Study Unit One

Foundations of Internal Auditing

This study unit covers **Section A. Foundations of Internal Auditing, subsections 1.-3. and 7.-8.**, in The IIA's Part 1 CIA Exam Syllabus. This section is 35% of Part 1.

The **learning objectives** of Study Unit 1 are

- Describe the Purpose of Internal Auditing according to the Global Internal Audit Standards
- Explain the internal audit mandate and responsibilities of the board and chief audit executive
- Recognize the requirements of an internal audit charter
- Identify situations where the independence of the internal audit function may be impaired
- Recognize the internal audit function's role in the organization's risk management process

1.1 Purpose of Internal Auditing

Internal auditing is “[a]n independent, objective assurance and advisory service 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.”

The **purpose statement** helps internal auditors and stakeholders to understand and articulate the value of internal auditing.

Internal auditing creates value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight.

It enhances

- Successful achievement of the organization’s objectives
- Governance, risk management, and control processes
- Decision-making and oversight
- Reputation and credibility with stakeholders
- The ability to serve the public interest

Internal auditing is most effective when it is

- Done by skilled professionals: It is performed by competent professionals who conform to the Global Internal Audit Standards.
- Independent: Its position in the organization allows independence with direct accountability to the board.
- Unbiased: Internal auditors are free of undue influence and committed to objective assessments.

Internal Audit Mandate

According to **Principle 6 Authorized by the Board**, the board establishes, approves, and supports the mandate of the internal audit function.

- The board is the highest-level body charged with governance, e.g., a board of directors, an audit committee, or a board of governors or trustees.

The mandate specifies internal audit’s authority, role, and responsibilities and is documented in the **charter**. It gives internal audit the right to provide the board and senior management with objective assurance, advice, insight, and foresight. Thus, internal audit has a dual-reporting relationship with the board and senior management. The mandate should be performed by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management, and control processes.

Standard 6.1 Internal Audit Mandate states that the chief audit executive (CAE) must give the board and senior management the information to establish the mandate. If a law or regulation prescribes the mandate, the charter must include the legal requirements.

- The CAE is a person in a senior position responsible for effectively managing the internal audit function in accordance with the Standards and ensuring the quality of internal audit services. The specific job title may vary depending on the organization.
- The board and senior management decide the extent and types of internal audit services to be offered. The CAE should work with both internal and external assurance providers. This cooperation helps everyone involved to clarify his or her specific roles and responsibilities.
- The CAE also must document or refer to the mandate in the board-approved charter.
- The CAE should regularly assess whether any changes in the organization require a conversation with the board and senior management regarding the audit mandate. If such changes are needed, the CAE must work with these groups to make sure that the internal audit's power, function, and duties continue to support the organization's goals and strategies.
- **The board must**
  - Talk with the CAE and upper management about the proper authority, functions, and duties of the internal audit team.
  - Approve the internal audit charter, including the mandate, scope, and types of services.
- **Senior management must**
  - Join conversations with the board and the CAE to share thoughts on what the board should expect from internal audit as they create its mission.
  - Encourage support for internal audit's role across the organization and emphasize the authority it has been given.

Implementation

The CAE informs the board and senior management about the characteristics of an effective internal audit function. The CAE shares knowledge about the Standards, relevant laws or regulations, and the results of research into leading practices.

The CAE also should discuss with the board and senior management the internal audit mandate and other key elements of the internal audit charter.

- **Authority** is based on a direct reporting relationship with the board, allowing for unrestricted access to the board and all organizational activities (for example, records, personnel, and physical property).
- The main job of the internal audit team is to carry out audit tasks and provide audit services. Sometimes, the CAE may also have additional duties that include risk management or compliance, beyond just internal auditing.

- Responsibilities consist of the obligations and accountability of the role(s) as well as the expectations of key stakeholders. They may include
  - Performance of audit services;
  - Communications;
  - Attention to compliance with laws, regulations, and policies;
  - Conformance with the Global Internal Audit Standards; and
  - Other activities.
- The **scope** of services for the internal audit function covers all of the organization's activities under review by the internal audit function.
  - The scope may include all activities, assets, and personnel or may be restricted to a subset defined by, for example, geography.
  - The scope may specify the nature of services (for example, assurance and advisory, financial statements, compliance with laws or regulations), or other limitations.
- **Internal audit services** may simply be assurance and advisory services or may be more specific, such as performance auditing, assurance regarding internal controls over financial reporting, and investigations.
  - In their performance of services, internal auditors should determine that their operating and program objectives have been established and conform to the organization.

Circumstances may justify a **follow-up discussion** with the board and senior management on the internal audit mandate or other aspects of the internal audit charter. These conditions may include

- A notable change in the Standards
- A significant acquisition or reorganization
- A significant change in the board or senior management
- A significant change in strategies, objectives, risk profile, or the operating environment
- A new law or regulation that may affect the nature or scope of services

The CAE should formally consider any such changes at least annually.

The CAE coordinates with assurance providers and advises the board about how other functions may contribute to the internal audit mandate. By helping the board understand the roles and responsibilities of other assurance providers and regulators, the CAE may clarify an appropriate mandate.

1.2 Internal Audit Charter

According to **Standard 6.2 Internal Audit Charter**, the CAE must develop and maintain a charter that specifies at a minimum the following internal audit functions:

- Purpose of Internal Auditing
- Adherence to the Standards
- Internal audit mandate, including scope and services, and the board's responsibilities and expectations about management's support of internal audit
- Organizational position and reporting relationships

The CAE must confirm that the proposed charter accurately reflects the board's and senior management's understanding and expectations of internal audit.

The board must

- Talk with the CAE and senior management about additional subjects that should be part of the internal audit charter to ensure the internal audit function operates effectively.
- Endorse the internal audit charter, which outlines its purpose, along with the range and kinds of services it will provide.
- Review the internal audit charter with the CAE to evaluate any modifications needed due to changes within the organization or the nature of services provided, such as hiring a new CAE, shifts in the nature and complexity of the risks the organization faces, or approval to offer advisory services.

Senior management must

- Communicate with the board and the CAE concerning management's expectations that deserve evaluation for incorporation in the charter.

Implementation

Requirements for the charter are outlined in Subunits 1.1 and 1.3.

The charter should describe administrative **reporting** responsibilities, such as the process for

- Approving the internal audit function's human resources administration and budgets
- Approving the CAE's expenses
- Reviewing the CAE's performance

If laws or rules define how reporting should occur, those should be clearly explained.

The CAE should tailor the internal audit charter to reflect the specific characteristics of the organization. This customization is important for shaping internal audit's mandate, scope, and the services it provides.

The CAE usually shares the final version of the internal audit charter at a board meeting for discussion and **approval**.

The CAE and the board need to decide how often they will examine the charter to ensure it still supports the goals of the internal audit function. It is good practice to review the charter at regular intervals, refer to it whenever there are questions about internal audit's role, and make updates when necessary.

The following are other topics relevant to inclusion in the charter:

- **Safeguards** for objectivity and independence, including processes for potential impairments and periodic reevaluation to ensure they are still effective.
- Unrestricted **access**, including how data, records, information, personnel, and physical properties are accessed to fulfill the mandate.
- **Communications**, including nature and timing, with the board and senior management.
- **Audit process**, including expectations about communications with management (before, during, and after an audit) and how disagreements with management are resolved.
- **Quality** assurance and improvement, including expectations for internal and external assessments of internal audit and communicating the results.
- **Approvals**, including any circumstances specified by the board and senior management.

1.3 Impairment of Independence

The **Purpose of Internal Auditing** cannot be fulfilled unless the CAE

- Reports directly to the board,
- Is qualified, and
- Is positioned in the organization so that the function can discharge its services and responsibilities without interference.

According to **Principle 7 Positioned Independently**, the board establishes and protects the internal audit function's independence and qualifications.

Independence is freedom from conditions that impair the function's ability to perform responsibilities without bias.

Standard 7.1 Organizational Independence states that the CAE must confirm to the board the organizational independence of the internal audit function **at least annually**.

- The CAE also communicates instances in which (1) independence may have been impaired and (2) actions or safeguards addressed the impairments.
- The CAE must document in the charter the reporting relationships and organizational position of the internal audit function determined by the board.
- The CAE should have many opportunities to communicate and interact directly with the board. Board meeting agendas and minutes often are evidence of internal audit's organizational independence.

The CAE must (1) discuss with the board and senior management any roles and responsibilities that may **impair** the function's independence and (2) recommend safeguards.

- When the CAE takes on additional roles outside internal auditing, the responsibilities, the type of work, and any protective measures must be clearly outlined within the internal audit charter.
  - If these responsibilities also fall under the scope of internal auditing, then alternative methods must be put in place to ensure proper oversight. This could involve hiring an independent and skilled external assurance provider who will report directly to the board.

If the CAE takes on nonaudit tasks temporarily, an independent third party must oversee those areas during this time and for the following 12 months.

If the governing structure does not allow for independence within the organization, the CAE needs to record the traits of this structure that restrict independence. The CAE also should note any measures that can be taken to help maintain this principle.

The board must

- Create a direct connection between the CAE and the internal audit team, which helps the internal audit team effectively carry out its responsibilities.
- Approve the hiring and dismissal of the CAE.
- Offer guidance to senior management to assist in assessing the performance and compensation of the CAE.
- Allow the CAE to have discussions with the board about important and sensitive issues, including the possibility of holding meetings where senior management is not present.
- Require that the CAE be in a position so that services and responsibilities can be performed without interference, including the ability to bring matters **directly** to senior management and escalate them to the board.
- Acknowledge impairments of independence when approving roles for the CAE that are beyond the scope of internal auditing.
- Engage with senior management and the CAE to establish safeguards if the CAE's roles and responsibilities impair independence.
- Engage with senior management to ensure that the internal audit function is free from interference when (1) determining its scope, (2) performing engagements, and (3) communicating results.

Senior management must

- Assign the internal audit function to a level in the organization that enables it to perform its services and responsibilities without interference.
- Recognize the CAE's direct reporting relationship with the board.
- Engage with the board and the CAE to (1) understand potential impairments of independence and (2) support the appropriate safeguards.
- Communicate to the board the reasons for appointment or removal of the CAE.
- Solicit input from the board on the performance evaluation and remuneration of the CAE.

Implementation

Internal audit is most effective when it **functionally (directly) reports** to the board. This relationship enables performing services and communicating results without interference or undue limitations. Examples of interference with internal audit's ability to operate effectively include management's

- Failing to provide timely information;
- Restricting access to information, personnel, or physical properties; or
- Unduly limiting resources (budget reduction).

The CAE's **administrative reporting** relationship is often to a member of management. Thus, the CAE has a dual-reporting relationship with the board and management. It enables access to senior management and the authority to challenge management's perspectives. The **leading practice** is for the CAE to report administratively to the chief executive officer or equivalent, although reporting to another senior officer may achieve the same objective given safeguards.

When evaluating impairment of independence, the CAE should consider reporting relationships, roles, and responsibilities to determine whether actual, potential, or perceived impairments exist.

Impairments of independence may include the following:

- The CAE lacks direct communication with the board.
- Management attempts to limit the scope of services previously approved by the board and documented in the charter.
- Management attempts to restrict access to data, records, information, personnel, and physical properties required to perform the internal audit services.
- Management pressures auditors to suppress or change findings.
- Reduction of internal audit’s budget leaves the function unable to meet its responsibilities.
- Internal audit performs, or the CAE supervises, an assurance engagement in a functional area in which the CAE has significant influence.
- Internal audit performs, or the CAE supervises, assurance services related to an activity managed by a senior executive (non-CEO) to which the CAE reports administratively.

The CAE may have a **nonaudit** role that may impair, or appear to impair, internal audit’s independence. Examples are the following:

- Development of risk management activities is needed immediately with a new regulation.
- The CAE is most qualified to adapt existing risk management activities to a new business segment or geographic market.
- The organization’s resources are too limited or it is too small to afford a separate compliance function.

When discussing nonaudit roles and responsibilities with the board and senior management, the CAE should identify appropriate **safeguards** depending on whether the roles are (1) permanent or (2) temporary and intended to be transferred to management.

When the board agrees that an impairment has occurred, the CAE should suggest potential safeguards to manage the risks. Also, a **timeline** should be specified for transferring temporary nonaudit responsibilities to management.

- The requirement is to have **assurance** activities overseen by an independent **third party** for the subsequent 12 months after the CAE completes temporary nonaudit responsibilities.
  - However, the CAE should discuss with the board and senior management whether 12 months is appropriate.

1.4 Role in Risk Management

According to **Principle 9 Plan Strategically**, the CAE plans strategically to position the internal audit function to fulfill its mandate and achieve long-term success. Planning strategically requires understanding

- The internal audit mandate and
- The organization's governance, risk management, and control processes.

Standard 9.1 Understanding Governance, Risk Management, and Control Processes states that an effective internal audit strategy and plan requires the CAE to understand, among other things, risk management.

- The IIA defines risk management as a "process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives."
- **Risk** is defined as the positive or negative effect of uncertainty on objectives.

To understand risk management, the CAE must consider how the organization identifies and assesses significant risks. The understanding includes how the organization identifies and manages the following:

- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations and programs
- Safeguarding of assets
- Compliance with laws or regulations

Implementation

The **CAE's understanding** is developed by gathering information broadly and viewing it comprehensively. Sources include

- Discussions with the board and senior management,
- Reviews of their minutes and presentations,
- Communications and workpapers from internal audit engagements, and
- Assessments and reports by other providers of assurance and advisory services.

The CAE should understand widely accepted risk management principles, frameworks, and models and professional guidance specific to the organization. The CAE then should gather information to assess the maturity of the risk management process and identify whether

- The **risk appetite** (types and amount of acceptable risk in pursuit of strategies and objectives) has been defined and
- A risk management strategy (or framework) has been implemented.

Discussions with the board and senior management help the CAE understand their perspectives and priorities related to risk management.

To gather risk information, the CAE should review recent risk assessments and related communications issued by

- Senior and operational management,
- Those charged with risk management,
- External auditors,
- Regulators, and
- Other internal and external providers of assurance services.

Three Lines Model

The IIA's Three Lines Model is a framework designed to help organizations manage risk and ensure effective governance. In a nutshell, it helps organizations better manage risks, achieve objectives, and ensure good governance, making it a valuable tool for any organization aiming for long-term success.

How it Works

The model outlines three key roles (each described as a line) within an organization that work together to support its goals and protect its assets.

- **First Line.** This involves the management and staff directly responsible for managing risks and achieving the organization's objectives. They do the day-to-day operations.
- **Second Line.** This role includes functions that provide oversight and support, such as risk management and compliance teams. They help ensure that the first line is managing risks appropriately.
- **Third Line.** This represents internal audit, which provides independent assurance that the organization's risk management processes are effective. Internal audit verifies that both the first and second lines are executing their tasks as intended.

Rationale for Implementation

The Three Lines Model is important because it promotes clear roles and responsibilities, which helps to

- Prevent confusion about responsibilities
- Ensure that all aspects of risk management are covered, leading to better decision making
- Enhance accountability by clearly defining oversight duties

The model also emphasizes creating and protecting value through alignment, communication, coordination, and collaboration, which enhances the reliability and transparency of information necessary for risk-based decision making.

Motivations for Implementation

Organizations want to implement the Three Lines Model because it helps

- Foster a culture of transparency and ethical behavior
- Coordinate efforts across different departments and avoid siloed operations, ensuring that all parts of the organization work together effectively
- Improve governance by ensuring that checks and balances are in place to uphold standards and protect organizational value

Principles

The IIA's Three Lines Model is based on six principles.

- **Principle 1: Governance.** Appropriate structures and processes should enable
  - Accountability by a governing body (generally the board) to stakeholders for organizational oversight. Stakeholders are those whose interests are served or affected.
  - Managerial actions (including risk management) to achieve objectives through risk-based decisions.
  - Assurance and advice by a competent, objective, and independent internal audit function that provides confidence and clarity and facilitates continuous improvement.
- **Principle 2: Governing body roles.** They include
  - Ensuring structures and processes exist for effective governance.
  - Ensuring objectives and activities align with stakeholder interests.
  - Giving management the responsibility and resources to achieve objectives and compliance with laws, regulations, and ethics.
  - Establishing and overseeing the internal audit function.
- **Principle 3: Management – First and second line roles.**
  - **First line roles** most directly relate to delivery of products or services to clients. They include support functions (e.g., human resources). They are directly responsible for risk management.
  - **Second line roles** (some of which may be assigned to specialists) assist with risk management (a first line role) by providing expertise, support, monitoring, and challenge. Specific objectives may relate to compliance, sustainability, ethics, internal control, IT, quality, or enterprise risk management (ERM).
- **Principle 4: Third line roles.**
  - Internal audit (1) provides assurance and advice on the adequacy and effectiveness of governance, risk management, and compliance and (2) reports to management and the governing body on objective achievement and continuous improvement. It may consider assurance from other internal or external providers when performing these responsibilities.
- **Principle 5: Third line independence.**
  - Internal audit independence is achieved through (1) accountability to the governing body; (2) unfettered access to people, resources, and data; and (3) freedom from bias and interference.

- **Principle 6: Creating and protecting value.**
  - Alignment of the activities of roles (communication, cooperation, and collaboration) collectively creates and protects value. It ensures the reliability, coherence, and transparency of risk-based decisions.

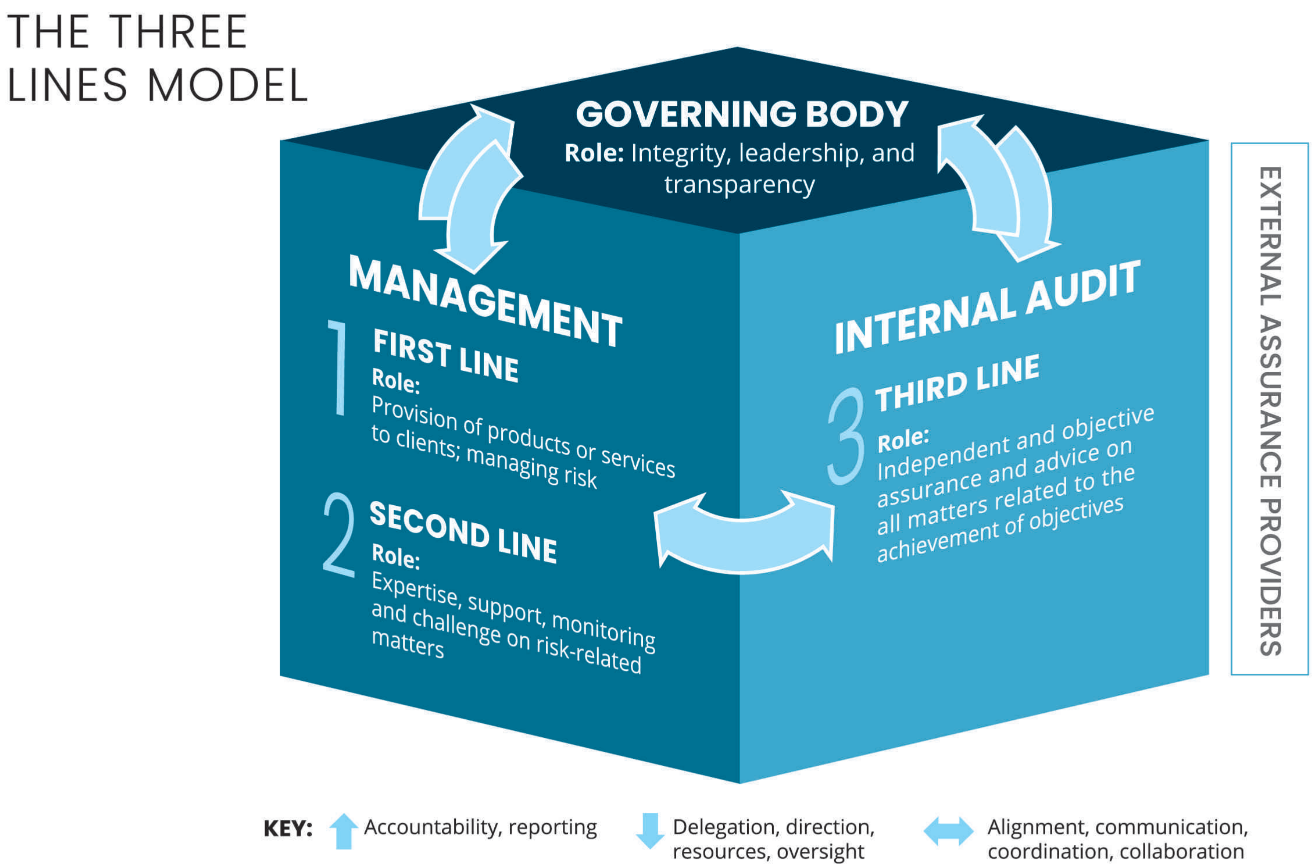

Figure 1-1

Success Tip

Understand the Three Lines Model, specifically, the difference between first, second, and third line roles.