CIA Part 1
Essentials of Internal Auditing

Part 1, Domain I
Foundations of Internal Auditing

Section A: The IIA's Authoritative Guidance System

Learning Outcomes:

1. Interpret The IIA's Mission of Internal Audit, Definition of Internal Auditing, and Core Principles for the Professional Practice of Internal Auditing, and the purpose, authority, and responsibility of the internal audit activity. Tested at Proficiency level.

A. **The Institute of Internal Auditors (IIA)** is an international professional association that provides leadership and guidance for the global profession of internal auditing.

   1. Amongst the objectives of The IIA are the following:

      a. Advocating and promoting the value internal audit professionals add to their organizations.

      b. Providing comprehensive professional educational and development opportunities, standards and other professional practice guidance, and certification programs.

      c. Researching, disseminating, and promoting knowledge concerning internal auditing and its appropriate role in control, risk management, and governance to practitioners and stakeholders.

      d. Educating practitioners and other relevant audiences on best practices in internal auditing.

      e. Bringing together internal auditors from all countries to share information and experiences.

   2. The IIA has promoted the professionalization of internal auditing primarily through:

      a. Adopting a common body of knowledge identifying the related disciplines and the various competencies that are to be possessed by internal auditors.

      b. Establishing a certification program (the CIA Program) including an examination.

      c. Administering a Continuing Professional Education (CPE) program and requiring CIAs to adhere to CPE requirements.

d. Establishing an International Professional Practices Framework that includes the IIA's authoritative guidance for the global profession of internal auditing.

e. Publishing a technical journal and making it available to its members.

B. **International Professional Practices Framework (IPPF)** is the conceptual framework that organizes guidance promulgated by The IIA. Its scope only includes authoritative guidance developed by the IIA international technical boards and committees following due process. The IPPF includes the following elements:

1. **Mission of Internal Audit** – The Mission of Internal Audit is a statement that describes what internal audit aspires to accomplish within an organization. The ultimate purpose of the IPPF is to guide internal auditors in achieving the Mission of Internal Audit. As stated in the IPPF, the mission of internal audit is:

   "To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight."

2. **Mandatory Guidance –** Conformance with the mandatory guidance is required and essential for the professional practice of internal auditing. Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are the:

   a. **Core Principles for the Professional Practice of Internal Auditing** – The Core Principles are the key elements that describe internal audit effectiveness. All the following core principles should be achieved for an internal audit function to be considered effective

      i. Demonstrates integrity.

      ii. Demonstrates competence and due professional care.

      iii. Is objective and free from undue influence (independent).

      iv. Aligns with the strategies, objectives, and risks of the organization.

      v. Is appropriately positioned and adequately resourced.

      vi. Demonstrates quality and continuous improvement.

      vii. Communicates effectively.

      viii. Provides risk-based assurance.

      ix. Is insightful, proactive, and future-focused.

      x. Promotes organizational improvement.

   b. **Definition of Internal Auditing** – will be discussed in the following pages.

   c. **Code of Ethics** – will be discussed in detail in the following pages.

   d. **International Standards for the Professional Practice of Internal Auditin**g (the Standards) – The Standards will be discussed in detail in the following pages and throughout the material.

3. **Recommended Guidance –** Recommended guidance is endorsed by the IIA through a formal approval process. It describes practices for effective implementation of the IIA's Core Principles, Definition of Internal Auditing, Code of Ethics, and Standards. The recommended elements of the IPPF are:
    a. **Implementation Guidance –** Assists internal auditors in applying the Standards as well as promoting good practices. Implementation Guides address internal audit approach, methodologies, and consideration, but do not detail processes or procedures. Prior to January 1, 2017, implementation guidance was referred to as "Practice Advisories."
    b. **Supplemental Guidance –** Provides detailed guidance for conducting internal audit activities. They include topical areas, sector-specific issues, as well as processes and procedures, tools and techniques, programs, step-by-step approaches, and examples of deliverables. Currently, the Supplemental Guidance includes the following series:
        i. Practice Guides – General.
        ii. Practice Guides – Public Sector.
        iii. Global Technology Audit Guides (GTAGs).
        iv. Guides to the Assessment of IT Risk (GAIT).

C. Definition of Internal Auditing – As defined by the Institute of Internal Auditors,

"Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes."

Passing Tip:	Internal auditing is: – Independent – Objective – Assurance and consulting – Designed to add value – Improve an organization's operations – Helps an organization accomplish its objectives – Evaluate and improve effectiveness of governance, risk management, and control processes.

1. The following functions represent the objectives of internal auditing and typical activities within the scope of internal auditing:
   a. Assisting members of the organization in the effective discharge of their responsibilities.
   b. Assessing an operating department's effectiveness in achieving stated organizational goals.
   c. Checking for compliance with laws and regulations.
   d. Evaluating established objectives and goals.
2. While the following functions "may" be carried out by internal auditing upon management's request, they are not typically amongst the objectives of internal auditing:
   a. Assist management with the design and implementation of accounting and control systems.
   b. Examine and evaluate the organization's accounting system as a service to management.
   c. Monitor the organization's internal control system for the external auditors.
   d. Assist the external auditor in order to reduce external audit fees.
   e. Perform studies to assist in the attainment of more efficient operations.
   f. Serve as the investigative arm of the audit committee.
   g. Safeguarding of assets.

Passing Tip:	Generally, internal auditors – Review – Assess – Provide assurance Internal auditors **DO NOT** – Design – Secure – Implement – Manage – Take responsibility for controls

D. **The International Standards**

1. **The Standards** are a set of principles-based mandatory requirements that provide a framework for performing and promoting internal auditing.
   a. The Standards refer to:
      i. Criteria by which the operations of an internal auditing department are evaluated and measured.
      ii. Statements intended to represent the practice of internal auditing as it must be.
      iii. Criteria that is applicable to all types of internal auditing services.
   b. They are numbered using a four-digit code and consist of:
      i. **Statements of core requirements** for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels.
      ii. **Interpretations** clarifying terms or concepts within the Standards. Interpretations, where needed, will immediately follow the associated standard.
   c. The structure of the Standards is divided between Attribute and Performance Standards:
      i. **Attribute Standards** address the attributes of organizations and individuals performing internal auditing.
      ii. **Performance Standards** describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured.
      iii. **Implementation Standards** are also provided to expand upon the Attribute and Performance standards, by providing the requirements applicable to assurance (A) or consulting (C) activities. Implementation Standards are denoted by a point and a standard number using A# for assurance and C# for consulting. For example, Implementation Standard 1000.A1 or 1000.C1.
   d. The Standards employ terms as defined specifically in the Glossary. To understand and apply the Standards correctly, it is necessary to consider the specific meanings from the Glossary. Specifically, the Standards use the word “must” to specify an unconditional requirement and the word “should” where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

Passing Tip:	When an internal auditor is operating in an environment that is subject to additional standards, the internal auditor should follow both the IIA Standards and any additional governmental, statutory, or other standards.

2. **Purpose** – According to the IPPF, the purpose of the Standards is to:
   a. Guide adherence with the mandatory elements of the International Professional Practices Framework.
   b. Provide a framework for performing and promoting a broad range of value-added internal auditing services.
   c. Establish the basis for the evaluation of internal audit performance.
   d. Foster improved organizational processes and operations.
3. **The IIA's Attribute Standards**
   a. **1000–Purpose, Authority, and Responsibility –** The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.
   b. **1100–Independence and Objectivity –** The internal audit activity must be independent, and internal auditors must be objective in performing their work.
   c. **1200–Proficiency and Due Professional Care –** Engagements must be performed with proficiency and due professional care.
   d. **1300–Quality Assurance and Improvement Program –** The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.
4. **The IIA's Performance Standards**
   a. **2000–Managing the Internal Audit Activity –** The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.
   b. **2100–Nature of Work –** The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.
   c. **2200–Engagement Planning –** Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.
   d. **2300–Performing the Engagement –** Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

e. **2400–Communicating Results –** Internal auditors must communicate the results of engagements.

f. **2500–Monitoring Progress –** The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

g. **2600–Communicating the Acceptance of Risks –** When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Studying Tip:	Both the Attribute Standards and the Performance Standards are discussed in greater detail in the relevant sections of the material. Questions in this domain may only be answered after completing the other sections. The complete Standards are presented in the Appendix of Part 1.

E. **IIA's Glossary of Terms** – The complete list of the IIA Glossary is included below. These definitions do not need to be memorized, however, understanding them is very important for the exam candidates.

1. **Add Value –** The internal audit activity adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.
2. **Adequate Control –** Present if management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.
3. **Assurance Services –** An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.
4. **Board –** The highest-level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the Standards refers to a group or person charged with governance of the organization. Furthermore, "board" in the Standards may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

5. **Charter –** The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.
6. **Chief Audit Executive –** Chief audit executive describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.
7. **Code of Ethics –** The Code of Ethics of The Institute of Internal Auditors (IIA) are Principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.
8. **Compliance –** Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.
9. **Conflict of Interest –** Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.
10. **Consulting Services –** Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation and training.
11. **Control –** Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

12. **Control Environment –** The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:
    a. Integrity and ethical values.
    b. Management's philosophy and operating style.
    c. Organizational structure.
    d. Assignment of authority and responsibility.
    e. Human resource policies and practices.
    f. Competence of personnel.
13. **Control Processes –** The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.
14. **Core Principles for the Professional Practice of Internal Auditing –** are the foundation for the International Professional Practices Framework and support internal audit effectiveness.
15. **Engagement –** A specific internal audit assignment, task, or review activity, such as an internal audit, Control Self-Assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.
16. **Engagement Objectives –** Broad statements developed by internal auditors that define intended engagement accomplishments.
17. **Engagement Opinion –** The rating, conclusion, and/or other description of results of an individual internal audit engagement, relating to those aspects within the objectives and scope of the engagement.
18. **Engagement Work Program –** A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.
19. **External Service Provider –** A person or firm outside of the organization that has special knowledge, skill, and experience in a particular discipline.
20. **Fraud –** Any illegal act characterized by deceit, concealment or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.
21. **Governance –** The combination of processes and structures implemented by the board to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives.

22. **Impairment –** Impairment to organizational independence and individual objectivity may include personal conflicts of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).
23. **Independence –** The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.
24. **Information Technology Controls –** Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.
25. **Information Technology Governance –** Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.
26. **Internal Audit Activity –** A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.
27. **International Professional Practices Framework –** The conceptual framework that organizes the authoritative guidance promulgated by The IIA. Authoritative guidance is composed of two categories – (1) mandatory and (2) recommended.
28. **Must –** The Standards use the word "must" to specify an unconditional requirement.
29. **Objectivity –** An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.
30. **Overall Opinion –** The rating, conclusion, and/or other description of results provided by the chief audit executive addressing, at a broad level, governance, risk management, and/or control processes of the organization. An overall opinion is the professional judgment of the chief audit executive based on the results of a number of individual engagements and other activities for a specific time interval.
31. **Risk –** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
32. **Risk Appetite –** The level of risk that an organization is willing to accept.
33. **Risk Management –** A process to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.
34. **Should –** The Standards use the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

35. **Significance –** The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.
36. **Standard –** A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.
37. **Technology-based Audit Techniques –** Any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and computer-assisted audit techniques (CAATs).

Section B: Internal Audit Charter

Learning Outcomes:

1. Explain the requirements of an internal audit charter (required components, board approval, communication of the charter, etc.). Tested at Basic level.

According to the Standards, the **purpose, authority, and responsibility** of the internal audit activity must be **formally defined in an internal audit charter**, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the **board** for approval.

A. Internal Audit Activity Charter

1. The internal audit charter is a formal document that:
    a. Defines the internal audit activity's purpose, authority, and responsibility.
    b. Establishes the internal audit activity's position within the organization.
    c. Authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and
    d. Defines the scope of internal audit activities.
2. The internal audit activity charter must recognize the mandatory nature of the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing.
3. The nature of both assurance and consulting services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

Passing Tip:	The internal audit charter does **NOT** specify the resources needed or available for the internal audit activity.

4. The charter is:
   a. **Prepared** by the Chief Audit Executive (**CAE**).
   b. **Approved** by the Chief Executive Officer (**CEO**) or other senior management officer.
   c. **Accepted** by the board of directors (**BOD**), **audit committee**, and/or other appropriate governing authority. The audit committee is discussed in more detail in the following pages.
   d. **Communicated** to engagement clients.

Passing Tip:	The internal audit charter is: Prepared ⇔ CAE Approved ⇔ Management Accepted ⇔ Board or Audit Committee Communicated ⇔ Engagement Clients

5. The CAE must periodically assess whether the purpose, authority, and responsibility, as defined in the charter, continue to be adequate to enable the internal audit activity to accomplish its objectives. The result of this periodic assessment must be communicated to senior management and the board for approval.
6. The nature of the work performed by the internal audit activity is defined in the charter. Any significant changes to the nature of work performed by the internal audit activity must be agreed with the audit committee and the changes must also be made to the charter. For example,
   a. If the internal audit activity performed only audits that provide cost-savings for the organization, this would normally constitute a significant change that requires the change to be agreed with the audit committee and the charter must be changed accordingly.
   b. If the internal audit activity was requested by management to perform services outside the scope identified in the charter, such change must be agreed with the audit committee in order to amend the charter accordingly.
7. **Advantages of a Formally Written Charter**
   a. It provides formal communication for review and approval by management and for acceptance by the board.
   b. It facilitates a periodic assessment of the adequacy of the internal audit activity's purpose, authority, and responsibility.

c. It establishes the role of the internal audit activity and provides a basis for management and the board to use in evaluating the operations of the function.

d. It provides a formal written agreement with management and the board about the role and responsibilities of the internal audit activity within the organization should a conflict arise.

B. The internal audit charter documents the following as they pertain to the internal audit activity:

- Purpose and Mission of the Internal Audit Activity
- Recognizing Mandatory Guidance
- Authority
- Scope of the Internal Audit Activity
- Independence and Objectivity
- Responsibility
- Quality Assurance and Improvement Program
- Sign-offs

The following is a model internal audit activity charter obtained from the IIA's guidance system. Studying this model charter is recommended as it illustrates the purpose, authority, and responsibility of the internal audit activity along with other elements typically included in an internal audit charter. Many of the aspects mentioned in this charter will be explained further throughout this book.

Sample Internal Audit Charter (Source IIA Website)

Purpose and Mission

Purpose

The purpose of the internal audit activity is to provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. The mission of internal audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. The internal audit activity helps the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

Recognizing Mandatory Guidance

Guidance

The internal audit activity will govern itself by adherence to the mandatory elements of The Institute of Internal Auditors' IPPF, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the International Standards for the Professional Practice of Internal Auditing, and the Definition of Internal Auditing. The CAE will report periodically to senior management and the board regarding the internal audit activity's conformance with the Code of Ethics and the Standards.

Authority

Authority

The CAE will report functionally to the board and administratively to the chief executive officer. To establish, maintain, and assure that the internal audit activity has sufficient authority to fulfill its duties, the board will:

1. Approve the internal audit activity's charter.
2. Approve the risk-based internal audit plan.
3. Approve the internal audit activity's budget and resource plan.
4. Receive communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters.
5. Approve decisions regarding the appointment and removal of the chief audit executive.
6. Approve the remuneration of the chief audit executive.
7. Make appropriate inquiries of management and the chief audit executive to determine whether there is inappropriate scope or resource limitations.

The CAE will have unrestricted access to, and communicate and interact directly with, the board, including private meetings without management present.

The board authorizes the internal audit activity to:

1. Have full, free, and unrestricted access to all functions, records, property, and personnel pertinent to carrying out any engagement, subject to accountability for confidentiality and safeguarding of records and information.
2. Allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports.

Obtain assistance from the necessary personnel of the organization, as well as other specialized services from within or outside the organization, in order to complete the engagement.

Scope

Scope of Internal Audit Activities

The scope of the internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the board, management, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for the organization. Internal audit assessments include evaluating whether:

1. Risks relating to the achievement of the organization's strategic objectives are appropriately identified and managed.
2. The actions of the organization's officers, directors, employees, and contractors are in compliance with the organization's policies, procedures, and applicable laws, regulations, and governance standards.
3. The results of operations or programs are consistent with established goals and objectives.
4. Operations or programs are being carried out effectively and efficiently.
5. Established processes and systems enable compliance with the policies, procedures, laws, and regulations that could significantly impact the organization.
6. Information and the means used to identify, measure, analyze, classify, and report such information are reliable and have integrity.
7. Resources and assets are acquired economically, used efficiently, and protected adequately.

The CAE will report periodically to senior management and the board regarding:

1. The internal audit activity's purpose, authority, and responsibility.
2. The internal audit activity's plan and performance relative to its plan.
3. Significant risk exposures and control issues, including fraud risks, governance issues, and other matters requiring the attention of, or requested by, the board.
4. Results of audit engagements or other activities.
5. Resource requirements.
6. Any response to risk by management that may be unacceptable to the organization.

The CAE also coordinates activities, where possible, and considers relying upon the work of other internal and external assurance and consulting service providers as needed. The internal audit activity may perform advisory and related client service activities, the nature and scope of which will be agreed with the client, provided the internal audit activity does not assume management responsibility.

All opportunities for improving management control, profitability, and the organization's image that are identified during audits must be communicated to the appropriate level of management.

Independence and Objectivity

Independence and Objectivity

The CAE will ensure that the internal audit activity remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of audit selection, scope, procedures, frequency, timing, and report content. If the CAE determines that independence or objectivity may be impaired in fact or appearance, the details of impairment will be disclosed to appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively and in such a manner that they believe in their work product, that no quality compromises are made, and that they do not subordinate their judgment on audit matters to others.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment, including:

1. Assessing specific operations for which they had responsibility within the previous year.
2. Performing any operational duties for the organization or its affiliates.
3. Initiating or approving transactions external to the internal audit activity.
4. Directing the activities of any employee not employed by the internal audit activity, except to the extent that such employees have been appropriately assigned to auditing teams or to otherwise assist internal auditors.

Where the CAE has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards will be established to limit impairments to independence or objectivity.

Internal auditors will:

1. Disclose any impairment of independence or objectivity, in fact or appearance, to appropriate parties.
2. Exhibit professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined.
3. Make balanced assessments of all available and relevant facts and circumstances.
4. Take necessary precautions to avoid being unduly influenced by their own interests or by others in forming judgments.

The CAE will confirm to the board, at least annually, the organizational independence of the internal audit activity.

The CAE will disclose to the board any interference and related implications in determining the scope of internal auditing, performing work, and/or communicating results.

Responsibility

Responsibility

The CAE has the responsibility to:

1. Submit, at least annually, to senior management and the board a risk-based internal audit plan for review and approval.
2. Communicate to senior management and the board the impact of resource limitations on the internal audit plan.
3. Review and adjust the internal audit plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.
4. Communicate to senior management and the board any significant interim changes to the internal audit plan.
5. Ensure each engagement of the internal audit plan is executed, including the establishment of objectives and scope, the assignment of appropriate and adequately supervised resources, the documentation of work programs and testing results, and the communication of engagement results with applicable conclusions and recommendations to appropriate parties.
6. Follow up on engagement findings and corrective actions, and report periodically to senior management and the board any corrective actions not effectively implemented.
7. Ensure the principles of integrity, objectivity, confidentiality, and competency are applied and upheld.
8. Ensure the internal audit activity collectively possesses or obtains the knowledge, skills, and other competencies needed to meet the requirements of the internal audit charter.
9. Ensure trends and emerging issues that could impact the organization are considered and communicated to senior management and the board as appropriate.
10. Ensure emerging trends and successful practices of internal auditing are considered.
11. Establish and ensure adherence to policies and procedures designed to guide the internal audit activity.
12. Ensure adherence to the organization's relevant policies and procedures, unless such policies and procedures conflict with the internal audit charter. Any such conflicts will be resolved or otherwise communicated to senior management and the board.
13. Ensure conformance of the internal audit activity with the Standards, with the following qualifications:
    a. If the internal audit activity is prohibited by law or regulation from conformance with certain parts of the Standards, the CAE will ensure appropriate disclosures and will ensure conformance with all other parts of the Standards.
    b. If the Standards are used in conjunction with requirements issued by other authoritative bodies, the CAE will ensure that the internal audit activity conforms to the Standards, even if the internal audit activity also conforms to the more restrictive requirements of other authoritative bodies.

Quality Assurance and Improvement Program

Quality Assurance

The internal audit activity will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. The program will include an evaluation of the internal audit activity's conformance with the Standards and an evaluation of whether internal auditors apply The IIA's Code of Ethics. The program will also assess the efficiency and effectiveness of the internal audit activity and identify opportunities for improvement.

The CAE will communicate to senior management and the board on the internal audit activity's quality assurance and improvement program, including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization.

Sign-offs

Prepared	*Accepted*
Chief Audit Executive	Audit Committee Chair

Approved

Senior Management

Must be regularly updated to remain valid

Date

The Audit Committee

Audit Committee is usually a subcommittee of the board of directors. It is composed of independent and financially literate members (as defined by any applicable regulation or the board of directors) with at least one member having expertise in financial reporting. The committee will include board members and outsiders that are appointed by a nominating committee.

A. **Purpose** – the purpose of the audit committee is to assist the board of directors (or other governing authority) in fulfilling its oversight responsibilities for the financial reporting process, the system of internal control over financial reporting, the audit process, and the company's process for monitoring compliance with laws and regulations and the code of conduct.

B. **Authority** – the audit committee has authority to conduct or authorize investigations into any matters within its scope of responsibility. It is empowered to:

   1. Retain outside counsel, accountants, or others to advise the committee or assist in the conduct of an investigation.
   2. Seek any information it requires from employees – all of whom are directed to cooperate with the committee's requests – or external parties.
   3. Meet with company officers, external auditors, or outside counsel, as necessary.

C. **Responsibility** – the audit committee's responsibilities are summarized as follows:

   1. **Financial statements**

      a. Review significant accounting and reporting issues, including complex or unusual transactions and highly judgmental areas, and recent professional and regulatory pronouncements, and understand their impact on the financial statements.

      b. Review with management and the external auditors the results of the audit, including any difficulties encountered.

      c. Review the annual financial statements, and consider whether they are complete, consistent with information known to committee members, and reflect appropriate accounting principles.

      d. Review other sections of the annual report and related regulatory filings before release and consider the accuracy and completeness of the information.

      e. Review with management and the external auditors all matters required to be communicated to the committee under generally accepted auditing standards.

      f. Understand how management develops interim financial information, and the nature and extent of internal and external auditor involvement.

g. Review interim financial reports with management and the external auditors before filing with regulators and consider whether they are complete and consistent with the information known to committee members.

2. **Internal control**

   a. Consider the effectiveness of the company's internal control over annual and interim financial reporting, including information technology security and control.

   b. Understand the scope of internal and external auditors' review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with management's responses.

3. **Internal audit**

   a. Review with management and the internal audit director the charter, plans, activities, staffing, and organizational structure of the internal audit function.

   b. Ensure there are no unjustified restrictions or limitations, and review and **concur in the appointment, replacement, or dismissal of the CAE**.

   c. Review the effectiveness of the internal audit function, including compliance with the IIA's *Standards for the Professional Practice of Internal Auditing*.

   d. On a regular basis, meet separately with the director of internal audit to discuss any matters that the committee or internal audit believes should be discussed privately.

4. **External audit**

   a. Review the external auditors' proposed audit scope and approach, including coordination of audit effort with internal audit.

   b. Review the performance of the external auditors, and exercise final approval on the appointment or discharge of the auditors.

   c. Review and confirm the independence of the external auditors by obtaining statements from the auditors on relationships between the auditors and the company, including non-audit services, and discussing the relationships with the auditors.

   d. On a regular basis, meet separately with the external auditors to discuss any matters that the committee or auditors believe should be discussed privately.

5. **Compliance**

   a. Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disciplinary action) of any instances of noncompliance.

   b. Review the findings of any examinations by regulatory agencies, and any auditor observations.

c. Review the process for communicating the code of conduct to company personnel, and for monitoring compliance therewith.

d. Obtain regular updates from management and company legal counsel regarding compliance matters.

6. **Reporting**

a. Regularly report to the board of directors about committee activities, issues, and related recommendations.

b. Provide an open avenue of communication between internal audit, the external auditors, and the board of directors.

c. Report annually to the shareholders, describing the committee's composition, responsibilities and how they were discharged, and any other information required by rule.

d. Review any other reports the company issues that relate to committee responsibilities.

7. **Other**

a. Perform other activities related to the audit committee charter as requested by the board of directors.

b. Institute and oversee special investigations as needed.

c. Review and assess the adequacy of the committee charter annually, requesting board approval for proposed changes.

d. Confirm annually that all responsibilities outlined in this charter have been carried out.

e. Evaluate the committee's and individual members' performance on a regular basis.

Section C: Assurance and Consulting Services

Learning Outcomes:

1. Interpret the difference between assurance and consulting services provided by the internal audit activity. Tested at Proficiency level.

A. As stated in the Definition of Internal Auditing, internal auditing is an "assurance and consulting activity". Therefore, internal auditing performs two major categories of services:

   1. **Assurance Services** involve the internal auditor's objective assessment of evidence to provide opinions or conclusions regarding an entity, operation, function, process, or systems. The purpose of assurance services is to provide an independent assessment on governance, risk management, and control processes for the organization. Examples of assurance engagements include financial, performance, compliance, system security, and due diligence engagements. The nature and scope of an assurance engagement are determined by the internal auditor. Parties involved in assurance services are:

      a. **The Process Owner** (auditee) – the person or group directly involved with the entity, operation, function, process, system or other subject matter.

      b. **The Internal Auditor** – the person or group making the assessment.

      c. **Users** (report recipients) – the person or group using the assessment.

   2. **Consulting Services** are advisory in nature and are generally performed at the specific request of an engagement client. The purpose of consulting services is to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Examples of consulting engagements include counsel, advice, facilitation, and training. Parties involved in consulting services are

      a. **The Internal Auditor** – the person or group offering the advice.

      b. **The Engagement Client** – the person or group seeking and receiving the advice.

B. **Types of Audits** – contrary to public misconception, internal auditors do not only perform financial audits. There are several types of audits that are performed by internal auditors:

   1. **Compliance Audit** is an audit to test whether the organization is operating in accordance with **conditions imposed** on the organization by **law** or **regulation**, **contractual agreement**, and/or the **policies** and **procedures** set by the organization's management.

   2. **Operational Audit** is an audit to test whether the functions within the organization are **effective** in achieving their **objectives** and are operating **efficiently** and economically.

3. **Financial Audit** is an audit of the economic activity to test the reliability and integrity of reported information and to ascertain that the company's assets are safeguarded.
4. **Information Systems Audit** is an audit to test the security and integrity of data processing systems in addition to the data generated by those systems. This includes determining that financial and operating records and reports contain accurate, reliable, timely, complete, and useful information.
5. **Performance Audits** include:
    a. **Economy and Efficiency Audit** is an audit of a certain program or activity concentrating primarily on the **economy and efficiency** of the function to test:
        i. Whether the entity is obtaining and using its resources economically and efficiently.
        ii. The reasons for inefficiencies, if applicable; and
        iii. Compliance with related laws and regulations pertaining to issues of economy and efficiency.
    b. **Program (Program-results) Audit** is an audit of a certain program or activity concentrating primarily on the **output (thus effectiveness)** to test:
        i. The achievement of the desired objectives that are preset.
        ii. The effectiveness of the programs or activities in achieving the desired objectives; and
        iii. Compliance with related laws and regulations pertaining to the program or function under audit.
6. **Environmental Audits include**:
    a. **Compliance audit** is a site-specific, detailed audit of on-going operations, past practices, and/or planned future operations to test for compliance with environmental laws.
    b. **Environmental management system audit** ascertains that the systems are operating properly to curtail any future environmental risk.
    c. **Transactional audit** is an audit to assess the potential risk/liability of a real property as a result of environmental contamination. *(Also referred to as Acquisition and Divestiture Audits, Property Transfer Site Assessments, Property Transfer Evaluations, and/or Due Diligence Audits)*
    d. **Treatment, storage, and disposal facility audit** is the audit of the tracking (cradle-to-grave) of hazardous materials documents and treatments. Any party involved with such hazardous materials may ultimately become liable if such materials cause any future environmental damage.

e. **Pollution prevention audit** refers to the elimination of the pollution at source through the following hierarchy:
   i. Recovery as a useable product
   ii. Elimination at source
   iii. Recycling and reusing
   iv. Conserving energy
   v. Treatment
   vi. Disposal
   vii. Release

f. **Environmental liability accrual audit** is the process of recognizing, quantifying, and reporting **liability accruals for environmental issues.**

g. **Product audit** is the audit of a product to ensure that it is in compliance with current environmental requirements.

Section D: Code of Ethics

Learning Outcomes:
1. Demonstrate conformance with the IIA Code of Ethics. Tested at Proficiency level.

INTRODUCTION

The purpose of The IIA's *Code of Ethics* is to promote an ethical culture in the profession of internal auditing.

> ***Internal auditing*** *is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.*

A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about governance, risk management, and control.

The Institute's *Code of Ethics* extends beyond the Definition of Internal Auditing to include two essential components:

1. **Principles** that are relevant to the profession and practice of internal auditing. The four principles are integrity, objectivity, confidentiality, and competency.
2. **Rules of Conduct** that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

"Internal auditors" refers to Institute members, recipients of or candidates for IIA professional certifications, and those who provide internal audit services within the Definition of Internal Auditing.

APPLICABILITY AND ENFORCEMENT

This *Code of Ethics* applies to both individuals and entities that provide internal auditing services.

For IIA members and recipients of or candidates for IIA professional certifications, breaches of the *Code of Ethics* will be evaluated and administered according to The Institute's Bylaws and Administrative Directives. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

Passing Tip:	When an internal auditor encounters a situation that is not explicitly addressed by the IIA Code of Ethics, the auditor must apply individual judgment and take action consistent with the principles embodied in the IIA Code of Ethics, even if this action violates the loyalty to the auditor's employer (role conflict).

The following tables include the four principles of the *Code of Ethics* along with the rules of conduct for each principle. Examples of acceptable and unacceptable behaviors under each principle are also provided.

INTEGRITY

Principle

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

Rules of Conduct

Internal auditors:

1. Shall perform their work with honesty, diligence, and responsibility.
2. Shall observe the law and make disclosures expected by the law and the profession.
3. Shall not knowingly be a party to any illegal activity or engage in acts that are discreditable to the profession of internal auditing or to the organization.
4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

Unacceptable Behavior

- Late arrivals and early departures from work because this practice is common in the organization.
- Respect and contribute to the objectives of the organization even if it is engaged in illegal activities.
- An auditor did not report significant observations about illegal activity to the board because management indicated that it would resolve the issue.
- Knowing that management was aware of the situation, an internal auditor purposely left a description of an unlawful practice out of the report.

Acceptable Behavior

- Comply with the Standards for the International Professional Practice Framework of Internal Auditing.
- Observe the law even in their personal lives.
- Respect and contribute to the legitimate and ethical objectives of the organization.
- An auditor reports significant observations about illegal activity to the board even if management indicated that it would resolve the issue.

OBJECTIVITY

Principle

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

Rules of Conduct

Internal auditors:

1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

Unacceptable Behavior

- Preparing the personal tax return, for a fee, for one of the company's division managers.
- Frequent luncheons and other socializing with major suppliers of the company without the consent of senior management.
- Acceptance of a material gift from a supplier even if it was customary in the industry and/or function.
- The CAE decides to delay the audit of a branch so that his nephew, the branch manager, will have time to "clean things up".
- Acceptance of airline tickets from an auditee.
- Serving as a consultant to suppliers.
- Serving as a consultant to competing organizations.
- Failing to report to management information that would be material to management's judgment.

Acceptable Behavior

- Disclosing material facts known to the auditor that could distort the report if not revealed.
- An internal auditor, with the knowledge and consent of management, accepted a token gift from a customer of the organization that was not presumed to impair and did not impair judgment.
- Writing a tax guide intended for publication and sale to the general public.
- Teaching an evening tax seminar, for a fee, at a local university.
- Preparing tax returns for elderly citizens, regardless of their associations, as a public service.
- Conducting an unrelated business outside of office hours with management's knowledge.

CONFIDENTIALITY

Principle

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

Rules of Conduct

Internal auditors:

1. Shall be prudent in the use and protection of information acquired in the course of their duties.
2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

Unacceptable Behavior

- An auditor used audit-related information in a decision to buy stock issued by the employer corporation.
- Purchasing stock in a target company after overhearing a company executive's discussion of a possible acquisition.
- Discussing audit plans or results with external parties.
- Promise a whistle blower absolute anonymity when they disclose sensitive information to the auditor, because the auditor may try to protect whistle blowers, they must act on any information received in the best interests of the organization.
- Bypass the CAE and discuss matters with the external auditors.
- Discussing and/or sharing findings/recommendations with auditors from another organization.

Acceptable Behavior

- An auditor was subpoenaed in a court case in which a merger partner claimed to have been defrauded by the auditor's company. The auditor divulged confidential audit information to the court.
- An auditor gave a speech at a local IIA chapter meeting outlining the contents of a program the auditor had developed for auditing electronic data interchange (EDI) connections. Several auditors from major competitors were in the audience.
- The CAE refuses to provide information about company operations to his father, who is a shareholder.
- An internal auditor shared audit techniques and/or organizational controls with auditors from another company.
- Based upon knowledge of the probable success of the employer's business, an internal auditor invested in a mutual fund that specialized in the same industry.

COMPETENCY	
Principle	Internal auditors apply the knowledge, skills, and experience needed in the performance of internal auditing services.
Rules of Conduct	Internal auditors: 1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience. 2. Shall perform internal auditing services in accordance with the *International Standards for the Professional Practice of Internal Auditing*. 3. Shall continually improve their proficiency and the effectiveness and quality of their services.
Unacceptable Behavior	– To save company resources, the CAE cancels all staff training for the next 2 years on the basis that all staff are too new to benefit from training. – To save company resources, the CAE limits the audit of foreign branches to confirmations from branch managers that no major personnel changes have occurred. – An auditor failing to engage in continuing professional education or other activities to improve knowledge, skills, and effectiveness.
Acceptable Behavior	– An internal auditor regularly attends specialized internal audit workshops and seminars and commingles with internal auditors of competing companies. – The CAE regularly rotates staff on engagements to enable them to learn hands-on in different areas.

Organizational Code of Conduct

The IIA's Code of Ethics for internal auditors must be distinguished from the code of conduct that may be applicable within the organization. The internal audit activity is responsible for assessing the ethical climate of the organization and reporting on it to the audit committee. Such assessment is to be in accordance with applicable codes of conduct/ethics, and/or universally accepted ethical standards.

A. The internal audit activity is responsible for periodically assessing the state of the ethical climate of the organization and the effectiveness of its strategies, tactics, communications, and other processes in achieving the desired level of legal and ethical compliance.

B. The effectiveness of the following features of an enhanced and highly effective ethical culture needs to be evaluated by the internal auditors:

    1. Formal code of conduct, which is clear and understandable, and related statements, policies (including procedures covering fraud and corruption), and other expressions of aspiration.
    2. Frequent communications and demonstrations of expected ethical attitudes and behavior by the influential leaders of the organization.
    3. Explicit strategies to support and enhance the ethical culture with regular programs to update and renew the organization's commitment to an ethical culture.
    4. Several, easily accessible ways for people to confidentially report alleged violations of the code, policies, and other acts of misconduct.
    5. Regular declarations by employees, suppliers, and customers that they are aware of the requirements for ethical behavior in transacting the organization's affairs.
    6. Clear delegation of responsibilities to ensure that ethical consequences are evaluated, confidential counseling is provided, allegations of misconduct are investigated, and case findings are properly reported.
    7. Easy access to learning opportunities to enable all employees to be ethics advocates.
    8. Positive personnel practices that encourage every employee to contribute to the ethical climate of the organization.
    9. Regular surveys of employees, suppliers, and customers to determine the state of the ethical climate in the organization.
    10. Regular reviews of the formal and informal processes within the organization that could potentially create pressures and biases that would undermine the ethical culture.
    11. Regular reference and background checks as part of hiring procedures, including integrity tests, drug screening, and similar measures.

C. The existence of the company's code of conduct implies that the company has established objective criteria against which employee actions may be evaluated.

D. The mere presence of a code of conduct does not ensure higher standards of ethical behavior. The code needs to be complemented by follow-up policies and monitoring activities to ensure adherence to it.

E. On the other hand, the absence of a formal code of conduct in a company should not prevent a successful audit of ethical behavior since such behavior may be documented in company policies and procedures.

Part 1, Domain II
Independence and Objectivity

Section A: Independence and Objectivity

Learning Outcomes:

1. Interpret organizational independence of the internal audit activity (importance of independence, functional reporting, etc.). Basic level.
2. Identify whether the internal audit activity has any impairments to its independence. Basic level.
3. Assess and maintain an individual internal auditor's objectivity, including determining whether an individual internal auditor has any impairments to his/her objectivity. Proficiency level.
4. Analyze policies that promote objectivity. Proficiency level.

Independence
Objectivity

According to the Standards, the internal audit activity must be **independent** and internal auditors must be **objective** in performing their work.

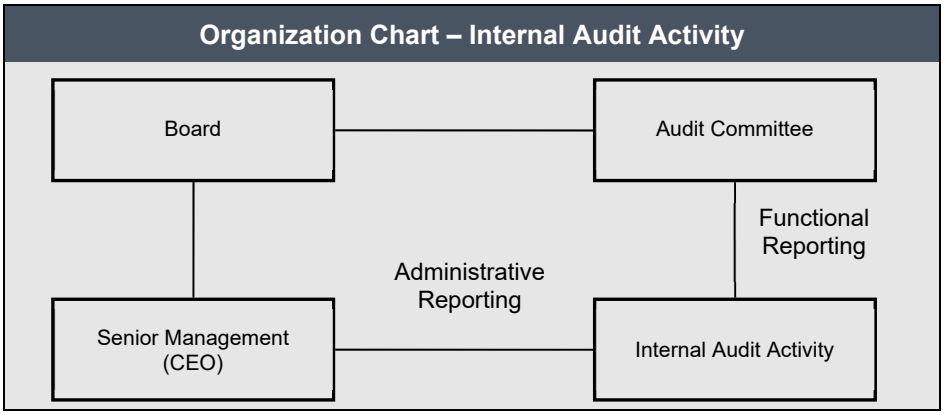
Independence

Independence
Objectivity

Internal auditors are independent when they can carry out their work freely and objectively. Independence permits internal auditors to render the impartial and unbiased judgments essential to the proper conduct of engagements.

Independence is defined as "the freedom from conditions that threaten the ability of the internal audit activity or the chief audit executive to carry out internal audit responsibilities in an unbiased manner." To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has **direct and unrestricted access to senior management and the board**. This can be achieved through a **dual-reporting relationship**. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

A. **Organizational Independence** of the internal audit activity implies that the CAE must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.

1. The CAE needs to be responsible to an individual in the organization with sufficient authority to promote independence and to ensure broad audit coverage, adequate consideration of engagement communications, and appropriate action on engagement recommendations. Therefore, it is necessary to consider the organizational placement and supervisory reporting lines of the internal audit to ensure organizational independence.
2. **Dual-reporting Relationship** – ideally, for enhanced independence, the CAE reports functionally to the board of directors and administratively to the chief executive officer or senior management of the organization.
3. 

   a. **Functional Reporting** – the functional reporting line for the internal audit function is the ultimate source of its independence and authority. A functional reporting line to the board provides the CAE with direct board access for sensitive matters and enables sufficient organizational status. It ensures that the CAE has unrestricted access to the board, typically the highest level of governance in the organization. Functional reporting to the board facilitates functional oversight by the board over the internal audit activity. Functional oversight requires the board to create the right working conditions to permit the operation of an independent and effective internal audit activity. Examples of functional reporting to the board involve the board:

      i. Approving the internal audit charter.

      ii. Approving the risk-based internal audit plan.

      iii. Approving the internal audit budget and resource plan.

      iv. Receiving communications from the CAE on the internal audit activity's performance relative to its plan and other matters.

      v. Approving decisions regarding the appointment and removal of the CAE.

      vi. Approving the remuneration of the CAE.

      vii. Making appropriate inquiries of management and the CAE to determine whether there are inappropriate scope or resource limitations.

b. **Administrative Reporting** – is the reporting relationship within the organization's management structure that facilitates the day-to-day operations of the internal audit function. Administrative reporting to a member of senior management provides the CAE with organizational status and authority to perform duties without impediment and to address difficult issues with other senior leaders. To enhance stature and credibility, The IIA recommends that the CAE report administratively to the chief executive officer (CEO). Administrative reporting typically includes:

   i. Budgeting and management accounting.

   ii. Human resource administration including personnel evaluations and compensation.

   iii. Internal communications and information flows.

   iv. Administration of the internal audit activity's policies and procedures.

4. In order to determine the organizational placement of the internal audit, the CAE's reporting lines, and the nature of board or senior management supervision, the CAE works with the board and senior management to reach a shared understanding. The decisions reached regarding these issues are reflected in the internal audit charter.
5. Support of senior management and the board for the internal auditors is necessary so that they can gain the cooperation of engagement clients and perform their work free from interference.
6. According to the Standards, "the internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results. The chief audit executive must disclose such interference to the board and discuss the implications." Such interference can be avoided largely by ensuring the organizational independence of the internal audit activity.

B. Additional Notes on the CAE Reporting Lines

1. Appropriate reporting lines are critical to achieve the independence, objectivity, and organizational stature for an internal audit function necessary to effectively fulfill its obligations.
2. CAE reporting lines are critical to ensure appropriate flow of information and access to key executives and managers that are the foundations of risk assessment and reporting of results of audit activities.
3. Any reporting relationship that impedes the independence and effective operations of the internal audit function must be viewed by the CAE as a serious scope limitation, which need to be brought to the attention of the audit committee or its equivalent.

4. CAE reporting lines are affected by the nature of the organization, common practices of each country, growing complexity of organizations, and the trend towards internal audit groups providing value-added services with increased collaboration on priorities and scope with their clients. Accordingly, other reporting relationships may be effective if there are clear distinctions between the functional and administrative reporting lines and appropriate activities are present in each line to ensure that the independence and scope of activities is maintained.
5. The factors to be considered when evaluating the appropriateness of the administrative reporting line include:
    a. Does the individual have sufficient authority and stature to ensure the effectiveness of the function?
    b. Does the individual have an appropriate control and governance mindset to assist the CAE in their role?
    c. Does the individual have the time and interest to actively support the CAE on audit issues?
    d. Does the individual understand the functional reporting relationship and support it?
6. Administrative reporting to a member of senior management provides the CAE with enhanced independence. For example, the CAE would not typically report to a controller or mid-level manager, who may be subject to audit routinely.
7. The CAE must ensure that appropriate independence is maintained if the individual responsible for the administrative reporting line is also responsible for other activities in the organization that are subject to audit. The CAE must be free to audit and report on any activity that also reports to its administrative head if (s)he deems that coverage is appropriate for its audit plan.
8. CAEs need to also consider their reporting relationships with other control and monitoring functions (such as risk management, compliance, security, legal, ethics, environmental, external auditing) and facilitate the reporting of material risk and control issues to the audit committee.

C. Board Interaction

1. The Standards require that “the chief audit executive must **communicate and interact directly** with the board.”
2. As discussed above, the CAE works with the board and senior management to determine the necessary organizational placement of the internal audit including the CAE’s reporting relationships to enable the internal audit to fulfill its duties. The reporting relationship typically includes a direct functional reporting relationship with the board.

3. The functional reporting relationship with the board enables the CAE to communicate and interact directly with the board, as required by the Standards. Regular communication with the board helps assure **independence** and provides means for the board and the CAE to keep each other informed on matters of mutual interest.
4. If the CAE has a direct functional reporting relationship with the board, then the board assumes the oversight responsibility mentioned earlier including approving the internal audit charter, internal audit plan, internal audit resource plan, evaluation and compensation of the CAE, and appointment and removal of the CAE. Further, the board monitors the ability of the internal audit to operate **independently** and fulfill its charter.
5. The following is an example of direct communication with the board:
    a. The CAE participates in audit committee or full board meetings, generally quarterly, to communicate such things as the proposed internal audit plan, budget, progress, and any challenges.
    b. The CAE has the ability to contact the chair or any member of the board to communicate sensitive matters or issues facing the internal audit or the organization.
    c. Conducting a formal private meeting, at least annually, with the board or audit committee and the CAE (without senior management's presence) to discuss matters of mutual interest.
6. When the CAE has no direct access to the board, the CAE discusses the importance of such relationship with the board to pursue a stronger relationship and direct access. The CAE can consider written communications to the board until a direct line of communication is available.
7. The CAE must confirm to the board, at least annually, the organizational independence of the internal audit activity.
8. Independence is enhanced when the board concurs in the appointment or removal of the CAE.

Passing Tip:	Independence is achieved largely through the organizational placement of the internal audit activity, including the CAE's reporting lines, as well as the direct interaction of the CAE with the board and senior management through a dual-reporting relationship.

Independence
Objectivity

Objectivity

According to the Standards, the internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

A. **Objectivity** is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made.

   1. Objectivity requires that internal auditors avoid conflicts of interest and do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

   2. Objectivity also requires assigning staff so that potential and actual conflicts of interest and bias are avoided. The CAE may support this process by:

      a. Periodically obtaining from the internal auditing staff information concerning potential conflicts of interest and bias.

      b. Ensuring that internal auditors who have moved to the internal audit activity from other departments are refrained from auditing the department for which they were previously responsible for at least one year after leaving that department.

      c. Periodically rotating staff assignments of internal auditors whenever it is practicable to do so.

   3. Performance evaluation and compensation practices can negatively affect an internal auditor's objectivity. For example

      a. If an internal auditor's performance evaluation, salary, or bonus are based on client satisfaction, the internal auditor may hesitate to report negative results that may cause the client to report low satisfaction.

      b. If the performance evaluation is based on the number of observations, it could cause the internal auditor to report a relatively minor issue as an audit finding.

      c. If the performance evaluation is based on staying within the audit budget, it could cause the internal auditor to ignore warning signs when the budget is nearly depleted.

      Therefore, the CAE needs to be thoughtful in designing the internal audit performance evaluation system. Ideally, the evaluation process will balance auditor performance, audit results, and client feedback measurements.

4. It is unethical for an internal auditor to accept a fee or gift from an employee, client, customer, supplier, or business associate.
    a. Accepting a fee or gift may create an appearance that the auditor's objectivity has been impaired.
    b. The appearance that objectivity has been impaired may apply to current and future engagements conducted by the auditor.
    c. The receipt of promotional items (such as pens, calendars, or samples) that are available to the general public and have minimal value would generally not hinder internal auditors' professional judgments.
    d. Internal auditors must report the **offer** of all material fees or gifts immediately to their supervisors.

Passing Tip:	Whenever an internal auditor is offered a gift (other than minor value promotional items), the required course of action is to report the issue to the CAE or audit management.

B. **Conflict of Interest**

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interest can make it difficult to fulfill his or her duties impartially. A conflict of interest may impair an individual's ability to perform his/her duties and responsibilities objectively.

1. A conflict of interest exists even if no unethical or improper act results.
2. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession.

Impairments to Independence and Objectivity

Impairments to Independence and Objectivity – independence or objectivity may be impaired in fact or appearance. When impairment occurs, the Standards require that details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

A. To effectively manage internal audit independence and objectivity, the CAE develops an internal audit policy manual that describes the expectations and requirements regarding independence and objectivity for every internal auditor. Such a policy manual emphasizes the critical importance of independence and objectivity to the internal audit profession, and describes the following:
    1. Typical situations that could undermine independence or objectivity.
    2. Actions the internal auditor should take when faced with a potential impairment.

B. Typical situations that could create impairments to independence or objectivity include:

1. **Scope Limitation,** which is a restriction placed on the internal audit activity precluding the internal audit activity from accomplishing its objectives and plans. Scope limitations may restrict
    a. Scope defined in the charter.
    b. Internal audit activity's access to records, personnel, and physical properties relevant to the performance of engagements.
    c. Approved engagement work schedule.
    d. Performance of necessary engagement procedures.
2. **Conflict of Interest** – As discussed earlier, conflict of interest may negatively affect the unbiased mental attitude of the auditor. For example, when the internal auditor audits an area where a relative or close friend is employed, the auditor will have a competing personal interest that may hinder the ability to fulfill his or her duties impartially.
3. **Lack of professional skepticism** constitutes an impairment to objectivity. For example, assuming that the function under audit has mitigated risks based solely on a prior positive audit or personal familiarity, without sufficient evidence.
4. **Undue Interference** – This may occur when the internal auditor modifies the audit plan or results based on the undue influence of another person without appropriate justification, even if that person is in a senior position.
5. **Resource limitations** constitute impairment to independence and objectivity especially when the internal audit budget (or other resource) is reduced to the point that the internal audit cannot fulfill its responsibilities.
6. **Inappropriate Organizational Placement and Reporting Lines** – as noted above, the organizational placement and supervisory reporting lines of the internal audit are necessary to ensure organizational independence. Examples of related impairments include:
    a. The CAE reports to a supervisor that has broader responsibility than the internal audit, and the CAE performs audit work within that supervisor's functional responsibility.
    b. There is no direct communication and interaction between the CAE and the board.

7. **Operations with prior or future operating responsibilities** – According to the Standards, internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an auditor provides **assurance services** for an activity for which the auditor had responsibility within the previous year or if the auditor assumes or (is to assume) operating responsibilities for that activity in the near future.
   a. Such a situation occurs when an employee transfers into the internal audit activity from a different functional area of the organization and is then assigned to audit that function. This situation constitutes an impairment to objectivity.
   b. However, internal auditors **may** provide **consulting services** relating to operations for which they had previous responsibilities. If internal auditors have potential impairments to independence or objectivity relating to consulting services, **disclosure must be made** to the engagement client prior to accepting the engagement.

Passing Tip:	An internal auditor must **NOT** be involved in auditing areas where he/she was responsible for during the previous year **or** if the auditor has been promoted (i.e., will be transferred) to the operating department under audit. If involved, adequate reporting and disclosure must be made.

8. **CAE Roles Beyond Internal Auditing** – The CAE may be asked to take on additional responsibilities outside internal auditing, such as responsibility for ensuring compliance, conducting risk management activities, or designing and operating controls. These roles and responsibilities may impair, or appear to impair, independence or objectivity.
   a. The Standards state that “where the chief audit executive has or is expected to have roles or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.”
   b. **Safeguards** are those oversight activities, often undertaken by the board, to address potential impairments. Those safeguards may include:
      i. Evaluating the CAE’s reporting lines and responsibilities periodically.
      ii. Developing alternative processes to obtain assurance related to the areas of additional responsibility.

c. According to the standards, assurance engagements for functions over which the CAE has responsibility must be overseen by a party outside the internal audit activity.

   i. Therefore, if the CAE has responsibilities over functions other than internal auditing, and these functions are subject to internal audit, the assurance services related to those functions would typically be assigned to another internal or external assurance provider that reports independently to the board.

d. **Disclosure** – Any impairment to independence or objectivity resulting from assigning responsibilities to the CAE beyond internal auditing must be adequately disclosed. The related details that should be disclosed typically include:

   i. The nature of those responsibilities.

   ii. The risks related to undertaking those responsibilities by the CAE.

   iii. The safeguards to the CAE's independence and objectivity along with the controls in place to ensure that the safeguards are operating effectively.

e. With full disclosure in the reporting process, **occasional performance** of non-audit work by internal auditors would not necessarily impair independence; however, careful consideration is required by the CAE and management to avoid impairing auditors' objectivity.

Passing Tip:	**Recommending** standards of control for systems or **reviewing** procedures before they are implemented do not impair the auditor's objectivity, while **designing, installing, drafting** procedures for, and/or **operating** such systems do impair the auditor's objectivity.

C. **Actions to be taken in the case of potential impairment** – The internal audit policy manual should describe the appropriate actions the internal auditor should take when faced with a potential impairment to independence or objectivity.

1. The internal auditor must first report the actual or potential impairment concerns to the CAE, who may decide on the appropriate course of action.
2. The CAE then determines whether the situation is truly an impairment and how to proceed.

3. The CAE is obligated by the Standards to disclose the details of the impairment to the appropriate parties. The determination of appropriate parties is dependent upon the nature of the impairment and the expectations of senior management and the board as described in the internal audit charter. The appropriate parties may be:
    a. **Operating management only** – When the CAE finds that the impairment is not real, but there could be an appearance of impairment, the CAE discusses the concern with the operating management (the head of the function under audit).
    b. **Senior management and the board** – When the CAE finds that the impairment is real, the CAE reports the impairment to the board and senior management and seeks their support to resolve the situation.
    c. **Operating management, senior management, and the board** – When the CAE knows about the impairment after the completion of the engagement, the CAE must disclose the impairment to all parties who had received the results of the engagement. That usually includes operating and senior management, as well as the board.

Independence and Objectivity in Consulting Engagements

A. Internal auditors are sometimes requested to provide consulting services relating to operations for which they had previous responsibilities or had conducted assurance services. Prior to offering such consulting services, the CAE must confirm that the board understands and approves the concept of providing consulting services. Once approved, the internal audit charter must be amended to include authority and responsibilities for consulting activities (if it does not already contain such scope), and the internal audit activity needs to develop appropriate policies and procedures for conducting such engagements.

B. Internal auditors must maintain their objectivity when drawing conclusions and offering advice to management. If impairments to independence or objectivity exist prior to commencement of the consulting engagement, or subsequently develop during the engagement, disclosure must be made immediately to management.

C. According to the Standards, internal auditors may provide assurance services where they had previously performed consulting services, provided the **nature of the consulting** did not impair objectivity and provided individual **objectivity is managed** when assigning resources to the engagement.

   1. **Nature of the Consulting** – Consulting engagements do not impair objectivity or independence when internal auditors avoid assuming management responsibilities during those engagements. That is achieved when the internal auditors are responsible for providing recommendations and management is responsible for accepting and implementing them.

   2. **Managing Individual Objectivity** – When assurance services are provided where consulting services were previously performed, the CAE could manage individual objectivity by assigning different auditors to perform each of the services.

D. Care must be taken, particularly involving consulting engagements that are ongoing or continuous in nature, so that internal auditors do not inappropriately or unintentionally assume management responsibilities that were not intended in the original objectives and scope of the engagement.

Part 1, Domain III
Proficiency and Due Professional Care

Section A: Proficiency and Due Professional Care

Learning Outcomes:

1. Recognize the knowledge, skills, and competencies required (whether developed or procured) to fulfill the responsibilities of the internal audit activity. Basic Level
2. Demonstrate the knowledge and competencies that an internal auditor needs to possess to perform his/her individual responsibilities, including technical skills and soft skills (communication skills, critical thinking, persuasion/negotiation and collaboration skills, etc.). Proficiency Level.
3. Demonstrate due professional care. Proficiency Level.
4. Demonstrate an individual internal auditor's competency through continuing professional development. Proficiency Level.

Proficiency

The proficiency (knowledge, skills, and competencies) of internal auditors is distinguished between:

- Individual proficiency of internal auditors
- Proficiency of the internal audit activity

Individually
Collectively

Individual Proficiency of Internal Auditors

Individually
Collectively

A. According to the Standards, "internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities."
   1. **Proficiency** is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities.

B. Internal auditors develop proficiency via education, experience, professional development opportunities, and qualifications. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

C. It is the responsibility of the CAE to ensure the individual proficiency of internal auditors and the collective proficiency of the internal audit activity.

1. The CAE reviews the responsibilities established in the internal audit charter, the scope of work, and the internal audit plan in order to determine the knowledge, skills, and other competencies needed to fulfill the responsibilities of the internal audit activity.
2. **The IIA's Global Internal Audit Competency Framework** defines the core competencies needed to fulfill the mandatory requirements of the IPPF for all internal auditing positions, including staff, management, and executives. The CAE may use The IIA's Global Internal Audit Competency Framework or a similar benchmark to establish the criteria by which to assess the proficiency of internal auditors.
3. The CAE then uses these criteria to create job descriptions and an inventory of the competencies needed in the internal audit activity. The filling of internal auditing positions needs to be in accordance with the criteria established by the CAE for the level of education and experience required. The CAE also obtains reasonable assurance as to each prospective auditor's qualifications and proficiency.

D. All internal auditors must possess knowledge, skills, and other competencies as follows:

1. Proficiency in applying the International Professional Practices Framework (IPPF), and the internal auditing procedures and techniques in performing engagements.
    a. **Proficiency,** in this context, refers to the ability of the internal auditor to apply knowledge to situations likely to be encountered, and to deal with them appropriately without extensive recourse to technical research and assistance.
    b. Proficiency in accounting principles and techniques is only required of auditors who work extensively with financial records and reports.
2. Understanding of management principles which would enable the auditor to recognize and evaluate the materiality and significance of deviations from good business practices.
    a. **Understanding** refers to the ability of the internal auditor to apply broad knowledge to situations likely to be encountered, to recognize significant deviations, and to be able to carry out the necessary research to arrive at reasonable conclusions.
3. Appreciation of the fundamentals of subjects such as accounting, economics, commercial law, taxation, finance, quantitative methods, information technology, risk management and fraud.
    a. **Appreciation** refers to the ability of the internal auditor to recognize the existence of problems or potential problems and to determine the degree of further research or assistance required.

4. While they are not expected to be experts in subjects such as economics, accounting, commercial law, taxation, etc., internal auditors must:
    a. Apply a thorough understanding of governance, risk and control appropriate to the organization.
    b. Have **sufficient knowledge to evaluate the risk of fraud** and the manner in which it is managed by the organization but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
    c. Have **sufficient knowledge of key information technology risks and controls** and **available technology-based audit techniques** to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.
    d. Maintain expertise of the relevant business environment, industry practices and specific organizational factors (**business acumen**).
    e. Promote and apply **professional ethics**.
    f. Have **critical thinking** skills – applying process analysis, business intelligence, and problem-solving techniques.
    g. Be **skilled in dealing with people and in communicating effectively**. This includes an understanding of human relations and the maintenance of satisfactory working relationships with engagement clients.
    h. Be **skilled in persuasion and collaboration** to persuade and motivate others through collaboration and cooperation.
    i. Be **skilled in oral and written communication** so that they can clearly and effectively convey such matters as engagement objectives, evaluations, conclusions, and recommendations.
    j. Be able **to recognize and evaluate the materiality** and **significance of deviations from good business practices**.

Proficiency of the Internal Audit Activity (Collective Proficiency)

Individually
Collectively

A. According to the Standards, the internal audit activity must collectively possess (or obtain) the knowledge, skills, and other competencies needed to perform its responsibilities.
B. If certain knowledge, skills, or other competencies required to perform all or part of an engagement is lacking, the CAE must seek external advice and assistance.
C. The CAE must only accept consulting engagements if the internal audit activity possesses (or obtains) the required knowledge, skills, or other competencies to complete the engagement.

Passing Tip:	When the internal audit activity lacks the skills to perform a required task, the following options are available to the CAE: – Consider the possibility of outsourcing the task. – Add an outside consultant to the audit staff to assist in the performance of the task. – If time and resources permit, consider the potential to develop appropriate expertise to perform the task.

Developing Internally or Obtaining External Services

A. If certain knowledge, skills, or other competencies required to perform all or part of an engagement is lacking (and are not internally developed), the CAE (or the board or senior management) must obtain competent advice and assistance to fill any gaps through hiring, training, or outsourcing to external service providers.

B. **External service provider** is a person or firm, independent of the organization, who has special knowledge, skill, and experience in a particular discipline such as:

- Actuaries
- Accountants
- Appraisers
- Environmental specialists
- Fraud investigators
- Lawyers
- Engineers
- Geologists
- Security specialists
- Statisticians
- Information technology specialists
- The organization's external auditors
- Others

C. Typical activities that may require external service providers are:

1. Auditing activities where a specialized skill and knowledge are required such as information technology, statistics, taxes, language translations, or to achieve the objectives in the engagement work schedule.
2. Valuations of assets such as land and buildings, works of art, precious gems, investments, and complex financial instruments.
3. Determination of quantities or physical condition of certain assets such as mineral and petroleum reserves.
4. Measuring the work completed and to be completed on contracts in progress.
5. Fraud and security investigations.
6. Determination of amounts by using specialized methods such as actuarial determinations of employee benefit obligations.
7. Interpretation of legal, technical, and regulatory requirements.
8. Evaluating the internal audit activity's quality improvement program in conformance with the Standards.

9. Mergers and acquisitions.
10. Consulting on risk management and other matters.

D. If an external service provider is used, the CAE needs to consider his/her competency, independence, and objectivity as they relate to the proposed assignment. (If the selection of the external service provider is made by someone other than the CAE, and the CAE determines that he or she should not use and rely on the work of the external service provider, the results of such assessment need to be communicated to senior management or the board.)
    1. When assessing the proficiency (knowledge, skills, and other competencies) of the external service provider, The CAE considers the following:
        a. Professional certification, license, or other recognition of the external service provider's competency in the relevant discipline.
        b. Membership of the external service provider in an appropriate professional organization and adherence to that organization's code of ethics.
        c. The reputation of the external service provider. This may include contacting others familiar with the external service provider's work.
        d. The external service provider's experience in the type of work being considered.
        e. The extent of education and training received by the external service provider in disciplines that pertain to the particular engagement.
        f. The external service provider's knowledge and experience in the industry in which the organization operates.
    2. When assessing the independence and objectivity of the external service provider to ensure that there are no financial, organizational, or personal relationships that will prevent the external service provider from rendering impartial and unbiased judgments and opinions, the following needs to be considered:
        a. The financial interest the provider may have in the organization.
        b. The personal or professional affiliation the provider may have to the board, senior management, or others within the organization.
        c. The relationship the provider may have had with the organization or the activities being reviewed.
        d. The extent of other ongoing services the provider may be performing for the organization.
        e. Compensation or other incentives that the provider may have.

E. The external service provider to perform extended audit services may be the organization's external auditor. If this is the case, the CAE needs to ascertain that work performed does not impair the external auditor's independence.
   1. Extended audit services are services performed beyond the requirements of the generally accepted auditing standards adhered to by external auditors.
   2. Independence needs to be assessed in relation to the full range of services provided to the organization.

F. It is recommended to obtain and document sufficient information regarding the scope of the external service provider's work to ascertain that the scope is adequate for the purposes of the internal auditing activity. To accomplish this, the CAE reviews the following with the external service provider:
   1. Objectives and scope of work including deliverable and time frames.
   2. Specific matters expected to be covered in the engagement communications.
   3. Access to relevant records, personnel, and physical properties.
   4. Information regarding assumptions and procedures to be employed.
   5. Ownership and custody of engagement working papers, if applicable.
   6. Confidentiality and restrictions on information obtained during the engagement.
   7. Where applicable, conformance with the Standards and the internal audit activity's standards for working practices.

G. If the CAE relies on an external service provider for internal auditing activities, the work of the provider is subject to the same compliance procedures as those that the internal audit activity and internal audit staff are subject to. The CAE evaluates the adequacy of work performed, which includes sufficiency of information obtained to afford a reasonable basis for the conclusions reached and the resolution of exceptions or other unusual matters.

H. If the CAE intends to refer to services performed by an external service provider, the CAE is required to obtain the approval of the provider prior to such reference.

Passing Tip:	When the internal audit activity lacks the skills to perform a required task, the services of an external service provider may be utilized. If the services of an external service provider are utilized, the CAE should treat the provider like its own staff in almost all respects.

Due Professional Care

A. According to the Standards, “internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.”

B. **Due Professional Care** implies that internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor under the same or similar circumstances. Internal auditors need to be alert to the following:

   1. Possibility of fraud and/or intentional wrongdoing
   2. Errors and/or omissions
   3. Waste and inefficiencies
   4. Ineffectiveness
   5. Conflicts of interest
   6. Circumstances where irregularities are most likely to occur
   7. Identifying inadequate controls that require improvement

C. Due professional care includes conforming with the Code of Ethics and, as appropriate, the organization’s code of conduct as well as the codes of conduct for other professional designations the internal auditors may hold.

D. Due professional care does not imply infallibility or extraordinary performance. Internal auditors are expected to conduct audits with reasonable examinations and verifications but are not required to perform detailed reviews of all transactions. As a result, internal auditors are not expected to provide absolute assurance, however, they are expected to consider the possibility of material irregularities or noncompliance at all times during an engagement.

E. Assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified, and thus the internal auditor must continuously be alert to significant risks that might affect objectives, operations, and/or resources.

F. In exercising due professional care, internal auditors must consider the use of technology-based audit and other data analysis techniques.

G. According to the Standards, the internal auditor must exercise due professional care by considering the following:

   1. Extent of work needed to achieve the engagement’s objectives.
   2. Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
   3. Adequacy and effectiveness of governance, risk management, and control processes.
   4. Probability of significant errors, fraud, or noncompliance.
   5. Cost of assurance in relation to potential benefits.

H. To ensure due professional care at the engagement level, the engagement should be properly supervised. The supervisor:
   1. Reviews the engagement workpapers, findings, and final communications;
   2. Obtains feedback from audit clients about the internal auditors' due professional care; and
   3. Provides feedback to the internal auditors who conducted the engagement.

I. For consulting services, the internal auditor must consider the following:
   1. Needs and expectations of clients, including the nature, timing, and communication of engagement results.
   2. Relative complexity and extent of work needed to achieve the engagement's objectives in addition to the required skills and resources.
   3. Potential organizational benefits and cost of the consulting engagement in relation to potential benefits.
   4. Possible motivations and reasons of those requesting the service.
   5. Effect on the scope of the audit plan previously approved by the audit committee.
   6. Potential impact on future audit assignments and engagements.

J. Proficiency and due professional care are the responsibility of the CAE and each internal auditor. However, the CAE assumes the overall responsibility for ensuring the due professional care and the proficiency of the internal audit activity.

Continuing Professional Development

A. Internal auditors are required by the Standards to enhance their knowledge, skills, and other competencies through continuing professional development regardless of whether they are holders of certificates such as the CIA or not. This includes:
   1. Maintaining their proficiency through continuing their education:
      a. Membership in professional societies.
      b. Attending conferences, seminars, college courses, and in-house training programs.
      c. Participation in research projects.
   2. Staying informed about improvements and current developments in the internal auditing standards, procedures, and techniques including the IIA's IPPF guidance.

B. The CAE is required to develop and implement a plan for continuing professional development for the internal audit staff. This may include on-the-job mentoring and, when possible, assigning staff to areas that would enhance their skills, knowledge and other competencies.

C. Internal auditors are encouraged (not required) to demonstrate their proficiency by obtaining appropriate professional certifications, such as the Certified Internal Auditor designation, and to maintain these certifications by meeting continuing education requirements.

D. Ultimately, continuing professional development is the responsibility of each internal auditor.

This page intentionally left blank.

Part 1, Domain IV Quality Assurance and Improvement Program

Section A: Components of the QAIP

Learning Outcomes:

1. Describe the required elements of the quality assurance and improvement program (internal assessments, external assessments, etc.). Basic Level.

According to the Standards, the CAE must develop and maintain a quality assurance and improvement program (QAIP) that covers all aspects of the internal audit activity.

A. **Developing QAIP**

1. **Quality** – In general, the quality of a service is the degree to which the service achieves its purpose by meeting the stakeholders' expectations. In internal audit context, the quality of internal audit work is determined by both meeting client expectations as well as mandatory requirements dictated in the IPPF. This can be ensured by developing and maintaining a comprehensive QAIP.
2. The overall responsibility for developing and maintaining a QAIP lies with the CAE.
    a. The CAE develops QAIP upon:
        i. Discussing senior management and the board,
        ii. Determining stakeholders' expectations,
        iii. Understanding the mandatory elements of the IPPF, and
        iv. Considering best practices in the internal audit profession.
    b. The QAIP must cover all aspects of the internal audit activity including planning, operating, and managing aspects.
    c. The development of the QAIP should begin with the structure and organization of the audit activity. During annual audit planning, the CAE reevaluates the QAIP and updates it as needed.

d. The CAE develops the QAIP in a manner that ensures quality is embedded into the structure of the internal audit activity. Therefore, audit work should be performed in accordance with a methodology that, by default, meets expectations, conforms to the Standards, and permits continuous improvement.

e. The CAE should encourage board oversight in the quality assurance and improvement program.

B. **Objectives of QAIP**

1. The primary objectives of the QAIP are:

   a. Evaluating the internal audit activity's conformance with the Standards and the Code of Ethics.

   b. Assessing the efficiency and effectiveness of the internal audit activity.

   c. Assessing the degree to which internal audit activity meets stakeholders' expectations and adds value.

   d. Identifying opportunities for improvement.

2. The QAIP can achieve these primary objectives by assessing:

   a. Adequacy of the internal audit activity's charter, goals, objectives, policies, and procedures;

   b. The coverage level of the audit universe;

   c. Performance metrics such as cycle time and the number of recommendations made by the internal audit activity and accepted by management;

   d. Contribution to the organization's governance, risk management, and control processes;

   e. Compliance with applicable laws, regulations, and government or industry standards;

   f. Effectiveness of continuous improvement activities and adoption of best practices; and

   g. Whether the auditing activity adds value and improves the organization's operations.

C. **Components of QAIP** – According to the Standards, the QAIP must include the following components (which will be covered separately):

1. **Internal Assessments**, which **must** include
   a. Ongoing monitoring of the performance of the internal audit activity, and
   b. Periodic self-assessments.
2. **External Assessments**, which **may** be one of the following forms
   a. A full external assessment, or
   b. A self-assessment with independent external validation.

Internal Assessments
External Assessments

Internal Assessments

The Standards state that internal assessment **must** include ongoing monitoring of the performance of the internal audit activity, and periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

Internal Assessments
External Assessments

A. **Ongoing monitoring**

1. Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is usually incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Code of Ethics, and the Standards. Ongoing monitoring typically results in conclusions and any necessary follow-up action to ensure appropriate improvements are implemented as the audit work is being done.
2. Ongoing monitoring occurs routinely through the implementation of standardized work practices. Therefore, ongoing monitoring may be achieved through the following continuous activities:
   a. Preapproval of the audit scope,
   b. Adequate internal audit activity planning and the regular assessments of engagement plans prior to fieldwork,
   c. Proper staff assignments to engagements,
   d. Adequate supervision of an internal auditor's work throughout each audit engagement,
   e. Checklists to provide assurance on internal auditors' compliance with established practices and procedures,
   f. Workpaper procedures and signoffs,
   g. Selective peer reviews of workpapers by staff not involved in the respective audits,

h. Review of reports and supporting documentation for comments.

i. Feedback from audit clients and other stakeholders regarding the efficiency and effectiveness of the internal audit team,

j. Establishing and maintaining key performance indicators (KPIs) and other performance metrics for staff and engagements, such as

   i. The number of certified internal auditors in the staff,

   ii. The years of experience of the members of the staff,

   iii. The number of continuing professional development hours accomplished during the year,

   iv. Timeliness of engagements,

   v. The number of recommendations accepted,

   vi. Stakeholder satisfaction,

   vii. Project budgets, audit plan completion, and cost recoveries.

Passing Tip:	QAIP performance metrics should focus on: – Adding value (meeting stakeholder expectations) – Effectiveness and efficiency – Continuous improvement

2. **Adequate Supervision** – As noted above, adequate supervision is an essential part of ongoing monitoring. Adequate supervision is a fundamental element of any quality assurance and improvement program. It is considered the first line of ensuring conformance with the Code of Ethics, and the Standards.

   a. According to the Standards, engagements must be properly supervised to ensure objectives are achieved, **quality is assured**, and staff is developed.

   b. Supervision covers all phases of the engagement. It begins with the planning phase and continues throughout the performance and communication phases of the engagement.

   c. The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement.

   d. Adequate supervision may be achieved through

      i. Setting expectations,

      ii. Ongoing communications among internal auditors and supervisors throughout the engagement work, and

      iii. Reviewing workpapers by supervisors.

   e. The CAE has overall responsibility for supervising engagements, whether performed by or for the internal audit activity. *(Appropriate supervision is covered in more detail in Part 2)*

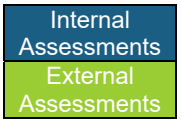
Passing Tip:	Appropriate supervision is the most fundamental element of any quality assurance and improvement program.

B. **Periodic Self-Assessments**

1. The major difference between periodic self-assessments and ongoing monitoring is that:
   a. Ongoing monitoring generally focuses on reviews conducted at the engagement level and addresses conformance with performance standards at the engagement level.
   b. Periodic self-assessments generally provide a comprehensive review of the entire internal audit activity, and address conformance with every standard.
2. **The purpose of Periodic Self-assessment** – Periodic self-assessments are conducted primarily to validate continued conformance with the Standards and the Code of Ethics. Specifically, periodic self-assessments focus on assessing:
   a. The adequacy and effectiveness of the ongoing monitoring activities.
   b. The internal audit activity's performance against the key performance indicators and criteria.
   c. The value added by the internal audit activity.
   d. The adequacy and appropriateness of the internal audit charter, plans, policies, and procedures.
   e. The adherence to internal audit charter, plans, policies, and procedures.
   f. The effectiveness of the internal audit activity in meeting stakeholder expectations.
   g. The quality of work performed.
3. To support the purpose of the periodic self-assessment, the following steps may be performed by the assessors:
   a. Conducting in-depth interviews and surveys of stakeholder groups to assess the internal audit activity's conformance with each standard.
   b. Benchmarking the internal audit activity's performance metrics against relevant best practices.
   c. Reviewing engagement results and workpapers on a sample basis to assess compliance with audit policies and procedures; the Standards; and the Code of Ethics.

4. Periodic self-assessments may be conducted by:
   a. Members of the internal audit activity who have extensive experience with the IPPF; or
   b. CIAs, or other competent audit professionals, who are currently assigned elsewhere in the organization.
5. Upon discussion with the board, the CAE determines the frequency of the periodic self-assessments. Larger internal audit activities may conduct periodic self-assessments **annually**, while smaller or less mature internal audit activities may perform them less frequently.
6. A periodic self-assessment performed within a short time before an external assessment can serve to facilitate and reduce the cost of the external assessment. If the external assessment takes the form of a self-assessment with independent validation (covered later), the periodic internal assessment can serve as the self-assessment portion of this process.
7. Those conducting ongoing monitoring and periodic self-assessments communicate the results directly to the CAE while performing the assessments.

External Assessments



A. **External Assessments** that appraise and express an opinion as to the internal audit activity's conformance with the Code of Ethics and the Standards must be conducted at least once every five years by a **qualified, independent** assessor or assessment team from outside the organization. The CAE must discuss the following issues with the board to reach shared decisions:
   1. The frequency of external assessments.
   2. The form of external assessments.
   3. The qualifications of the external assessor or assessment team.
   4. The independence of the external assessor or assessment team, including any potential conflict of interest.

B. **The Frequency of External Assessments**
   1. The Standards require the internal audit activity to undergo an external assessment **at least once every five years**. However, a more frequent external assessment may be appropriate. The decision to determine the appropriate frequency of the external assessment must be taken upon discussion with senior management and the board. Reasons to consider a more frequent review include
      a. Changes in the organization's leadership.
      b. Changes in internal audit policies and procedures.
      c. Significant changes in the structure of the organization.

d. Emerging environmental issues.

e. High staff turnover in the organization.

C. **Forms of External Assessments** – The Standards state that "External assessments may be accomplished through a full external assessment, or a self-assessment with independent external validation." Accordingly, external assessments may be accomplished using one of these two approaches.

1. **Full External Assessment** – A full external assessment is conducted by a qualified, independent external assessor or assessment team. The scope of a full external assessment normally includes evaluating the following major elements:

   a. Conformance with the Standards and the Code of Ethics. This usually involves reviewing the internal audit charter, plans, policies, procedures, and practices, as well as, applicable regulatory requirements.

   b. The efficiency and effectiveness of the internal audit activity. This may involve an assessment of:
      i. The tools, processes, and techniques employed by the internal audit activity to accomplish its objectives.
      ii. The mix of knowledge, experience, and disciplines within the internal audit staff.

   c. The extent to which the internal audit activity meets expectations of stakeholders and adds value to the organization's operations.

   d. The integration of the internal audit activity into the organization's governance process, including the relationships between and among key groups involved in the process.

   e. A full external assessment also identifies areas and other opportunities that offer continuous improvements to the internal audit activity and its staff.

2. **Self-Assessment with Independent Validation (SAIV)** – The SAIV is usually conducted by the internal audit activity and then validated by a qualified, independent external assessor. The scope of the SAIV process typically includes the following:

   a. A team under the direction of the CAE performs and fully documents a comprehensive self-assessment process. This process should imitate the full external assessment in evaluating the internal audit activity's conformance with the Standards and the Code of Ethics.

   b. A qualified, independent reviewer or review team performs sufficient on-site tests of the self-assessment to validate the results and express the indicated level of the activity's conformance.

   c. Limited attention to other areas such as operational improvements, benchmarking, and interviews with senior and operating management.

3. SAIVs are less expensive to conduct when compared to external assessments, as any outside provider will charge both the actual costs plus a premium for overhead and profits, whereas the company will only incur the actual costs in internal assessments.

D. **Qualifications of the External Assessor**

1. The Standards require the external assessors to be independent and qualified. Therefore, regardless of the form selected for the external assessment (a full external assessment, or an SAIV), the assessment must be completed by an independent, qualified external assessor or assessment team.
2. The judgment on the assessor or assessment team qualifications to conduct the external assessment is usually made by the CAE upon discussion with senior management and the board.
3. Assessors or assessment teams **must** demonstrate competence in tow main areas:
    a. The professional practice of internal auditing, including in-depth knowledge of the IPPF.
    b. The external quality assessment process.
4. Other preferred attributes of qualified assessors include:
    a. The assessors should possess sufficient educational background, technical and business experience, with at least one member possessing adequate knowledge of the organization’s industry.
    b. The assessors should have sufficient recent experience in practicing internal audit work at senior level and hold a certification as an internal audit professional.
    c. The assessors should have sound judgment, excellent analytical and communication skills.
    d. The assessment team leader or the independent validator typically should have additional qualifications and competencies including:
        i. Comparable experience to that of the CAE.
        ii. Completion of a training course in external assessment.
        iii. An additional experience in performing external assessment.
    e. Experience gained in organizations of similar size, complexity, sector or industry, and technical issues is more valuable than less relevant experience.
    f. Collectively, the assessment team should possess all required qualifications and have access to any specialized technical expertise when necessary. Each individual on the team does not have to possess all of the preferred competencies.

E. Independence and Objectivity of the External Assessor

1. The assessor or assessment team **must** not have actual, apparent or potential conflicts of interest, and must not be an insider and/or working independently or within an organization that is under the control of the organization to which the internal audit activity under audit belongs.
2. The CAE should encourage board oversight in the external assessment to reduce perceived or potential conflicts of interest.
3. For the purpose of external assessment, potential impairments to independence or objectivity include any current, previous, or future relationships between the external assessors and the organization or its personnel. Therefore, the following parties are considered to have potential impairments for the purpose of providing external assessment:
    a. Individuals from within the organization, even if they are from other departments and organizationally separate from the internal audit activity.
    b. Individuals from related entities such as a parent, a sister, or a subsidiary entity.
    c. External auditors of the organization, especially when the external auditors rely on the work of the internal audit activity.
    d. External consultants with previous or future participation in internal quality assessments.
    e. External consultants providing other types of services such as risk management, IT, financial reporting, internal control, or governance consultancies.
    f. External parties with personal relationships with the organization personnel.
4. When potential assessors were previous employees of the company, consideration should be given to how long those potential assessors were independent from the company i.e., how long have they been out of the company, and whether that is sufficient time to be considered independent.
5. The internal audit activity in a public sector entity may be independent for the purpose of assessing another public entity's internal audit activity, even if they all belong to the same tier of government, **unless** they report to the same CAE.
6. Peer reciprocal assessments of at least three independent companies may be considered independent, i.e., the CAE of company 1 may conduct the assessment of company 2, the CAE of company 2 conducts the assessment of company 3, and the CAE of company 3 can assess company 1.
    a. CAEs of two companies performing reciprocal external assessments are not considered independent.

Section B: Reporting on the QAIP

Learning Outcomes:

1. Describe the requirement of reporting the results of the quality assurance and improvement program to the board or other governing body. Basic Level.

A. According to the Standards, the chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board. Disclosure should include:

   1. The scope and frequency of both the internal and external assessments.
   2. The qualifications and independence of the assessment team, including potential conflicts of interest.
   3. Conclusions of assessors.
   4. Corrective action plans.

B. The CAE is responsible for communicating the results of the entire QAIP. The CAE establishes the form, content, and frequency of this communication through discussions with senior management and the board. The results of the QAIP may be distributed to various stakeholders, including senior management, the board, and external auditors.

C. **Timing of the Communications**

   1. The results of ongoing monitoring are communicated to the board and senior management at least **annually**.
   2. The results of periodic self-assessments are communicated to the board and senior management **upon completion** of such assessments.
   3. The results of external assessments are communicated to the board and senior management **upon completion** of such assessments.

D. **Components of the final communication of the QAIP Results**

   1. The final communication must include the **scope** and **frequency** of both the internal and external assessments.
   2. When reporting the results of a full external assessment or an SAIV, the CAE must include in the communication report:
      a. The qualifications of the external validator or the external assessment team.
      b. The independence and objectivity of the external validator or the external assessment team.
      c. Any actual, potential, or perceived conflicts of interest.

3. **Conclusions of Assessors** – the communicated results of the QAIP must include the assessor's or assessment team's conclusions with respect to the following:
    a. The degree of the internal audit activity's **conformance** with the Standards and the Code of Ethics. Final conclusion regarding conformance is preferably made against an objective rating scale such as the IIA's standard quality assessment rating system which includes three levels to show the degree of conformance:
        i. **Generally Conforms** – whereby the internal audit activity, its charter, its policies, procedures, audits, and reports are in conformance with the Code of Ethics, and the Standards.
        ii. **Partially Conforms** – whereby the internal audit activity has some deficiencies in practice, but these deficiencies are not precluding it from performing its responsibilities.
        iii. **Does Not Conform** – whereby the internal audit activity has major deficiencies that are so significant that they are precluding it from performing its responsibilities.
    b. The internal audit activity's conformance with its charter, plans, policies, procedures, practices, and any applicable legislative and regulatory requirements.
    c. The efficiency and effectiveness of the internal audit activity in carrying out its responsibilities.
    d. The continuous improvement efforts within the internal audit activity.

E. **Action Plans**

1. During the external and internal assessment, the assessments may
    a. Identify areas that are not in conformance with the Standards, Code of Ethics, or other applicable criteria.
    b. Identify opportunities for improving the internal audit activity.
    c. Provide recommendations to address non-conformance as well as opportunities for improvement.
2. In this case, the CAE must
    a. **Develop** action plans to address findings and recommendations from the internal or external assessments.
    b. **Communicate** those action plans to senior management and the board.

Section C: Conformance with the Standards

Learning Outcomes:

1. Identify appropriate disclosure of conformance vs. nonconformance with The IIA's International Standards for the Professional Practice of Internal Auditing. Basic Level.

According to the Standards, "indicating that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing is appropriate **only** if supported by the results of the QAIP."

A. The QAIP is performed primarily to evaluate, and express an opinion on, the internal audit activity's conformance with the Standards and the IIA's Code of Ethics.

B. The CAE may state that "the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing" if ALL the following conclude that the internal audit activity is in conformance with the Code of Ethics, and the Standards:

    1. Internal assessments conducted in accordance with the frequency disclosed to the board (within the time frame communicated to the board), and
    2. An external assessment conducted at least once within every five-year period.

C. For example, below are some possible scenarios about the use of the conformance statement:

    1. The internal audit activity may **NOT indicate** that it is operating in conformance with the Standards when:
        a. The current internal assessment or the most recent external assessment concludes that the internal audit activity does not operate in conformance with the Standards and the Code of Ethics.
        b. The internal audit activity has been in existence for at least five years and has not completed an external assessment, even though, the current internal assessment concludes conformance.
        c. The internal audit activity has completed an external assessment within the past five years but has not conducted an internal assessment within the time frame communicated to the board.
        d. The most recent external assessment was conducted more than five years ago.
    2. The internal audit activity may **indicate** that it is operating in conformance with the Standards when:
        a. The internal audit activity has been in existence for less than five years and the periodic self-assessments conducted at the "communicated frequency" continue to support that conclusion.
        b. An external assessment validates conformance with the Standards and the internal assessments continue to support that conclusion.

D. If an external assessment (a full external assessment, or an SAIV) concludes that conformance is not achieved, the internal audit activity must cease using the conformance statement until the deficiencies are corrected and a new external assessment to validate the conformance with the Standards is conducted.

Disclosure of Nonconformance

According to the Standards, when non-conformance with the Code of Ethics or the Standards impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

A. Internal and external assessments of the QAIP may uncover instances of non-conformance with the Standards that may affect the internal audit activity's ability to fulfill its responsibilities to stakeholders.

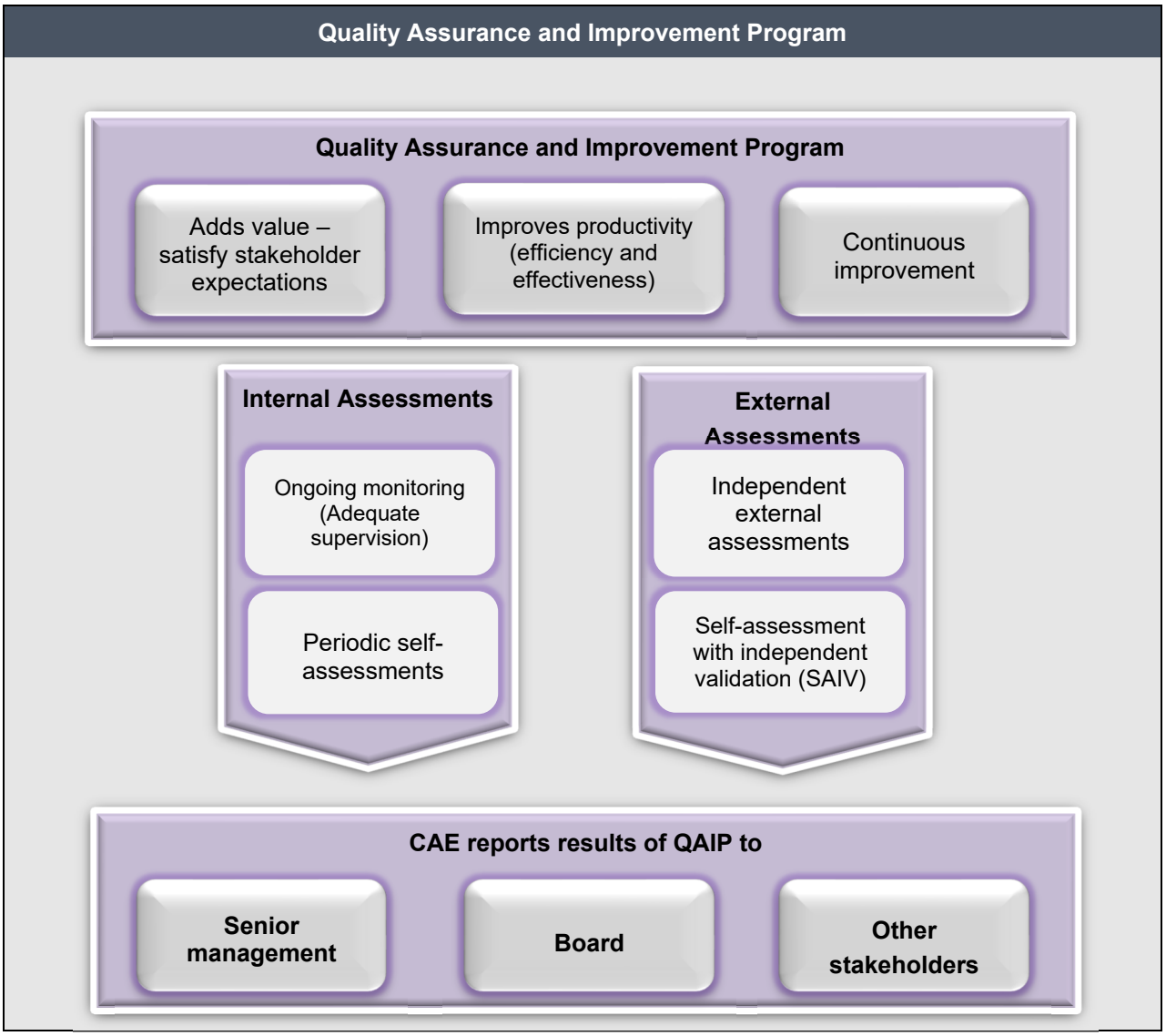
B. The CAE is responsible for disclosing such instances of non-conformance that impact the overall scope or operation of the internal audit activity to senior management and the board.

C. Instances of non-conformance include:

   1. Failure to obtain an external assessment within a five-year period.
   2. Impairments to independence or objectivity.
   3. Scope or resource limitations.

D. Common examples of non-conformance may include:

   1. John was assigned to audit the procurement department of LargeCo. The procurement manager happens to be John's spouse.
   2. Mark was the CAE of Diamond Jewelers. Last year, the engagement work schedule included a physical inventory and a valuation of the diamonds held in stock. Mark did not have anyone on his team with sufficient expertise to value diamonds, but to save on resources, he did not recruit an independent expert. He went online, read a few articles on the valuation of diamonds and started valuing the diamonds himself. Mark was not in conformance of the Standards as he failed to exercise due professional care. A few online articles are not sufficient to examine diamonds for valuation purposes.
   3. Due to time pressure, Cynthia did not arrange for an external quality assessment since her department had the initial external assessment 7 years ago.
   4. Sophie, the CAE of First Bank prepared the annual audit plan without considering the associated risks. She thought that the risk assessment and prioritization exercise was time consuming and since she has been the CAE for the past three years, she can choose engagements without the need for a structured risk assessment exercise.



Part 1, Domain V
Governance,
Risk Management, and Control

Section A: Governance

Learning Outcomes:

1. Describe the concept of organizational governance. Basic Level.
2. Recognize the impact of organizational culture on the overall control environment and individual engagement risks and controls. Basic Level.
3. Recognize and interpret the organization's ethics and compliance-related issues, alleged violations, and dispositions. Basic Level.

Introduction

The IIA Standards requires the internal audit activity to evaluate and contribute to the improvement of the organization's governance, risk management, and control processes. Therefore, it is important for the candidate to understand the relationships among these three concepts: governance, risk management and control. In this introduction, we will provide a brief definition of these concepts and the relationships among them. Each concept will be discussed in detail later.

A. **Governance** (or corporate/organizational governance) is the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

   1. Organizational governance is the system by which organizations are directed and controlled. It includes the rules, relations, and processes that balance the interests of the organization's various stakeholders such as the board, management, shareholders, creditors, customers, suppliers, regulators, and the community.
   2. Organizational governance pertains to the set of rules, processes, and any other interrelated elements that govern an organization. The organizational governance process usually involves a set of interrelated elements and factors that ultimately shape or manage an organization.
   3. Organizational governance involves determining the distribution of rights and responsibilities among the organization's various stakeholders.

4. Organizational governance provides the structure for determining the objectives of the organization and attaining those objectives, as well as, monitoring performance.
5. As a result, organizational governance deals with many aspects such as monitoring, oversight, assurance, risk management, control, relationships among stakeholders, goals setting, appropriate disclosure, ethical environment, and accountability.

B. **Risk Management** is a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

C. **Control** (or internal control) is any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

D. **Relationships among Governance, Risk Management, and Control**

1. Governance represents the broad framework that directs the behavior of the organization in its journey towards its goals, while risk management and control are two fundamental components of good governance.
2. Effective governance requires the governing body (the board) to identify and manage all risks when setting goals and strategy. Risk management involves identifying risks and setting an internal control system to manage all risks across the organization and increase the likelihood that established goals will be achieved. Conversely, risk management and control system rely on the effectiveness of other governance practices such as monitoring, oversight, assurance, ethical environment, tone at the top, risk culture, and accountability.

E. Implementation Guide 2100 of the IPPF discusses the role of internal auditors in governance, risk management, and control. It is summarized below:

1. According to the Standards, the internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

2. Internal auditors are required to understand the concepts of governance, risk management, and control. It is also important for the internal audit activity to have an understanding of organizational objectives, as well as the roles and responsibilities of each stakeholder with respect to governance, risk management, and control. Typically:
    a. **The Board** is responsible for guiding the governance process.
    b. **Senior Management** is accountable for leading risk management and control processes.
    c. **The Internal Audit** is responsible for providing objective assurance and consulting activities related to the three processes.
3. To assess the organization's governance, risk management, and control processes, the CAE typically considers the level of maturity of the three processes as well as the organization's culture. Then, the CAE assesses the risks associated with the three processes.
4. The CAE will also review the organization's mission, key objectives, critical risks, and the key controls used to mitigate such risks to an acceptable level.
5. During the assessment, the CAE may use established frameworks adopted by senior management to guide the assessment, such as the COSO framework, COSO-ERM framework, the King Report on Corporate Governance, or ISO 31000 (all these frameworks will be discussed in this Domain).
6. If an established framework has not been adopted to guide the organization's governance, risk management, and control processes, the CAE may consider recommending an appropriate framework to guide senior management in their pursuit of enhancing these processes.
7. The CAE documents and discusses with senior management any relevant observations and conclusions. The CAE also makes recommendations to strengthen the processes and may escalate significant observations to the board.

Governance

A. Many governance issues arise because of the separation of ownership and management in business corporations, which is called the **agency problem** or the **principal–agent conflict**. The senior management (the agent) runs the company on behalf of the shareholders (the principals), but the management may not always act in the best interests of the shareholders because managers and shareholders have different pecuniary interests. This conflict of interests increases the need for a good organizational governance practices to enhance managerial accountability and protect the interests of the shareholders and the other stakeholders. This could be accomplished by, among other organizational governance elements, the supervision and monitoring performed by the board of directors over the corporate and the performance of its senior management. That is why the board of directors plays the major role in organizational governance.

B. The high-profile corporate scandals occurred in the early 2000s, and the financial crisis in 2008, increased interest in the organizational governance practices, and this has led to the development of many organizational governance frameworks and models. In the following pages, we will discuss the general concepts of organizational governance. In addition, we will include a brief summary of the most common organizational governance reports and frameworks which include:

   1. Sarbanes-Oxley Act in the USA,
   2. The King Report on Corporate Governance (King IV),
   3. The OECD Principles of Corporate Governance, and

C. Organizational governance refers to the procedures utilized by the representatives of the organization's stakeholders to provide oversight of risk and control processes administered by management.

   1. It is the board's responsibility (**NOT the responsibility of internal audit**) to ensure that the organization's operations are in the best interests of its shareholders and other stakeholders (or in accordance with the objectives and the best interests of beneficiaries for not-for-profit organizations). Directors of the board are expected to take active roles in organizational governance to ensure successful strategic management.
   2. Management is responsible to all stakeholders for providing authoritative direction and control of the organization. Risk management is considered an important aspect of the governance process.

D. There are many definitions of governance. For the purpose of the CIA exam, the candidate should be familiar specifically with the definition of governance listed in the IIA Glossary:

   "**Governance is the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives."**

Governance Principles

A. There are many important frameworks and models developed as regulations or guidance on organizational governance principles. The most influential models are: The Principles of Corporate Governance (OECD, 2015), the Sarbanes-Oxley Act (US, 2002), and the King IV report (Southern Africa, 2016). The following is a summary of the common governance factors or principles extracted from those codes:

1. **Stakeholder Interests and Involvement** – Organizations must take into account the interests of all stakeholders. In addition to the shareholders, organizations must recognize the interests of other non-shareholders stakeholders who include a wide range of people and groups affected by their operations, such as employees, investors, creditors, suppliers, local communities, customers, and regulators. Stakeholders also should be involved in governing and controlling the organization.
2. **Stewardship by the board** – Effective governance requires an independent and objective board of directors with sufficient expertise and authority to oversee the organization and its management. The composition of the board should be balanced in order to represent the interests of the shareholders. The board roles in organizational governance will be covered under Interaction among Stakeholders below.
3. **Laws and Regulations** – Laws and regulations contribute to the governance by enforcing certain requirements and prohibiting certain actions. Sound and well-developed laws and regulations protect people who have invested in the organization or who are affected by its operations. Examples include maximum work hours, minimum wage, anti-discrimination, consumer protection, antitrust law, insider trading, and health and safety rules.
4. **Integrity and Ethical Behavior** – Ethical behavior requires organizations to act in ways consistent with what society and stakeholders typically consider to be fair and honest. The board should support the establishment of an ethical culture and standards in the organization and monitor the conformance with these standards. The ethical standards should be given priority for all important decisions such as choosing corporate officers and board members. The following factors contribute to the ethical culture:
    a. Properly enacted and monitored Code of Conduct that promotes ethical and responsible decision making.
    b. A whistleblowing policy allowing employees to voice their concerns to appropriate parties on top management questionable practices.
    c. Integrity, openness, and accountability of Board Members and key Officers.

5. **Objectives of the Organization** – the organization's objectives also contribute to its governance and are used to measure organizational and individual performance. Clearly defined objectives help the organization in shaping its mission, vision and strategies in a manner that enables a balanced range of performance measures that ensure identifying and managing risks to effective performance.
6. **Transparent Disclosure** – Good governance requires timely and accurate disclosure of all material information concerning the organization, including its financial position and results. Relevant information should be equally accessible to all stakeholders in order to help them exercise their rights and make informed assessments of the organization's performance. The board should oversee the disclosure practices and ensure its adequacy and transparency.
7. **Accountability** – The organization should be structured in a way that clearly identifies lines of responsibility and accountability. The chain of accountability starts with individual employees and goes through each level of command up to the board of directors. For instance, individual employees are accountable to lower managers, the lower managers are accountable to middle managers, the middle managers are accountable to senior managers and the CEO, the senior managers and the CEO are accountable to the board of directors, and the board of directors has the overall accountability to the stakeholders because they delegates the board to perform monitoring and assurance activities over the organization on their behalf.
8. **Risk Management** – A clearly defined risk management policies and processes should be implemented and embedded into the organizational systems and processes. The board should monitor the adequacy and effectiveness of risk management policies and processes throughout the organization.
9. **Internal Control** – A strong system of internal control should exist in the organization to address all risks that have been identified. This system should be monitored by the senior management and the board.
10. **Internal Audit** – The existence of an internal audit function in the organization contributes to good governance. Properly positioned internal audit function with sufficient skills, independence, and expertise can assess and provide assurance about risk management, control and governance processes in the organization, as well as, provide recommendations to enhance these processes.
11. **External Audit** provides an independent and competent review of the financial reports before they are published. The outside assurance provided by the external audit improves the quality of the information communicated to the stakeholders and, therefore, enhance governance.
12. **Audit Committee** – The audit committee should be comprised of only non-executive directors in order to enhance its independence in providing an oversight of the internal control and governance process. Audit committee should have direct links with internal and external auditors, as well as, a direct line to the shareholders via a separate report in the annual reports.

13. **Compensation Policies** – The compensation policy in the organization should encourage appropriate behavior consistent with the objectives and values of the organization, especially for directors and senior management.
14. **Effective Interaction** among the board, management, and the other parties involved in the organizational governance is a key factor for good governance. This will be covered separately below.

B. **Interaction among Stakeholders** – The interaction among the various stakeholders of an organization plays a significant role in its governance. The stakeholders include owners, shareholders, employees, suppliers, customers, creditors, banks, Board of Directors, senior management, etc. Usually, public organizations are the ones with significant interaction between the various stakeholders which shape the organizational governance. More closely held organizations are usually tightly managed by the owners, and thus the owners' concentration on management and the operations would provide sufficient controls over the governance. In public organizations, there are usually a set of interacting interests, rules and regulations that are almost universal contributing to the organizational governance. The three primary interacting groups are shareholders, Board of Directors, and management.

1. **Shareholders** – Individuals or entities purchase the shares of the Company and become Shareholders. Shareholders are the true owners of a corporation. They contribute to governance by electing Board members who will oversee the operations of the Company.
    a. Shareholders are entitled to certain rights:
        i. Right to elect directors for the Board.
        ii. Right to elect and remove members of the board.
        iii. Right to obtain information on a regular basis.
        iv. Right to receive dividends (if declared).
        v. Right to purchase additional shares or sell their existing shares.
        vi. Right to the remaining assets upon liquidation after paying all other parties.
        vii. Right to vote on significant changes to the organization.
    b. The above rights provide shareholders with relative control and oversight over the corporation thus contributing to the overall governance.
2. **The Board of Directors** consists of members elected by the shareholders. Members of the Board do not have any authority to act individually, rather the Board collectively has the decision-making authority. The Board makes decisions in accordance with the corporate bylaws which usually stipulate the number of votes required for the various decisions which can range from a majority to unanimously. The directors' compensation is derived from dividends and capital gains resulting from the appreciation of share prices. The Board usually has the following duties:

a. Appointment and removal of management officers.

b. Setting management compensation.

c. Supervision and oversight of the organization and its officers.

d. Appointment of the CAE and external auditors – The Board may have a sub-committee of directors acting as an audit committee which appoints both the CAE and the external auditors.

e. Making strategic decisions including decisions for mergers and acquisitions, and decisions with amounts beyond management's authorities per the corporate bylaws or internal policies ultimately set and approved by the Board.

f. Initial adoption and changes to bylaws.

g. Fundamental changes to the organizational structure.

h. Declaring dividends.

i. Overall responsibility for the organization

j. Board Members' Fiduciary Duties

i. Duty of loyalty to act in the best interests of the company and not to have any conflicts of interest while serving on the Board.

ii. Duty of due care i.e., to make decisions with reasonable care. Board members are not infallible, but they should carry out their duties with reasonable care and judgment.

3. **Senior Management** including Chief Executive Officer (CEO), Chief Operating Officer (COO), and Chief Financial Officer (CFO) manage the overall operations, take major decisions, and introduce major changes. They derive their authority from the powers given to them by the Board. In return, senior managers are accountable to the Board for their operating and governance activities.

a. Like directors, senior managers have fiduciary duties towards the organization and they have the rights of indemnification and right of receiving compensation.

b. Senior managers may also be shareholders and/or Directors, however, for strong organizational governance, it is preferred that the majority of the Board be independent.

C. Organizational governance practices or mechanisms can be either internal or external

1. **Internal** governance mechanisms are exercised by internal parties and include:

a. Stewardship and monitoring by the board.

b. Policies, procedures and bylaws.

c. Assurance functions such as internal audit.

d. Risk management.

e. Internal control processes.
f. Balance of power in the organizational structure.
g. Performance measurement and remuneration.

2. **External** governance mechanisms are exercised by external parties and include
   a. Governmental laws and regulations.
   b. Requirements of influential external parties such as labor unions.
   c. Contractual covenants.
   d. External auditors.
   e. Media pressure.

D. **Governance Benefits** – As a summary, we can conclude that good governance practices seek to ensure that:
   1. Board Members act in the best interests of shareholders and other stakeholders.
   2. The board is structured to act independently.
   3. Shareholders are treated fairly and empowered to participate in the governance of the organization.
   4. The rights of stakeholders are respected and communicated.
   5. Appropriate risk management practices and controls are in place.
   6. The organization complies with legal and regulatory rules.
   7. The organization satisfies the accepted business norms, ethical principles, and social expectations of society.
   8. The organization reports fully and truthfully to its stakeholders and general public to ensure accountability for its actions and performance.

Internal Audit Role in Governance

The internal audit activity's ultimate role in governance is to evaluate and provide recommendations to improve governance. This role is clearly stated in the IIA standards. The IIA Implementation Guide number 2110 discusses the internal audit roles in governance. It is summarized below:

A. According to the Standard 2110, the internal audit activity must **assess** and make appropriate **recommendations** to improve the organization's governance processes for:
   1. Making strategic and operational decisions.
   2. Overseeing risk management and control.
   3. Promoting appropriate ethics and values within the organization.
   4. Ensuring effective organizational performance management and accountability.

5. Communicating risk and control information to appropriate areas of the organization.
6. Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

B. The internal auditors need to attain a clear understanding of the concept of governance and the characteristics of typical governance processes. They should also consider the formal definition of governance, as it appears in the IIA glossary and become familiar with globally accepted governance frameworks and models.

C. How an organization designs and practices the principles of effective governance depends on factors such as its size, complexity, life cycle, maturity, stakeholder structure, and the legal requirements to which the organization is subject. The CAE's approach to assessing governance and making recommendations to management will vary based on the framework or model the organization uses.

D. Governance does not exist as a set of independent processes and structures. Rather, governance, risk management, and control are interrelated. For example, effective governance activities consider risk when setting strategy. Equally, risk management relies on effective governance (e.g., tone at the top; risk appetite, tolerance, and culture; and the oversight of risk management). Likewise, effective governance relies on internal controls and communication to the board about the effectiveness of those controls.

E. The CAE needs to gain insight into the role the board plays in the organization's governance, especially regarding strategic and operational decision-making. The CAE may also need to gain a clearer understanding of the organization-specific processes and assurance activities already in place. If the organization is regulated, the CAE may want to review any governance concerns identified by regulators.

F. To ensure agreement and an alignment of expectations about what constitutes governance, the CAE discusses with the board and senior management:

1. The definition of governance and the nature of governance processes within the organization.
2. The requirements of Standards.
3. The internal audit activity's role.
4. Any changes to the internal audit activity's approach and plan that may improve its conformance with the standard.

G. Usually, a single audit of governance is not attempted. Rather, the internal audit activity's assessment of governance processes is likely to be based on information obtained from numerous audit assignments over time.

H. Standard 2110 specifically identifies the internal audit activity's responsibility for assessing and making appropriate recommendations to improve the organization's governance processes for:

1. **Making strategic and operational decisions** – To evaluate an organization's governance processes for making strategic and operational decisions, the internal audit activity may review past audit reports as well as board meeting minutes, the board policy manual, or related governance documents, which can help provide an understanding of how such decisions are discussed and ultimately made. This review typically reveals whether established, consistent decision-making processes have been developed.
2. **Overseeing risk management and control** – The internal audit activity typically reviews the process for conducting the annual risk assessment. The internal audit activity may also review minutes from meetings wherein risk management strategy was discussed, as well as previously conducted risk assessments. The information obtained can be compared to benchmarking and industry trends to ensure all relevant risks have been considered.
3. **Promoting appropriate ethics and values within the organization** – To assess how an organization promotes ethics and values, both internally and among its external business partners, the internal audit activity reviews the organization's related objectives, programs, and activities. These could include mission and value statements, a code of conduct, hiring and training processes, and an anti-fraud and whistleblowing policy. Surveys and interviews may be used to gauge whether the organization's efforts result in sufficient awareness of its ethical standards and values.
4. **Ensuring effective organizational performance management and accountability** – To evaluate how an organization ensures effective performance management and accountability, the internal audit activity could review the organization's policies and processes related to staff compensation, objective setting, and performance evaluation. The internal audit activity may also review performance measurements and incentive plans to determine whether they are appropriately designed and executed.
5. **Communicating risk and control information to appropriate areas of the organization** – The internal audit activity could access internal reports, newsletters, relevant memos and emails, and staff meeting minutes to determine whether information regarding risks and controls is complete, accurate, and distributed timely. During assurance and advisory engagements, the internal audit activity also evaluates how the area under review communicates risk and control information.

6. **Coordinating the activities and communicating information** – To assess an organization's ability to coordinate activities and communicate information among the board, external and internal auditors, other assurance providers, and management, the internal audit activity could identify the meetings that include these groups and determine how frequently they occur. Members of the internal audit activity may attend the meetings, and they may review the meeting minutes, work plans, and reports distributed among the groups to learn how these parties coordinate activities and communicate with each other.

Organizational Governance Frameworks

In the following pages, we will present a brief summary of the most common organizational governance reports and frameworks. Studying these frameworks is not required for the CIA exam purpose, however, reading them provides the candidate with a deeper understanding of current governance concepts. The frameworks to be presented are:

- The King Report on Corporate Governance (King IV),
- The OECD Principles of Corporate Governance, and
- Sarbanes-Oxley Act.

King IV Report on Corporate Governance

The King Report on Corporate Governance is a principle-based mandatory governance framework for publicly traded companies in South Africa. Building on three previous versions issued in 1994, 2002 and 2009, the fourth version (King IV™) was published in 2016 by The Institute of Directors in Southern Africa. The King IV report is considered by many professionals as the most effective summary of the best practices in corporate governance.

At the heart of this report is the King IV **Code™ on Corporate Governance** which contains 17 basic principles followed by recommended practices for each principle. In the following few pages, we will provide the basic concepts of King IV report and a summary of the Code on Corporate Governance.

A. Definition of Corporate Governance

1. King IV report defines corporate governance as: the exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes:
   a. Ethical culture
   b. Good performance
   c. Effective control
   d. Legitimacy
2. "**Corporate**" in the term "corporate governance" refers to organizations that are incorporated to form legal entities separate from their founders.

B. **The Philosophy** – The central concept underpinning King IV is “Integrated Thinking”. Integral thinking takes account of the connectivity and interdependencies between the factors that affect the ability of the organization to create value over time. Integrated thinking forms the basis for all of the following:
   - Seeing the organization as an integral part of society,
   - Corporate citizenship,
   - The stakeholder-inclusive approach,
   - Sustainable development, and
   - Integrated reporting.

   1. **The Organization as an Integral Part of Society** – Organizations operate in a societal context, which they affect and by which they are affected. Organizations are dependent on this broader society to provide the operating environment, the customer base, and the skills required by the organization. In turn, organizations contribute to the society as creators of wealth; providers of goods, services and employment; and developers of human capital.
   2. **Corporate Citizenship** – As the organization is an integral part of society, it has corporate citizenship status. This status confers rights, obligations and responsibilities on the organization towards society and the natural environment on which society depends.
   3. **Stakeholder-Inclusive Approach** – There is an interdependent relationship between the organization and its stakeholders. The organization’s ability to create value for itself depends on its ability to create value for others. The board must take into account the needs, interests, and expectations of material stakeholders. Therefore, instead of prioritizing the interests of the providers of financial capital (shareholders), the board balances the needs, interests and expectations of stakeholder groupings in a dynamic and ongoing process.
   4. **Sustainable Development** – Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their needs. Sustainable development is a fitting response to the organization being an integral part of society; its status as a corporate citizen; and its stakeholders' needs, interests, and expectations.
   5. **Integrated Reporting** – King IV emphasizes that companies must report beyond financial results to their public stakeholders. In addition to financial reporting and other legally required reports, King IV requires the governing body (the board) to oversee that the organization issues an integrated report at least annually. An integrated report is a concise communication about how an organization’s strategy, governance, and performance lead to the creation of value over the short, medium and long term. An integrated report includes the following elements:
      a. An overview about the work of the organization and its external environment.
      b. The governance structure of the organization and how it supports the organization’s ability to create value.

c. The business model employed by the organization.
d. The risks and opportunities that affect the organization's ability to create value over time.
e. The organization's strategy and resource allocation.
f. The organization's performance in achieving its strategic objectives for the period.
g. The challenges and uncertainties the organization is likely to encounter in pursuing its strategy.

C. **The Code on Corporate Governance** is the most important part of King IV report. It includes the basic 17 principles that should guide the journey towards corporate governance. Achieving these principles, and therefore ultimately good governance, enables the organization to realize the intended governance outcomes mentioned earlier. Each principle is followed by recommended practices for the board to achieve the related principle. The following is a summary of the Code on Corporate Governance.

1. **Leadership**: The board should lead ethically and effectively.
    a. **Ethical leadership** implies integrity, competence, responsibility, accountability, fairness and transparency. It involves the prevention of the negative consequences of the organization's activities on the economy, the society, and the environment.
    b. **Effective leadership** is about achieving strategic objectives and positive outcomes. Effective leadership focuses on effective and efficient execution.
2. **Ethics**: The board should govern the ethics of the organization and support the establishment of an ethical culture.
3. **Corporate Citizenship**: The board should ensure that the organization is a responsible corporate citizen.
    a. The board should oversee and monitor how the consequences of the organization's activities affect its status as a responsible corporate citizen.
4. **Strategy and Performance**: The board should appreciate that the organization's core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process.
5. **Reporting**: The board should ensure that reports issued by the organization enable stakeholders to make informed assessments of the organization's performance and its short, medium and long-term prospects.
    a. The board should oversee that reports such as the annual financial statements, sustainability reports, social and ethics committee reports are issued to comply with legal requirements, and to meet the legitimate and reasonable information needs of material stakeholders.
    b. The board should oversee that the organization issues an integrated report at least annually.

6. **Primary Role and Responsibilities of the Board**: The board should serve as the custodian of corporate governance in the organization.
    a. Significant emphasis is placed on the governing body's (the board) role and responsibility for the governance of the organization. The board should exercise its leadership role by:
        i. **Steering** the organization and setting its strategic direction as the basis on which management will develop the strategy.
        ii. **Approving** the strategy, the policies, and the operational plans developed by the management.
        iii. **Overseeing** and monitoring management's execution of the strategy.
        iv. **Ensuring** that there is accountability for organizational performance through, among others, reporting and disclosure.
7. **Composition of the Board**: The board should comprise the appropriate balance of knowledge, skills, experience, diversity and independence for it to discharge its governance role and responsibilities objectively and effectively.
8. **Committees of the board**: The board should ensure that its arrangements for delegation within its own structures promote independent judgment and assist with balance of power and the effective discharge of its duties.
    a. The board should consider establishing an **audit committee**, the role of which should be to provide independent oversight of the effectiveness of the internal and external assurance functions and services.
9. **Performance of the Board**: The board should ensure that the evaluation of its own performance supports continued improvement in its performance and effectiveness.
10. **Appointment and Delegation to Management**: The board should ensure that the appointment of, and delegation to, management contribute to role clarity and the effective exercise of authority and responsibilities.
    a. The board should appoint the CEO, who should be responsible for leading the execution of approved strategy, policy and operational planning. The CEO should be accountable, and report to, the board.
    b. The board should set the direction and parameters for the powers which are to be reserved for itself, and those that are to be delegated to management via the CEO.

11. **Risk Governance:** The board should govern risk in a way that supports the organization in setting and achieving its strategic objectives.
    a. The board should set the direction for how risk should be approached and addressed. Risk governance should encompass both:
        i. The opportunities and associated risks to be considered when developing strategy.
        ii. The potential positive and negative effects of these risks on the achievement of organizational objectives.
    b. The board should consider the need to receive periodic independent assurance on the effectiveness of risk management.
    c. The board is responsible to oversee the continual assessment and management of risks and should ensure that there are processes in place enabling complete, timely, relevant, accurate, and accessible risk disclosure to stakeholders.
12. The board should **govern technology and information** in a way that supports the organization setting and achieving its strategic objectives.
13. **Compliance Governance**: The board should govern compliance with applicable laws, rules, codes, and standards in a way that supports the organization being ethical and a good corporate citizen.
    a. The board should assume responsibility for the governance of compliance by setting the direction for how compliance should be approached and addressed.
    b. The board should exercise ongoing oversight of compliance and receive periodic independent assurance on the effectiveness of compliance management.
14. **Remuneration Governance**: The board should ensure that the organization remunerates fairly, responsibly and transparently.
15. **Assurance**: The board should ensure that assurance services enable an effective control environment and supports the integrity of information for internal and external reports.
    a. The board should assume responsibility for assurance by setting the direction concerning the arrangements for internal and external assurance services. The board (or audit committee) should oversee that those arrangements are effective in achieving the following:
        i. Enabling an effective internal control environment.
        ii. Covering effectively the organization’s significant risks.
        iii. Supporting the integrity of internal and external reports.

b. The board should assume responsibility for internal audit by setting the direction for the internal audit arrangements needed to provide objective and relevant assurance that contributes to the effectiveness of governance, risk management and control processes.

c. The board should approve the internal audit charter and the appointment of the CAE.

d. The board should ensure the independency of the CAE from management who designs and implements the controls in place.

16. **Stakeholders**: The board should adopt a stakeholder-inclusive approach that balances the needs, interests and expectations of material stakeholders in the best interests of the organization over time.

    a. The board should assume responsibility for the governance of stakeholder relationships by setting the direction for how stakeholder relationships should be approached.

    b. The board should exercise ongoing oversight of stakeholder relationship management and ensure that it achieves the following:

        i. Identifying individual stakeholders and stakeholder groupings.

        ii. Determining material stakeholders based on the extent to which they affect, or are affected by, the activities of the organization.

        iii. Managing stakeholder risk as a part of organization-wide risk management.

        iv. Employing formal mechanisms for communication with stakeholders.

        v. Evaluating the quality of relationships with material stakeholder.

17. **Institutional Investor**: The board of an institutional investor organization should ensure that responsible investment is practiced by the organization to promote the good governance and the creation of value by the companies in which it invests. (This principle applies to institutional investors only, while the other 16 principles can be applied by any organization)

OECD Principles of Corporate Governance

A. The Organization for Economic Co-operation and Development (OECD) published a set of corporate governance principles in 1999. These principles were revised in 2015 and endorsed by the G20. Currently, the G20/OECD principles are recognized globally and serve as a reference for the national corporate governance codes in the EU countries and beyond. The G20/OECD principles focus on publicly traded companies but are useful in benchmarking and improving governance practices in any organization.

B. **Definition of Corporate Governance** – in the introduction of the principles, the OECD defines corporate governance as follows “Corporate governance involves a set of relationships between a company’s management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined”.

C. **G20/OECD Principles of Corporate Governance** – The OECD provides six key governance principles. Each key principle is followed by a number of supporting sub-principles. An extract of the G20/OECD corporate governance principles are shown below:

1. **Ensuring the basis for an effective corporate governance framework** – The corporate governance framework should promote fair markets, and the efficient allocation of resources. It should be consistent with the rule of law and support effective supervision and enforcement.

    a. This principle emphasizes the importance of the legal, regulatory, and institutional framework that market participants can rely on when they establish their contractual relations. This governance framework typically comprises elements of legislation, regulation, self-regulatory arrangements, voluntary commitments and business practices. Well established framework promotes effective corporate governance.

2. **The rights and equitable treatment of shareholders** – The corporate governance framework should protect and facilitate the exercise of shareholders’ rights and ensure the equitable treatment of all shareholders.

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

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

    c. 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.

    d. 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.

    e. 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 disproportionate to their equity ownership should be disclosed.

f. 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.

g. Minority shareholders should be protected from abusive actions.

h. Markets for corporate control (acquisition) should be allowed to function in an efficient and transparent manner.

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.

   a. Institutional investors acting in a fiduciary capacity should disclose their corporate governance and voting policies with respect to their investments. Disclosure should also include how they manage material conflicts of interest that may affect the exercise of key ownership rights regarding their investments.

   b. Proxy advisors, analysts, brokers, rating agencies and others that provide advice relevant to decisions by investors should disclose and minimize conflicts of interest that might compromise the integrity of their advice.

   c. Insider trading and market manipulation should be prohibited and the applicable rules enforced.

4. **The role of stakeholders in corporate governance** – The corporate governance framework should recognize the rights of stakeholders and encourage active co-operation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.

   a. The rights of stakeholders that are established by law or through mutual agreements are to be respected.

   b. Where stakeholder interests are protected by law, stakeholders should have the opportunity to obtain effective redress for violation of their rights.

   c. Mechanisms for employee participation in corporate governance should be permitted to develop.

   d. Where stakeholders participate in the corporate governance process, they should have access to relevant, sufficient, and reliable information on a timely and regular basis.

   e. 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.

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.

a. Disclosure should include material information on:
    i. The financial and operating results of the company.
    ii. Company objectives and non-financial information.
    iii. Remuneration of members of the board and key executives.
    iv. Information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board.
    v. Related party transactions.
    vi. Foreseeable risk factors.
    vii. Governance structures and policies, and the process by which they are implemented.
b. Information should be prepared and disclosed in accordance with high quality standards of accounting and financial and non-financial reporting.
c. An annual audit should be conducted by an independent, competent and qualified auditor in order to provide an external and objective assurance to the board and shareholders that the financial statements fairly represent the financial position and performance of the company.
d. 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.

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.
    a. 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.
    b. The board should apply high ethical standards. It should take into account the interests of stakeholders.
    c. Board members should have access to accurate, relevant and timely information.
    d. The board should fulfill certain key functions, including:
        i. 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.
        ii. Monitoring the effectiveness of the company's governance practices and making changes as needed.

iii. Selecting, compensating, monitoring and replacing key executives and overseeing succession planning.

iv. Aligning key executive and board remuneration with the longer term interests of the company and its shareholders.

v. Ensuring a formal and transparent board nomination and election process.

vi. Monitoring and managing potential conflicts of interest of management, board members and shareholders, including misuse of corporate assets and abuse in related party transactions.

vii. 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.

viii. Overseeing the process of disclosure and communications.

e. The board should be able to exercise **objective independent** judgment on corporate affairs.

i. 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.

ii. Boards should consider setting up specialized committees to support the full board in performing its functions, particularly in respect to audit, risk management and remuneration.

iii. Boards should regularly carry out evaluations to appraise their performance.

Sarbanes-Oxley Act

A. After several accounting scandals, mainly Enron, the US Congress enacted the Sarbanes-Oxley Act on January 23, 2002 (often referred to as SOX) to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. The Act added additional responsibilities to the audit committee, and thus contributes to the organizations' governance process.

B. Sarbanes-Oxley Act is primarily concerned with public companies and does NOT apply to non-issuers or privately held companies.

C. Summary of Sarbanes-Oxley Act requirements

1. The Act requires that the Public Company Accounting Oversight Board (PCAOB) be established to regulate and oversee the auditing profession, which had been self-regulated before the law. The PCAOB is responsible for:
    a. Registering public accounting firms that prepare audit reports for issuers.
    b. Establishing and/or adopting auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers.
    c. Inspecting, investigating, enforcing compliance and sanction (when appropriate) on, registered public accounting firms that are subject to the securities laws.
2. The Act requires that work of a registered public accounting firm providing audit services be approved by the audit committee in advance.
3. The audit committee is responsible for the appointment, compensation, independence and oversight of the external independent auditor. This includes resolution of financial reporting disagreements between management and auditor.
4. Services provided by external auditors were limited and reporting by those auditors is made directly to the audit committee.
5. The audit committee must establish procedures for:
    a. The monitoring of internal controls
    b. The receipt, retention, and treatment of complaints regarding internal accounting controls and auditing matters.
    c. The confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.
6. The Act requires each member of the audit committee to be independent, which includes not accepting any consulting, advisory or other compensatory fees from the company.
7. The Chief Executive Officer (CEO) and Chief Financial Officer (CFO) must attest to the financial statements and internal controls.

D. As relevant for the scope of this section of the CIA exam, only sections (201, 203, 302, & 404) of SOX will be covered:

1. **Section 201** – Services outside The Scope of Practice of Auditors
    a. SOX prohibits public accountants to provide an audit client contemporaneously with the audit, any non-audit service, including:
        i. Bookkeeping or other services related to the accounting records or financial statements of the audit client;
        ii. Financial information systems design and implementation;
        iii. Appraisal or valuation services, fairness opinions, or contribution-in-kind reports;

iv. Actuarial services;

v. Internal audit outsourcing services;

vi. Management functions or human resources;

vii. Broker or dealer, investment adviser, or investment banking services;

viii. Legal services and expert services unrelated to the audit; and

ix. Any other service that the Board determines, by regulation, is impermissible.

b. Any non-audit service not specifically prohibited per the list above, including tax services, may be conducted only if approved in advance by the audit committee of the issuer.

2. **Section 203** – Audit Partner Rotation

a. SOX prohibits the lead (or coordinating) audit partner or the audit partner responsible for reviewing the audit to have performed audit services for an issuer in the previous 5 fiscal years i.e., lead and reviewing audit partners must be rotated regularly and should not have provided services for more than five years to an issuer.

3. **Section 302** – Corporate Responsibility for Financial Reports - SOX requires the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that:

a. The signing officer has reviewed the report;

b. Based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

c. Based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

d. The signing officers:

i. Are responsible for establishing and maintaining internal controls;

ii. Have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

iii. Have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and

iv. Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

e. The signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function):

   i. All significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

   ii. Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

f. The signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

4. **Section 404** – Management Assessment of Internal Controls

   a. SOX require that the annual report contain an internal control report which:

      i. States the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

      ii. Contains an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

   b. As part of the annual audit report for an issuer, the registered public accounting firm shall attest to, and report on, the assessment made by the management of the issuer, and shall not be the subject of a separate engagement.

Section B: Corporate Social Responsibility

Learning Outcomes:
1. Describe corporate social responsibility. Basic Level.

A. Corporate Social Responsibility (CSR) refers to corporations' commitment and responsibility towards their societies. The IIA published a relevant Practice Guide: Evaluating Corporate Social Responsibility/Sustainable.

B. CSR presents significant risks and opportunities for organizations. Stakeholders expect boards and management to accept responsibility and implement strategies and controls to manage their impact on society and the environment, to engage stakeholders in their endeavors, and to inform the public about their results. Internal auditors should understand the risks and controls related to CSR objectives. Internal auditors should maintain the skills and knowledge necessary to understand and evaluate the governance, risks, and controls of CSR strategies.

C. **CSR Definitions** – Governmental and nongovernmental organizations have published many definitions of CSR, including:

   1. CSR is the continuing commitment by business to behave ethically and contribute to economic development while improving the quality of life of the workforce and their families as well as of the local community and society at large. (World Business Council for Sustainable Development.)

   2. Generally, CSR is understood to be the way firms integrate social, environmental, and economic concerns into their values, culture, decision-making, strategy and operations in a transparent and accountable manner and thereby establish better practices within the firm, create wealth, and improve society. (Government of Canada.)

D. Some organizations focus on economic and CSR objectives, where the environment is included as one element of CSR, along with ethics, transparency, health and safety, corporate governance, human rights, and community investment. Other organizations follow a Triple Bottom Line reporting strategy, which covers three measures of success: economic, environmental, and social responsibility.

E. **Responsibility for CSR**

   1. **The board** has overall responsibility for the effectiveness of governance, risk management, and internal control processes associated with CSR.

   2. **Management** is responsible for ensuring that

      a. CSR objectives are established

      b. Risks are managed

      c. Performance is measured

      d. Activities are appropriately monitored and reported.

3. **The Internal Audit Activity** may be required to perform assurance or consulting services related to CSR which will be discussed in the following paragraphs.
4. Generally, CSR activities are pervasive throughout the organization; thus, every employee has a responsibility for ensuring the success of CSR objectives.

F. **CSR Risks** – Organizations are exposed to a variety of risks associated with CSR activities. The board and management are responsible for performing a risk assessment and determining what is important to their organization and the controls they will implement to manage those risks. Internal auditors should understand these risks and the related controls to help them develop appropriate audit procedures.

1. **Reputation** – The organization's brand or reputation could be damaged due to violations of law or principles, errors or omissions in disclosed CSR information, under-performance compared with targets, or the appearance of indifference to social issues. Organizations have the opportunity to enhance their reputation by behaving in a socially responsible manner and involving stakeholders in decisions that affect them.
2. **Compliance** – Organizations may fail to comply due to the extent, complexity, and volume of regulations relating to the environment, health and safety, employment, governance, political contributions, conflict of interest, fraud, etc. Compliance risk also arises from contractual obligations with third parties, and from voluntary adoption of standards. Compliance risk increases for organizations operating in multiple countries.
3. **Liability** – Liability risk exists when contracting for CSR terms and conditions and ensuring third-party compliance. Activists or specific classes/special interest groups may take legal action for alleged harm done by the organization
4. **Operational** - Risk arises from the CSR "pressure points" for the organization's manufacturing processes, products, services and impact on the environment. Other examples of potential risk scenarios include: under-performance of other targets due to inappropriate CSR strategies, or over-emphasis on CSR strategies; failure to integrate CSR objectives into processes, or to educate staff appropriately; failure to develop well-controlled systems for CSR initiatives; risk associated with reporting CSR activities and results.
5. **Stock Market** – Organizations may lose investors, or limit their pool of investors, if they do not qualify for Socially Responsible Investment or similar funds.
6. **Employment Market** – Employees want to work for organizations that respect their rights, have a culture of integrity, and commit to social and community concerns.

7. **Sales Market** – Customers might boycott products or services for environmental or social issues. Organizations have an opportunity to increase sales and advertising if they are recognized by “socially responsible consumer” groups.
8. **External Business Relationships** – Customers, suppliers, or partners could violate CSR terms and conditions, principles, or laws, yet the organization could be included as a wrongdoer by association. Developing and monitoring the controls over and within external business relationships may be a challenge for some organizations.

G. **CSR Business Activities** – generally include:

1. Determining and communicating policies and procedures for areas including corporate governance, business ethics, human resources and employment, supply chain management, stakeholder relations, donations and political contributions, the environment, and health and wellness.
2. Setting objectives, performance targets, and strategies, such as:
   a. Reduce carbon emissions and waste.
   b. Comply with laws and regulations.
   c. Donate a percentage of net profits to charitable organizations.
   d. Increase indigenous workforce.
   e. Reduce safety incidents.
   f. Create a culture of transparency.
   g. Facilitate employee volunteerism.
   h. Become the employer of choice and extend the ethical culture throughout the supply chain.
3. Communicating and embedding CSR principles and controls into business decision making processes.
4. Tracking, measuring performance of, analyzing trends around, and benchmarking activities.
5. Stakeholder engagement, including:
   a. Advisory or focus groups as part of research and development.
   b. Involvement in policy development and feedback.
   c. Satisfaction surveys.
   d. Complaint management.

6. Auditing:
    a. Disclosures in public reports.
    b. Internal controls and management systems.
    c. Contractual compliance with CSR terms and conditions.
7. Reporting results internally and externally, along.

H. **CSR Reporting –** Many organizations report their CSR results to the public. Reports help audiences, such as investors, employees, suppliers, and customers make informed decisions about their involvement with the organization. There are several laws that require organizations in particular sectors to publicly disclose certain CSR practices and activities. To meet stakeholder demands for accountability, many organizations are using verification and assurance processes for all or part of the reports. Organizations have used internal reviewers (including internal auditors), independent third parties, community or expert advisory panels, or a combination of these to perform the assurance process. There are also international not-for-profit organizations, such as AccountAbility, that produce standards (AA1000) for assurance of CSR reports to help strengthen the assurance process.

I. **Approaches to Evaluating CSR –** As part of the risk assessment and audit planning process, the CAE considers the CSR risks and whether to include all or part of the processes in its audit universe and audit plans. The CAE also should be aware of CSR issues in order to respond to any special requests by the board or senior management.

1. Consulting – The internal audit activity may consult on project design and implementation for CSR programs and reports or serve as an adviser on CSR governance, risk management, and internal controls.
2. Facilitating – The internal audit activity may facilitate a management self-assessment of CSR controls and results. This process would be developed based on a risk assessment and results in action items for control improvements.
3. Auditing – The internal audit activity may choose to evaluate the CSR programs as a whole and determine whether the organization has adequate controls to achieve its CSR objectives. This option would likely require a significant allocation of resources because of the broad scope of the subject. Such an audit is not likely to be done to develop the first opinion on CSR controls; rather the CAE would develop a one- to three-year plan to obtain sufficient and reliable information about the various elements of CSR within the organization. There are many approaches to auditing CSR controls, including:
    a. Separate audits of each element of. Typical CSR elements include governance, community investment, environment, ethics, health, safety, transparency, working conditions, and human rights.

b. Audits of CSR programs related to each significant stakeholder group affected by CSR activities. Stakeholders could include customers, employees and their families, neighboring communities, shareholders, and suppliers.

c. Audits of the internal controls over risk management, recording, measuring, and reporting of CSR activities within each department or function that is covered in the audit plan.

d. Assurance audits of public disclosures of financial and non-financial information related to CSR or any of the individual CSR elements. Most organizations with stated CSR objectives provide public information about their approach and results.

e. Audits of third parties for contractual compliance, including compliance with CSR terms and conditions. A proactive role may also be taken. For example, internal auditors could perform a review as part of a supplier pre-qualification process.

J. **Audit Considerations**

1. **Use of Audit Opinion** – Senior management or the board may choose to publicly state that it relies on its internal controls to produce reliable information for public reporting. Management might also ask the CAE to provide a statement for the CSR report, saying that the internal audit activity has provided assurance on the information contained in the report. Caution should be taken to manage liability associated with the opinion, if it is published.

2. **Independence and Objectivity** – Often, the internal audit activity may have an operating role within the CSR processes. This would put the auditors in the position of evaluating and reporting on their own activities, which threatens their independence and objectivity. However, this could be overcome by using independent auditors to assess the related portions of the CSR program and reports.

3. **Skills and Body of Knowledge** – Any internal audit activity that collectively lacks the appropriate skills and knowledge should not undertake an internal audit, facilitation, or consulting engagement. Specific CSR competencies could include expertise in regulations, management systems and best practices relating to the environment, health and wellness, safety, ethics, community investment, human rights, working conditions, and governance. Language and other communication skills are also important considerations.

4. **Resources** – The number of auditors and skills required depends on the audit approach.

5. **CSR Maturity Model** – The CAE considers the organization's CSR maturity level at the time of the internal audit, and the level to which the organization hopes to progress. This information will help the auditor frame recommendations as audit findings or as ideas to help move the organization toward its goal. A sample maturity scale could include:
    a. Senior management and the board have not initiated any CSR objectives or strategies.
    b. The CSR strategy is "to comply with laws and contractual commitments."
    c. Ad hoc recognition of specific CSR risks and strategies to meet objectives exists in some divisions of the organization. The organization's goal is to exceed compliance requirements. Reporting is selective.
    d. A set of integrated and managed CSR strategies and performance measures — reported to the public — with governance processes is in place.
    e. CSR is a primary feature of the organization's mission, principles, and performance measures. Formal reports are produced for the public, stakeholder engagement processes are in place, and CSR factors are embedded into business decision-making processes throughout the organization, including at board levels.

ISO 26000

A. ISO 26000 provides guidance on how businesses and organizations can operate in a socially responsible way. This means acting in an ethical and transparent way that contributes to the health and welfare of society.

B. Unlike the famous ISO 9000 standards which companies can be certified in, IS0 26000 provides guidance rather than requirements. It helps clarify what social responsibility is, helps businesses and organizations translate principles into effective actions and shares best practices relating to social responsibility, globally.

C. **Principles of ISO 26000** – ISO 26000 concentrates on the following seven key principles of socially responsible behavior:
    1. **Accountability** – Organizations must be accountable for their actions and impact on the society, the economy, and the environment.
    2. **Transparency** – Organizations' decisions and actions that affect the society, the economy, and the environment must be conducted with openness and effective communication.
    3. **Ethical Behavior** – Organizations' actions must be in conformance with commonly accepted norms of good conduct.
    4. **Respect for the Rule of Law** – Compliance with laws and regulations.
    5. **Respect for International Norms of Behavior** – Compliance with international laws and regulations.

6. **Respect for Stakeholder Interests** – Taking into consideration the rights and interests of all parties who are affected by the organization's actions.
7. **Respect for Human Rights** – Organizations must respect human rights listed in the international Bill on Human Rights.

D. **The Core Subjects of ISO 26000** – ISO 26000 provides guidance about the following seven core subjects or components of social responsibility:

1. **Organizational Governance** – addresses governance practices that ensure implementing the principles of social responsibility.
2. **Human Rights** – addresses the following areas
   a. Due diligence.
   b. Human rights risk situations.
   c. Discrimination and vulnerable groups.
   d. Civil and political rights.
   e. Economic, social and cultural rights.
   f. Fundamental principles and rights at work.
3. **Labor Practices** – addresses the following areas:
   a. Employment
   b. Conditions of work and social protection
   c. Social dialogue
   d. Health and safety at work
   e. Human development and training in the workplace
4. **The Environment** – addresses the following areas:
   a. Prevention of pollution.
   b. Sustainable resource use.
   c. Climate change mitigation and adaptation.
   d. Protection of the environment, biodiversity and restoration of natural habitats.
5. **Fair Operating Practices** – addresses the following areas:
   a. Anti-corruption.
   b. Responsible political involvement.
   c. Fair competition.
   d. Promoting social responsibility through the value chain.
   e. Respect for property rights.

6. **Consumer Issues** – addresses the following areas:
    a. Fair marketing, factual and unbiased information and fair contractual practices.
    b. Protecting consumers' health and safety.
    c. Sustainable consumption.
    d. Consumer service, support, and complaint resolution.
    e. Consumer data protection and privacy.
    f. Access to essential services.
    g. Education and awareness.
7. **Community Involvement and Development** – addresses the following areas:
    a. Community involvement.
    b. Education and culture.
    c. Employment creation and skills development.
    d. Technology development and access.
    e. Wealth and income creation.
    f. Health.
    g. Social investment.

Environmental and Social Safeguards

A. Environmental and social safeguards are policies and measures that enable the adoption and integration of precautionary environmental and social principles and considerations into programs and projects, as well as the development of internal organizational policies. The objective is to prevent and mitigate undue harm to the environment and people at the earliest possible stage. Normally, safeguard policies include:
    1. Standards and performance metrics, against which the compliance of activities is assessed and measured.
    2. Processes, like screening, environmental and social assessment, and mechanisms such as community consultations and review panels; and
    3. Internal measures such as training, reporting, and incentives to ensure compliance and accountability.
B. Companies should strive for positive development outcomes in the process of achieving their organizational goals and should continuously target social and environmental sustainability of their operations.

C. Environmental and social safeguards are required to identify risks, reduce social and environmental costs, benefiting communities, and preserving the environment. Safeguards need to be in place to ensure:
   1. Adequate social and environmental assessment and management.
   2. Labor rights are reasonably protected and working conditions are proper.
   3. Pollution prevention is in place.
   4. Cultural heritage is maintained, and the rights of indigenous people are maintained.
   5. Adequate safeguards for the community, health, safety, and security of all the company's stakeholders.
   6. The company's operations are environmentally and socially responsible.

Auditing Environmental and Social Safeguards Policies

A. The risks related to environmental noncompliance, fines and penalties and other mismanagement may result in significant losses for the organization. Chief audit executive (CAE) must include the environmental, health, and safety risks in any entity-wide risk management assessment. Among the risk exposures that should be evaluated are:
   1. Organizational reporting structures.
   2. Likelihood of causing environmental harm, fines, and penalties.
   3. Expenditures mandated by environmental governmental agencies.
   4. History of injuries and deaths.
   5. Record of losses of customers, and episodes of negative publicity and loss of public image and reputation.

B. An environmental audit program could be:
   1. Compliance-focused – verifying compliance with laws, regulations, and the entity's own EH&S policies, procedures, and performance objectives.
   2. Management systems-focused – providing assessments of management systems intended to ensure compliance with legal and internal requirements and the mitigation of risks.
   3. A combination of both approaches.

C. **Audit Approach –** Environmental auditing includes assessing how compliance with laws, regulations, and contractual obligations is managed. Some of the questions that internal auditors may use in this assessment include:
   1. Are social and environmental impact assessments performed:
      a. As part of risk management programs?
      b. As part of investment decision-making and approval processes?
      c. Do they include conflict risk?
   2. Are life cycle value assessments done for assets and product development?

3. Are green or socially responsible procurement processes in place? How are they monitored?
4. Are incidents reported, managed, and resolved appropriately?
5. Are environmental program performance measures and metrics maintained and reported? Are benchmarking and trend analysis also performed and reported to senior management and the board?
6. Are reduce, reuse, and recycle concepts integrated into operations?
7. Do risk assessments consider air (greenhouse gas and other emissions, climate change, and carbon footprint), water (use and effluent), land (reclamation, recreational spaces, garbage and disposal of hazardous wastes, conservancy, and stewardship), and animals (product testing, ecosystems, and biodiversity)?
8. Do environmental emergency plans exist? Do these plans balance privacy of personal information with access to information for employees and the community?
9. Does the organization calculate its carbon footprint and does it have offset programs in place? If so, are calculations accurate and complete, and are the strategies effective?

D. In those instances where the environmental audit function is organizationally independent of the internal audit activity, the CAE should:
   1. Foster a close working relationship with the chief environmental officer and coordinate activities with the plan for environmental auditing.
   2. Offer to review the environmental audit plan and the performance of engagements.
   3. Evaluate the organizational placement and independence of the environmental audit function to ensure that significant matters are reported to the audit committee or the board.
   4. Periodically schedule a quality assurance review of the environmental audit function to determine if the environmental risks are being adequately addressed.
   5. Evaluate whether the environmental auditors are in compliance with recognized professional auditing standards and code of ethics.

Section C: Risk Management

Learning Outcomes:

1. Interpret fundamental concepts of risk and the risk management process. Proficiency Level.
2. Describe globally accepted risk management frameworks appropriate to the organization (COSO - ERM, ISO 31000, etc.). Basic Level.
3. Examine the effectiveness of risk management within processes and functions. Proficiency Level.
4. Recognize the appropriateness of the internal audit activity's role in the organization's risk management process. Basic Level.

Risk

A. **Risk** (as defined in the IIA's Glossary) is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

   1. Based on this comprehensive definition of risk the following conclusions can be derived:

      a. Ensuring the achievement of the objectives requires the organization to install a system for managing risks effectively. Good systems of risk management keep the organization's objectives firmly in mind when addressing risks.

      b. In the context of achieving objectives, risk may have a positive or a negative impact. That is, risk can represent a threat to achieving objectives or an opportunity that should be utilized and not missed or ignored.

B. **Types of Risks** – there are several types of risks, some of which may overlap:

   1. **Strategic Risk** – is the risk that the company has to monitor to adjust its operations and strategies accordingly. They are risks that cannot be controlled by the company such as political impediment risks, the risk of an economic slowdown, technological innovation, and/or changes in customer preferences.

   2. **Operational Risk** – is further subdivided to business operational risk and information technology risk. They are the risks encountered as a result of human error, system failure, inadequate monitoring, employee fraud, management fraud, and product failure. They are the risks that result from inadequate or failed internal processes, people, or systems. Operational risks do not cover reputational or strategic risks.

      a. **Business Risk** – is considered to be one type of operational risks that is related to risks arising from efficiency, supply chain, and/or business cycles.

      b. **Legal Risk** – is one type of operational risk. Legal risks include, but are not limited to, exposure to fines, penalties, settlements, and/or punitive damages resulting from operations.

3. **Hazard Risk** – is the risk that an adverse event such as fire, flood, theft, storm, etc. may affect a business. A hazard risk is a risk that can be waived away through insurance. Insurance companies in that context provide coverage for property damage, business interruption, workers' compensation, general liability, automobile liability and many other losses. This type of insurance can cover the death of a key employee or any other event that can stop the continuity of the business.
4. **Financial Risk** – is the risk that might affect the profit of the organization as a result of interest rate fluctuations, counterparty default, commodity price fluctuations, business interruptions, or credit risks.
5. **Compliance Risk** – is the risk that an institution might face as the result of not complying with the laws and regulations applicable to its industry or it is the risk of not complying with the companies' own internal processes and policies and procedures.
6. **Political Risk** – is the risk that a company might have to face as a result of a new regulation that affects the continuity of a project and/or product or the risk that the company incurs due to a civil war taking place in the country where operations are being done. It is also the risk of having a new regulation that affects the enterprise's ongoing operations. The best way to cope with this kind of risk is to lobby against regulations that would adversely affect the business.

C. **Impact of Volatility and Time on Risk**

1. **Volatility** is defined as the changes that occur to the value of a project or to a company's operations within a certain period of time. Volatility is often measured by standard deviation where a higher standard deviation indicates higher volatility and thus higher risk. The higher the volatility, the higher the risk.
2. **Time** impact usually affects organizations in a way that the higher estimated time required to finish a project or make a deliverable, the higher the risk. Time impact and risk are positively correlated. The longer the time-frame, the more likely that circumstances that were anticipated, budgeted, known, etc. will change.

Risk Management

A. Organizations rarely operate in isolation; rather, they operate in extremely dynamic environments. As a result, the risks affecting each organization will continuously change. To effectively manage risks in such environments, a risk management system must be established to ensure that potential risks are addressed to the ultimate achievement of organizational objectives.

B. **Risk Management** (as defined in the IIA's Glossary) is a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

   1. The ultimate objective of risk management strategies and techniques is to provide reasonable **assurance** regarding the achievement of the organization's objectives.

C. Maximizing shareholder value is an essential objective in most organizations. This broad objective encompasses other objectives of minimizing costs and losses while maximizing revenues, market share, and overall organizational performance. Proper risk management contributes to maximizing shareholder wealth by the following:

   1. Improved risk management leads to lower costs associated with risks and thus enhanced shareholder value.
   2. Improved risk management leads to enhanced operational competitiveness and thus enhanced shareholder value.
   3. Improved risk management reduces the risk profile of the company, which leads to better credit rating, lower costs of funds, lower weighted average cost of capital and thus enhanced financial competitiveness and enhanced shareholder value.

D. The benefits of risk management include:

   4. Anticipating and identifying risks as early as possible to minimize any potential negative consequences.
   5. Assisting in quantifying possible losses so that the firm would be able to provision for the expected losses.
   6. Better allocation of resources so that more resources are made available to riskier processes.
   7. Supporting strategic and business planning.
   8. Promoting continuous improvements.
   9. Reducing fluctuations and unexpected surprises.
   10. Help in grasping new opportunities.
   11. Providing more assurance to all stakeholders on the future of the organization.

E. The techniques used by various organizations for their risk management practices can vary significantly. Depending on the size and complexity of the organization's activities, risk management processes can be:

1. Formal or informal
2. Quantitative or subjective
3. Embedded in the business units or centralized at a corporate level.

F. The organization designs risk management processes based on its culture, management style, and business objectives. The methodology chosen should be sufficiently comprehensive and appropriate for the nature of the organization's activities. For example,
   1. Use of derivatives or other sophisticated capital markets products by the organization could require the use of quantitative risk management tools.
   2. Smaller, less complex organizations could use an informal risk committee to discuss the organization's risk profile and to initiate periodic actions.

G. The risk management framework can be divided to five core phases:

1. Risk identification
2. Risk assessment and prioritization
3. Risk responses to address identified risks
4. Controls to ensure that risk responses are executed properly
5. Reporting and monitoring

Risk Identification

A. The first step in the risk management process is to identify all risks that affect the organization's objectives. The organization's objectives can be at risk due to internal or external factors that must be identified.
   1. External factors include technological developments, changing customer needs or expectations, competition, new legislation and regulation, natural catastrophes, and economic changes.
   2. Internal factors include human errors, systems' failures, the quality of personnel hired, and a change in management responsibilities, the nature of the entity's activities, and an unassertive or ineffective board or audit committee.

B. All imaginable risks that may affect the success of the organization must be identified, ranging from the more significant business risks down to the less important risks related to individual projects or smaller business units.

C. Risk identification should involve all parties who have expertise and influence over the operations of the organization. The identification process can be done through each department or considering the organization as one entity. It can also be performed on project-by-project level or function by function.

D. An organization's risk identification methodology may be comprised of a set of different techniques that use both historical and future events:

1. **Event Inventories –** event inventories is the process of listing events that are common to the industry in which the organization is functioning. This list of events could be developed by the organization's personnel internally or externally from a generic list of events. If this list of events is internally developed, it could be used to ensure a consistent view across similar activities within the organization. If externally developed, the inventory is enhanced and it could be tailored to the organization's risk to become a learning lesson. For Example: If a bank is going to buy a new software, the inventory would be the experience of other banks in acquiring such a system.
2. **Facilitated Workshops –** this technique involves bringing together cross-functional or multi-level individuals for the purpose of drawing on the group's collective knowledge to develop a list of events that relate to the company's strategic objectives. For each objective, the facilitator will prompt discussion on events originating from the following factors and their related effects:
   - External
   - Internal
   - Economic
   - Technology
   - Infrastructure
   - Natural Environment
   - Personnel
   - Political
   - Process
   - Social

   Usually, the outcome of these meetings is to gain consensus of the risk tolerance, and to discuss internal and external factors that driver potential events relative to the objective. In addition, these meetings determine which events represent risks to achieving the objective and which represent opportunities.
3. **Interviews –** Interviews are usually conducted to have an idea about the individual's candid views and knowledge of past and potential risks that might take place while implementing the project.
4. **Questionnaires and Surveys –** Questionnaires and Surveys are used to address several issues to be considered by the participants thinking of any internal or external factors that may give rise to risks. The process allows for brainstorming the various potential risks that may occur.
5. **Process Flow Analysis –** This step involves defining all the processes in a diagrammatic representation with the goal of better understanding the interrelationships, component inputs, tasks, outputs, and responsibilities. Once mapped, events can be identified and tested against process objectives.

6. **Leading Event Indicators and Escalation Triggers –** Leading event indicators often called leading risk indicators are thresholds that are agreed upon by the management and that provide insight into potential events like an increase beyond the expected level in the price of raw materials. To be useful, these leading indicators should be provided to management in timely manner.
7. **Loss Event Data Tracking –** Monitoring data helps organizations keep track of past negative impact incidents along with the associated losses in order to predict future occurrences. This data could be provided externally, yet some industries like banks or insurance companies keep records internally of their previous losses. This data helps management in estimating the likelihood and impact of future events.
8. **Ongoing Event Identification –** Potential events are identified on ongoing basis in connection with routine business activities. Then these events are matched against external and internal factors that gave rise to events.

Risk Assessment

A. The next step is to assess and analyze the risks that have been identified.
   1. **Risk Assessment** is a systematic process for assessing and integrating professional judgments about probable risks or events. It is about measuring the likelihood and relative significance of the identified risks.

B. **Risk measurement** is a process that uses the quantitative techniques to understand the size of the firm's risk profile. These techniques include statistically modeling the frequency and the impact of the risk events and creates statistical predictions of the future risk profile.

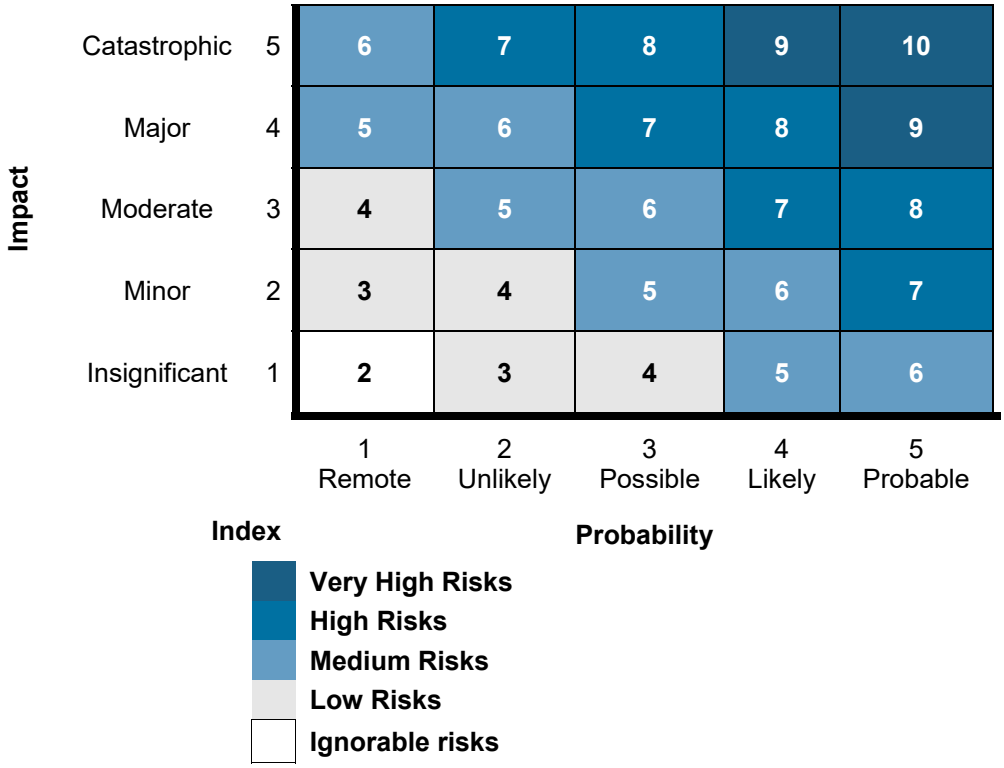
C. The risk assessment process in most risk management models is a function of two parameters:
   1. **Likelihood** of a risk occurring.
   2. **Potential impact** of the risk on the organization's objectives.

D. There are several methods used for the risk assessment and analysis process, but most would assign quantitative weights to each of the risk assessment parameters likelihood and potential impact. For each parameter, qualitative factors as assessed by the risk management team may be used also. The basic idea is to assess all identified risks and to rank them in terms of likelihood and impact in a consistent manner.

1. **Likelihood –** the likelihood (or probability) of the risk occurring may be done on a scale of 3 factors, 5 factors, or more depending on the organization. For demonstration purposes, a 5-factor model will be used:
    a. 1 – Remote
    b. 2 – Unlikely
    c. 3 – Possible
    d. 4 – Likely
    e. 5 – Probable (almost certain)
2. **Potential Impact –** the potential impact of the risk on the objectives of the organization may be done on a scale of 3 factors, 5 factors, or more depending on the organization. For demonstration purposes, a 5-factor model will be used:
    a. 1 – Insignificant
    b. 2 – Minor
    c. 3 – Moderate
    d. 4 – Major
    e. 5 – Catastrophic

E. **Risk Mapping** is the process of plotting the identified risks on a map (sometimes referred to as a heat map). Mapping the identified risks helps the organization in prioritizing risks.

Illustration Risk Weighting and Mapping (Heat Map)



F. **Risk Prioritization –** typically, risk prioritization refers to ranking identified risks in accordance with their priorities. Typically, probable risks are prioritized over less probable regardless of potential impact. For demonstration purposes, a 3-factor model will be used in the illustration below:

Illustration of Risk Prioritization

The following is the prioritizing of risks. Likely risks are given first priority before possible risks (regardless of criticality), and risks with remote likelihood have least priority.

		Likelihood		
		Likely	Possible	Remote
Impact	Critical	1	4	7
	Major	2	5	8
	Minor	3	6	9

G. Expected Value – A Quantitative Risk Assessment Technique

1. When there is sufficient quantitative information about the identified risks, the organization can assess and prioritize those risks based on their expected values. This can be performed by estimating the value impact of each risk and then applying that value to the risk probability to derive an expected value or loss of the risk.
2. **The expected loss** is defined as a loss that the organization may expect based on a probability forecast.

Illustration of Probability of Loss – Mutually Exclusive Events

Verda Corporation is being sued for a deficient product. Its lawyers estimated the following probabilities and associated settlements that may be made. The company's lawyers maintained that a loss is probable, and the range of probabilities of the exact amount of the loss is as follows:

Probability	Operating Loss
5%	$200,000
30%	250,000
10%	300,000
15%	350,000
40%	400,000

What is the expected loss of Verda Corporation?

Solution:

Probability		Operating Loss		Expected Loss
5%	x	$200,000	=	$10,000
30%	x	250,000	=	75,000
10%	x	300,000	=	30,000
15%	x	350,000	=	52,500
40%	x	400,000	=	160,000
100%				**327,500**

Verda's expected loss from the settlements is $327,500. The Company is certain to lose money. The minimum loss expected is $200,000 with a 5% chance. The maximum loss possible is 400,000 with a 40% chance.

However, sometimes different risk probabilities are assigned to different event types that are not mutually exclusive.

Illustration of Probability of Loss – Independent Events

Verda Corporation conducted a risk inventory and identified five primary risks that its operations is subject to. After careful consideration of each individual risk, Verda determined the following probability of occurrence and expected loss for each individual risk. What is the total expected risk exposure for Verda?

Risk	Probability	Expected Loss
Risk 1	5%	800,000
Risk 2	25%	300,000
Risk 3	50%	200,000
Risk 4	80%	100,000
Risk 5	1%	1,000,000

Solution:

Risk	Probability		Expected Loss		Risk Exposure
Risk 1	5%	x	800,000	=	20,000
Risk 2	25%	x	300,000	=	75,000
Risk 3	50%	x	200,000	=	100,000
Risk 4	80%	x	100,000	=	80,000
Risk 5	1%	x	1,000,000	=	10,000
					285,000

Risk Response

A. **Risk Responses** are the means by which an organization elects to manage individual risks.

B. After identifying and assessing the risks, the third step in risk management is to develop a risk response plan to address those risks. Risk responses should be consistent with the organization's risk appetite.

C. **Risk Appetite** (or tolerance) is the amount of risk that an organization is willing to accept in the pursuit of its objectives. Any form of business/operation will entail a certain level of risk. Different organizations and/or different managers tend to tolerate different levels of risk depending on their appetite for risk. The more aggressive the organization/manager, the more risk they would tend to assume.

D. If, for example, an identified risk is assessed to be beyond the risk appetite of the organization, an appropriate risk response should be devised to manage the risk to be within the risk appetite of the organization. After applying risk responses and completing the risk management process, risks are divided between managed and residual risks.

1. **Inherent Risk** is also referred to as gross risk. It is the risk that the firm might face without taking into consideration any response actions to the risk. Distinguishing this type of risk is very important because when responses and controls are not applied, the firm will be exposed to the entire (inherent) risk.
2. **Managed Risk** refers to the part of the inherent risk that has been mitigated and/or managed.
3. **Residual Risk** refers to any part of the risk remaining after the risk management process has been applied to mitigate or manage the risks. Businesses assume risks and are rewarded with profits. Profits typically are the reward for residual risks that businesses assume. Residual risk is also referred to as the net risk. Residual risk is typically not eliminated since it will be very expensive to the firm if not impossible. Part of doing business involves assuming risks. The residual risk should always be within the risk appetite of the organization.

E. As mentioned earlier, risk responses are the means by which an organization elects to manage individual identified risks. Managing identified risks is usually done through affecting the probability of occurrence (i.e., the probability of a risk) and/or mitigating impact should such risk occur (i.e., reducing the adverse consequences of the risk). The main categories of risk responses are (these four categories should be memorized):

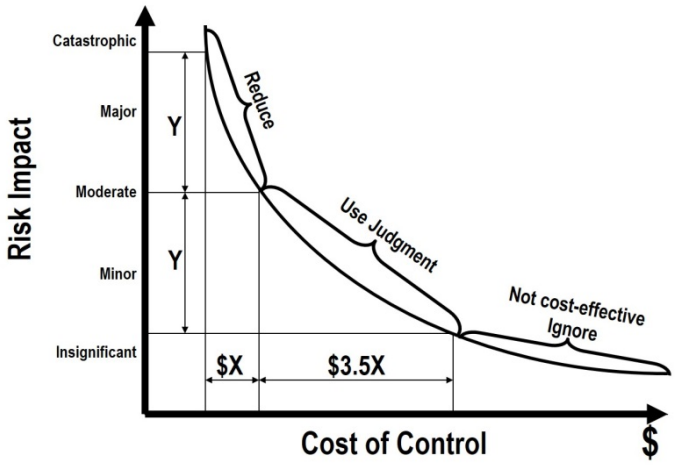
1. **Avoid** (or terminate) the risk – this method implies that the organization is unwilling to take a specified risk that is why it eliminates it completely. The organization usually avoids unwarranted or unrewarded risks. Unwarranted risks are typically excessively high levels or risk for which there is usually no need to assume, as they will not be rewarded. Examples include:
    a. A supermarket chain wishes to reduce the probability that it sells tobacco to minors. One alternative would be to eliminate the sale of tobacco altogether.
    b. As a result of lack of security in a particular neighborhood, a store manager may decide not to accept any forms of cash payments.
    c. Selling or terminating the business unit or product line that gives rise to a risk.
2. **Reduce** the risk – taking actions to mitigate impact and/or mitigate probability of the risk.
    a. The internal control is the most important way of reducing potential risks. Other ways include business decisions such as product or investment diversification which may reduce the risk of too reliance on one key product or investment.
    b. The benefits derived from any control must out-weight the costs, otherwise the controls are not justified. In some cases, the cost-benefit of a control can be quantitatively evaluated. In other instances, the cost-benefit is subjective. For example:

i. In a small company, the employees' working hours are not accurately accounted for, and thus there is a risk that the company is overpaying in payroll expenses every month. The company's accountant estimated that it is costing the company $2,000 per year in wages for hours not worked. In this case, implementing strict controls, and assigning a dedicated employee to log the workers' hours would be unjustified since the cost would significantly out-weight the benefits.

ii. In a larger company, with more than 5,000 employees, the cost of installing a workers' log system to account for actual hours worked would likely be justified as a one hour difference for each employee per month would account for 5,000 employee hours per month and 60,000 employee hours per year.

c. Generally, the cost of implementing controls and risk reduction would follow the below pattern:

Cost of Risk Reduction



1. The graph shows the cost of controls to mitigate risk impact. To reduce the first Y from catastrophic to moderate, it would cost $X. To reduce an additional Y from moderate to insignificant, it would cost $3.5X.
2. Risks that are catastrophic MUST be reduced.
3. It is not cost-justified to reduce insignificant risks, and they are normally ignored.
4. Reduction of risks that range from moderate to insignificant would be subject to management's judgment and would also be dependent upon management's risk appetite.

3. **Transfer** (or share) the risk – this refers to various measures that may be taken to transfer the risk to another party or to share the risk and rewards with them. If after establishing mitigating controls, the residual risk remains higher than the level of acceptable risk (as defined by organization's risk appetite), the residual risk (or part of it) may be transferred through many measures such as:
    a. **Insuring** refers to the practice of obtaining insurance coverage in cases of loss for a premium paid to an insurance company willing to accept the associated risks. Insurance policies come in a variety of customized forms covering a wide range of potential losses. Insurance policies can be constructed to cover losses due to fire, theft and losses caused by human errors. Whatever the insurance will cover, the company must be very clear about what the insurance policy will cover and when to expect payout.
    b. **Hedging** is the activity of trading futures with the objective of reducing or controlling risks by transferring the risk to the speculator (hedging is discussed below under financial risk responses)
    c. **Factoring** refers to selling accounts receivable to third parties at a discount, thus transferring the risk of uncollectible accounts to the factor.
4. **Accept** (or tolerate) the risks as they currently are because either it is not cost-effective to mitigate them, or they do not pose a significant or material threat. The organization should look at the risk's likelihood and impact in light of its established risk appetite and then decide whether to accept that risk or not. By nature, conducting business is associated with taking risks. The market will reward businesses and entrepreneurs for such assumed risks.
    a. **Pursue Risks:** In some cases, the organization may elect to exploit certain types of risks to pursue a high return on investment. Pursue or exploit risks adds to the risk management model a new dimension of "positive" risks that represent opportunities that should be utilized.

F. **Compliance Function** – critical areas within an organization may warrant maintaining separate compliance functions to better manage perceived high risks.
    1. Brokers, banks, and insurance companies may view risks as sufficiently critical to warrant continuous oversight and monitoring and thus may establish a separate compliance function.
    2. Companies dealing with the use of hazardous environmental materials may also wish to maintain a separate environmental compliance function to avoid high-cost liabilities.

G. **Managing Financial Risks** – Organizations usually use many financial tools to optimize the amount of risk they handle with their financial interests. These tools are essentially used to **reduce** or **transfer** financial risks; therefore, they can be included under the risk response "Reduce or Transfer". Financial risks include exchange rate risk, interest rate fluctuations risk, commodity risk, and volatility risk. Some of the tools that are used to response to these financial risks include but are not limited to the following:

1. **Hedging** is a means of reducing the risk of adverse price movements by taking an offsetting position in a related product. It is a way to insure against the price movement. The main tools used in hedging are futures and options.

   a. **Futures Contract** – is an agreement between two parties to perform some act (usually the trading of assets for cash), in accordance with the terms of the agreement, at some future point in time. Futures are standardized contracts that are traded in specialized markets.

   b. **Forward Contract** – is similar to a futures contract, however, it is usually negotiated between the related parties and does not normally trade in a standard market. Unlike the standardized futures contracts, forward contracts are customized subject to the needs of the contracting parties.

Comparison Between Forward and Future		
	Forward	**Future**
Nature	Customized	Standardized
Underlying Assets	Any asset	Assets frequently traded
Contract Size	Any size	Standardized
Contract	Negotiated between the parties	Organized and traded in special markets

   c. **Options** are contracts that represent a right by one party to request performance and an obligation by the second party to perform. Thus, only the holder of the option has the right to request performance of the contract. The party granting the option is the issuer, and party purchasing the option is the holder. Options may be either call or put options.

      i. **Call Options**

      - Are options that permit the holder to purchase stock at (or before) a given date (obliges the issuer to sell the stock) according to a preset price.
      - Issuers of a call option anticipate that the price of the stock will not exceed the price set in the option contract, while holders of the call option anticipate that the price may exceed that set in the option contract.

ii. **Put Options**

- Are options that permit the holder to sell stock at (or before) a given date (obliges the issuer to purchase the stock) according to a preset price.
- Issuers of a put option anticipate that the price of the stock will exceed the price set in the option contract, while holders of the call option anticipate that the price may not exceed that set in the option contract.

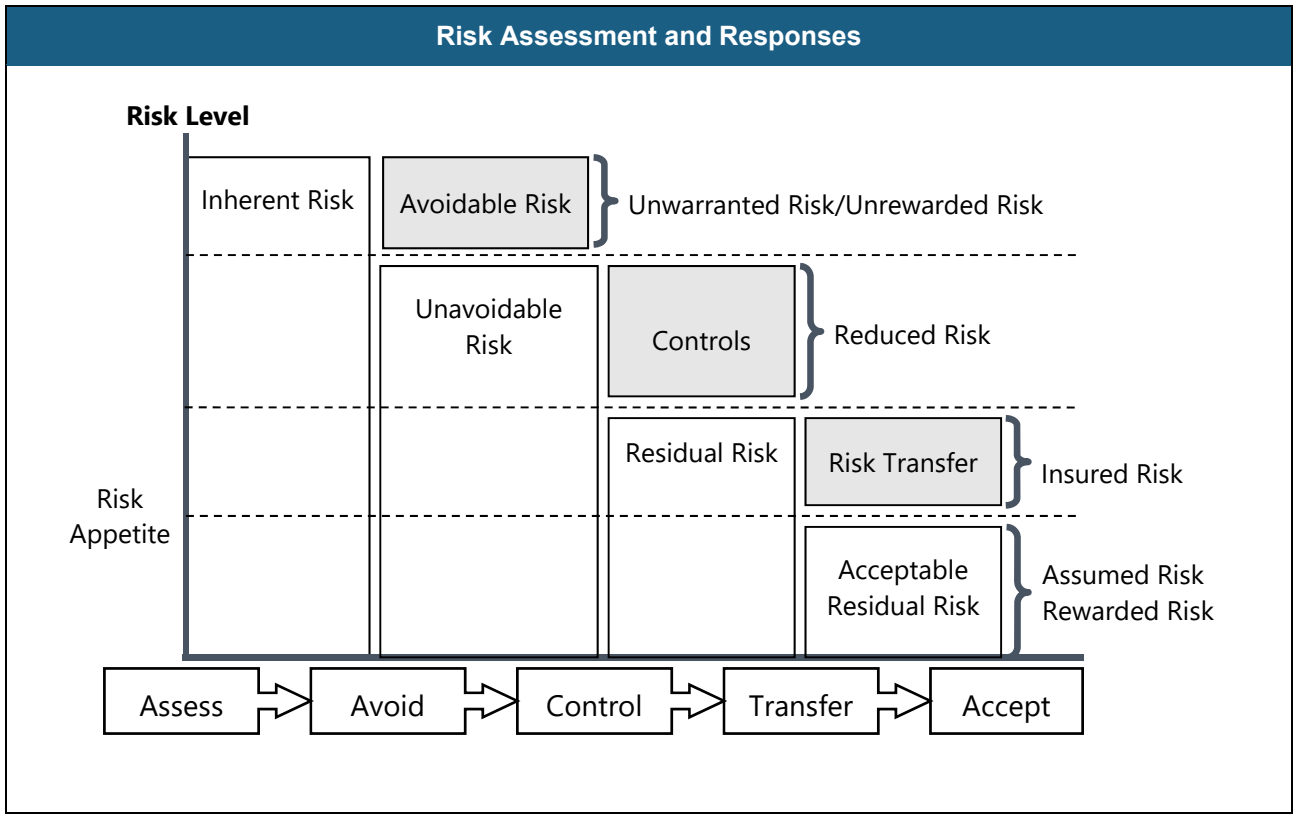
d. **Summary of Option Strategies**

Strategy	Expectations About Asset Price
Buy a call	Rising
Sell a call	Stable or falling
Buy a put	Falling
Sell a put	Stable or rising

2. **Diversification** is the strategy of combining different assets in one portfolio in varying proportions to create a portfolio with a lower standard deviation of return than the weighted average of these two individual assets.
3. **Swap** which is the process of exchanging interest rate risk or currency fluctuation risk between two parties. A swap is a contractual agreement between two parties (called counterparties) in which the counterparties agree to exchange a stream of future cash flows for a stipulated period of time, based on certain agreed-upon parameters and the price fluctuations in some underlying specified commodity or market index.

H. The following chart illustrates the basic risk responses and their effect on inherent risk. This illustration involves a five-step process: Assess – ACT – Accept

1. **Assess:** Assess inherent risks.
2. **Avoid:** Avoid unwarranted or unrewarded risks. Unwarranted risks are typically excessively high levels or risk for which there is usually no need to assume, as they will not be rewarded.
3. **Reduce through Controls:** Establish controls to reduce unavoidable risks.
4. **Transfer:** If after establishing controls, the residual risk remains higher than the level of acceptable risk (as defined by management's risk appetite), transfer risk through insurance, outsourcing, hedging, etc.
5. **Accept:** The remaining risk is considered the residual unavoidable risk that management is willing to accept in order to conduct business. By nature, conducting business is associated with taking risks. The market will reward businesses and entrepreneurs for such assumed risks.



Control

A. **Control** (or internal control) is any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Controls are the means by which management ensures that the organization is operating in accordance with its directives.

B. After selecting appropriate risk responses, the organization should establish control activities and procedures necessary to ensure that the risk responses are executed in a timely and efficient manner.

C. Internal control is an essential component of the risk management process. Using control activities in reducing the identified risks has already been discussed above in Risk Responses. However, control activities should also be tightly linked to all other risk responses in order to manage risks and ensure the effectiveness of risk responses.

D. Internal control activities and components will be discussed in the next Section of this Domain.

Reporting and Monitoring

A. Relevant information about risks must be captured and reported timely to relevant parties in order for the risk management process to achieve its intended objectives. Information should flow down, across, and up the organization.

B. The reporting process is an overall reaching process for all stages of the risk management framework. For example, the risk assessment stage receives input information about the identified risks from the risk identification stage. The risk assessment stage also sends information about the significance of risks to the risk responses stage.

C. Information must also be reported up the chain of command in the organization. This reporting would be usually done directly by the risk management department to the board of directors or it could in the form of a report that is addressed to each concerned department with a summary to senior management and the board.

D. The risk management framework should include a mechanism to ensure that relevant stakeholders receive timely information regarding the risk management processes in the organization.

E. **Monitoring** – The entire risk management process and results should be monitored and updated on a continual basis. Organizations operate in extremely changing environments that introduce new risks. Continuous monitoring helps ensure that the risk management process is working effectively on a continuous basis. Monitoring should involve updating the risk management processes and evaluating the validity of the applied responses. Potential new risks that need to be addressed may arise from the following changes (amongst others):

1. New employees.
2. New processes, systems, lines, products, and/or technology.
3. Rapid expansion of operations.
4. Corporate restructuring or business process reengineering.
5. Changes in operating or regulatory environment.

Enterprise Risk Management (ERM)

A. The difference between traditional risk management and enterprise risk management is:

1. **Traditional risk management** generally considers risks in isolation where each department or operation assesses and manages its own risks individually at a local level. Traditional risk management adopts a narrow view of risks and is conducted in a bottom up manner. For example, the lending department manages credit risk and the accounting department manages risks related to disclosure requirements. Risk information is then reported to the upper levels of management with limited communication between the parties that manage different types of risks.

2. **Enterprise risk management (ERM)** is an extension and integration of traditional risk management across the organization. ERM adopts a broader view of risks and is conducted in a top down manner. It starts with the strategic planning and objectives setting to identify risks to the achievement of the organization's objectives and the appropriate risk appetite. ERM would then flow to middle and local levels to identify and implement appropriate risk responses and controls, as well as, to establish a monitoring process to ensure that the risks stay within the approved risk appetite. ERM seeks to make addressing risks an integral part of conducting business.

B. **Enterprise Risk Management (ERM)** refers to a consistent, structured and continuous process for identifying, assessing, responding to, and reporting opportunities and threats across the organization that would affect the achievement of organizational objectives.

1. ERM does not guarantee the achievement of organizational objectives but seeks to identify and eliminate factors that may hinder their achievement.

2. ERM is concerned with management's selection of the response to identified risks that falls within the enterprise's risk appetite i.e., each organization might select a different response to the same risk depending on its risk appetite.

C. There are two well-known frameworks that consolidate current thinking on enterprise risk management:

1. The COSO - Enterprise Risk Management (ERM) Framework.

2. The ISO 31000 - Risk Management Framework.

COSO-ERM
ISO 31000

Internal auditors should be familiar with those two frameworks to use them as benchmark in assessing the risk management function within an organization. The two frameworks are summarized in the following pages.

The COSO - Enterprise Risk Management (ERM) Framework

COSO-ERM
ISO 31000

The Committee of Sponsoring Organizations (COSO) issued in 1992 the "Internal Control – Integrated Framework" report to provide guidance for designing and implementing effective internal controls. With the significant emphasis on risk management and the underlying premise that entities exist to provide value to their shareholders, and such value is normally provided by assuming risks, it was essential to integrate ERM into COSO model. In 2001, COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework that would be readily usable by management to evaluate and improve their organizations' enterprise risk management.

A. The COSO-ERM Framework defines enterprise risk management as a process, effected by an entity's board of directors, management and other personnel, 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.

    1. **Events**, in this definition, can have a negative impact, a positive impact, or both.

        a. Events with a negative impact represent risks, which can prevent the achievement of objectives.

        b. Events with a positive impact may offset negative impacts or represent opportunities, which can support the achievement of objectives.

B. The above definition of ERM reflects the following concepts about enterprise risk management:

    1. ERM is an ongoing process.
    2. ERM is applied in strategy setting.
    3. ERM is applied across the organization at every level and unit, and includes taking an entity level portfolio view of risk.
    4. ERM is designed to identify potential events.
    5. ERM manages risks to keep them within the organization's risk appetite.
    6. ERM can only provide reasonable assurance.
    7. ERM supports the achievement of key objectives.

C. According to the COSO-ERM Framework, enterprise risk management encompasses:

    1. **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. Risk appetite refers to the extent that risks may be assumed or taken by management. Management typically assumes a risk appetite anywhere on a continuum from a conservative approach to a highly aggressive approach. The strategies that may be achieved by companies are related to the amount of risk appetite that their management may assume, and thus both should be aligned.

2. **Enhancing risk response decisions –** Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance. ERM formalizes the process of identifying risks and means to manage such risks.
3. **Reducing operational surprises and losses –** Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses. By formalizing the process of capturing events that may be considered risks, surprises would be minimized.
4. **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. In some instances, two independent risks each with a mild consequence may combine to cause a significant combined catastrophe. ERM would consider the implications of the combination and interrelation of risks across the organization.
5. **Seizing opportunities –** By considering a full range of potential events, management is positioned to identify and proactively realize opportunities. In the process of identifying events that may constitute risks or opportunities, management would certainly be in a better position to seize opportunities.
6. **Improving deployment of capital –** Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation. With such information, management would be in a better position to deploy its resources to areas that would provide optimum risk results.

D. The COSO-ERM model consists of three dimensions. The first is the four categories of the entity's objectives. ERM is normally geared towards achieving the entity's objectives in the four categories:

1. **Strategic –** high-level and long-term objectives aimed at achieving the organization's mission.
2. **Operations –** support the day-to-day objectives of efficiency and effectiveness in using resources.
3. **Reporting –** adequately reliable reporting free from bias and misstatements.
4. **Compliance –** with the applicable laws and regulations.

E. The second dimension is the eight main components of ERM. The eight interrelated components of ERM that are derived from the way management runs an organization and are an integral part of the organization's management are:

1. **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.
2. **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.
3. **Event Identification –** Internal and external events affecting the 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.
4. **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.
5. **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.
6. **Control Activities –** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
7. **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.
8. **Monitoring –** The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

F. The third dimension in COSO-ERM framework represents the levels of the organization. The objectives in the four categories represent what an entity seeks to achieve, and the eight components of ERM represent what is needed to be done in order to achieve those objectives. In pursuit of the four main objectives, the eight components operate across the entire organization at various levels, which are:

1. Entity level.
2. Division level.
3. Business unit level.
4. Subsidiary level.

G. **Risk and Organizational Objectives** – The COSO-ERM discussion indicates that risk assessment is inseparable from the organizational objectives and its control system. The objectives of an organization typically aim to identify potential risks, and whether there are sufficient controls to mitigate such risks. Generally, the objectives of an organization may be broadly categorized to three main categories:

1. **Operational Objectives –** these objectives pertain to the efficiency and effectiveness of the entity's operations. Operational risks associated with operational objectives include the risks encountered by management on a daily basis in addition to legal risks. Operational risks are managed by maintaining a strong operational risk culture, developing a strong internal control culture including establishing clear lines of responsibility, clear segregation of duties, effective internal reporting, and effective contingency planning. For example, some operational objectives for an organization's payroll cycle would be:
    a. All employees should be paid their wages when due according to time spent.
    b. Employee's timesheets are validated by an independent party.
    c. Only valid and existing employees are recorded on the payroll:
        i. New employees are added to the payroll while terminated employees are removed from the payroll on due time.
        ii. Only valid and existing employees are added to the payroll.
    d. Employees are receiving their wages at the rate agreed upon in their contracts (and/or adjusted to later promotions).
2. **Financial Reporting Objectives –** these objectives pertain to the presentation of reliable published financial statements, including the prevention of fraudulent public financial reporting. For example, some financial reporting objectives for an organization's payroll cycle would be:
    a. Payroll expense should be correctly calculated and reported.
    b. Year-end wages should be accrued even when not made as of the closing date of the financial statements.
    c. All employee benefits should be properly calculated and accrued (if not paid during the year).
    d. There is sufficient disclosure on payroll in the financial statements.
3. **Compliance Objectives –** these objectives pertain to adherence to applicable laws and regulations. For example, compliance objectives for an organization's payroll cycle would be:
    a. The employer is deducting the correct amounts for employee payroll taxes.
    b. The employer is deducting the employees' share of social security.
    c. The employer is making remittances for payroll taxes and social security on due time.
    d. The employer is adhering to any minimum wage regulations.

4. From the objectives above identified, risks will arise such as (only a sample is mentioned):
    a. The organization is paying payroll in excess of the time actually spent by employees.
    b. The organization is making payroll payments to fictitious employees.
    c. The organization is not properly reporting and/or disclosing its payroll expenses.
    d. The organization is not adhering to applicable laws and regulations.

ISO 31000

COSO-ERM
ISO 31000

ISO 31000 is a risk management framework that was developed by the International Organization for Standardization in 2009 and updated in 2018. The Standard provides the framework, principles and process for managing risk. According to the Standard, managing risk

- Assists organizations in setting strategy, achieving objectives and making informed decisions.
- Is part of governance and leadership.
- Is part of all activities associated with an organization.
- Considers the external and internal context of the organization.

Copied by Powers Resources Corporation with the permission of the Standards Council of Canada (SCC) on behalf of ISO.

A. **Principles –** The purpose of risk management is **the creation and protection of value**. The following principles provide the characteristics of effective and efficient risk management.
    1. **Integrated** – Risk management is an integral part of all organizational activities.
    2. **Structured and Comprehensive** – A structured and comprehensive approach to risk management contributes to consistent and comparable results.
    3. **Customized** – The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.
    4. **Inclusive** – Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered.
    5. **Dynamic** – Risk management anticipates and responds to changes in risks in an appropriate and timely manner.
    6. **Best Available Information** – The inputs to risk management should be timely, clear and available to relevant stakeholders.

7. **Human and Cultural Factors** – significantly influence all aspects of risk management.
8. **Continual Improvement** – Risk management is continually improved through learning.

B. **Framework –** The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions. The components of the framework for managing risk according to ISO 31000 are:

1. **Leadership and Commitment** – Top management and oversight bodies should ensure that risk management is integrated into all activities and should demonstrate leadership and commitment.
2. **Integration** – Everyone in an organization has responsibility for managing risk. Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.
3. **Design** – the design of the framework for managing risk involves:
    a. Understanding the organization and its external and internal context. **External context** includes the social, political, legal, financial, technological, economic and environmental factors. **Internal context** includes the organization's vision, mission, culture, strategy, structure, governance and resources
    b. Articulating risk management commitment by top management and oversight bodies.
    c. Assigning roles and responsibilities for risk management.
    d. Allocating sufficient resources for risk management.
    e. Establishing communication and consultation in order to support the framework.
4. **Implementation** – developing an implementation plan and implementing risk management process disrobed below.
5. **Evaluation** – periodically measuring risk management framework performance against its purpose.
6. **Improvement** – improving the framework to address external and internal changes.

C. **Process** – The risk management process comprises the activities described below

1. **Communication and Consultation** – to assist relevant stakeholders in understanding risk.
2. **Scope, Context and Criteria –** Defining the scope of the risk management process, understanding the external and internal context, and defining risk evaluation criteria.

3. **Risk Assessment** – includes risk identification, risk analysis, and risk evaluation.
4. **Risk Treatment** – Selecting and implementing risk treatment options (such as retaining, avoiding, and sharing).
5. **Monitoring and Review** – to assure and improve the quality and effectiveness of process design, implementation and outcomes.
6. **Recording and Reporting** – The risk management process and its outcomes should be documented and reported through appropriate mechanisms.

Means to Enhance Risk Management

Risk management effectiveness in any organization can be enhanced by the following means:

A. **Board Involvement** – The active involvement of the board of directors in driving and overseeing the risk management process contributes to the effectiveness of risk management. The active oversight of the board to risk management could be fulfilled by:
   1. Factoring risk as an integral part of organizational strategy.
   2. Taking actions to encourage an organizational culture of risk awareness.
   3. Developing risk management strategy and policy in liaison with senior management.
   4. Following up on the communication of risk policies and procedures to all employees to ensure that they are incorporated into the organizational culture.
   5. Monitoring the implementation of risk management policies and procedures.
   6. Obtaining regular assurance that risk management is functioning as intended.

B. **Employees Support** – The employees are the foundation of risk management because their behavior determines whether an organization succeeds or fails in achieving its objectives. The risk management process should not be perceived as something that happens to employees and they have to deal with its requirements. Everyone in an organization should have some responsibility for enterprise risk management through participating in the identification and treatment of risks. Measures to enhance employees' engagement in risk management include ensuring that:
   1. Employees are encouraged to identify new risks and opportunities.
   2. Risk information is shared throughout the organization.
   3. Employee's contribution to risk management is encouraged and recognized in performance evaluation.

4. Risk policies and procedures are communicated clearly to all people across the organization.
5. Periodic control and risk self-assessment is performed with a collective participation of management and staff of all levels (control self-assessment is covered overleaf).

C. **Chief Risk Officer (CRO)** – In larger organizations, risk management frameworks can be enhanced by appointing a chief risk officer. The CRO is a person in charge of coordinating and directing risk management efforts across the organization. The CRO usually reports to senior management and the Board. The roles of CROs may include:

1. Developing a strategic approach to risk management.
2. Establishing a risk reporting system.
3. Helping in establishing and implementing the risk policy.
4. Supporting the establishment of risk awareness culture across the organization.
5. Providing risk related consulting and training programs.

D. **Control Self-Assessment (CSA),** or control and risk self-assessment, is the examination and assessment process of the effectiveness of risk management and internal control system within the organization. The process is shared amongst all the employees in an organization, and thus responsibility for control is increased for all individuals in the organization and all employees become process owners. The main objective of the CSA is ensuring that the organization is meeting its objectives in both an efficient and effective manner.

1. CSA is a process through which risk management and internal control effectiveness are examined by people from within the area being assessed. This requires gathering all people of that area, management and staff, for meetings or interviews to participate in assessing their internal controls. CSA usually works better if a person from outside the area being assessed acts as a facilitator for CSA process.
    a. **Facilitating** means working with a group to make it easier for that group to achieve the objectives that the group has agreed on. Facilitating involves listening, challenging, observing, questioning and supporting the group and its members. However, it does not involve doing the work or taking decisions.
    b. Many individuals in the organization may be able to perform the CSA facilitator role, but internal auditors can be the best choice for this role because of their qualifications and position within the organization.

c. The CSA method in commonly used by internal auditors as part of their job in auditing and improving risk management and control processes in the organization. Rather than performing a typical internal audit, in CSA, the internal auditor works with members in the audited area and encourage them to assess their current internal controls and identify opportunities for improving the internal control system.

2. CSA enhances risk management and internal control by helping in:
   a. Identifying potential risks.
   b. Evaluating and assessing the cost-benefits of existing controls over identified risks.
   c. Developing adequate control measures to highlighted risk areas.
   d. Replacing costly and/or ineffective controls with more cost-justified effective controls.
   e. Emphasizing management's responsibility for developing, maintaining, and monitoring effective internal control systems.
   f. Communicating results for a better understanding of the entire business process/activity.
3. **Advantages of CSA**
   a. Provides employees with an enhanced understanding of business risks and controls.
   b. Increases employees' control consciousness.
   c. Early risk detection
   d. Solicits open communication, teamwork, and encourages continuous improvements.
   e. Empowers employees and improves accountability.
   f. Provides more on-hand information about risk and control processes, thus enables concentration on weak areas
4. **CSA Approaches** – There is a wide variety of approaches used for CSA processes. The approach used needs to be suitable for the unique characteristics of the organization:
   a. **Facilitated team** where work teams of different levels in the function hold discussions leading to a rough report. The report is then reviewed by the group. Such workshops may take several forms, as follows:
      i. **Risk-based format:** A comprehensive method whereby members considering all possible risks that may hinder goal achievement, assess related controls for effectiveness, and highlight residual risks.
      ii. **Control-based format:** Having the risks and controls already identified for them, team members in this type of workshop assess the effectiveness of the controls against management's expectations.

iii. **Process-based format:** Focuses on selected activities in processes. Members identify the objectives of, and aim at generally developing, the process and its component activities.

iv. **Objective-based format:** Focuses on determining the best way to achieve business objectives. Members examine the effectiveness of controls in supporting the objectives and then check the level of the residual risks for reasonableness.

b. **Questionnaire –** is another approach of CSA used in gathering information on risks and controls within the organization. Questionnaires typically include simple "yes-no" questions that are easy to understand. Questionnaires usually save time and money and ensure more honest feedback.

c. **Self-certification approach –** in this approach the internal auditors use the information gathered from managers' assertions about the state of internal controls within their units or functions. The internal auditors may synthesize these certifications with other information to enhance the understanding about controls and to share the knowledge with managers in business or functional units as part of the organization's CSA program.

5. The internal audit activity's role in the CSA program could range from owning the process (designing, implementing, etc.) to playing the role of consultant and verifying the final evaluations.

Internal Audit Roles in Risk Management

A. Responsibilities for Risk Management

1. As in governance and control processes, the **risk management** process is also an integral and ongoing **responsibility** of the organization's **senior management** and **the board**.

   a. **Senior management** is responsible for leading the establishment and administration of risk management and control processes. Senior management sets the tone at the top and should assume the responsibility and ownership of risk management and control. For management to achieve the organizational objectives, it ensures that sound risk management processes are in place and functioning. This includes:

      i. Determining how the risks are best managed.

      ii. Updating the organizational risk management processes based on risk exposures.

      iii. Designing controls to mitigate the identified risks.

   b. **The Board and audit committees** have a guiding and **oversight role** to determine that appropriate risk management and control processes are in place and that these processes are adequate and effective.

2. **Internal auditors** are responsible for providing objective assurance and consulting activities related to risk management and control. As consultants, internal auditors assist both senior management and the board by evaluating and providing assurance on the adequacy and effectiveness of management's risk and control processes. Internal auditors' role in risk management is covered in more details in the next pages.

Passing Tip:	Responsibilities in the Risk Management and Control Framework Responsibility ⇔ Management Oversight ⇔ Board or Audit Committee Assistance/Assurance (Consultancy) ⇔ Internal Audit Activity

B. **Internal Audit's Role in Risk Management** – Implementation Guide 2120 of the IPPF discusses the roles that the internal audit function is expected to undertake in risk management. It is summarized below:

1. **According to the Standards**

   a. The internal audit activity must **evaluate** the effectiveness and contribute to the **improvement** of risk management processes.

   b. The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

      i. Achievement of the organization's strategic objectives.

      ii. Reliability and integrity of financial and operational information.

      iii. Effectiveness and efficiency of operations and programs.

      iv. Safeguarding of assets.

      v. Compliance with laws, regulations, policies, procedures, and contracts.

   c. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by **actually managing risks**.

1. Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

   a. Organizational objectives support and align with the organization's mission.

   b. Significant risks are identified and assessed.

   c. Appropriate risk responses are selected that align risks with the organization's risk appetite.

   d. Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

2. In evaluating the organization's risk management, the internal auditors start by attaining a clear understanding of the organization's mission, vision, objectives, risk appetite, and the risks identified by management in order to assess whether the organization's objectives support and align with its mission, vision, and risk appetite.
    a. Understanding the organization's risk appetite enables the internal audit activity to conduct its own risk assessments and recommend risk responses consistent with the organization's risk appetite.
    b. The internal audit activity may consider using an established risk management framework (e.g., COSO-ERM or ISO 31000) to assist in risk management evaluation.
3. The internal audit activity should obtain sufficient information to evaluate the effectiveness of the organization's risk management processes and look for opportunities for improvement. The internal audit activity should alert management to new risks, as well as risks that have not been adequately mitigated, and provide recommendations and action plans for an appropriate risk response (e.g., accept, pursue, transfer, mitigate, or avoid).
4. The internal audit activity should understand how the organization identifies and addresses risks and how it determines which risks are acceptable. The internal audit activity will typically evaluate the responsibilities and risk-related processes of the board and those in key risk management roles.
5. **Evaluating Risk Responses** – In cases where management chooses to employ a risk mitigation strategy in response to identified risks, the internal audit activity should evaluate the adequacy and timeliness of the response by reviewing the control designs and testing the controls and monitoring procedures.
6. **Communicating Risk Information**
    a. Internal auditors should assess whether relevant risk information is captured and communicated timely across the organization. This can be accomplished by interviewing staff and determining whether the objectives, significant risks, and risk appetite are articulated sufficiently and understood throughout the organization.
    b. The internal audit should also assess whether the most significant risks are communicated timely to the board and whether the board is acting to ensure that management is responding appropriately.

7. **Communicating the Acceptance of Risks** – In reviewing risk management processes, if the CAE concludes that management has accepted a level of risk that may be unacceptable according to the organization's risk appetite, the CAE must discuss the matter with senior management. If the CAE determines that the matter has not been resolved, the CAE must communicate the matter to the board.
8. Finally, the internal audit activity should take the necessary steps to ensure that it is managing its own risks, such as audit failure, false assurance, and reputation risks. Likewise, all corrective actions should be monitored.

C. **The Three Lines of Defense Model** – The IIA have introduced a model to enhance the understanding of risk management and control processes by clarifying essential roles and duties in those processes. The following is a summary of this model.

The underlying premise of the Three Lines of Defense model is that three separate groups (or lines) within the organization are necessary for effective management of risk and control. The roles of each of the lines are:

- Own and manage risk and control (operating management).
- Oversee risk and control (risk management and compliance functions).
- Provide independent assurance concerning the effectiveness of management of risk and control (internal audit).

1. **The First Line of Defense: Operational Management** – Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives. The first line owns the risks, and the design and execution of the controls to respond to those risks. Senior management has overall responsibility for all first line activities.
2. **The Second Line of Defense: Risk Management and Compliance Functions** – The second line of defense includes various risk management and compliance functions put in place by management to help ensure controls and risk management processes implemented by the first line of defense are designed appropriately and operating as intended. Management establishes these functions to ensure the first line of defense is properly designed and operating.
    a. Typical functions in this second line of defense include:
        i. A risk management function that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.

ii. A financial control function that monitors financial risks and financial reporting issues.

iii. Compliance functions to monitor various specific risks, such as

- Information security
- Physical security
- Quality assurance
- Health and safety
- Compliance with applicable laws and regulations
- Legal
- Environmental

b. The responsibilities of these functions vary typically but can include:

i. Assisting management in the design and development of processes and controls to manage risks.

ii. Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.

iii. Providing risk management frameworks and training related to risk management and control processes.

iv. Identifying and monitoring known and emerging issues affecting the organization's risks and controls.

v. Identifying shifts in the organization's implicit risk appetite and risk tolerance.

c. Each of the second-line functions has some degree of independence from the first line of defense, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems. Therefore, the second line of defense serves a vital purpose but cannot offer truly independent analyses to the board regarding risk management and internal controls.

3. **The Third Line of Defense: Internal Audit** – Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives. Internal auditors provide the board and senior management with assurance based on the highest level of independence within the organization. This high level of independence is not available in the second line of defense.

a. The internal audit function typically does not perform management functions in order to protect its objectivity and organizational independence. In addition, it has a primary reporting line to the board. As such, the internal audit function is an assurance not a management function, which separates it from the second line of defense.

b. In order to contribute to effective organizational governance, the internal audit function must maintain its independence and professionalism by:

   i. Acting in accordance with recognized international standards for the practice of internal auditing.

   ii. Reporting to a sufficiently high level in the organization to be able to perform its duties independently.

   iii. Having an active and effective reporting line to the board.

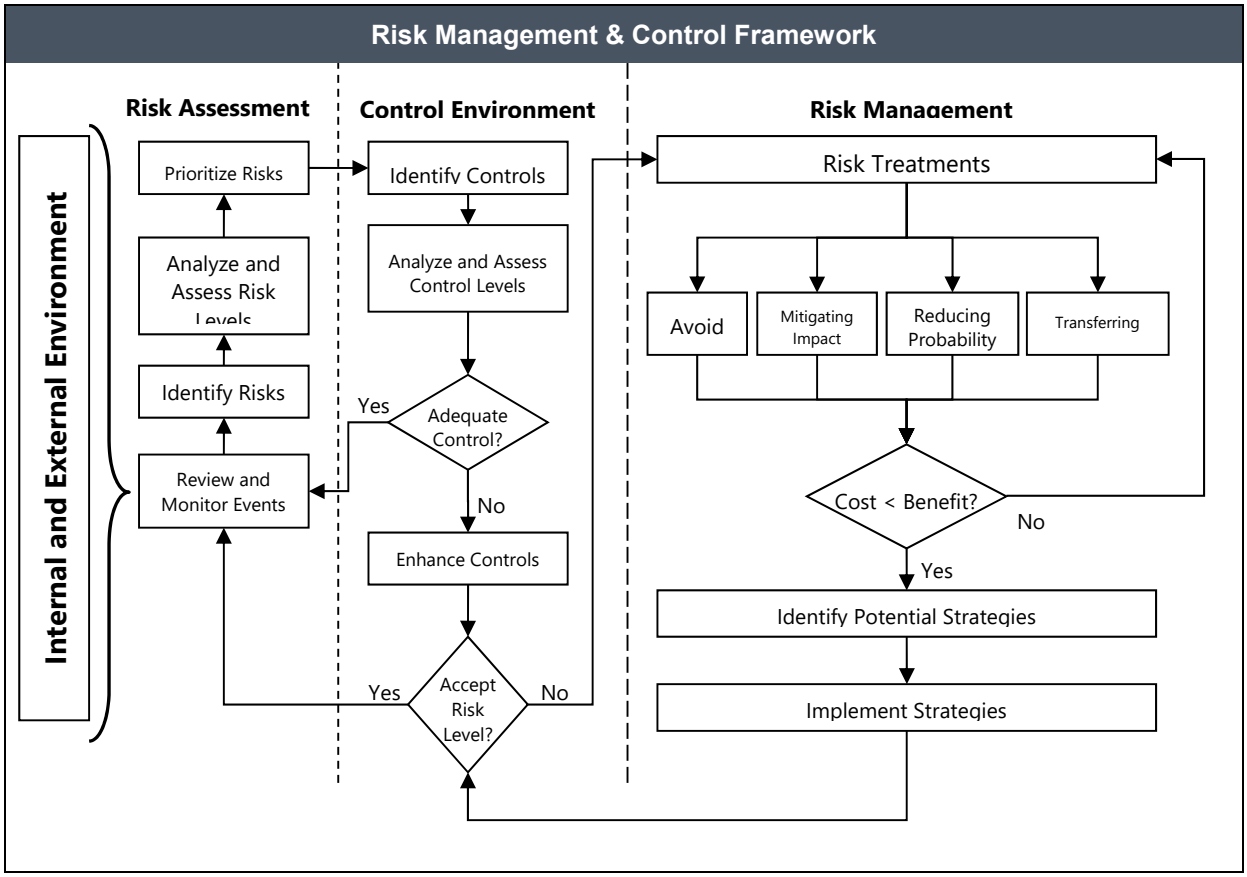
4. **Other External Bodies** – External auditors, regulators, and other external bodies can have an important role in the organization's governance and control structure. This is particularly the case in regulated industries, such as financial services or insurance.

   a. Regulators sometimes set requirements intended to strengthen the controls in an organization and on other occasions perform an independent and objective function to assess the whole or some part of the first, second, or third line of defense.

   b. When coordinated effectively, those external bodies can be considered as additional lines of defense, providing assurance to the organization's stakeholders, including the board and senior management.

Risk Management and Control Framework

Risk management and control are the core components of governance processes in any organization. The following diagram illustrates how risk management and control processes work together in addressing risks to provide reasonable assurance that the objectives of the organization will be achieved.



Section D: Internal Control

Learning Outcomes:

1. Interpret internal control concepts and types of controls. Proficiency Level.
2. Apply globally accepted internal control frameworks appropriate to the organization (COSO, etc.). Proficiency Level.
3. Examine the effectiveness and efficiency of internal controls. Proficiency Level.

A. Definitions

1. The following control related definitions are from the IPPF:
    a. **Control** (or internal control) is any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
    b. **Control Environment** is the attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:
        i. Integrity and ethical values.
        ii. Management's philosophy and operating style.
        iii. Organizational structure.
        iv. Assignment of authority and responsibility.
        v. Human resource policies and practices.
        vi. Competence of personnel.
    c. **Control Processes** are the policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

2. Another broadly accepted definition of control is the one introduced by the COSO Internal Control framework. As per COSO, internal control is defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    a. Effectiveness and efficiency of operations.
    b. Reliability of financial reporting.
    c. Compliance with applicable laws and regulations.
3. **Control Risk** refers to the risk that a control does not achieve the desired objectives.

B. The following are the key attributes of internal control. **Internal Control** is:

1. The actions taken to offset inherent risks and mitigate them or reduce these inherent risks to acceptable levels to increase the likelihood that the organization's objectives are met.
2. Primarily focused towards the achievement of organizational objectives at the various levels.
3. A process comprised of interrelated ongoing tasks and activities, and is considered a means to an end, rather than an end by itself.
4. Effected by people – it is not merely about policies and procedures' manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control.
5. Capable of providing "reasonable assurance" rather than absolute assurance to the entity's stakeholders. No system of internal control is 100% fault proof. Collusion of employees, management override, and/or cost/benefit restrictions on the design of the internal control system may lead to internal control risks.
6. A good system of internal control must have the "right" flexibility since too rigid may prove unpractical and not cost-effective, and too flexible may increase control risks. It must also be adaptable to the organization's structure.
7. The benefits of any internal control system must always be greater than its cost.

C. **Objectives of Internal Control (IC)**

Per the COSO Internal Control Framework, the objectives of IC may be grouped as follows:

1. **Entity Operations (Effectiveness and efficiency) Objectives –** referring to the entities' effectiveness and efficiency of operations including operational and financial performance goals, profitability goals and safeguarding assets (resources).

2. **Entity Reporting Objectives –** referring to the entity's internal and external published financial and non-financial reporting and may cover reliability, timeliness, transparency, and/or other terms as set forth by regulators, standard setters, or the entity's policies.
3. **Entity Compliance Objectives –** referring to the entity's adherence to all applicable laws and regulations.

D. **Importance of Internal Control**

1. A strong internal control system will provide many benefits to an entity including:
    a. Improving probability of achieving the objectives of the organization and minimizing surprises because internal control has a key role in the management of risks to the fulfillment of the organization's objectives,
    b. Promoting the efficiency and effectiveness of operations,
    c. Ensuring the reliability of internal and external reporting,
    d. Improving decision making based on more reliable information,
    e. Ensuring compliance with laws and regulations,
    f. Better control and protection of the entity's assets, and
    g. Lower audit (both internal and external) costs (via reliance on internal controls).
2. A weak internal control system exposes an entity to various exposures and risks including:
    a. Employee theft and losses,
    b. Loss of control over critical information relating to operations,
    c. Inefficiencies in operations,
    d. Scandals and failures,
    e. Poor decision-making; and/or
    f. A potential increase in audit fees as auditors may have to carry out their audit in a high substantive audit approach with minimal or no control reliance.

E. **Responsibility for Internal Control** – while internal control is the responsibility of every individual in an organization, ultimate responsibility for the establishment and the maintenance of the entity's internal control rests with senior management and the board of directors. Management must exercise its judgment to obtain reasonable assurance on an ongoing basis that its control objectives are being met in a cost-effective manner.

Control Classifications

There are several different classifications (types) of control activities based on when they occur within the activity being carried out and what their objective is.

A. Primary control classification:

1. **Directive Controls** are actions taken to cause or encourage a desirable event to occur. Directive controls ensure that there is a clear sense of direction and drive towards achieving the intended objectives.
2. **Preventive (proactive, steering, preliminary) Controls** are actions taken prior to the occurrence of transactions with the intent of stopping errors from occurring. They are controls that anticipate outcomes and maneuver the process to meet the desired objectives.
3. **Detective controls** are controls that identify errors after they have occurred.
4. **Corrective controls** correct the problems identified by detective controls.

B. Another way for classifying controls

1. **Feedforward Controls** (another term for preventive controls) involve anticipating and preventing problems before they occur**.**
2. **Monitoring (concurrent, screening) Controls** are designed to ensure the quality of the control system's performance over time. They provide ongoing monitoring of activities to prevent them from deviating too far from the standards.
3. **Feedback (reactive, post-action) Controls** improve future performance by analyzing past performance and learning from previous mistakes. These controls compare the results of a process with the acceptable standards to evaluate past performance and serve to eliminate future deviations.

C. Other types of controls

1. **Deterrent Controls** are controls that reduce the likelihood of a deliberate act to cause a loss or an error.
2. **Compensating Controls** are controls designed to compensate for shortcomings elsewhere in the control structure. They are controls that may be affected to offset the control risk i.e., if the original control fails and/or it is deemed too difficult or impractical to implement then compensating controls will attempt to achieve the desired objectives. For example, a security guard is at the entrance of the building to prevent unauthorized people from entering the building, however, additional controls are in place so that if an intruder manages to enter the building, they do not have the required access to enter any room and/or use the elevators. In this case, should someone manage to slip past the security guard, controlled access will compensate for that weakness by not allowing the intruder to proceed any further.
3. **Yes/No controls** are controls that match an activity to a pre-determined standard whereby only those activities that meet the standards are permitted to proceed.

D. **Manual vs Automated Controls**

1. **Manual controls** are controls that are conducted manually. For example, at a bank, a cash count is conducted at the end of each business day by both the cash custodian and a supervisor. Conducting the cash count on a daily basis is a control and is performed manually by the relevant employees.
2. **Automated controls** are controls that are automated and do not require employee intervention. For example, if a country is on an embargo list, and the company is not permitted to conduct any transactions with residents of that country, the company's online store may be programmed to detect IP addresses and deny any transactions with customers logging in from the IP addresses of that country.
3. **Partially automated (hybrid) controls** are a combination of both automated and manual controls. For example, when conducting a spell check on a document, the computer will automatically highlight potential spelling and grammar mistakes in the document but will allow the user to manually accept or reject the recommended changes for each highlighted error.

E. **Application Controls** are controls over business functions performed by a particular computer-based information system to ensure that the recording, processing, and reporting of data are performed as intended. Application controls include the following primary three types (covered in detail later):

1. **Input controls** are techniques and procedures used to validate, verify, and edit data to ensure that only authorized and correct data are input into the system for processing.
2. **Processing controls** are procedures to provide reasonable assurance that data input is processed as authorized and master files are updated in a complete and accurate manner.
3. **Output controls** are controls to ensure that output from the information system are accurate, complete, and distributed only to authorized individuals.

F. **Entity-Level and Activity-Level Controls**

1. **Entity-Level Controls** are designed to provide assurance that objectives of the entity as a whole are met. Examples of such controls include oversight performed by the board of directors over senior management performance, or the existence and proper communication of financial reporting policies and procedures in the entity.
2. **Activity-Level Controls** relate to a particular class of transactions. Examples include segregation of accounts payable transaction processing from bank reconciliations or requiring that the person authorized to initiate a payment to a vendor is not also authorized to sign vendor payment checks.

G. Hard Controls and Soft Controls

1. **Hard Controls** are controls that directly change employees' behavior or actions. Hard controls are tangible and objective in nature and therefore can be clearly observed and tested. Examples of hard controls include organizational structure, delegation of authority and responsibility, reconciliations, human resources policies, segregation of duties, and physical security controls.
2. **Soft Controls** are controls that indirectly influence employees' motivation, loyalty, integrity, and values. Soft controls are intangible and subjective in nature and therefore are difficult to be observed and tested. Examples of soft controls include morale, integrity, ethical climate, openness, and shared values. In the COSO framework, the control environment factors include soft controls.
3. The importance of soft controls has increased with the advances in technology. Technology has empowered lower employees and made organizations much looser and freer which increased the need for more efficient control systems. Soft controls are the foundation of efficient and stronger hard controls. Soft controls influence individuals' behavior and ensure compliance with hard control procedures.

H. The following table summarizes the most important types of controls along with examples on each type:

Classification	Description	Examples
Directive Controls	– Cause desirable events to occur. – Ensure there is a clear sense of direction towards objectives.	– Clear policy and procedure manuals. – Employee training
Preventive Controls	– Avoid the occurrence of an unwanted event. – Prevent an error, omission, or negative act from occurring. – Controls that are designed to predict potential problems before they occur. – Preventive controls are more preferred than detective controls because the benefits typically outweigh the costs.	– Segregation of duties, (which is covered in more detail later in this section). – Employ only qualified personnel. – Control access to physical facilities. – Use well-designed documents to prevent errors. – Establish suitable procedures for authorization of transactions. – Use access control software that allows only authorized personnel to access sensitive files.
Detective Controls	– Detect (discover) the occurrence of an unwanted event. – Controls put in place to detect or indicate that an error or a bad thing has happened. – Controls intended to back up preventive controls by detecting errors after they have occurred. – Detective controls complement preventive controls and are essential components of a well-designed control system.	– Reconciliation of bank statements is an example of a detective control over cash assets. – Check points in a production job. – The Internal Audit function. – The analysis of periodic performance reports with variances. – The analysis of past-due account reports.
Deterrent Controls	– Controls that reduce the likelihood of a deliberate act to cause a loss or an error.	– Barriers or warning signs.

Corrective Controls	– Correct an undesirable event that has already occurred. – Minimize the impact of a threat. – Enable a risk or deficiency to be corrected before a loss occurs. – Identify the cause of a problem. – Remedy problems discovered by detective controls. – Modify the system(s) to minimize future occurrences of problems.	– A check subroutine that identifies an error and makes a correction before enabling the process to continue. – Contingency planning. – A backup procedure. – Fire appliances and extinguishers. – Requiring that all cost variances beyond a certain amount be reviewed and justified.
Monitoring Controls	– Monitor the performance and quality of the internal control system over time. – They ensure regular functioning and attempt to identify loopholes and/or to optimize the performance of controls.	– A shift supervisor touring over the cubicles of tellers during rush hour monitors that tellers are performing their work as should be. – A pilot during the cruising phase of a flight regularly monitors all the readings to ensure that the auto-pilot is functioning as intended.
Feedback Controls	– Feedback controls provide timely feedback on the entity's operations allowing managers to discover, investigate, and learn from past issues.	– Financial reporting including financial statements may be considered feedback controls. – Customer service satisfaction surveys and employee performance metrics/reports. – Budget variance analysis report providing feedback on the sources and potential causes of budget variances.
Compensating Controls	– Controls that indirectly mitigate a risk or the lack of controls directly acting upon a risk. – Designed to compensate for shortcomings elsewhere in the control structure.	– Bank reconciliation process performed by a party who is independent of accounts payable can compensate for a number of flaws in the controls over these types of transactions.

Limitations of Internal Control

The internal control system cannot be designed to provide absolute assurance that the objectives of an organization will be achieved. Instead, it can only provide reasonable assurance. That is because of the inherent limitations in internal control systems. These limitations should be considered when assessing the efficiency and effectiveness of internal control systems. They include:

A. **Management Override** – Senior manager may have the authority to override some control procedures for legitimate or illegitimate purposes. In fact, many of the financial scandals in the last decade involved management overriding controls in order to commit financial statement fraud (window dressing). In order to enhance the effectiveness of the internal control system, any decision involving control override should be documented and formally authorized at the appropriate level in the organization. In general, control override should be discouraged.

B. **Resource Limitations** – The design of an internal control system is restricted by the rule that the benefits of controls must outweigh their costs. Proper authorization, segregation of duties, independent checks, and supervision can suffer where there is insufficient staff or resources to perform those controls. Adequate management trail may compensate in such circumstances as it enables determining who initiated a transaction for later reviews.

C. **Collusion** – Control systems can be circumvented by employee collusion. For example, two or more employees who are intended by the system of internal control to check over each other's activities can instead collude to circumvent the system for personal gain.

D. **Incorrect Judgment** – Many business decisions are based on professional judgment and the information at hand. Judgment also applies to those decisions related to the designing and implementation of the internal control system. Professional judgments may sometimes be incorrect. Therefore, the effectiveness of the control system will be limited by the quality of judgments and the information available.

E. **Human Errors** – The people responsible for operating the internal control system may simply make mistakes and errors that threaten the effectiveness of the system.

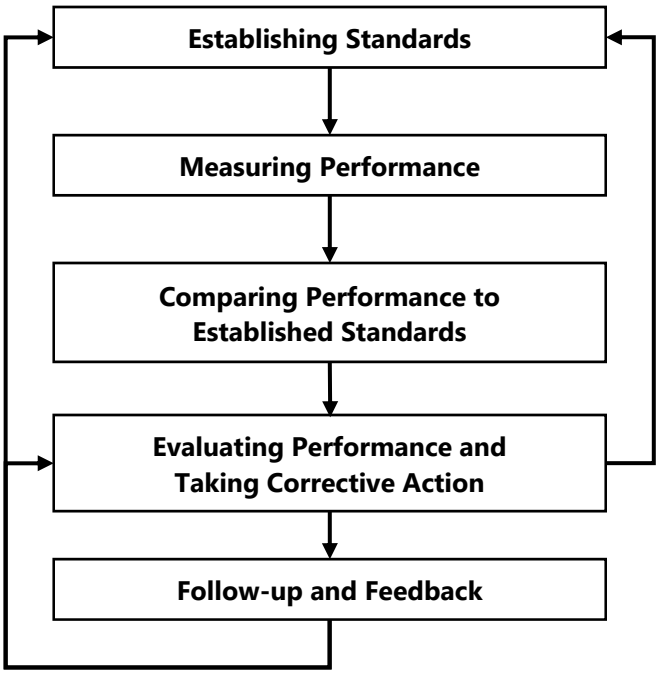
Passing Tip:	It should be noted that effective systems of internal control are most likely to detect an irregularity perpetrated by a single employee. Detection of irregularities resulting from collusion of a group of employees or a management position may be more difficult since collusion of employees allows them to successfully perpetrate the control systems and managers are able to override existing controls.

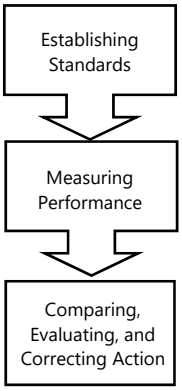
Control Process

A. Control system refers to the integrated collection of control components and activities that are used by an organization to achieve its objectives and goals. An effective control system requires feedback on the results of the organization's operations for the purposes of measurement and correction

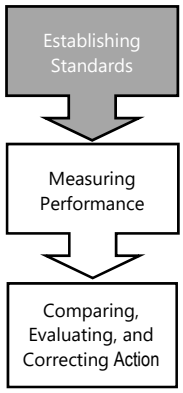
B. The control process is a continuous process that includes:

1. Establishing standards for the activity to be controlled.
2. Measuring performance against the established standards.
3. Comparing performance to the established standards and analyzing deviations.
4. Taking corrective actions.
5. Monitoring the process and reevaluating the standards based on experience.





Establishing Standards

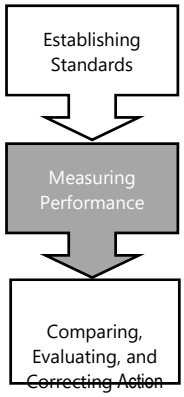


A. Standards should be specific goals and/or objectives against which performance is compared. Standards may be for:
   1. Time
   2. Cost
   3. Quantity
   4. Quality

B. Standard setting improves productivity and cost control.

C. Characteristics of an **effective standard-setting system** include:
   1. **Goal congruence** or the alignment of organizational objectives with individual and departmental goals.
   2. Standards set must be **attainable**.
   3. **Acceptance** by employees as being fair and achievable.
   4. Standards must achieve the "right" **tightness**:
      a. Tight standards may improve employee productivity and motivation
      b. Standards that are perceived as difficult or impossible to attain may have adverse consequences.
   5. **Flexibility** including a range of performance for combinations of factors rather than static or absolute limits for performance.
   6. Standards must be **relevant** especially in changing environments.
   7. Standards should be regularly **updated** to reflect changes in the organization.
   8. Standards should be affected at points before significant progress takes place. Thus, the selection of points where performance is measured is critical. Standards may not be implemented for every aspect of the production process because:
      a. The process needs to be cost-effective.
      b. Excessive control reduces employee morale.
      c. Performance measurement should be relevant to the required objectives.
      d. Excessive standards would create an overload for supervisors to follow-up on.

Measuring Performance



A. Measuring performance should be an ongoing activity.

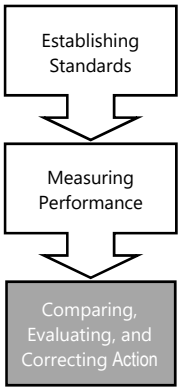
B. Selecting valid and appropriate performance measures under the circumstances is a requirement for effective controls.

C. Measurement of activity needs to be carefully selected as comprehensive measurement is not feasible.

D. Should be performed after special considerations to behavioral aspects:

   1. Who does the measuring?
   2. What is measured?
   3. Second party measures need to be carefully implemented to avoid resistance and hostility by employees.
   4. When to use self-measurement?
      a. Self-measurement may have its benefits in building confidence and improving the learning process.
      b. Self-measurement may have negative aspects if concealment of information, or delayed reporting occurs.

Comparing, Evaluating, and Correcting Performance



A. Comparing performance should be made to the related standards. Any change in the process may result in comparing performance to inapplicable standards.

B. Deviations or variances from standards should be evaluated and corrected in a timely manner.

C. Evaluation should be made after a thorough review of the applicable process and standards.

D. Corrective action should be constructive rather than destructive.

E. Employee participation in the control systems allows for cooperation and better acceptance of the standards and the control system as a whole.

Control Mechanisms

Control Mechanisms are those procedures or activities that help ensure that operations are within the acceptable boundaries set by management. They are the means by which control is achieved. There are three principles relating to control mechanisms:

- The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
- The entity selects and develops general control activities over technology to support the achievement of objectives.
- The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.

Each control framework approaches control from a different perspective, but most of them encompass the mechanisms discussed below.

A. Organizational Structure

1. Organizational structure refers to the relationships (formal or informal) between individuals in an organization. Different organizational structures will have varying risk/control implications. Generally, a more structured organizational structure will be least flexible, yet least risky with high levels of control (the army is the typical example). On the other end of the continuum, a flat free-reign organizational structure will be extremely flexible, yet risky and with relatively lower levels of control.
2. Organizational structure provides the framework within which activities to achieve organizational objectives are planned, executed, controlled and monitored. It defines key areas of authority and responsibility and establishes appropriate reporting lines.
3. The organizational structure depends in part on the organization’s size and nature of activities.
4. The appropriateness of an organizational structure depends on the circumstances but should be able to provide the necessary information flow to manage activities.
5. The positioning of the internal audit within an organization, including the functional and administrative reporting lines, will reflect on the appropriateness of organizational structure from a control perspective.
6. Individual responsibility should be clearly defined.
7. Job descriptions and job analyses should accurately define tasks for particular jobs and determine the skills to perform them.

B. Delegation of Authority and Assignment of Responsibility

1. The delegation of authority, assignment of responsibility, and the establishment of reporting relationships and authorization protocols all reflect on the control environment of an organization.
2. Employees need sufficient authority to perform their jobs, yet, they also should be held responsible for their actions or any abuse pertinent to their authorized duties.
3. Responsibility and authority should always be matched. An officer should not be responsible for areas beyond his authority.
4. Authorities should be divided so that no one individual will control all phases of any transaction (this will be discussed further in Segregation of Duties).
5. The more important the transaction, the higher the level of authority needed to approve it.
6. The limits of authority and the degree to which individuals and teams are encouraged to exercise initiative in decision-making and problem solving depend on the organization, its culture, its values, its employees, and its activities.

C. Board of Directors or Audit Committee

1. The functioning and active involvement of an independent body in the management of the company sets the tone from the top and reflects directly on the control environment of the organization.
2. The following attributes of the board/committee and its members are considered when assessing the control environment of an organization:
    a. Attitude towards controls and risks including the risk appetite (the risk levels that the board/audit committee consider appropriate) and the sufficiency and timeliness with which the board or audit committee acted upon improper acts and dealt with difficult/sensitive situations.
    b. Independence from key decision makers and the absence of actual or potential conflicts of interest with the organization and its operations.
    c. Knowledge and experience of its members in controls and governance.
    d. Stature and involvement of the members including frequency and timing of meetings with the CFO, accounting officers, internal auditors and external auditors.

D. Management’s Philosophy and Operating Style

1. Management’s attitudes and operating style affect the way the organization is managed including what constitutes acceptable and unacceptable behavior in addition to their risk appetite.
2. The operating style and control consciousness of management would also be reflected in the attitude toward financial reporting, selection of accounting practices, and attitude toward data processing, accounting functions, and personnel.

3. Other factors that reflect on management's control consciousness include the means of control over operations, the use of budgets, standards, attention paid by management to various control aspects, and attitude of management towards internal and external auditors.
4. Management's interaction with its own personnel including frequency and means of interaction will reflect on the overall control environment. For example, more involvement with company personnel, an open-door policy, and more interaction with remote offices all positively reflect on the organization's control environment.

E. **Management's Integrity and Ethical Values**

1. Management sets the tone of the organization as management should create a control environment in which people are motivated to comply with controls. The ultimate responsibility for control rests with management.
2. Integrity and ethical values of an organization start with top management by reflecting integrity and commitment to ethical values.
3. The integrity and ethical values of top management impact the design, administration, and monitoring of other internal control components since the design of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them.
4. The following are examples of practices that reflect good management integrity and ethical values:
    a. Sound and profitable business practices that set realistic performance targets rather than concentration on bottom-line sales or profits at any cost.
    b. Formal codes of conduct that communicate the organization's expectations along with necessary communication channels and monitoring.
    c. Management actions and examples that demonstrate integrity and commitment to ethical values.

F. **Human Resource Policies and Practices**

1. Human resource policies and practices encompass many practices such as recruiting, hiring, orientation, training, performance evaluation, promotion, compensation and disciplinary actions. They send messages to staff regarding expected levels of integrity, ethical behavior and competence.
2. Good policies and practices that emphasize control include:
    a. Recruiting practices that provide insightful information about the entity's history, culture and operating style as well as realistic job previews.
    b. Recruiting only people with the required qualifications for their duties.
    c. Conducting background checks of new hires especially with respect to honesty and reliability.
    d. Providing employees with the necessary training and necessary tools enabling them to do their jobs.

e. Proper supervision at all levels.

f. Periodic performance appraisals and a commitment to promoting qualified personnel to higher levels of responsibility.

g. Disciplinary actions reinforcing that violation of expected behavior will not be tolerated.

h. A well-structured compensation system that is perceived as fair and objective by the employees. An unfair compensation system will cause talent drain, and/or create motives for employee fraud. An aggressively generous compensation system may also motivate employees to commit reporting fraud to meet aggressive objectives and receive generous commissions and bonuses.

G. **Policies**

1. By definition, policies are stated rules or principles that guide or restrict actions.
2. An effective set of policies would have the following attributes:
   a. Clear
   b. Concise
   c. Written
   d. Available in an organized manner (in handbooks or online)
   e. Communicated to the users (explained to the users, and the users' understanding should be gauged and confirmed.
   f. Conforms to applicable laws and regulations.
   g. Promotes conduct in an effective and efficient manner.
   h. Regularly reviewed and updated.

H. **Procedures** by definition are instructions in a certain way or order for conducting an activity. They are the detailed instructions to execute activities in a particular manner that conform to the organization's policies. For stronger control, procedures should:

1. Allow for sufficient segregation of duties so that one person's work is checked by an independent party in a timely manner. When cost/benefit relationships do no hold if duties are segregated, then preventive controls (such as employee background checks and training) and feedback controls (such as independent checks/reconciliations) should be in place to compensate for the lack of segregation of duties.
2. Procedures should have the "correct" tightness. Too strict procedures might hinder creativity and use of judgment, while lack of sufficient procedures may affect quality and the consistency.

3. Successful procedures are those that are efficient yet effective while not overlapping, conflicting, duplicative, and/or complicated. Simple procedures allow for employees to easily understand and implement them successfully.
4. The systems and related procedures should regularly be reviewed and updated to ensure they are concurrent with current risks, technologies, and current business operations.

I. **Compliance with Applicable Laws and Regulations**

1. An organization is required to follow many laws and regulations that are imposed upon it externally. The organization should establish internal controls in the form of policies, plans, and procedures to ensure planned, systematic, and orderly operation.
2. Failure to comply with such controls jeopardizes the firm's compliance with the associated laws and regulations.
3. Some of the key laws and regulations that are overreaching in the USA include the Foreign Corrupt Practices Act (FCPA) and Sarbanes-Oxley Act (both are discussed in this section).

J. **Budgeting**

1. A comprehensive budgeting process significantly contributes to the organization's internal control and is best when participatory.
2. Departmental budgets should contribute towards goal congruence. When one department meets its budgets, it will contribute towards the overall achievement of organizational goals.
3. Good budgets must set reasonably achievable and measureable objectives. When the budgets are perceived as too farfetched, managers and employees will be demotivated.
4. When set correctly, budgets contribute to performance evaluations of employees and business units.
5. Budgeting is both a steering and preventive control. It allows management to plan the efficient allocation of its scarce resources. By setting the goals in advance, budgets map the goals, the path, and the direction that a company should strive to achieve.
6. Budgets allow for cost control on both the overall firm level and on each department/managerial level. The budget sets the limits of spending and thus minimizes the potential for overspending.
7. Regular comparisons of actual numbers to budgets serve as a monitoring control.
8. Period end investigations of variances from budgets serve as feedback controls to highlight areas that were either incorrectly budgeted and/or areas that did not operate as intended.

K. Accounting

1. Accounting measures the transactions and events that the company engaged in.
2. Accounting mirrors in quantitative terms the real state of the company's operations, and thus accurate accounting will reflect the true situation of the company and contribute to management's control whereas inaccurate, incomplete, and/or untimely accounting will not reflect the true state of the company and thus management will not have sufficient tools to exercise its managerial control responsibilities.
3. It is usually challenging to determine which numbers to measure, how to measure them, and when to measure them.
4. Proper accounting would:
    a. Focus on substance over form (i.e., what the true nature of the transaction is rather than how it was recorded),
    b. Identify controllable costs separately,
    c. Be based on responsibility lines, and
    d. Meet the cost/benefit constraint.
5. Accounting systems facilitate stronger controls when:
    a. The accounting function has well-structured systems using the various controls to ensure accurate, timely, and objective capturing of transactions and events.
    b. The accounting system is structured in a manner that would group activities along responsibility lines.
    c. The accounting process is subject to various checks and balances that minimize the chances of errors or intentional misleading information.
    d. Adequate segregation of duties is maintained between the initiator of the transaction, the person authorizing it, the accounting for it, and the custodian of any related assets.
    e. Regular reconciliations and confirmations are done on the recorded accounting numbers.
    f. Regular rotation of duties is done for sensitive positions.

L. Reporting

1. Budgeting and accounting are incomplete without the reporting process. Efficient, timely, accurate, and meaningful reports are needed by management for their decision-making process and for the overall control process.
2. Reporting should be done on a need to know basis i.e., report information to the extent that users need it to perform their duties.
3. Reporting should highlight exceptions.

4. Reports should be done to those within the organization that are capable of acting on the reports and any exceptions noted.
5. Recent trends have highlighted that reporting is becoming a burden on managers because of the volume and frequency of reporting. This is also affecting the quality of reports since valuable information becomes submersed in piles of reports that are not meaningful. The reporting process should therefore ensure that only useful reports are generated by regularly evaluating the reporting.

M. **Information and Communication**

1. Information and communication are the means by which transactions are recorded, processed, and reported in a timely and useful manner. Effective communication occurs in all directions (top-down, bottom-up, and across).
2. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal with internally generated data and with information about external events, activities and conditions necessary to informed business decision-making and external reporting.
3. Communication must be effective and must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There are also needs to establish effective communication with external parties, such as customers, suppliers, regulators and shareholders.
4. The three principles relating to information and communication are:
    a. The entity obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
    b. The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
    c. The entity communicates with external parties regarding matters affecting the functioning of other components of internal control.
5. To be effective, the information and communication system must accomplish the following goals for transactions:
    a. Identify and record all valid transactions.
    b. Describe on a timely basis,
    c. Measure the value properly,
    d. Record in the proper time period,

e. Properly present and disclose,

f. Communicate responsibilities to employees.

N. **Performance management**

1. The performance measurement and management system are another key control that will control the risk of poor performance and inefficiency. A well-structured performance system provides assurance that the organization is doing the right things at the right time and cost.
2. Performance management system should:
   a. Measure the output against fair and clearly defined standards.
   b. Be integrated with the risk management and control systems.
   c. Be reliable, flexible, and accepted by all participants.
   d. Reflect authority and accountability.
   e. Be based on the organization's culture, values, vision, and objectives.
   f. Be based on timely, reliable, and comparable information.
   g. Encourage compliance with applicable laws, regulations, and the control system.

O. **Monitoring**

1. Monitoring relates to the procedures established to assess the quality of the performance of internal control over time.
2. Monitoring may be in the form of periodic evaluations and/or as an ongoing management task with internal control deficiencies reported to higher levels of management, and serious matters reported to the highest level of management and the Board.

P. **External Audit**

1. The management is typically responsible for maintaining a system of internal control (design, implementation, maintenance, and monitoring) within an organization and to prepare regular reports to stakeholders. They are typically responsible for the preparation and fair presentation of financial statements that are reasonably free from material misstatements, whether due to error or fraud.
2. External parties require some form of assurance about management's assertion that the financial statements are prepared and presented fairly in accordance with the relevant financial reporting framework (typically the US GAAP in the United States of America and IFRS in countries that have adopted IFRS). However, as the financial reports are prepared by management, external parties require an independent party that is impartial and unbiased to provide assurance on the financial statements, and therefore, the appointment of an external auditor is required.

3. The external auditor must be an independent party, licensed in the jurisdiction as a public accountant. The auditor is typically appointed by a company's audit committee or Board of Directors to provide an opinion on the financial statements based on an audit conducted in accordance with the relevant auditing standards (the Generally Accepted Auditing Standards (GAAS) in the United States of America, and the International Auditing Standards in countries that have adopted them).
4. A financial audit is an audit of the firm's financial statements. The objective of a financial audit is to determine whether the overall financial statements fairly represent the firm's operations and financial condition. The auditor may conduct an audit of financial reports for a department or a segment of a department. The audience for a financial audit is the board of directors and senior management.
5. In the United States of America, public companies are also required to have their external auditor report on internal controls under Public Company Accounting Oversight Board (PCAOB) that was created by the Sarbanes-Oxley Act of 2002. In reference to the PCAOB Auditing Standard No. 5: "An Audit of Internal Control Over Financial Reporting That Is Integrated With An Audit of Financial Statements". This standard establishes requirements and provides directions that apply when an auditor is engaged to perform an audit of management's assessment of the effectiveness of internal control over financial reporting ("the audit of internal control over financial reporting") that is integrated with an audit of the financial statements.
6. Effective internal control over financial reporting provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes. If one or more material weaknesses exist, the company's internal control over financial reporting cannot be considered effective.
7. The external auditor's main objective in an audit of internal control over financial reporting is to express an opinion on the effectiveness of the company's internal control over financial reporting.
8. Internal controls of an entity cannot be considered effective if one or more material weaknesses exist. To form a basis for expressing an opinion, the external auditor must plan and perform the audit to obtain appropriate evidence that is sufficient to obtain reasonable assurance about whether material weaknesses exist as of the date specified in management's assessment. A material weakness in internal control over financial reporting may exist even when financial statements are not materially misstated.
9. **Audit Risk** refers to the auditor risk that an auditor may unwittingly fail to modify his/her opinion on materially misstated financial statements. Audit risk is the product of three components:

Audit risk = Inherent risk x Control risk x Detection risk

a. **Inherent Risk (IR)** is the susceptibility of a financial statement assertion to material misstatement in the absence of related controls. IR is greater for some assertions than for others, e.g., cash has a greater inherent risk than property, plant, and equipment.

b. **Control Risk (CR)** is the risk that a possible material misstatement of an assertion will not be prevented. This risk depends on the effectiveness of the design and operation of those controls or detected by the related controls in a timely manner.

c. **Detection Risk (DR)** is the risk that a material misstatement of an assertion will not be detected by the auditor, for example, because the auditor merely sampled the account balance or class of transactions, selected an inappropriate audit procedure, misapplied an audit procedure, or misinterpreted the audit results.

10. Auditors must maintain audit risk within acceptable limits, and the only risk within their control is detection risk i.e., to reduce detection risk, the auditor would do more audit work. Therefore, when an auditor is faced with situations that have high inherent risk and/or high control risks, the auditor would tend to conduct more audit work to maintain the overall audit risk within acceptable limits.

Q. **Internal Audit**

1. By definition, internal audit is designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

2. Therefore, internal audit is a control mechanism that can be utilized in the internal control system of an organization. The role of internal audit in control will be discussed in the following pages.

R. **Safeguarding assets**

3. The objective of safeguarding assets requires that access be limited to authorized personnel only. Access includes both direct physical access and indirect access through the preparation or processing of documents that authorize the use or disposition of assets.

1. Examples of controls to safeguard assets:

a. The various means of segregation of duties.

b. The use of cash registers, establishment of a lockbox system for collecting cash receipts from customers, e.g., direct deposit in a bank, intact deposit of daily receipts, and custody of cash by the treasury function.

c. Controls to prevent improper granting of credit, approval of credit memos by persons other than sales agents, and approval of write-offs of uncollectible by a person independent of the credit manager or the accounts receivable function.

d. Use of sequentially pre-numbered documents accounted for by an independent third party to permit detection of unrecorded and unauthorized transactions.

e. Requiring proper documentation, that is, purchase order, supplier's invoice, and receiving report, before authorization of payment for goods received; and cancelation of vouchers and supporting documents to prevent duplicate payments.

f. Preparation of payroll from time cards approved by line supervisors; distribution of paychecks by the treasury function, not line supervisors; and custody of unclaimed checks by an independent party.

g. Custody of securities by the treasury function, the presence of at least two authorized persons when the safe deposit box is opened, recording and reconciliation of identifying information about securities, and registration in the name of the owner.

h. Controls over excess use of materials in production; custody of inventories by the storekeeper, with proper documentation of transfers; and perpetual inventory records.

i. Restriction of access to property, plant, and equipment and periodic inspections by internal auditing.

j. The controls over computer processing.

k. Physical measures taken to protect assets from natural disasters (e.g., floods, wind damage, or earthquakes).

2. Reconciliation of recorded accountability with assets

a. The purpose of comparing recorded accountability with assets is to determine whether the actual assets agree with the recorded accountability.

b. Examples of this comparison include cash and securities counts, bank reconciliations, and physical inventories.

c. A comparison revealing that the assets do not agree with the recorded accountability provides evidence of unrecorded or improperly recorded transactions.

d. When assets are susceptible to loss through errors or fraud, the comparison with recorded accountability should be made independently.

e. An independent reconciliation or check, performed by someone other than the person responsible for the initial preparation, increases the likelihood that the control will be effective because, in the absence of collusion, the same person will not be in the position to perpetrate and conceal an error or fraud in the course of his/her normal duties.

f. The reconciliation frequency for the purpose of safeguarding assets depends on the nature and amount of the assets involved and the cost of making the comparison.

g. For example, it may be reasonable to count cash daily, but not reasonable to take a physical inventory at that interval. However, a daily inventory of products in the custody of route salesmen, for example, may be necessary as a means of determining their accountability for sales. Similarly, the value and vulnerability of some products may make frequent complete inventories worthwhile.

S. Segregation of Duties

1. Segregation of duties is an internal control which intends to prevent fraud and errors by having more than one person complete a task. If one person is able to complete a task, he/she will be in a position enabling him/her to conceal an error or fraud. For example, one person should not have the authority to hold cash and account for it. As a result, the following tasks should be segregated:

   a. Authorizing a transaction.

   b. Recordkeeping: Recording the transaction, preparing source documents, maintaining journals.

   c. Keeping physical custody of the related asset: For example, receiving checks in the mail.

   d. The periodic reconciliation of the physical assets to the recorded amounts for those assets.

2. Segregation of duties does not guarantee that fraud will not occur; two or more employees could collude with one another to commit fraud, covering for one another and benefiting from the proceeds.

3. Examples of the application of segregation of duties in various cycles include:

Cycle	Segregation of Duties Application
Production cycle	– Separating the functions of planning production and inventory levels, inventory custody, inventory recording, cost accounting, and reconciliation of materials requisitions to production reports.
Payroll cycle	– Separating the functions of authorization of pay rates and deductions, hiring and termination of employees, payroll preparation, check distribution, and reconciliation of checks cut and cleared to the payroll register and HR records.
Sales-receivables cycle	– Separating the functions of authorization of customer credit levels, authorization of a sale to a customer, custody of product, custody of cash, record keeping, and reconciliation of accounts receivable records to cash receipts. – One staff has authority to adjust accounts receivable, while a different staff posts payments on customer accounts. Without segregation here, one staff could divert cash receipts and then falsify the account balances of the customers who paid the cash in order to conceal the diversion. – One staff has custody of cash receipts, while a different person has the authority to authorize account write-offs. Without segregation, one staff could authorize a false write-off while diverting the collection on the account. – One person is responsible for preparing the bank deposit, while a different person reconciles the checking account. Without segregation, one person could divert cash receipts and cover the activity by creating “reconciling items” in the account reconciliation.
Purchases-payables cycle	– Separating the functions of the initiation of a purchase, receipt and checking in of the merchandise, authorization to pay the vendor, custody of the merchandise, record keeping for the merchandise, and verification that the amounts of the merchandise on hand match the amounts in the books. – One person authorizes issuance of purchase orders, while a different person is responsible for recording receipt of inventory. Without such segregation, one person could issue a purchase order to a fictitious vendor using a rented post office box, then prepare a fictitious receiving record and mail an invoice to the company using a post office box personally rented for that purpose, resulting in the company’s paying for something it never ordered or received.

4. In an information system environment, segregation of duties is a key control to minimize exposure to potential IS related risks. The various IS functions in an organization need to be structured in a manner that achieves the proper segregation of duties. This helps reduce the potential damage from the actions of one person.
5. Separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code or data without detection.
6. Role based access control is frequently used in IT systems where segregation of duties is required. Strict control of software and data changes will require that the same person or function perform only one of the following roles:
    a. Identification of a requirement (or change request) e.g., user.
    b. Authorization and approval e.g., an IT steering committee or IT manager.
    c. Design and development e.g., a developer.
    d. Review, inspection and approval e.g., another developer or architect.
    e. Implementation in production e.g., typically a software change or system administrator.
7. To successfully implement segregation of duties in IS, the followings need to be addressed:
    a. The process used to ensure a person's authorization rights in the system is in line with his/her role in the organization.
    b. The authentication method used, such as knowledge of a password, possession of an object (key, token) or a biometrical characteristic (fingerprint).
    c. Circumvention of rights in the system can occur through database administration access, user administration access, tools which provide back-door access, or supplier installed user accounts. Specific controls such as a review of an activity log may be required to address this specific concern.
8. Depending on the organization's size, if its functions and duties cannot be separated, compensating controls should be in place. (Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness). There are several control mechanisms that can help to enforce the segregation of duties:
    a. **Audit trails** – these enable IT managers or auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. Good audit trails should be enabled to provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.

b. **Reconciliation** of applications whereby an independent party verifies that the applications running are those that are authorized to run. This is achieved by ensuring the authorized and tested applications are running with only the approved modifications/additions.

c. **Exception reports** are handled at supervisory level, backed up by evidence noting that exceptions are handled properly and in timely fashion. A signature of the person who prepares the report is normally required.

d. **Manual** or **automated** system or application transaction **logs** should be maintained, which record all processed system commands or application transactions.

e. **Supervisory review** should be performed through observation and inquiry.

9. Below is an example of the application of segregation of duties in IT systems. The key functions (Roles) that need to be segregated in IT systems are:

Function (Role)	Description
Programming	Responsible to write, test and document computer software. They are able to modify programs, data files and system controls. This group should not have access to the computers and programs that are in actual use for processing.
Operations	Responsible to run the computer systems, ensuring that the machines and computers are running properly in the organization (The computer operator normally works in a server room or a data center). The role also includes maintaining records and logging events, listing each backup that is run, each machine malfunction and program abnormal termination. This group should not have programming functions and should not be able to modify any programs.
Data Administration	Responsible for the installation, configuration, upgrading, administration, monitoring, maintenance, and security of databases in an organization. The role includes the development and design of database strategies, system monitoring and improving database performance and capacity, and planning for future expansion requirements. They may also plan, co-ordinate and implement security measures to safeguard the database This group should be **independent of computer operations.**
Systems Analysis	Responsible to analyze, design and implement information systems. System analysts assess the suitability of information systems in terms of their intended outcomes and liaise with end users, software vendors and programmers. This group should be independent of the programmer and computer operations groups.

Information Technology Controls

There are several layers of control for information systems' protection. The following is the outline for IT controls that will be covered in detail in Domain-II of Part-3 in accordance with the IIA Exam Syllabus.

A. Systems Controls
B. General Controls
    1. Access controls – Physical access and environmental controls
    2. Access controls – Logical access controls
    3. Hardware controls
    4. Program development and documentation controls
    5. Organizational and operational controls
C. Application Controls
    1. Input controls
    2. Processing controls
    3. Output controls
    4. Integrity controls
    5. Audit trail
D. Data Transfer Controls
E. Database Controls
F. Network Controls

Foreign Corrupt Practices Act (FCPA)

A. A public corporation that must meet the provisions of the Foreign Corrupt Practices Act of 1977 should have a compliance program that includes all of the following steps:
    1. Documentation of the corporation's existing internal accounting control systems.
    2. A cost/benefit analysis of the controls and the risks that are being minimized.
    3. A system of quality checks to evaluate the internal accounting control system.

B. The FCPA has two main provisions: anti-bribery provisions and accounting provisions.
    1. **Anti-bribery provisions** – the principal purpose of the Foreign Corrupt Practices Act of 1977 was to prevent the bribery of foreign officials, foreign political parties or candidates for political office in the foreign country by U.S. firms seeking to do business overseas. However, if the company does not abide by the Act, the company may be assessed fines up to $2,000,000 and imprisonment for up to 5 years.
    2. **Accounting provisions** Section 102 of the FCPA requires all companies who are subject to the Securities Exchange Act of 1934 to
        a. Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
        b. Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:
            i. Transactions are executed in accordance with management's general or specific authorization;
            ii. Transactions are recorded as necessary (i) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and (ii) to maintain accountability for assets;
            iii. Access to assets is permitted only in accordance with management's general or specific authorization;
            iv. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

C. The accounting and record-keeping provisions apply to all U.S. companies that are regulated by the SEC (Securities Exchange Commission), not only those with foreign operations. This includes all publicly-held companies, as well as companies that are privately-held but have voluntarily registered with the SEC.

The Role of the Internal Audit Activity in Control

Responsibility for Risk Management and Control

A. As described earlier in Risk Management Section, the **risk management and control** process are an integral and ongoing **responsibility** of the organization's **senior management** and **the board**.

   1. **Senior management** is responsible for leading the establishment and administration of risk management and control processes. Senior management sets the tone at the top and should assume the responsibility and ownership of risk management and control. For management to achieve the organizational objectives, it ensures that sound risk management processes are in place and functioning. This includes:

      c. Determining how the risks are best managed.

      d. Updating the organizational risk management processes based on risk exposures.

      e. Designing controls to mitigate the identified risks.

   2. **The Board and audit committees** have a guiding and **oversight role** to determine that appropriate risk management and control processes are in place and that these processes are adequate and effective.

B. **Internal auditors** are responsible for providing objective assurance and consulting activities related to risk management and control. As consultants, internal auditors assist both senior management and the board by evaluating and providing assurance on the adequacy and effectiveness of management's risk and control processes. Internal auditors' role in control process was covered in more details in Section A of this domain.

Passing Tip:	Responsibilities in the Risk Management and Control Framework Responsibility ⇔ Management Oversight ⇔ Board or Audit Committee Assistance/Assurance (Consultants) ⇔ Internal Audit Activity

The Implementation Guide 2130 of the IPPF provides guidance on the roles of the internal audit activity in control systems. It is summarized below:

A. **According to the Standards**

   1. The internal audit activity must assist the organization in maintaining effective controls by **evaluating** their effectiveness and efficiency and by **promoting** continuous improvement.

2. The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:
    a. Achievement of the organization's strategic objectives.
    b. Reliability and integrity of financial and operational information.
    c. Effectiveness and efficiency of operations and programs.
    d. Safeguarding of assets.
    e. Compliance with laws, regulations, policies, procedures, and contracts.

B. Internal auditors are required to attain a clear understanding of the concept of control and the characteristics of typical control processes. They should also obtain a thorough understanding of the control framework adopted by the organization and to become familiar with globally recognized control frameworks such as COSO Internal Control – Integrated Framework (COSO will be discussed later).

C. Internal auditors should consider the risk appetite, risk tolerance, and risk culture of the organization. It is also important to understand the critical risks that could inhibit the organization's ability to achieve its objectives, and the controls that have been implemented to mitigate risks to an acceptable level.

D. Internal auditors should be aware of the laws and regulations with which the organization must comply.

E. Internal auditors should also understand the responsibilities related to maintaining effective controls. Typically:
    1. **Senior management** oversees the establishment, administration, and assessment of the control system.
    2. **Management** is responsible for the assessment of controls within their respective areas.
    3. **The internal audit activity** provides assurance about the effectiveness of the control processes.

F. The internal audit activity should understand the organization's control processes, alert management to new control issues, and provide recommendations and action plans for corrective actions and monitoring. The internal audit activity should obtain sufficient information to evaluate the effectiveness of the organization's control processes.

G. Controls are designed to mitigate risks at the entity, activity, and transaction levels. A competent evaluation of the effectiveness of controls entails assessing the controls in the context of risks to objectives at each of those levels. A **risk and control matrix** may help the internal auditor facilitate such assessments.
    1. **Risk and Control Matrix (RCM)** is a matrix that provides an overview of different risks facing the organizations and the corresponding controls to safeguard the organization against such risks. Some controls may address one risk for each control, and other controls may address more than one risk for

each control, on the other hand, some risks may need more than one control to be adequately addressed. A risk and control matrix are used for illustrating those matching relationships between controls and risks.

a. For example, reconciling the cash account balance on the entity's books to its bank records and investigating the differences could address more than one risk. This control could identify whether any payments recorded by the entity were not received by its bank, or whether any withdrawals recorded by the bank were not accounted for by the company. The risk of improperly authorized payments via the bank and the risk of lost deposits could be addressed by this control.

2. The following is an example of Risk and Control Matrix

Risk and Control Matrix

	Risk A	Risk B	Risk C	Risk D
Control 1				●
Control 2	●	●		
Control 3			●	
Control 4				●
Control 5		●		

3. Risk and Control Matrix can assist the internal audit activity in:

   a. Identifying objectives and the risks to achieving them.

   b. Determining the significance of risks, taking into consideration the impact and likelihood.

   c. Ascertaining the appropriate response to significant risks (e.g., accept, pursue, transfer, mitigate, or avoid).

   d. Ascertaining the key controls management uses to manage risks.

   e. Evaluating the design adequacy of controls to help determine whether it may be appropriate to test controls for effectiveness.

   f. Testing controls that have been deemed adequately designed to determine whether they are operating as intended.

H. To evaluate the efficiency of controls, the internal audit activity typically determines whether management monitors the costs and benefits of controls. This includes identifying whether the resources used in the control processes exceed the benefits.

I. To promote continuous improvement of control effectiveness, the internal audit activity may:

1. Recommend the implementation of a control framework if one is not already in place.
2. Provide training on controls and ongoing self-monitoring processes.
3. Facilitate control (or risk and control) assessment sessions for management.
4. Help management establish a logical structure for documenting, analyzing, and assessing the organization's design and operation of controls.
5. Assist in developing a process for identifying, evaluating, and remediating control deficiencies.
6. Help management keep abreast of emerging issues, laws, and regulations related to control.
7. Monitor technological advancements that may assist with control efficiency and effectiveness.
8. Make recommendations that enhance the control environment (e.g., a tone at the top that promotes a culture of ethical behavior and a low tolerance for noncompliance).

Internal Control Frameworks

An internal control framework represents an approach to control that provides a better understanding of an organization. There are several comprehensive models that were developed over time. While each framework approaches control from its own perspective, they all provide a basis for understanding control in an organization in addition to providing criteria against which the effectiveness of the organization's internal control system is measured.

Each model provides a systematic method of evaluating and addressing the adequacy of controls in multiple dimensions of a business, but each model highlights a different dimension more than others do. A company may use any comprehensive framework as long as it identifies, assesses, and mitigates organizational risks.

Generally, there are six commonly referred to control frameworks:

- Cadbury Report
- COSO (Committee of Sponsoring Organizations Model)
- CoCo (Criteria of Control Model)
- eSAC (Electronic Systems Assurance and Control)
- COBIT 5 (Control Objectives for Information and Related Technologies)

Cadbury
COSO
CoCo
eSAC
COBIT 5

The Cadbury Report

Cadbury
COSO
CoCo
eSAC
COBIT 5

Following the large number of company failures in the 1980s, there was a growing need to reevaluate internal control. Audit failures and financial reporting fraud led to the establishment of the Committee on the Financial Aspects of Corporate Governance led by Sir Adrian Cadbury to review "those aspects of corporate governance specifically related to financial reporting and accountability". The Cadbury Report was published in 1992 with recommendations "focused on the control and reporting functions of boards, and on the role of auditors".

A. The Cadbury Report described corporate governance and the roles of directors, shareholders, and external auditors:
    1. **Corporate governance** is the system by which companies are directed and controlled.
    2. **Boards of directors** are responsible for the governance of their companies. The responsibilities of the board include setting the company's strategic aims, providing the leadership to put them into effect, supervising the management of the business and reporting to shareholders on their stewardship.
    3. **The shareholders'** role in governance is to appoint/elect the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place.
    4. **The external auditors'** role is to provide the shareholders with an external and objective check on the directors' financial statements which form the basis of that reporting system.

B. Cadbury report highlighted the importance of having an effective internal control system as a key corporate governance mechanism, and considered the internal audit function as an integral part of the company's system of internal control:
    1. **Internal Control** – directors need to maintain a system of internal control over the financial management of the company, including procedures designed to minimize the risk of fraud. Since an effective internal control system is a key aspect of the efficient management of a company, the directors should report on the effectiveness of their system of internal control, and that the auditors should report on their statement.
    2. **Internal Audit** – the function of the internal auditors is complementary to, but different from, that of the outside auditors. The report stated that it is a good practice for companies to establish internal audit functions to undertake regular monitoring of key controls and procedures. Such regular monitoring is an integral part of a company's system of internal control and helps to ensure its effectiveness. An internal audit function is well placed to undertake investigations on behalf of the audit committee and to follow up any suspicion of fraud. It is essential that heads of internal audit should have unrestricted access to the chairman of the audit committee in order to ensure the independence of their position.

C. The primary output of the Cadbury report was the Code of Best Practice designed to achieve the necessary high standards of corporate behavior. This code was ultimately incorporated into the Listing Rules of the London Stock Exchange. The Code of Best Practice is based on three fundamental principles of corporate governance:

1. **Openness** – on the part of companies, within the limits set by their competitive position that serves as the basis for the confidence which needs to exist between a business and all those who have a stake in its success. An open approach to the disclosure of information contributes to the efficient working of the market economy, prompts boards to take effective action and allows shareholders and others to scrutinize companies more thoroughly.
2. **Integrity** – means both straightforward dealing and completeness. What is required of financial reporting is that it should be honest and that it should present a balanced picture of the state of the company's affairs. The integrity of reports depends on the integrity of those who prepare and present them.
3. **Accountability** – boards of directors are accountable to their shareholders and both have to play their part in making that accountability effective. Boards of directors need to do so through the quality of the information which they provide to shareholders, and shareholders through their willingness to exercise their responsibilities as owners.

D. **The Code of Best Practice**

1. **The Board of Directors**

   a. The board should meet regularly, retain full and effective control over the company and monitor the executive management.

   b. There should be a clearly accepted division of responsibilities at the head of a company, which will ensure a balance of power and authority so that no one individual has unfettered powers of decision.

   c. The board should include non-executive directors of sufficient caliber and number for their views to carry significant weight.

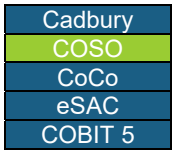
   d. The board should have a formal schedule of matters specifically reserved to it for decision to ensure that the direction and control of the company are firmly in its hands.

   e. There should be an agreed upon procedure for directors, in the furtherance of their duties to take independent professional advice if necessary at the company's expense.

   f. All directors should have access to the advice and services of the company secretary, who is responsible to the board for ensuring that board procedures are followed and that applicable rules and regulations are complied with.

2. **Non-Executive Directors**
    a. Non-executive directors (NED) should bring an independent judgment to bear on issues of strategy, performance, and resources, including key appointments and standards of conduct.
    b. The majority of NEDs should be independent of management and free from any business or other relationship which could materially interfere with the exercise of independent judgment, apart from their fees and shareholdings.
    c. NEDs should be appointed for specified terms and re-appointment should not be automatic.
    d. NEDs should be selected through a formal process and both this process and their appointment should be a matter for the board as a whole.
3. **Executive Directors**
    a. Directors' service contracts should not exceed three years without shareholders' approval.
    b. There should be full disclosure of a director's total compensation and those of the chairman and highest paid UK directors, including pension contributions and stock options.
    c. Executive directors' pay should be subject to the recommendations of a remunerations committee made up wholly or mainly of NEDs.
4. **Reporting and Controls**
    a. It is the board's duty to present a balanced and understandable assessment of the company's position.
    a. The board should ensure that an objective and professional relationship is maintained with the auditors.
    b. The board should establish an audit committee of at least three NEDs with written terms of reference which deal clearly with its authority and duties.
    c. The directors should explain their responsibility for preparing the accounts next to a statement by the auditors about their reporting responsibilities.
    d. The directors should report on the effectiveness of the company's system of internal control.
    e. The directors should report that the business is a going concern, with supporting assumptions or qualifications as necessary.

The COSO Model



The Committee of Sponsoring Organizations (COSO) of the Treadway Commission issued in 1992 the "Internal Control - Integrated Framework" report. It establishes a common definition of internal control and provides principles-based guidance for designing and implementing effective internal controls. COSO defines internal control as follows:

> ***Internal control*** *is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*
>
> - *Effectiveness and efficiency of operations.*
> - *Reliability of financial reporting.*
> - *Compliance with applicable laws and regulations.*

A. COSO's definition of internal control reflects certain fundamental concepts:

1. **A Process –** Internal control is a process. It's a means to an end, not an end in itself. Internal control is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive and are inherent in the way management runs the business.
2. **People –** Internal control is affected by people. It's not merely policy manuals and forms, but people at every level of an organization. Internal control is affected by a board of directors, management and other personnel in an entity. It is accomplished by the people of an organization, by what they do and say. People establish the entity's objectives and put control mechanisms in place.
3. **Reasonable Assurance –** Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board. Internal control, no matter how well designed and operated, can provide only reasonable assurance to management and the board of directors regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems.
4. **Objectives –** Internal control is geared to the achievement of objectives in one or more separate but overlapping categories. Every entity sets out on a mission, establishing objectives it wants to achieve and strategies for achieving them. Objectives may be set for an entity as a whole or be targeted to specific activities within the entity. Though many objectives are specific to a particular entity, some are widely shared.

a. COSO classifies organizational objectives into three categories. This categorization allows determining what can be expected from the internal control system in each category of these objectives:

   i. **Entity Operations Objectives** – referring to the entities' effectiveness and efficiency of operations including operational and financial performance goals, profitability goals and safeguarding assets (resources).

   ii. **Entity Reporting Objectives** – referring to the entity's internal and external published financial and non-financial reporting and may cover reliability, timeliness, transparency, and/or other terms as set forth by regulators, standard setters, or the entity's policies.

   iii. **Entity Compliance Objectives** – referring to the entity's adherence to all applicable laws and regulations.

b. Internal control systems can be easily expected to provide reasonable assurance of achieving reporting and compliance objectives because those objectives depend largely on activities within the entity's control. On the other hand, achievement of operations objectives is not always within the entity's control because bad decisions or adverse external events can cause a business to fail to achieve operations goals. Therefore, the internal control system can provide reasonable assurance only that management and the board are timely made aware of the extent to which the entity is moving toward those objectives.

B. **Roles and Responsibilities** – Everyone in an organization has responsibility for internal control.

1. **Management** – The chief executive officer is ultimately responsible and should assume "ownership" of the system. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions.

2. **Board of Directors** – Management is accountable to the board of directors, which provides governance, guidance and oversight.

3. **Internal Auditors** – Internal auditors play an important role in evaluating the effectiveness of control systems and contribute to ongoing effectiveness.

4. **Other Personnel** – Internal control is, to some degree, the responsibility of everyone in an organization and therefore should be an explicit or implicit part of everyone's job description.

C. **Components of Internal Control** – COSO framework stated that internal control consists of five interrelated components:

1. **Control Environment** – The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The core of any business is its people and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests. Control environment factors include:

   a. **Integrity and Ethical Values** – An entity's objectives and the way they are achieved are based on preferences, value judgments and management styles. Those preferences and value judgments, which are translated into standards of behavior, reflect management's integrity and its commitment to ethical values. Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of other internal control components.

   b. **Commitment to Competence** – Competence should reflect the knowledge and skills needed to accomplish tasks that define the individual's job. Management needs to specify the competence levels for particular jobs and to translate those levels into requisite knowledge and skills.

   c. **Board of Directors or Audit Committee** – The control environment is influenced significantly by the entity's board of directors and audit committee. Factors include the board or audit committee's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and the appropriateness of its actions. Another factor is the degree to which difficult questions are raised and pursued with management regarding plans or performance. Interaction of the board or audit committee with internal and external auditors is another factor affecting the control environment.

   d. **Management's Philosophy and Operating Style** – Management's philosophy and operating style affect the way the enterprise is managed, including the kinds of business risks accepted. An informally managed company may control operations largely by face-to-face contact with key managers. A more formally managed one may rely more on written policies, performance indicators and exception reports. Other elements of management's philosophy and operating style include attitudes toward financial reporting and attitudes toward data processing and accounting functions and personnel.

   e. **Organizational Structure** – An entity's organizational structure provides the framework within which its activities for achieving objectives are planned, executed, controlled and monitored. It refers to the organization of activities within an entity and the relationships (formal or informal) between individuals.

f. **Assignment of Authority and Responsibility** – This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols.

g. **Human Resource Policies and Practices** – Human resource practices send messages to employees regarding expected levels of integrity, ethical behavior and competence. Such practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating and remedial actions.

2. **Risk Assessment** – Risk assessment is the identification and analysis of risks to achievement of entity's objectives, forming a basis for determining how the risks should be managed:

   a. **Objectives** – A precondition to risk assessment is establishment of entity's objectives.

   b. **Risk Identification** – An entity's performance can be at risk due to internal or external factors that must be identified.

      i. External factors include technological developments, changing customer needs or expectations, competition, new legislation and regulation, natural catastrophes, and economic changes.

      ii. Internal factors include a disruption in information systems processing, the quality of personnel hired, a change in management responsibilities, the nature of the entity's activities, and an unassertive or ineffective board or audit committee.

   c. **Risk Analysis** – After the entity has identified risks, a risk analysis needs to be performed. The process usually includes:

      i. Estimating the significance of a risk;

      ii. Assessing the likelihood (or frequency) of the risk occurring;

      iii. Considering how the risk should be managed.

   d. **Managing Change** – Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

   e. **Circumstances Demanding Special Attention** – Because of their potential impact, certain conditions should be the subject of special consideration. Such conditions are:

      i. Changed operating environment.

      ii. New personnel.

      iii. New or revamped information systems.

      iv. New technology.

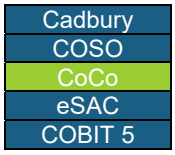
      v. New lines, products, activities.

vi. Corporate restructurings.

vii. Foreign operations.

3. **Control Activities** – Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include:
   a. Top level reviews of actual performance versus budgets, forecasts, prior periods and competitors.
   b. Direct functional or activity management.
   c. Controls on information processing to check accuracy, completeness and authorization of transactions.
   d. Physical controls.
   e. Performance indicators.
   f. Segregation of duties among different people to reduce the risk of error or inappropriate actions.
4. **Information and Communication** – Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities.
   a. **Information** systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal with internally generated data and with information about external events, activities and conditions necessary to informed business decision-making and external reporting.
   b. **Communication** must be effective and must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There are also needs to establish effective communication with external parties, such as customers, suppliers, regulators and shareholders.
5. **Monitoring** – Monitoring internal control systems is a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

The CoCo Model



The Criteria of Control Model CoCo is a Canadian model developed by the Canadian Institute of Chartered Accountants (CICA). This model defines control and sets out criteria for effective control in an organization that can be used to assess the effectiveness of control.

Control Definition – The CoCo model defines control as follows:

> ***Control*** *comprises those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives.*

Criteria – The CoCo model includes 20 criteria of control classified into four categories: purpose, commitment, capability, and monitoring and learning. These criteria can serve as the elements of control evaluation programs:

A. **Purpose**

1. Objectives should be established and communicated
2. The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.
3. Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated, and practiced so that people understand what is expected of them and the scope of their freedom to act.
4. Plans to guide efforts in achieving the organization's objectives should be established and communicated.
5. Objectives and related plans should include measurable performance targets and indicators.

B. **Commitment**

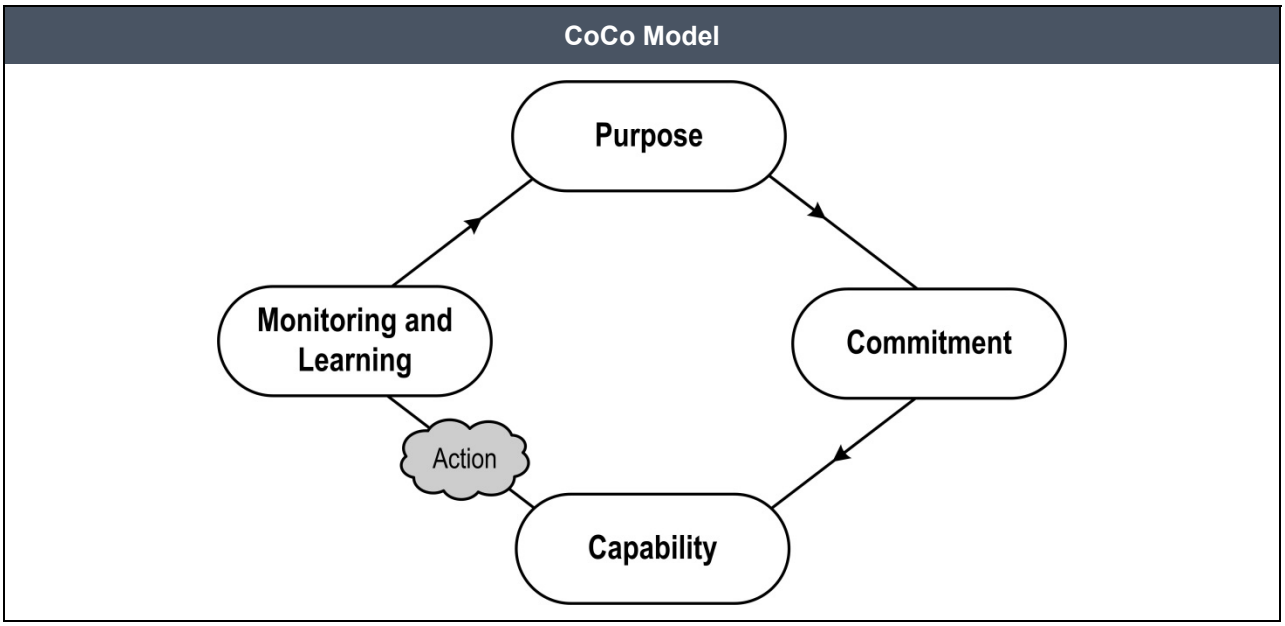
1. Shared ethical values, including integrity, should be established, communicated, and practiced through the organization.
2. Human resource policies and practices should be consistent with an organization's ethical values and with achievement of its objectives.
3. Authority, responsibility, and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.
4. An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.

C. **Capability**

1. People should have the necessary knowledge, skills, and tools, to support the achievement of the organization's objectives.
2. Communication processes should support the organization's values and the achievement of its objectives.
3. Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.
4. The decisions and actions of different parts of the organization should be coordinated.
5. Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.

D. **Monitoring and Learning**

1. External and internal environments should be monitored to obtain information that may signal a need to reevaluate the organization's objectives or controls.
2. Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.
3. The assumptions behind an organization's objectives and systems should be periodically challenged.
4. Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.
5. Follow-up procedures should be established and performed to ensure appropriate change or action occurs.
6. Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.



Electronic Systems Assurance and Control (eSAC)

Cadbury
COSO
CoCo
eSAC
COBIT 5

The eSAC is an internal control framework pertaining to IT published by the IIA. The eSAC model sets the stage for effective technology risk management by giving companies a framework to guide an evaluation of the e-business control environment. The model recognizes the importance of governance to ensure effective security, auditability, and control of information.

The eSAC model provides a framework to help management, corporate governance entities, and internal auditors understand, evaluate, monitor, and mitigate technology risks. The eSAC model includes the following components:

A. **Organization's Mission and Outcomes –** The organization typically pursues its mission through establishing strategies and objectives consistent with its values. The organization aims to achieve desired results while enhancing or preserving its reputation and learning how to improve its performance.

B. **Control Context –** A sound control environment helps the organization stay on its path as it moves from mission to results. The eSAC model adopts the broad control context from COSO objectives:

   1. Effectiveness and efficiency of **operations.**
   2. Financial and other management **reporting.**
   3. **Compliance** with laws and regulations.
   4. **Safeguarding** of assets.

C. **Assurance Objectives –** The eSAC provides control attributes that are particularly pertinent for e-business activities. They represent assurance objectives and provide a "framework" through which eSAC is discussed. The basic assurance objectives included in the eSAC model are:

1. **Availability –** means that the information, processes, and services must be available when needed. The organization must be able to receive, process, and support transactions as required. In the event of a problem, controls must provide for swift recovery. To ensure availability, the auditor evaluates controls that deal with potential causes of business interruption. These might include:
    a. Physical and logical security of system resources.
    b. Mechanical failure of file storage devices.
    c. Malfunction of software or unexpected incompatibilities.
    d. Inadequate capacity planning.
2. **Capability –** means that the system allows end-to-end reliable and timely completion and fulfillment of all transactions i.e., the system has adequate capacity, communications, and other aspects to consistently meet the needs placed on the system. This requires:
    a. Monitoring usage.
    b. Examining service-level agreements with internet service providers (ISPs).
    c. Examining Service-level agreements with application service providers.
    d. Identifying and eliminating bottlenecks in the system.
    e. Examining controls over system maintenance, often called change controls.
3. **Functionality –** means that the system provides the facilities, responsiveness, and ease of use to meet users' needs. Adequate functionality should provide for recording control information and other issues of concern to management.
4. **Protectability –** means that the system includes logical and physical security controls that ensure authorized access and deny unauthorized access to servers, applications, and information assets. Due to the vast access possible via the internet, absolute security is difficult to maintain, and thus controls are needed to safeguard IT assets against losses and identify such losses when they occur. Controls would tend to reduce the risk of significant damage, and internal fraud but could rarely eliminate such risks. To ensure protectability, the auditor would evaluate the following:
    a. Data security, integrity, and confidentiality; including privacy issues
    b. Program security
    c. Physical security

5. **Accountability –** means that transaction processing is accurate, complete, and non-refutable. Accountability identifies individual roles, actions, and responsibilities including concepts of data ownership, identification, and authentication to be able to identify who or what caused a transaction. The audit or transaction trail should have enough information-and be retained long enough for transactions to be confirmed, if necessary. Accountability also includes the concept of non-repudiation which means that once authenticated, a user cannot disclaim a transaction. To support accountability, information must be sufficient, accurate, timely, and available to management to meet its responsibilities.

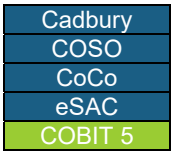
D. **Building Blocks –** Achieving the previous assurance objectives requires an adequate infrastructure, resources, and organizational commitment. The eSAC model refers to those resources as building blocks. They include:

1. People
2. Technology
3. Processes
4. Investment
5. Communication

E. **External Forces –** The eSAC model defines external factors that impact assurances and business objectives. Those factors include customers, competition, regulators, community, owners, providers, alliances, and agents.

F. **Dynamic Environment –** The dynamic environment is what many call the control environment. It is the context to all of the other components of the model. Monitoring and Oversight are key elements of the environment. Monitoring and oversight means that pertinent risks, whether internal or external to the organization, are recognized and addressed on an ongoing basis and controls are confirmed to be functioning as intended.

COBIT 5



COBIT was first released by the Information Systems Audit and Control Association (ISACA) in 1996. The most recent version is COBIT 5 that was released in 2012. *(source COBIT 5 ©2012 ISACA. All rights reserved. Used by Permission)*

COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interest of internal and external stakeholders. COBIT 5 is based on five key principles for governance and management of enterprise IT:

A. **Principle 1: Meeting Stakeholder Needs –** enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all the processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices.

B. **Principle 2: Covering Enterprise End-to-End –** COBIT 5 integrates governance of enterprise IT into enterprise governance:

    1. It covers all functions and processes within the enterprise; COBIT does not focus only on the “IT function,” but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
    2. It considers all IT-related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone – internal and external – that is relevant to governance and management of enterprise information and related IT.

C. **Principle 3: Applying a Single, Integrated Framework –** there are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.

D. **Principle 4: Enabling a Holistic Approach –** efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. The COBIT 5 framework defines seven categories of enablers:

    1. Principles, policies, and frameworks
    2. Processes
    3. Organizational structures
    4. Culture, ethics, and behavior
    5. Information
    6. Services, infrastructure, and applications
    7. People, skills, and competencies

E. **Principle 5: Separating Governance From Management –** the COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:

1. Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger complex enterprises.
2. Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

This page intentionally left blank.

Part 1, Domain VI
Fraud Risks

Section A: Fraud Risks and Types

Learning Outcomes:

1. Interpret fraud risks and types of frauds and determine whether fraud risks require special consideration when conducting an engagement. Proficiency Level.

A. **Fraud Definition** – The IPPF defines fraud as "any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

B. **Fraud Risk** is the probability that fraud will occur and the potential consequences to the organization when it occurs.

C. **Types of Fraud** – Fraud encompasses an array of irregularities and illegal acts characterized by intentional deception or misrepresentation. It can be perpetrated by persons outside as well as inside the organization for the benefit of the organization, or to the detriment of the organization.

Passing Tip: Fraud always involves scienter i.e., **intentional** false representations or concealment of material facts.

1. **Fraud designed to benefit the organization** generally produces such benefit by exploiting an unfair or dishonest advantage that also may deceive an outside party. Perpetrators of such frauds usually accrue an indirect personal benefit. Examples of frauds designed to benefit the organization include:
    a. **Improper payments** such as illegal political contributions, bribes, kickbacks, and payoffs to government officials, intermediaries of government officials, customers, or suppliers.
    b. **transfer pricing fraud** is intentional, improper valuation of goods or services exchanged between related organizations. By purposely structuring pricing techniques improperly, management can improve the operating results of an organization involved in the transaction to the detriment of the other organization.
    c. **Related-party** transactions in which one party receives some benefit not obtainable in an arm's-length transaction.

d. **Financial statement fraud** involves misrepresenting the financial statements. Financial statement fraud is typically perpetrated by organization managers to enhance the economic appearance of the organization and benefit from the fraud by selling stock, receiving performance bonuses, or using the false report to conceal another fraud. Examples of financial statement fraud include:
   i. Intentional, improper representation or valuation of transactions.
   ii. Overstating assets or revenue.
   iii. Understating liabilities and expenses.
   iv. Intentional failure to record or disclose significant information to improve the financial picture of the organization.
   v. Providing false information to those outside the organization.
e. **Prohibited business activities** such as those that violate government statutes, rules, regulations, or contracts.
f. **Tax fraud** is intentional reporting of false information on a tax return to reduce taxes.

2. **Fraud perpetrated to the detriment of the organization** generally is for the direct or indirect benefit of an employee, outside individual, or another organization. Some examples are:
   a. **Corruption** is the misuse of entrusted power for private gain. Corruption includes acceptance of bribes or kickbacks. In most cases, corruption crimes are uncovered through tips or complaints from third parties, often via a fraud hotline. Corruption often involves the purchasing function. Any employee authorized to spend an organization's money is a possible candidate for corruption. Another example is a corrupt lending officer who demands a kickback in exchange for approving a loan.
   b. **A conflict of interest** occurs where an employee of an organization has an undisclosed personal economic interest in a transaction that adversely affects the organization or the shareholders' interests.
   c. **Diversion** to an employee or outsider of a potentially profitable transaction that would normally generate profits for the organization.
   d. **Embezzlement**, as typified by the misappropriation of money or property, and falsification of financial records to cover up the act, thus making detection difficult.
   e. Unauthorized use of confidential or proprietary information to wrongly benefit someone.
   f. **Skimming** is theft of cash before it is recorded on the organization's books. For example, an employee accepts payment from a customer, but does not record the sale.

g. **False claims for compensation** submitted for services or goods not actually provided to the organization.

h. **Expense reimbursement fraud** occurs when an employee is paid for fictitious or inflated expenses such as personal travel, nonexistent meals, or extra mileage.

Common Forms of Fraud

1. Outright stealing company assets including:
   - Cash
   - Stamps, supplies, inventory, equipment, tools, etc.
   - Checks payable to the organization or to suppliers
2. Concealing theft by manipulating records:
   - Collecting cash, pocketing it, and not recording the sale.
   - Charging to expense accounts illegitimate expenses or expenses for personal benefits
   - Lapping accounts receivable (collecting cash from customer 1 and pocketing it, then collecting cash from customer 2 and recording it to customer 1 account, then collecting cash from customer 3 and recording it to customer 3, etc.)
   - Issuing fake receipts for customer collections and pocketing the cash.
   - Collecting written-off accounts, or collecting accounts, not recording it and charging it off.
   - Falsifying customer returns and credits
   - Changing dates of deposit slips
   - Adding fake employees or manipulating rates and hours to existing employees to pocket the payroll differences.
   - Recording discounts that are not granted to customers.
   - Making false payments by using previously paid vouchers, or to fake suppliers or through collusion with suppliers.
   - Manipulating inventory records

D. **Fraud Triangle (Characteristics of Frauds)** – Fraud triangle is a model for explaining the reasons that result in someone committing occupational fraud. The three common reasons or characteristics of fraud can be summarized as pressure, opportunity, and rationalization.

1. **Pressure or Incentive** – refers to the need that an individual attempts to satisfy by committing fraud. Examples of the needs may include:

   a. Financial need arising because the individual is facing problems such as gambling, drugs addiction, or extreme medical bills.

   b. The need to meet high-performance standards at work, or to cover up poor performance.

c. The psychological need for recognition for job performance.

d. The need to meet or beat analysts' estimates in the market for publically traded companies.

e. The desire to maintain certain performance results or standard of living.

2. **Opportunity** – is the ability to commit fraud without being detected. The opportunity to commit fraud exists when workers have access to assets or information in a manner that allows them to both commit and conceal fraud. Opportunity is created by factors such as weak internal controls, poor management, lack of board oversight, or the use of one's authority to override controls. Executives' ability to override controls increases the opportunity for executive-level fraud. That is why the cost of fraud committed by executives is far higher than the cost of low-level employee fraud. Opportunity is the one factor that organizations can influence the most by proper preventive and detective internal controls, audits, and oversight.

3. **Rationalization** – is the ability for a person to justify a fraud in a way that is acceptable by his or her morals. Rationalization involves a person reconciling his/ her behavior with the commonly accepted notions of decency and trust. Examples include justifying theft in the context of saving a family member by paying high medical bills, labeling the theft as "borrowing" and intending to pay the stolen money back later, or justifying fraud by believing that the organization is not paying fair enough salary. Rationalization may be reduced through:

   a. Implementing fair work and pay practices.

   b. Equitable and consistent treatment of employees.

   c. Management practices that provide a model for the behavior expected of employees "tone at the top".

E. Considering Fraud when Conducting Engagements

1. According to the Standards, internal auditors must have sufficient knowledge of fraud to identify situations that indicate fraud may have been committed. This knowledge includes the reasons of fraud (fraud triangle), the common types of fraud schemes associated with the activities under audit, and fraud red flags including any control deficiency that may allow committing fraud.

2. When conducting an engagement, the internal auditor must maintain awareness for potential fraud. This includes:

   a. Identifying common potential types of fraud associated with the engagement area.

   b. Noticing any indicators or symptoms of fraud.

   c. Designing appropriate engagement steps to address significant risk of fraud.

   d. Employing audit tests to detect fraud.

   e. Determining if any suspected fraud merits investigation.

3. For example:
    a. An auditor was planning an audit for the loans of a bank that has 50 different locations. In the planning phase, the auditor conducted analytical audit procedures, and realized that 3 distinct areas had abnormal results with a high percentage of repeat loans to the same individuals and significantly lower bad debts compared to the average. The auditor would normally plan the audit to give these areas more attention as the loans may be fraudulent loans covering or hiding a lapping scheme.
    b. On a different assignment, the auditor noticed a bright red Ferrari in the parking lot of the company. Upon inquiring, she was informed that the car belongs to an employee who holds a sensitive middle management position of one of the company's divisions. Upon inquiring further, she learnt that the car was won in lottery. The auditor checked online and noticed that the employee's name was on the winners of the car. While an extravagant lifestyle may be seen as a red flag, in this case, there are no reasons to doubt or require special considerations.

Passing Tip:	The internal auditor must have sufficient knowledge to identify indicators that fraud may have been committed, must be able to identify control weaknesses that could allow fraud to occur, and must be able to evaluate the indicators of fraud sufficiently to determine if a fraud investigation is warranted.

Section B: Fraud Risk Management

Learning Outcomes:

1. Evaluate the potential for occurrence of fraud (red flags, etc.) and how the organization detects and manages fraud risks. Proficiency Level.

Financial losses caused by fraud annually are confirmed to be significant. Some researches indicate that organizations, on average, lose five percent of their revenue because of fraud. However, the full cost of fraud is even higher than just the loss of money, given its impact on time, productivity, reputation, and customer relationships. Thus, it is important for organizations to have a strong fraud management program that includes **awareness**, **prevention**, and **detection** measures, as well as a **fraud risk assessment** process to identify and prioritize fraud risks within the organization. The risk of fraud can be reduced with basic prevention and detection internal controls and effective audits and oversight.

Fraud Indicators

A. During the planning stage of an engagement, the auditor must consider the potential for fraud in order to address it during the engagement, and therefore, the auditor needs to be knowledgeable of the risk factors and indicators of fraud. The internal auditor is required to be able to identify typical fraud indicators (red flags) throughout the engagement.

1. **Red flags** are items or actions that have been associated with fraudulent conduct.
2. Red flags are subjective in nature, and thus some red flags might not come to the auditor's attention even during the course of a properly planned and conducted audit.
3. The auditor need only be aware of red flags that may warrant further search for facts and need not document identified red flags during the engagement.
4. Difficulties in using red flags as fraud indicators include:
    a. Red flag information is not gathered as a normal part of an audit engagement.
    b. The subjectivity of red flags makes them difficult to quantify or evaluate.
    c. Many common red flags are not always associated with situations of fraud.
5. Red flags include, but are not limited to:
    a. The existence of complex sales transactions and transfers of funds between affiliated companies.
    b. Transactions that lack documentation or normal approval.
    c. Generous performance-based reward systems.
    d. Unrealistic performance goals (e.g., sales or production goals)
    e. A domineering management
    f. An unusual large amount of sales returns recorded after year-end.
    g. Reporting high profits when similar businesses suffer losses.
    h. An increase in reported sales without a relative increase in cost of goods sold.
    i. Missing documents.
    j. Unusual delays in providing requested information.
    k. Payments to vendors that are considered unusually high.
    l. Unusual changes in customers or vendors.
    m. Customer complaints about delivery.
    n. An individual handling a sensitive job for an extended period of time without any rotation of duties and without vacations.
    o. The presence of significant internal control weakness.
    p. Overrides of controls by management.
    q. The existence of unusual or non-routine journal entries.

r. Irregular or poorly explained management behavior.
s. Employees or management hand-delivering checks.
t. No segregation of incompatible duties.
u. Unclear division of responsibility and accountability within departments.
v. Rapid turnover of financial executives.
w. Management's preoccupation with increased financial performance.
x. A person's living and/or lifestyle is beyond their normal means.
y. An employee with close relationship with vendors.
z. An employee with addiction to drugs, alcohol or gambling.

6. The mere existence of red flags would not immediately warrant a fraud investigation nor should the auditor discuss the issue with management, legal counsel, or the audit committee. However, the existence of red flags indicates a need for heightened audit attention and further search for facts. Those discussions occur only after the auditor has gathered sufficient factual evidence that suggests the occurrence of fraud.
7. With the proper combination of fraud education and literature, experience, and skills, internal auditors may be able to identify common types of fraud associated with the various engagement areas.

Passing Tip:	The mere existence of red flags does not mean an employee is actually committing fraud and would not immediately warrant a fraud investigation nor should the auditor discuss the issue with management, legal counsel, or the audit committee. These discussions occur only after the auditor has gathered sufficient factual evidence that suggests the occurrence of fraud.

Fraud Prevention and Detection

A. **Fraud Prevention** – Fraud prevention involves those actions taken to discourage the commission of fraud and limit fraud exposure when it occurs. Fraud prevention mechanisms include:

1. **Fraud Training** is usually a key factor in the deterrence of fraud. Employees must understand the ethical behavior expected of them to act accordingly within the organization. Training may cover:

a. The organization's expectations for employees' conduct.
b. The procedures and standards necessary to implement internal controls.
c. Fraud awareness including types of fraud and the employees' responsibilities to report misconduct.
d. Management's regular communication to educate employees about fraudulent activities.

2. **Organizational Culture** – Instilling a strong ethical culture and setting the correct tone at the top.
3. **Internal Control System** – Effective internal controls are one of the strongest deterrents to fraudulent behavior and fraudulent actions. Simultaneous use of preventive and detective internal controls enhances any fraud risk management program's effectiveness. Management is primarily responsible for establishing and maintaining internal controls in an organization. Internal control system is covered in Domain-II of Part-1.

B. **Fraud Detection** – Fraud detection entails activities and programs designed to identify fraud or misconduct that is occurring or has occurred. Fraud detection often relies on detective controls that are designed to provide warnings or evidence that fraud is occurring or has occurred. Detective internal controls are not intended to prevent fraud. They are intended to detect and provide evidence that fraud exists. Fraud detection activities may include:

1. Routine and surprise audits in high fraud risk areas.
2. Continuous monitoring of critical data and related trends to identify unusual situations or variances.
3. Routine matching of public data or proprietary data against relevant transactions, vendor lists, employee rosters, and other data.
4. Encouraging employees, suppliers, and other stakeholders to report their concerns about illegal or unethical behaviors. Methods to collect this information include:
    a. Whistleblower hotline where the whistleblower can remain anonymous.
    b. Code of conduct confirmation — the employees are asked to sign an annual code of conduct outlining their responsibilities in the prevention and detection of fraud and to report any known violations.
    c. Exit Interviews — conducting exit interviews of terminated employees or those who have resigned can help identify fraud schemes.
    d. Proactive Employee Survey — routine employee surveys can be conducted to solicit employee knowledge of fraud and unethical behavior within the organization.

C. **Cost-Effectiveness**: It may be not cost-effective for an organization to try to eliminate all fraud risk. The organization may choose to design its controls to detect, rather than prevent fraud risks. If the cost of designing and implementing internal controls exceeds the estimated impact of the risk, it may not be cost-effective to implement the internal controls.

Fraud Risk Assessment

A. **Fraud Risk Assessment** is a tool that assists management and internal auditors in systematically identifying where and how fraud may occur and who may be in a position to commit fraud. A fraud risk assessment is a component of an organization's larger enterprise risk management.

   1. A fraud risk assessment concentrates on fraud schemes and scenarios to determine the presence of internal controls and whether or not the controls can be circumvented.
   2. An important role of management is to provide oversight for the successful completion of a fraud risk assessment so that management has a better understanding of fraud risks and the controls in place to mitigate those risks.
   3. The fraud risk assessment is typically conducted by a team that is composed of individuals from the internal audit activity, finance, legal, IT, security, and potentially other functions depending on the nature of the organization.

B. The fraud risk assessment process generally includes the following key steps:

   1. **Identify relevant fraud risk factors and potential fraud schemes**. The fraud risk assessment team needs to identify fraud risk factors and indicators, and to anticipate both fraud schemes and the individuals within and outside the organization who could be in a position to perpetrate each scheme. This can be achieved by gathering information about the organization's activities and relationships to gain an understanding of fraud indicators and fraud risks. This process includes:
      a. Brainstorming.
      b. Management interviews.
      c. Analytical procedures.
      d. Review of documentation of previous frauds and suspected frauds committed against or on behalf of the organization.
      e. Evaluation of related frauds at similar organizations.
      f. Review of the organization's performance measures over the past few years compared with competitors.
      g. Review common fraud schemes relevant to the industry, geography, and programs.
   2. **Prioritize potential fraud schemes based on risk**. After identifying fraud risks and schemes, the fraud risk assessment team must prioritize fraud risks considering the following factors:
      a. Monetary impact.
      b. Impact to the organization's reputation.
      c. Loss of productivity.

d. Integrity and security over data.

e. Loss of assets.

f. Liquidity of assets.

g. Volume, size, and location of transactions.

h. Potential criminal/civil actions including potential regulatory noncompliance.

3. **Map existing controls to potential fraud schemes and identify gaps**. The fraud risk assessment team should identify preventive and detective controls in place to address each fraud risk. In this respect, the risk of management's override of controls needs to be considered and the cost/benefit for controlling that risk should be evaluated. Common anti-fraud controls include:

   a. Whistleblower hotline and whistleblower protection policy.

   b. Board oversight.

   c. Continuous monitoring.

   d. Code of conduct.

   e. The tone of management's communications regarding the tolerance for fraud risks.

4. **Test the effectiveness of fraud prevention and detection controls**. Internal auditing typically plays an important role in assessing the effectiveness of internal controls. Internal auditors consider not only the existence of the internal controls, but also the effectiveness of these controls through periodic testing.

   a. For example, a security policy over network passwords requires passwords to be changed every 30 days; however, the network system access controls do not block user access if the password is not changed as required. In this case, the internal control is present, but is not effective.

5. **Document the fraud risk assessment**. The fraud risk assessment process should be documented. Key elements that should be documented for each business area include:

   a. The types of fraud that have some chance of occurring.

   b. The inherent risk of fraud in specific business areas.

   c. The adequacy of existing anti-fraud monitoring and preventative controls.

   d. The gaps in the organization's fraud controls, including segregation of duties.

   e. The likelihood of a fraud occurring and impact.

6. **Report the fraud risk assessment.** According to Standards, the CAE must report periodically to senior management and the board significant risk exposures and control issues, including fraud risks. Management and the CAE must update the board periodically on the status and results of the fraud risk assessment. These updates report on the effectiveness of existing anti-fraud programs, as well as corrective actions taken by management to address gaps identified during the assessment.

Roles and Responsibility for Fraud Prevention and Detection

A. **Board of Directors** – The board of directors has responsibility for effective and responsible corporate fraud governance. The role of the board is to oversee and monitor management's actions to manage fraud risks. Since the board is the organization's highest authority, it is responsible for setting the tone for fraud risk management within an organization. The board's roles in fraud prevention and detection also include:

   1. Evaluating management's identification of fraud risks and the implementation of anti-fraud measures.
   2. Hiring external auditors to report on the financial statements of the organization and provide recommendations on internal control.
   3. Overseeing the internal audit activity.
   4. Overseeing controls to prevent or detect management fraud and to prevent senior management override of controls.

B. **Management** – Management is responsible for overseeing the activities of employees and typically does so by implementing monitoring processes and internal controls. Specifically, management is responsible for:

   1. Establishing and maintaining an effective internal control system.
   2. Identifying and assessing fraud risks.
   3. Implementing anti-fraud measures.
   4. Creating the right tone at the top.
   5. Developing policies and procedures for effective fraud investigations and for handling investigation results.

C. **External Auditors** – The organization's external auditors are responsible for auditing the organization's financial statements to obtain reasonable assurance about whether the financial statements are free of material misstatement and whether the misstatements were caused by error or fraud. Whenever the external auditor has determined there is evidence that fraud may exist, the external auditor is required to report the matter to an appropriate level of management. The external auditor reports fraud involving senior management directly to those charged with governance (the audit committee or the board).

D. **Internal Auditors** – Internal auditors usually have a continual presence in the organization that provides them with a better understanding of the organization and its control systems. Internal auditors provide an independent appraisal, examination, and evaluation of an organization's activities as a service to the organization. The IPPF outlines the following Standards pertaining to fraud and the internal auditor's roles and responsibilities relating to fraud. These Standards should be studied carefully:

- "Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud."
- "Internal auditors must exercise due professional care by considering the Probability of significant errors, fraud, or noncompliance."
- "The CAE must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the Standards. **Reporting must also include significant risk and control issues, including fraud risks,** governance issues, and other matters that require the attention of senior management and/or the board."
- "The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk."
- "Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives."

Therefore, internal auditors' responsibilities in fraud management may be summarized in the following points:

1. Internal auditors are responsible for assisting in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of internal controls. In carrying out this responsibility, internal auditors, for example, determine whether:
   a. The organizational environment fosters control consciousness.
   b. Realistic organizational goals and objectives are set.
   c. Written policies (e.g., code of conduct) exist that describe prohibited activities and the action required whenever violations are discovered.
   d. Appropriate authorization policies for transactions are established and maintained.
   e. Policies, practices, procedures, reports, and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas.
   f. Communication channels provide management with adequate and reliable information.
   g. Recommendations need to be made for the establishment or enhancement of cost-effective controls to help deter fraud.
2. Internal auditors have a responsibility to exercise "due professional care" as defined in the Standards with respect to fraud detection.

3. Internal auditors need to be alert to the signs and possibilities of fraud within the organization. Thus, internal auditors have a responsibility to obtain sufficient skills and competencies to evaluate the risk of fraud, including knowledge of fraud indicators and schemes.
4. Internal auditors may assist management in establishing fraud prevention measures and providing consulting expertise.
5. Internal auditors' responsibilities for fraud during audit engagement include:
    a. Have sufficient knowledge of fraud to be able to identify indicators that fraud may have been committed. This knowledge includes the need to know the characteristics of fraud, the techniques used to commit fraud, and the types of frauds associated with the activities reviewed.
    b. Consider fraud risks in the assessment of internal control design. Internal auditors should obtain reasonable assurance that business objectives for the process under review are being achieved and material control deficiencies are detected.
    c. Be alert to opportunities, such as control weaknesses, that could allow fraud. If significant control weaknesses are detected, additional tests should be conducted by internal auditors to identify whether fraud has occurred.
    d. Evaluate whether management is actively overseeing and monitoring the fraud risk management program, and that timely and sufficient corrective measures have been taken with respect to any noted control deficiencies or weaknesses.
    e. Evaluate the indicators that fraud may have been committed and decide whether any further action is necessary or whether an investigation needs to be recommended.
    f. Notify the appropriate authorities within the organization if a determination is made that there are sufficient indicators of the commission of a fraud to recommend an investigation.
6. Internal auditors' roles in relation to fraud risk management could also include
    a. Conducting initial or full investigation of suspected fraud.
    b. Providing root cause analysis and control improvement recommendations.
    c. Monitoring of a reporting/whistleblower hotline.
    d. Providing ethics training sessions.

7. Internal auditors are not expected to have knowledge equivalent to that of a person whose primary responsibility is detecting and investigating fraud. Also, audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.
8. The objective of internal auditing in fraud management is to assist members of the organization in the effective discharge of their responsibilities by furnishing them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed.

E. A well-designed internal control system should not be conducive to fraud. Tests conducted by auditors, along with reasonable controls established by management, improve the likelihood that any existing fraud indicators will be detected and considered for further investigation.

F. Detection of fraud consists of identifying indicators of fraud sufficient to warrant recommending an investigation. These indicators may arise as a result of controls established by management, tests conducted by auditors, and other sources both within and outside the organization. The presence of more than one indicator at any one time increases the probability that fraud may have occurred.

Section C: Fraud Controls and Awareness

Learning Outcomes:

1. Recommend controls to prevent and detect fraud and education to improve the organization's fraud awareness. Proficiency Level.

A. While not a guarantee on its own, a system of strong internal controls is amongst the best means to prevent or detect fraud. Simultaneous use of preventive and detective internal control procedures enhances the effectiveness of fraud risk management. Management is primarily responsible for establishing and maintaining internal controls in an organization. However, internal auditors are required to test controls for fraud risk and provide related improvement recommendations.

B. The auditors would normally map processes and complete a process review in the early phases of an audit (usually during the planning phase) in order to identify potential control weaknesses, identify areas of potential fraud, recommend improvements to the controls, and thus deter or prevent fraud.

C. The mapping of processes, as covered in other sections of this part and other parts, involves documenting the processes, preferably in flowcharts, which enables the auditor to have a clear big picture of these processes. This understanding and visual presentation allows the auditor to review existing controls, and to improve any weaknesses and/or control deficiencies.

D. The following table includes typical fraud schemes and related controls:

Typical Fraud Schemes and Related Controls		
Function/Activity	**Indicators**	**Controls to Prevent or Detect**
Procurement/ Purchasing	– Purchasing agent's standard of living has increased. – Significant internal control weaknesses. – Cost of purchases is higher than prior years. – Cost of purchases is higher than budget. – Purchases from particular vendors are higher than normal. – Cost of purchases is higher than market values. – Unjustified buildup of inventory or an increase in inventory turnover in days. – Buyer is not taking any vacations and refused a promotion. – Buyer accompanies a vendor on regular excursions.	– Corporate code of ethics prohibiting the acceptance of kickbacks. – Corporate policy prohibiting the acceptance of anything of value. – Establishing and approving long-term contracts with major vendors. – Require that only approved vendors are paid for purchases, and only based on production activity. – Requiring mandatory vacations – Requiring frequent rotation of duties. – Maintaining proper segregation of duties between the ordering, receiving, payable, and accounting functions.
Kiting (which refers to the recording of a deposit from an interbank transfer in this period, while failing to record the related disbursement until the next period)	– Significant deposits in a bank account towards the end of a period. – Management's pre-occupation with increased financial performance. – An otherwise poor cash or current assets position.	– Typically, the auditor would examine a schedule of bank transfers for the week before and week after period end searching for checks that should have been listed as outstanding in the prior period but were not.
Lapping (which refers to the concealment of the first customer's payments, then allocating the second customer's payment to the account of the first, and the third to the account of the second, etc.)	– Several discrepancies between the books and customers' confirmations. – Lack of adequate segregation of incompatible duties. – Employees failing to take vacations and/or refusing promotions. – Unexplained lifestyle	– Mandatory vacations and/or rotations of duties. – Segregation of duties between sales, collections, and book keeping. – Regular confirmations of customers' balances and immediately investigating differences.

Senior Management	– Managers regularly assume subordinates' duties – Managers dealing in matters outside their normal scope of responsibility. – Managers failing to comply with corporate directives and procedures. – Management's pre-occupation with increased financial performance. – A domineering management – Generous performance-based reward systems.	– Managers subject to formal performance reviews. – Strong Board and Audit Committee oversight – Ethical management
Sales	– Compensation is significantly dependent on sales and/or profitability. – Significant returns after period end. – No shipping documents available for sales invoices. – An increase in bad debts.	– Strong controls
Inventory	– Poor controls over the warehousing. – "Accidental" fires or other forms of "environmental" damages	– Strong controls

E. **Organizational Fraud Awareness** – The internal audit activity must support a culture of fraud awareness and encourage the reporting of improprieties. Organizational culture plays a significant role in the actions (or lack thereof) of all members within the organization. Some means to support a culture of fraud awareness include:

1. Ensuring that there is continuous emphasis from the top management levels on supporting a culture of fraud awareness. The tone at the top is very significant to achieve the desired objectives.
2. Continuously conducting fraud awareness seminars and training, as in some cases, fraud perpetrators might not be fully aware of the consequences of their fraudulent conduct, and or claim not being aware that what they conducted was fraud in the first place.
3. Encouraging actions consistent with proper practices and discouraging and/or recommending penalties for improprieties.

4. Establishing a safe and secure manner for whistle-blowers to report improprieties to appropriate management levels and/or internal audit within the organization without fear of reprisals.
5. Encourage an open-door policy at the senior management level to allow employees to voice concerns, which in some cases may be valuable input to deter or detect fraud.

Section D: Forensic Auditing

Learning Outcomes:

1. Recognize techniques and internal audit roles related to forensic auditing (interview, investigation, testing, etc.). Basic Level.

A. **Forensic auditing** refers to the application of auditing skills to situations that have potential legal implications and/or consequences. The role of forensic auditing is to facilitate the prevention, detection, and/or investigation of fraud. During such audits, the evidence gathered by the auditor could be presented in a court of law.

B. Typical applications of forensic auditing include audits during which the auditor is investigating for fraud. It would be used when the auditor has suspicions about fraud, and thus, the auditor requires forensic evidence to prove or negate the suspicions, identify the parties involved, and gather and maintain evidence that may be subsequently presented in disciplinary or criminal proceedings.

C. Forensic auditing requires consideration to the following issues:

1. Proper authorization of the related audit.
2. Relevant evidence has been adequately documented and safeguarded.
3. Legal rules that govern the admissibility of gathered evidence.
4. Reporting the findings in a manner that meets legal requirements.
5. Obtaining legal advice when appropriate.
6. Assessment and evaluation of the gathered evidence to ensure that the case is sustainable.
7. Confidentiality.

Passing Tip:	Forensic auditors are primarily engaged in audit assignments since they possess knowledge of what constitutes evidence acceptable in a court of law.

Fraud Investigation

A. When indicators of fraud are noted, the internal auditor expands activities to determine whether an investigation is warranted.

B. If there is sufficient evidence that fraud has occurred, the internal auditor must inform senior management and the board/audit committee of the findings and discuss further investigation. The internal auditor may recommend whatever investigation is considered necessary in the circumstances.

C. Investigating a fraud is not the same as auditing for fraud.

   1. **Auditing for fraud** is an audit designed to proactively detect indications of fraud in those processes or transactions where analysis indicates the risk of fraud to be significant.

   2. **Investigation of fraud** consists of performing extended procedures necessary to determine whether fraud, as suggested by the indicators, has occurred, the loss or exposures associated with the fraud, who was involved, and how it happened. It includes gathering sufficient information about the specific details of a discovered fraud.

      a. Internal auditors, lawyers, investigators, security personnel, and other specialists from inside or outside the organization are the parties that usually conduct or participate in fraud investigations.

D. Management (not internal auditors) is responsible for developing controls over the investigation process. Those controls are often documented in a fraud policy which includes standards for:

   1. The qualifications of those authorized to conduct investigations.

   2. Developing policies and procedures for effective investigations.

   3. Preserving evidence.

   4. Handling and reporting the results of the investigations.

   5. Considering the rights of individuals and the relevant laws where the frauds occurred.

E. The role of the internal audit activity in investigations needs to be defined in the internal audit charter, as well as in the fraud policies and procedures. Internal auditing may have the primary responsibility for fraud investigations, may assist in fraud investigations, or may have no role in fraud investigations. Any of these roles can be acceptable as long as the impact of these activities on internal auditors' independence and objectivity is recognized and handled appropriately.

F. **Investigative Procedures** – Generally, common investigative procedures include:

1. **Obtaining Evidence**: The collection and preparation of evidence is critical to understand the fraud and to support the conclusions reached by the investigators. The investigators may use computer forensic procedures or computer-assisted data analysis. All evidence obtained should be recorded chronologically in an inventory or log. Examples of evidence include:
   a. Letters and correspondence, both in hard copy or electronic form.
   b. Computer files, general ledger postings, or other financial or electronic records.
   c. System access records and internal phone records.
   d. Security and time keeping logs.
   e. Customer or vendor information, such as contracts, invoices, and payment information.
   f. Public records.
2. **Interviewing**: The investigator will interview individuals such as witnesses and facilitating personnel. Typically, the accused individual is interviewed after most applicable evidence has been obtained. Many investigators prefer to approach the accused with sufficient evidence that will support the goal to secure a confession. Interview and interrogation techniques are discussed in more details in the following pages.

G. When conducting fraud investigations, internal auditors:

1. Assess the probable level and the extent of complicity in the fraud within the organization. This can be critical to ensuring that the internal auditor avoids providing information to or obtaining misleading information from persons who may be involved.
2. Determine the knowledge, skills, and other competencies needed to carry out the investigation effectively. An assessment of the qualifications and the skills of internal auditors and of the specialists available to participate in the investigation needs to be performed to ensure that engagements are conducted by individuals having appropriate types and levels of technical expertise. This includes assurances on such matters as professional certifications, licenses, reputation, and that there is no potential conflict of interest with those being investigated or with any of the employees in the organization.
3. Design procedures to follow in attempting to identify the perpetrators, extent of the fraud, techniques used, and cause of the fraud.
4. Coordinate activities with management personnel, legal counsel, and other specialists as appropriate throughout the course of the investigation.
5. Be cognizant of the rights of alleged perpetrators and personnel within the scope of the investigation and the reputation of the organization itself.

H. Once a fraud investigation is concluded, internal auditors need to assess the facts known in order to:
   1. Determine if controls need to be implemented or strengthened to reduce future vulnerability.
   2. Design engagement tests to help disclose the existence of similar frauds in the future.
   3. Help meet the internal auditor's responsibility to maintain sufficient knowledge of fraud and thereby be able to identify future indicators of fraud.

I. **Reporting** of fraud is the responsibility of the CAE. It consists of the various oral or written, interim or final communications to management regarding the status and results of fraud investigations.
   1. It includes
      a. The reason for beginning an investigation.
      b. The timeframe.
      c. Observations and conclusions.
      d. Resolution and corrective action taken (or recommendations) to improve controls.
   2. Additional considerations in reporting of fraud are as follows:
      a. When the incidence of significant fraud or erosion of trust has been established to a reasonable certainty, senior management and the board must be notified immediately.
      b. The report of fraud needs to be written in a manner that provides confidentiality for some of the people involved.
      c. The results of a fraud investigation may indicate that fraud has had a previously undiscovered significant adverse effect on the financial position and results of operations of an organization for one or more years on which financial statements have already been issued. Internal auditors must inform senior management and the board of such a discovery.

d. In some cases, a draft of the proposed final communications on fraud is submitted to legal counsel for review. For example, the internal auditor wants to invoke client privilege, consideration should be given to addressing the report with legal counsel.

e. Management or the board determines whether to inform entities outside the organization such as law enforcement, regulatory agencies, oversight bodies, insurers, or bankers.

Passing Tip:	If an internal auditor has sufficient corroborated evidence to suspect fraud, the next step would be to notify the appropriate level of audit management, who ultimately considers all information, and notifies the correct level of management within the organization and NOT external parties (external auditor, external legal counsel, the police, SEC, etc.)

J. **Resolution** of fraud incidents consists of determining the actions that the organization will take after the investigation is complete. Management and the board are responsible for resolving fraud incidents. Resolution may include:

1. Providing closure to persons who were found to be innocent.
2. Disciplining an employee.
3. Requesting voluntary financial restitution.
4. Terminating contracts with suppliers.
5. Reporting the incident to law enforcement, regulatory bodies, or similar authorities; encouraging them to prosecute the fraudster.
6. Entering into civil litigation to recover the amount taken.
7. Filing an insurance claim.
8. Recommending control enhancements.

Interview and Interrogation Techniques

The following notes are adapted from the article "Interview & Interrogation Techniques for Auditors Reviewing Projects" by Richard B. Lanza which relies on work performed by Stan B. Walters in his book "Principle of Kinesic Interview and Interrogation"

Internal auditors are not normally involved in the interrogation of suspected perpetrators of the fraud, however, it is reasonable for internal auditors to know (at awareness levels) the interrogation/investigative techniques in case management requested the auditor to conduct a fraud investigation.

Passing Tip:	The internal auditor does not normally get involved in fraud investigations, unless specifically requested by management or the Board.

A. Interview and Interrogation (I&I) Techniques

1. I&I techniques are those tools and procedures that can be used to gather honest information from auditees. They are based on human behavior and the associated communication skills of humans, which are both verbal and non-verbal. Some studies have proven that human communication is mostly nonverbal (65%) so the auditor should be able to comprehend this type of communication to identify points of deception.
2. If the interviewee's nonverbal communication does not denote any deceptive behavior, it can be relied on as it provides **reasonable assurance** that the interviewee is being honest.
3. The goal of all I&I techniques is to determine whether the individual is being dishonest and then exactly what they are being dishonest about. This would be achieved by noting verbal and nonverbal communication during an interview and noting when the interviewee's communication may be deceptive. In such areas, the interviewer needs to "dig" for facts.

B. The Need for Interview and Interrogation Techniques

1. I&I techniques are needed simply because asking questions does not provide the same level of assurance of getting to the truth in particular matters such as when fraud is suspected or involved.
2. In fact, the range of deceptive behavior in an interview can range from unintentional misrepresentations that have no effect on the result of the interview to properly planned responses intended to deceive the interviewer. Such behavior is usually the result of stress.

C. Introduction to the I&I Process

1. **Stress** is otherwise known as the “fight or flight” pattern whereby an individual reacts to their environment and can be traced back to animal instincts. People generally flow through five stages but many times will skip a stage or move quickly through them, preferably ending in acceptance. The five stages are:
    a. **Anger –** more akin to the “fight” pattern whereby the individual becomes defensive, attacks the interviewer, and/or attacks the facts being presented in an attempt to maintain dominance and control over the interview.
    b. **Depression –** is an internalized anger whereby the subject attacks him/herself in an attempt to find a safe haven within oneself until the interview is over.
    c. **Denial –** whereby the interviewee denies any wrongdoing or any knowledge of the activity in question. This usually takes the form of selective memory where the subject remembers only pieces of events.
    d. **Bargaining –** the interviewee would be opening him/herself up by rationalizing what has happened, begging for sympathy, and ultimately, trying to see what will happen if the truth is told.
    e. **Acceptance –** the interviewee accepts the wrongdoing and understands that deceptive behavior so far has not been effective.
2. The following checklist is useful during the interview. It is separated into the five states stated in the previous section and then into two cross-sections explained below:
    a. **Verbal –** signs of deception whereby a person will change their voice quality, quantity, and/or content.
    b. **Nonverbal –** signs of deception seen through body language. These signs are generally the easiest to identify as it is difficult for the individual to hide these signals. It should be noted that just showing a nonverbal signal is not a conclusion of a person being deceptive but rather further confirmation of the verbal signals being provided by the individual.

State	Verbal Clues	Non-Verbal Clues
Anger	• Attacks interviewer • Attacks facts • Threatens interviewers job or status • Uses a plethora of obscene language	• Increasing redness in face • Physically touching the interviewer • V shaped eyebrow while staring at interviewer • Hand holding head with fingers in “L” shape • Agitated feet or legs (“itchy feet”)
Depression	• Mentions being down or depressed • Notes poor health or personal problems	• Sinking head down into chest (staring at ground) • Crying or otherwise sad facial expressions
Denial	• Takes a long time to respond to questions or uses fragmented sentences • Has memory lapses (especially selective lapses) • Asks questions rather than answering (e.g., Why would I risk my job like that?) • Uses phrases like “Honestly I don’t know” • Modifies the answer by using terms such as “possibly” or “occasionally”	• Showing a poker face and/or solid stare at the interviewer. • Blocking mouth with hand (touching eye, nose, or mouth) • Squeezing or pursing lips • A break in the normal eye contact pattern for that person. • Nervous use of hands (e.g., finger tapping or cleaning nails) • Crossed arms
Bargaining	• Complains for sympathy • Tries to rationalize why a third person would do the same thing • Is overly courteous to the interviewer	• False smile (wide or obtrusive) • Open arms (palms up) and/or leaning to the interviewer • Crying or otherwise sad facial expressions
Acceptance	• Asks, “What would happen to me if I did do it?” • Says, “I didn’t do it, but if you want me to say I did, I will”	• Rolling eyes back in the head with eyelids closing • Open arms (palms up) and/or leaning to the interviewer • A deep sigh

3. The following table summarizes the interviewer's recommended response for each state of the interviewee:

Interviewee's State	Interviewer's Response
Anger	– Remain professional and neutral: Simply ask questions – NOT get angry – Return to areas in the interview where the individual was in a more pleasant mood to calm the situation
Depression	– Understand and accept their depression – Try to comfort him/her – Question at key points regarding key facts
Denial	– Question with facts and figures and keep showing them to the individual – NOT force a confession from someone who is genuinely telling the truth and NOT showing verbal/nonverbal signs
Bargaining	– Listen openly and try to understand the person's position: Form a bond with the individual – NOT destroy their ego: Make understanding statements like "Anyone in your shoes would have done the same thing"
Acceptance	– LISTEN, LISTEN, and LISTEN some more – NOT destroy their ego: Make understanding statements like "Anyone in your shoes would have done the same thing"

D. The Process

1. Before the interview, identify an area where questionable information was given by the individual in the past or there may be a concern.
2. At the beginning of the interview, make the individual "feel at home" by discussing a general topic unrelated to the area in question. When doing so, note the individual's eye contact, body language, and verbal mannerisms as this represents their baseline state.

3. During the interview, ask that the person to discuss the area in question from start to finish and do not interject but rather listen completely. This also puts the person at ease, allowing them to either present an honest picture or a contrived one that can be easily remembered by the individual. As to their verbal/nonverbal signals at this point, they should still be generally in a comfortable state.
4. Finally, have the person recap key sections within the area in question by asking, "Let's go back to this part of the discussion …. how exactly did you calculate that figure?" Be sure to do so in a non-linear fashion so as to make the individual have to recap their previous start to finish explanation at various different points, almost in a non-logical fashion. At this point in the interview, be sure to pay close attention to the verbal/nonverbal signals as these would normally represent areas where the individual would use deceptive behavior, if in fact the person was dishonest. Once deceptive behavior is suspected, the interviewer should use the responses listed in the States of Dishonesty section of this outline (or the I&I Checklist) depending on the response being given.

Passing Tip:	During an interrogation, the interrogator should – Attempt to obtain general information prior to obtain specific information. – Consider making follow-up questions based upon interviewee's response and should not strictly adhere to a predetermined order. – Avoid leading questions, that is, questions that suggest an answer. – Concentrate on a certain subject or topic so as not to confuse the interviewee. – Take the role of one seeking the truth and avoid attempting to obtain confessions.

Legal Hazards

A. While interrogating suspected fraud committers, the internal auditor must be aware of their common law and statutory rights. Violation of these rights may enable suspects to sue the interrogator and the organization.

1. **Libel and Slander –** an employee accused of fraud may sue the auditor or the organization for defamation. This could take the form of libel or slander.
   a. **Defamation** is the allegation made by a fraud suspect. It could be in the form of either libel or slander.
   b. **Libel** is a false statement communicated to others in a written form.
   c. **Slander** is a false statement communicated to others in an oral or spoken form.
2. **False Imprisonment –** occurs if the employer unreasonably restrains an employee's freedom of mobility. Such restraint may be in the form of physical restraint (locking the employee in a room) or in the form of intimidating the employee or telling them they cannot leave the room or the city.

3. **Malicious Prosecution –** refers to the groundless prosecution of an employee with the intent of causing damage to the employee. The employer does not have sufficient evidence, and/or the employee did not commit the related fraud, however, the employer went through the prosecution.
4. **Compounding a Felony –** according to the law in some countries, the right to punish or forgive a criminal is reserved to the judiciary authorities i.e., the employer may neither impose a punishment on an employee nor can the employer negotiate not to prosecute an employee for a committed crime in return for a compensation. The employer may accept compensation or restoration of amounts lost, however, the acceptance of such amounts should not be bargained for by the employer on the grounds that they will not prosecute.

B. **Confessions –** the auditor needs to be cognizant to the fact that mere confessions by perpetrators may not constitute sufficient evidence if such confessions are not voluntarily made after the offense, and/or are made by the employee under pressure. Such confessions may be repudiated in court.

C. **Admissions –** while a confession is a complete acknowledgement of wrongdoing, an admission is a relevant statement of a fact that may be used against the suspect but is not as complete as a confession.

D. **Auditor's Recommended Actions**

1. The golden rule for auditors when a probability of legal hazards exists is to consult legal counsel.
2. During interrogations, the auditor would be better off in the presence of a witness.
3. The auditors should "do their homework" by researching issues prior to interviews and having sufficient background information on the topics to be raised during the interview.

This page intentionally left blank.

Supplement

International Standards for the Professional Practice of Internal Auditing

All Section	–	This section is included for reference. It compiles the IIA Standards as of the date of printing of this material.

International Standards for the Professional Practice of Internal Auditing

Attribute Standards

1000 – Purpose, Authority, and Responsibility

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

Interpretation:
The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization, including the nature of the chief audit executive's functional reporting relationship with the board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.

1000.A1 – The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

1000.C1 – The nature of consulting services must be defined in the internal audit charter.

1010 – Recognizing Mandatory Guidance in the Internal Audit Charter

The mandatory nature of the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing must be recognized in the internal audit charter. The chief audit executive should discuss the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework with senior management and the board.

1100 – Independence and Objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

Interpretation:

Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

1110 – Organizational Independence

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

Interpretation:

Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:

- *Approving the internal audit charter.*
- *Approving the risk-based internal audit plan.*
- *Approving the internal audit budget and resource plan.*
- *Receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters.*
- *Approving decisions regarding the appointment and removal of the chief audit executive.*
- *Approving the remuneration of the chief audit executive.*
- *Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.*

1110.A1 – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results. The chief audit executive must disclose such interference to the board and discuss the implications.

1111 – Direct Interaction with the Board

The chief audit executive must communicate and interact directly with the board.

1112 – Chief Audit Executive Roles Beyond Internal Auditing

Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.

Interpretation:

The chief audit executive may be asked to take on additional roles and responsibilities outside of internal auditing, such as responsibility for compliance or risk management activities. These roles and responsibilities may impair, or appear to impair, the organizational independence of the internal audit activity or the individual objectivity of the internal auditor. Safeguards are those oversight activities, often undertaken by the board, to address these potential impairments, and may include such activities as periodically evaluating reporting lines and responsibilities and developing alternative processes to obtain assurance related to the areas of additional responsibility.

1120 – Individual Objectivity

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Interpretation:

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.

1130 – Impairment to Independence or Objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Interpretation:

Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity's and the chief audit executive's responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.

1130.A1 – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

1130.A2 – Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

1130.A3 – The internal audit activity may provide assurance services where it had previously performed consulting services, provided the nature of the consulting did not impair objectivity and provided individual objectivity is managed when assigning resources to the engagement.

1130.C1 – Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

1210 – Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Interpretation:

Proficiency is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities. It encompasses consideration of current activities, trends, and emerging issues, to enable relevant advice and recommendations. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

1210.A1 – The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

1210.C1 – The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

1220 – Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A1 – Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or noncompliance.
- Cost of assurance in relation to potential benefits.

1220.A2 – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

1220.A3 – Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

1220.C1 – Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results.
- Relative complexity and extent of work needed to achieve the engagement's objectives.
- Cost of the consulting engagement in relation to potential benefits.

1230 – Continuing Professional Development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

1300 – Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Interpretation:

A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement. The chief audit executive should encourage board oversight in the quality assurance and improvement program.

1310 – Requirements of the Quality Assurance and Improvement Program

The quality assurance and improvement program must include both internal and external assessments.

1311 – Internal Assessments

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity.
- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

Interpretation:

Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Code of Ethics and the Standards.

Periodic assessments are conducted to evaluate conformance with the Code of Ethics and the Standards.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

1312 - External Assessments

External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The chief audit executive must discuss with the board:

- The form and frequency of external assessment.
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

Interpretation:

External assessments may be accomplished through a full external assessment, or a self-assessment with independent external validation. The external assessor must conclude as to conformance with the Code of Ethics and the Standards; the external assessment may also include operational or strategic comments.

A qualified assessor or assessment team demonstrates competence in two areas: the professional practice of internal auditing and the external assessment process. Competence can be demonstrated through a mixture of experience and theoretical learning. Experience gained in organizations of similar size, complexity, sector or industry, and technical issues is more valuable than less relevant experience. In the case of an assessment team, not all members of the team need to have all the competencies; it is the team as a whole that is qualified. The chief audit executive uses professional judgment when assessing whether an assessor or assessment team demonstrates sufficient competence to be qualified.

An independent assessor or assessment team means not having either an actual or a perceived conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs. The chief audit executive should encourage board oversight in the external assessment to reduce perceived or potential conflicts of interest.

1320 – Reporting on the Quality Assurance and Improvement Program

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board. Disclosure should include:

- The scope and frequency of both the internal and external assessments.
- The qualifications and independence of the assessor(s) or assessment team, including potential conflicts of interest.

- Conclusions of assessors.
- Corrective action plans.

Interpretation:

The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the board and considers the responsibilities of the internal audit activity and chief audit executive as contained in the internal audit charter. To demonstrate conformance with the Code of Ethics and the Standards, the results of external and periodic internal assessments are communicated upon completion of such assessments, and the results of ongoing monitoring are communicated at least annually. The results include the assessor's or assessment team's evaluation with respect to the degree of conformance.

1321 – Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"

Indicating that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing is appropriate only if supported by the results of the quality assurance and improvement program.

Interpretation:

The internal audit activity conforms with the Code of Ethics and the Standards when it achieves the outcomes described therein. The results of the quality assurance and improvement program include the results of both internal and external assessments. All internal audit activities will have the results of internal assessments. Internal audit activities in existence for at least five years will also have the results of external assessments.

1322 – Disclosure of Nonconformance

When nonconformance with the Code of Ethics or the Standards impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

Performance Standards

2000 – Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation:

The internal audit activity is effectively managed when:

- *It achieves the purpose and responsibility included in the internal audit charter.*
- *It conforms with the Standards.*

- *Its individual members conform with the Code of Ethics and the Standards.*
- *It considers trends and emerging issues that could impact the organization.*

The internal audit activity adds value to the organization and its stakeholders when it considers strategies, objectives, and risks; strives to offer ways to enhance governance, risk management, and control processes; and objectively provides relevant assurance.

2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:

To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

2010.A1 – The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2 – The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

2020 – Communication and Approval

The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2030 – Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Interpretation:

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

2040 – Policies and Procedures

The chief audit executive must establish policies and procedures to guide the internal audit activity.

Interpretation:

The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.

2050 – Coordination and Reliance

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Interpretation:

In coordinating activities, the chief audit executive may rely on the work of other assurance and consulting service providers. A consistent process for the basis of reliance should be established, and the chief audit executive should consider the competency, objectivity, and due professional care of the assurance and consulting service providers. The chief audit executive should also have a clear understanding of the scope, objectives, and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the chief audit executive is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.

2060 – Reporting to Senior Management and the Board

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the Standards. Reporting must also include significant risk and control issues, including fraud risks, governance issues, and other matters that require the attention of senior management and/or the board.

Interpretation:

The frequency and content of reporting are determined collaboratively by the chief audit executive, senior management, and the board. The frequency and content of reporting depends on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management and/or the board.

The chief audit executive's reporting and communication to senior management and the board must include information about:

- *The audit charter.*
- *Independence of the internal audit activity.*
- *The audit plan and progress against the plan.*
- *Resource requirements.*
- *Results of audit activities.*
- *Conformance with the Code of Ethics and the* Standards*, and action plans to address any significant conformance issues.*
- *Management's response to risk that, in the chief audit executive's judgment, may be unacceptable to the organization.*

These and other chief audit executive communication requirements are referenced throughout the Standards.

2070 – External Service Provider and Organizational Responsibility for Internal Auditing

When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.

Interpretation

This responsibility is demonstrated through the quality assurance and improvement program which assesses conformance with the Code of Ethics and the Standards.

2100 – Nature of Work

The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

2110 – Governance

The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

2110.A1 – The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation:
Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- *Organizational objectives support and align with the organization's mission.*
- *Significant risks are identified and assessed.*
- *Appropriate risk responses are selected that align risks with the organization's risk appetite.*
- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

2120.C1 – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

2130 – Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

2130.*C*1 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.

2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.

- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

2201.A1 – When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

2210 – Engagement Objectives

Objectives must be established for each engagement.

2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

2210.A3 – Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.

Interpretation:

Types of criteria may include:

- Internal (e.g., policies and procedures of the organization).
- External (e.g., laws and regulations imposed by statutory bodies).
- Leading practices (e.g., industry and professional guidance).

2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

2210.C2 – Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

2220 – Engagement Scope

The established scope must be sufficient to achieve the objectives of the engagement.

2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

2220.A2 – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

2220.C1 – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

2220.C2 – During consulting engagements, internal auditors must address controls consistent with the engagement’s objectives and be alert to significant control issues.

2230 – Engagement Resource Allocation

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

Interpretation:

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the engagement. Sufficient refers to the quantity of resources needed to accomplish the engagement with due professional care.

2240 – Engagement Work Program

Internal auditors must develop and document work programs that achieve the engagement objectives.

2240.A1 – Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

2240.C1 – Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

2300 – Performing the Engagement

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2310 – Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Interpretation:

Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Reliable information is the best attainable information through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organization meet its goals.

2320 – Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

2330 – Documenting Information

Internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

2330.A1 – The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

2330.A2 – The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2330.C1 – The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2340 – Engagement Supervision

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

Interpretation:

The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.

2400 – Communicating Results

Internal auditors must communicate the results of engagements.

2410 – Criteria for Communicating

Communications must include the engagement's objectives, scope, and results.

2410.A1 - Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans. Where appropriate, the internal auditors' opinion should be provided. An opinion must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

Interpretation:
Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the engagement results and their significance.

2410.A2 – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

2410.A3 – When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.

2410.C1 – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

2420 – Quality of Communications

Communications must be accurate, objective, clear, concise, constructive, complete, and timely..

Interpretation:

Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

2421 – Errors and Omissions

If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"

Indicating that engagements are "conducted in conformance with the International Standards for the Professional Practice of Internal Auditing" is appropriate only if supported by the results of the quality assurance and improvement program.

2431 – Engagement Disclosure of Nonconformance

When nonconformance with the Code of Ethics or the Standards impacts a specific engagement, communication of the results must disclose the:

- Principle(s) or rule(s) of conduct of the Code of Ethics or the Standard(s) with which full conformance was not achieved.
- Reason(s) for nonconformance; and
- Impact of nonconformance on the engagement and the communicated engagement results.

2440 – Disseminating Results

The chief audit executive must communicate results to the appropriate parties.

Interpretation:

The chief audit executive is responsible for reviewing and approving the final engagement communication before issuance and for deciding to whom and how it will be disseminated. When the chief audit executive delegates these duties, he or she retains overall responsibility.

2440.A1 – The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2 – If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization.
- Consult with senior management and/or legal counsel as appropriate.
- Control dissemination by restricting the use of the results.

2440.C1 – The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

2440.C2 – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

2450 – Overall Opinions

When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

Interpretation:

The communication will identify:

- *The scope, including the time period to which the opinion pertains.*
- *Scope limitations.*
- *Consideration of all related projects, including the reliance on other assurance providers.*
- *The risk or control framework or other criteria used as a basis for the overall opinion.*
- *The overall opinion, judgment, or conclusion reached.*

The reasons for an unfavorable overall opinion must be stated.

2500 – Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

2600 – Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Interpretation:

The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.