadian public companies (the CSA Rules). The CSA Rules closely follow Sarbanes-Oxley and the consequential rules and guidelines established by the US Securities and Exchange Commission (SEC) and US stock exchanges.

QUESTION 5

a) **Compare** and **contrast** the ‘unitary’ and ‘two tier’ Board structures.  

(40 marks)

b) **Explain** the significance and the geographical spread of ‘concentrated ownership’ of corporations.  

**Compare** and **contrast** ‘concentrated ownership’ with the ‘insider system’ in place in the Americas, the UK and Australasia.  

(60 marks)

Question 5 Answer

**Syllabus Reference**

Unit Six: Corporate Governance in the UK: The Third Sector

This question draws attention to the increasing importance of the third sector in terms of employment.

**Part a) answer**

In spite of structural differences between two-tier and unitary board systems, there are similarities in actual board practices in that both systems recognise a supervisory function and a managerial function, although the distinctions between the two functions tend to be more formalised in the two-tier structure.

The unitary board of directors and the supervisory board (in the two-tier structure) are elected by shareholders although in some countries employees may elect some supervisory body members (see above).

Both the unitary board and the supervisory board appoint the members of the managerial body. In the case of the two-tier system, the management board whereas in the unitary system, the board appoints and delegates to a group of managers.

The responsibility for accurate financial reporting and appropriate control systems together with compliance with legal and regulatory requirements rests with the unitary and supervisory board.

Each board system has been perceived to offer unique benefits. The one-tier system may result in a closer relation and better information flow between the supervisory and managerial bodies; however, the two-tier system encompasses a clearer, formal separation between the supervisory body and those being “supervised.” With the influence of the corporate governance best practice movement, the distinct
perceived benefits traditionally attributed to each system appear to be lessening as practices converge.

European governance codes express remarkable consensus on issues relating to board structure, roles and responsibilities; many suggest practices designed to enhance the distinction between the roles of the supervisory and managerial bodies, including supervisory body independence, separation of the chairman and CEO roles, and reliance on board committees.

**Part b) answer**

There are some significant differences in the ownership and control of corporations particularly with regard to the concentration of ownership within the three main areas of the world economy (The North America, South America, Europe, and Southeast Asia).

These three zones account for nearly 90% of the world economy. (The exception is The United Kingdom which is included with North America.)

Concentration of ownership is high on Continental Europe, in France and Germany more than 80 per cent of the largest 170 listed companies, has a single shareholder owning more than 25 per cent of shares and in more than 50 per cent of these companies, there is a single majority shareholder. High levels of ownership concentration are also discernible for the Far East and South America where the small number of publicly listed companies are owned and controlled by a small number of major shareholders. The nature of ownership in these regions comprise of large share blocks primarily held by families, governments, corporations or other institutions (or family holding companies) and other companies. Inter-company holdings of large blocks of shares are commonplace, frequently in the form of pyramids of shareholdings, cross shareholdings or complex webs of ownership. Bank holdings of shares vary and holdings by government also vary appreciably and ownership and control are rarely traded.

This model uses a system of interlocking networks for corporate control and was first described as an ‘insider system’ by Franks and Mayer.

In the United States, the United Kingdom, Canada, Australia, New Zealand, and Singapore, the level of ownership differs from the insider system in that most of the large firms are controlled directly by managers but owned (and controlled indirectly) by a dispersed ownership. In the United Kingdom in only 16 per cent of the largest 170 listed companies is there a single shareholder owning more than 25 per cent of shares and in only 6 per cent is there a single majority shareholder. The nature of that ownership also differs, the shares of listed companies in North America and the United Kingdom are primarily held by institutions, such as pension funds, life insurance firms and mutual funds as well as individual investors. Ownership is dispersed in that no one institution or individual holds a large stake in any one corporation. This is described as the ‘outsider system’.

The significance of the insider and outsider system becomes apparent when considering the pressures affecting those independent boards of public companies operating within the outsider system.
In the outsider system operating in the USA and the UK, market demand for the shares of an organisation is a measure of success of a listed organisation; as a general rule the higher the price the more successful or perceived or actual the organisation is deemed to be. Likewise if a listed company’s performance is deemed below expectations then the shareholders sell the shares and drive the price down. Boards are driven by stock market pressure to deliver short-term share value by its dispersed shareholders and it is the level of dispersion dictates the degree of organisational accountability.

**QUESTION 6**

a) **Explain** how the regulation of business and of risk management has converged.  

(30 marks)

b) **Describe** and **summarise** either the COSO or the ISO31000 ‘enterprise risk management’ framework and process.  

(70 marks)

**Question 6 Answer**

**Unit Ten: Internal Control and Risk Governance:** The critical understanding of the merger of regulatory systems, internal audit and risk management

**Syllabus Reference**

**Part a) answer**

The regulation of business and corporate risk management has converged; regulation through corporate governance enables the management of risks and risk management is a form of self-regulation. In the field of regulatory systems and internal control processes, the distinction between regulation and risk management has become blurred as the risk management blueprint of assessment, evaluation and control influence the design of regulatory systems.

The demand for governments to regulate both man-made and natural risks is on the increase and the response by the legislature has been two-fold:

Command and Control Regulation, this is state regulation by means of the legal framework

Enforced Self-Regulation (ESR) is a combination of state and corporate regulation; ‘they seek to penetrate the everyday life of the company and to harness its management tools in such a way as to align regulatory objectives and corporate strategy.’ ESR is employed in several areas such as health and safety, sustainable development and corporate governance.

Within the field of corporate governance it is in the area of internal control systems where regulatory systems and risk management has converged.
Robust Internal Control promotes efficient and operations of business processes through the creation of communication and the provision of information within an organisation thereby increasing management awareness of unexpected issues. It can be seen that an effective risk management fuses with internal control so that organisations are in a better position to react to any event or circumstance impacting on objectives and strategies.

**Part b) answer**

COSO proposes eight interrelated components of ERM. ‘They are derived from the way management runs a business and are integrated with the management process.’ The components are:

(1) Internal Environment: Internal environment is considered the foundation of all other ERM components because it provides the discipline and structure. It comprises of the corporate culture in terms of business ethics, education and training, management style and delegation of authority. It is from this corporate culture that management establishes risk culture, risk appetite and integrates ERM with related strategy and business initiatives.

(2) Objective Setting: Objectives must exist before management can identify events that may effect their achievement. There are four categories:

(3) Event Identification: This is the consideration of external factors (economic, business, natural environment, political, social and technological) and internal factors (infrastructure, personnel, process and technology) and the techniques and smart tools used to identify uncertainties including interrelationships between identified events.

(4) Risk Assessment: Here the management of an entity considers the likelihood and impact of potential events and how might affect the achievement of objectives. An entities risk assessment methodology normally compromises qualitative and quantitative techniques.

Risk assessment is first applied to inherent then residual risk with short, medium and long term horizons.

(5) Risk Response: Actions that have an effect on event-likelihood and impact in terms of risk tolerance and cost/benefits. The consideration of risk responses and selecting and implementing risk response are considered integral to ERM.

To an extent, the inclusion of cost/benefit analysis acknowledges that some level of residual risk will always exist. The Report also acknowledges the future uncertainties and limitations inherent in all activities as a further reason for residual risk.

(6) Control Activities: These are the policies and procedures that help ensure risk responses are executed. There are two elements: a policy establishing what should be done and procedures to affect the policy.

Of significance in this area is the operational risk of reliance on information systems.
There are two groups of control activities: general and application

(7) Information and Communication
This involves management in the identification, capturing, processing, refining, analysing and communication and reporting of large volumes of data into actionable coherent information this includes risk-based information.

One of the most critical communication channels is that between senior management and the board of directors, the latter must be kept up to date by the former on issues such as performance, developments and risk.

Management provides specific and directed communication addressing behavioural expectations and the responsibilities of personnel including the company’s ERM philosophy and risk culture.

External communications allows managers to align risk appetite, risk tolerance to that of its customers, suppliers and partners, and ensure that the company does not take on too much risk through business interactions.

(8) Monitoring: The report describes monitoring as ‘a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways: through on-going activities or separate evaluations.’
The Structure of ISO 31000

There are three main sections to The Guide:

- Risk Management Principles
- Risk Management Framework
- Risk Management Process

RISK MANAGEMENT FRAMEWORK

The Framework provides the foundations and arrangements that will embed and integrate risk management in the organization’s process.

Mandate and commitment
- Defines risk management policy and aligns it with organisation’s culture
- Determine performance indicators and align with the objectives and strategies of the organisation.
- Ensure legal and regulatory compliance
- Determine responsibilities and accountabilities
- Analyse resource requirements
- Communicate benefits of risk management to stakeholders
- Continually review appropriateness of risk management framework

Design of framework for managing risk
- Understanding the organization and its context
- Establishing a risk management policy
- Ensure accountability of risk owners
- Integrate into other processes of the organisation
- Allocate appropriate resources
- Establish internal and external communications and reporting mechanisms

Implementing risk management
- Implement framework for managing risk
- Implement processes (see below)

Monitoring and review of framework
- Measure performance against indicators on an agreed time basis
- Measure deviation from standards
- Review appropriateness and effectiveness of risk management policy, plan and framework
RISK MANAGEMENT PROCESS

The Process is the engine room of ISO 31000 risk governance and The Standard identifies five key activities:

(I) Communication and consultation
(II) Establishing the context
(III) Risk assessment
(IV) Risk treatment
(V) Monitoring and review

Each step should be integrated in management processes, embedded in the culture and tailored to suit the organisation.

(I) Communication and consultation
This area emphasises the transparency approach and encourages communication with external and internal stakeholders during all stages of the process.

Consultation Plans should include a description of the risk, its causes and possible effects and risk treatment.

(II) Establishing the context
The context establishes the objectives, defines parameters of managing risk as well as setting the scope and risk criteria for The Process. This is a detailed study and concentrates on:

- Establishing the external content
- Establishing the internal context
- Establishing the context of the risk management process
- Defining risk criteria

Establishing the external context: This is the organisation’s external environment (political, environmental, social, technological, legal and regulatory or PESTLE, cultural considerations, market factors and stakeholder management).

Establishing the internal context: Internal context is anything that can influence the way on organisation manages risks. Risk management processes should be aligned to that of the organisation in terms of strategy, culture, structure, policies, standards, processes and systems, resources, contractual relationships, information and communication systems.

Establishing the context of the risk management process This involves defining goals and objectives, scope, responsibilities, assets, products, services, projects, processes and functions.

Defining risk criteria: The factors to be considered include risk tolerance, nature, causes, likelihood, and consequences of risk with agreed measures, timeframe with stakeholder inputs during the process.
(III) Risk Assessment
The object of Risk Assessment is to provide decision-makers and other responsible parties with an understanding of risks that could affect achievement of objectives, as well as of the adequacy and effectiveness of controls already in place.

The ISO Risk management – Risk assessment techniques (ISO/IEC 31010:2009) was developed as a guidance to risk practitioners in implementing the risk assessment process. It considers current good practice and addresses the following:

What can happen and why?
What are the consequences?
What is the probability of their future occurrence?
Are there any factors that mitigate the consequences of the risk and/or that reduce the probability of the risk?

The Risk Assessment process is a classic structure and includes:

- Risk Identification
- Risk analysis
- Risk Evaluation

Risk Identification: This process includes identification of significant risk causes/scenarios and sources of events (whether controllable or not), areas of impact and potential consequences (including cascade and cumulative effects). The risk of not pursuing an activity or course of action should also be taken into consideration.

Risk analysis: The object of Risk Analysis is to understand causes and sources of risks, their positive and negative consequences (singular or multiple) and their likelihood of occurring and thus affecting objectives.

The level of analysis is subject to the level, quality and accuracy of available data and can be qualitative, quantitative or a mixture of the two. The available data will probably determine the basis of analysis; this can be hard systems methodologies such as statistical techniques or soft systems methodologies.

Risk Evaluation: Evaluate to assist decision-making based on the outcomes of the risk analysis process by comparing with criteria, to determine how to treat and prioritise risk.

(IV) Risk Treatment:
This is the cyclical process of modification or controlling risks through the selection and implementation of given options. It involves:

Assessment of a risk treatment option
Assessment of residual risk and risk tolerance
If not tolerable, opting for other risk treatment(s)
Assessing the effectiveness of the risk treatments(s)

(v) Monitoring and review
Planned periodic or ad hoc monitoring and review is an essential part of the risk management process. The purpose is to:

- Ensure controls are effective and efficient (in design and operation)
- Obtain new or further information to improve risk assessment
- Analysing events, near misses, changes, trends, successes and failures and learning lessons from them.

To complete the control environment loop, the risk management process should be recorded in order to provide traceability and basis for continuous improvement.