# Study Unit Six

## Governance



This study unit covers **Section C. Governance, Risk Management, and Control, subsections 1.-3.**, in The IIA's Part 1 CIA Exam Syllabus. This section is 30% of Part 1.

The **learning objectives** of Study Unit 6 are

- Describe the concept of organizational governance
- Recognize the impact of organizational culture on the overall control environment and individual engagement risks and controls
- Recognize ethical and compliance-related issues

# 6.1 Governance Principles

**Governance** is “the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward achievement of its objectives.” It involves establishing the relationships between an organization’s management, its board, its shareholders, and other stakeholders who have an interest in its activities and outcomes.

- **Stakeholders** are parties with a direct or indirect interest in an organization’s activities and outcomes. They may include (1) the board, (2) management, (3) employees, (4) customers, (5) vendors, (6) shareholders, (7) regulators, (8) financial institutions, (9) external auditors, and (10) the public.

Key components of governance include setting objectives, determining how to achieve them, and monitoring performance. Stakeholders can range from employees and customers to regulators and the public, and their expectations greatly influence governance practices.

Governance is closely linked with risk management and control, ensuring that the organization operates effectively within acceptable risk levels. The board of directors or similar governing body oversees these processes, holds senior management accountable, and makes critical decisions regarding the organization’s direction, resources, and risk strategies.

In essence, effective governance ensures that an organization is well managed, accountable to its stakeholders, and aligned with its objectives while also being responsive to risks and changes in the environment.

The IIA defines governance as “[t]he 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” (The IIA Glossary).

- Governance is a set of relationships among an organization’s management, its board, its shareholders, and other stakeholders. In every organization, there is a clear hierarchy to ensure effective governance, which involves oversight, accountability, and decision making.
  - Governance also is the structure through which objectives are set, and the means of attaining those objectives and monitoring performance are determined (Organization for Economic Co-operation and Development).

Governance may be influenced by internal or external mechanisms.

- Internal mechanisms include corporate charters and bylaws, boards of directors, and internal audit functions.
- External mechanisms include laws, regulations, and the government regulators who enforce them.

Governance does not exist independently of risk management and control. Rather, governance, risk management, and control are interrelated.

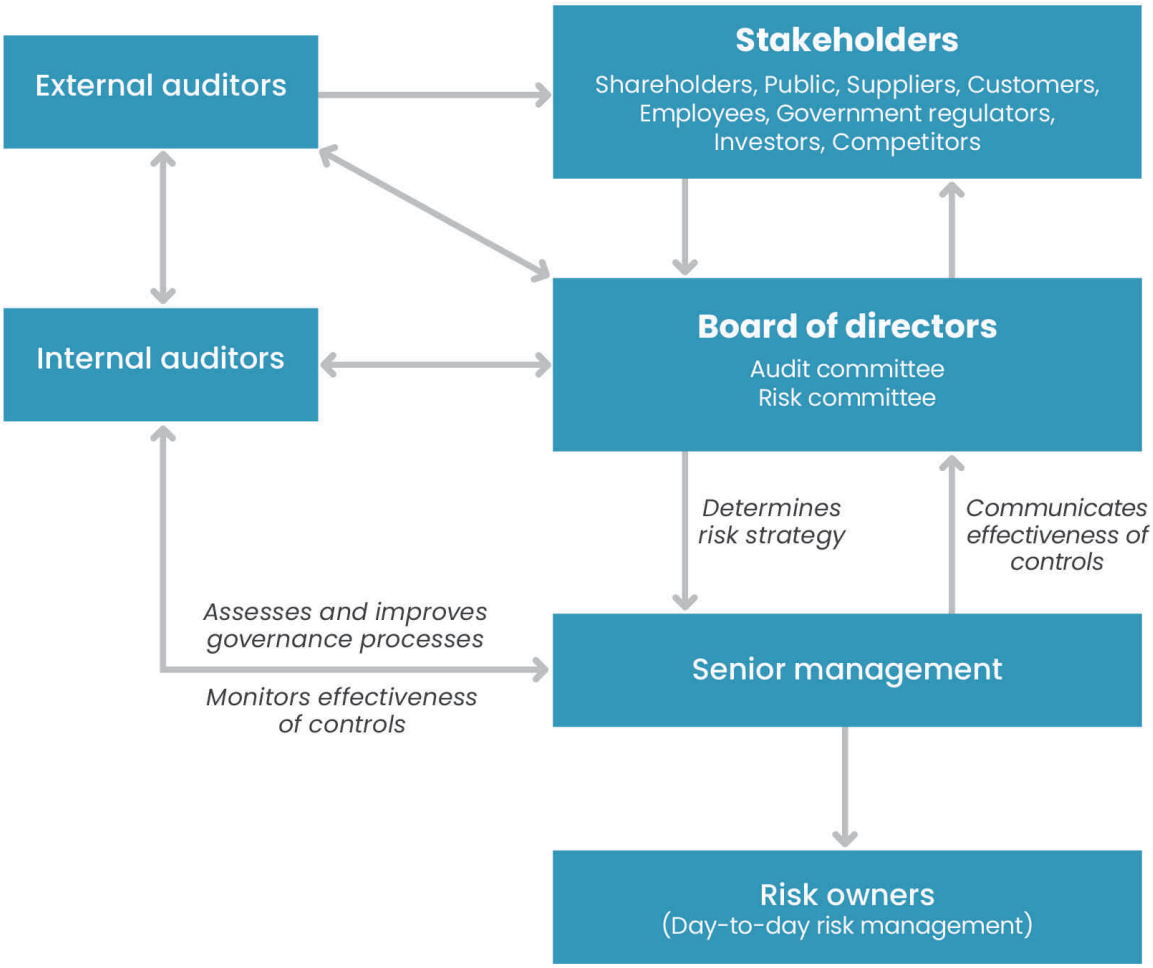


Figure 6-1

- Effective governance considers risk when setting strategy, and risk management relies on effective governance (e.g., tone at the top, risk appetite and tolerance, risk culture, and the oversight of risk management).
- Effective governance relies on controls to manage risks and on communication of their effectiveness to the board.

The following is a summary of governance principles:

- An independent and objective board with sufficient expertise, experience, authority, and resources to conduct independent inquiries
- An understanding by senior management and the board of the operating structure, including structures that impede transparency
- An organizational strategy used to measure organizational and individual performance
- An organizational structure that supports accomplishing strategic objectives
- A governing policy for the operation of key activities
- Clear, enforced lines of responsibility and accountability
- Effective interaction among the board, management, and assurance providers
- Appropriate oversight by management, including strong controls
- Compensation policies (especially for senior management) that encourage appropriate behavior consistent with the organization's values, objectives, strategy, and internal control
- Reinforcement of an ethical culture, including employee feedback without fear of retaliation
- Effective use of internal and external auditors, ensuring their independence, the adequacy of their resources and scope of activities, and the effectiveness of operations
- Clear definition and implementation of risk management policies and processes
- Transparent disclosure of key information to stakeholders
- Comparison of governance processes with national codes or best practices
- Oversight of related-party transactions and conflicts of interest

Governance has two major components: **strategic direction** and **oversight**.

1. **Strategic direction** determines the
   - Business model,
   - Overall objectives,
   - Approach to risk taking (including the risk appetite), and
   - Limits of organizational conduct.
2. **Oversight** is the governance component with which internal auditing is most concerned. It is also the component to which risk management and control processes are most likely to be applied. The elements of oversight are
   - Risk management activities performed by senior management and risk owners and
   - Internal and external assurance activities.

According to The IIA, the **board** is the "highest-level body charged with governance," such as a board of directors, an audit committee, a board of governors or trustees, etc. Its main role is to guide and supervise the organization's actions and ensure that senior managers are held responsible for their performance.

- Governance structures may differ based on location and industry, but usually, a board consists of directors (individuals) not involved in day-to-day management. Absent a board, the term refers to either a group or an individual who serves as the governing authority for the organization, such as the head of the organization and senior management. Directors must have certain qualities to be effective.
  - A majority of the board should be outside directors.
  - Directors generally should have years of experience in either the industry or corporate governance.
  - Directors must be willing to challenge management's choices. Complacent directors increase the chances of adverse consequences.
- When an organization has multiple governing groups, the "board" is the group that grants internal audit its power to operate.
  - Another key duty is to recognize **stakeholders**. The board needs to understand what stakeholders want and identify the results they will not tolerate.
- The board has the following duties:
  - Selection and removal of officers
  - Decisions about capital structure (mix of debt and equity, consideration to be received for shares, etc.)
  - Adding, amending, or repealing bylaws (unless this authority is reserved to the shareholders)
  - Initiation of fundamental changes (mergers, acquisitions, etc.)
  - Decisions to declare and distribute dividends
  - Setting of management compensation (sometimes performed by a subcommittee called the compensation committee)
  - Coordinating audit activities (most often done by the audit committee)
  - Evaluating and managing risk (sometimes done by the risk committee)
- A **risk committee** may be created that (1) identifies key risks, (2) connects them with risk management processes, (3) delegates them to risk owners, and (4) considers whether risk tolerances are consistent with the organization's risk appetite.
  - Some functions of risk committees, such as delegating to risk owners, may be tasks otherwise reserved for management. But the risk committee's overall role is still oversight.

**Management** performs day-to-day governance functions. Senior management carries out board directives (within specified tolerances for unacceptable outcomes) to achieve objectives.

- Senior management determines
  - Where specific risks are to be managed,
  - Who will be **risk owners** (managers responsible for specific day-to-day risks), and
  - How specific risks will be managed.
- Senior management establishes reporting requirements for risk owners related to their risk management activities.
- Governance expectations, including tolerance levels, must be periodically reevaluated by the board and senior management. The result may be changes in risk management activities.

**Risk owners** are responsible for

- Evaluating the adequacy of the design of risk management activities and the organization's ability to carry them out as designed;
- Determining whether risk management activities are operating as designed;
- Establishing monitoring activities; and
- Ensuring that information to be reported to senior management and the board is accurate, timely, and available.

Each level works together to create a structure of accountability and oversight–this is the essence of governance. The board asks management to achieve objectives while considering stakeholder interests and potential risks. The risk committee supports this by focusing on risk management, allowing for informed decision making.

By clearly defining roles and responsibilities, the organization can effectively navigate risks and ensure that it not only meets its goals but also does so in a responsible and sustainable manner. This framework helps prevent failures and ensures that all actions are aligned with the organization's mission, ultimately building trust and confidence among stakeholders. Proper governance leads to better decision making, ethical practices, and greater organizational success.

## 6.2 Organizational Culture

Governance practices reflect the organization's unique culture and largely depend on it for effectiveness.

Organizational culture consists of the attitudes, behaviors, and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision, and core values of the organization.

- **Mission** is the organization's core purpose.
- **Vision** is the organization's aspirations for what it intends to achieve over time.
- **Core values** are the organization's essential beliefs about what is acceptable or unacceptable.

Accordingly, organizational culture is reflected in

- Setting values, objectives, and strategies;
- Defining roles and behaviors;
- Measuring performance;
- Specifying accountability; and
- Complying with corporate social responsibilities.

Organizational culture affects the **control environment** and individual engagement risks and controls. The control environment consists of the attitudes and acts of the board and management regarding organizational control. It provides the discipline and structure for achieving the primary objectives of internal control.

**Example 6-1 Organizational Culture and the Control Environment**

If an organization's culture is risk aggressive, it is more likely to have a lesser degree of regard for internal control, and internal auditors are more likely to underestimate engagement risks.

But, if an organization's culture is risk averse, it is more likely to have a higher degree of regard for the importance of internal control, and internal auditors are more likely to overestimate engagement risks.

**Senior management** is primarily responsible for establishing and maintaining an organizational culture.

For example, an "unhealthy" organizational culture might impose unreasonable expectations on its employees. This could negatively affect the objectivity of decision making and would increase the risk to the effectiveness of the governance structure in supporting organizational objectives.

Governance practices may use various legal forms, structures, strategies, and procedures. They ensure that the organization

- Complies with society's legal and regulatory rules;
- Satisfies generally accepted business norms, ethical principles, and expectations of society;
- Provides overall benefit to society and enhances the interests of the specific stakeholders in both the long and short term; and
- Reports fully and truthfully to its stakeholders, including the public, to ensure accountability for its decisions, actions, and performances.

## Ethical Culture

The ethical culture is an important component of the organizational culture and is crucial to the effectiveness of governance. Because decision making is complex and dispersed in most organizations, each person should be an ethics advocate, whether officially or informally.

Codes of conduct and vision statements are issued to state

- The organization's values and objectives;
- The behavior expected; and
- The strategies for maintaining a culture consistent with legal, ethical, and societal responsibilities.

A **code of conduct** addresses an organization's values, objectives, and legal responsibility. In addition, the code should address ethical issues employees may encounter and provide guidance on how to resolve the issues.

The **board** oversees the organization's ethical climate.

**Senior management** has ultimate responsibility for promoting and setting the example of ethical behavior (i.e., setting the tone at the top).

- Senior management is also responsible for establishing and maintaining sound ethics-related objectives and programs.

To promote an ethical culture, an organization may designate a chief ethics officer.

**Internal auditors** may have an active role in support of the organization's ethical culture. Roles may include chief ethics officer, member of an ethics council, or assessor of the ethical climate.

- In some circumstances, the role of chief ethics officer may conflict with the independence attribute of the internal audit function.
  - The organizational independence of the internal audit function is necessary because it performs internal assurance services.

Internal auditors periodically assess the elements of the ethical climate of the organization and its effectiveness in achieving legal and ethical compliance. Thus, they evaluate the effectiveness of the following:

- A formal code of conduct and related statements and policies (including procedures covering fraud and corruption)
- Demonstrations of ethical attitudes and behavior by influential leaders
- Explicit strategies to support the ethical culture
- Confidential reporting of alleged misconduct
- Regular declarations by employees, suppliers, and customers about the requirements of ethical behavior
- Clear delegation of responsibilities for providing counsel, investigation, and reporting
- Easy access to learning opportunities
- Personnel practices that encourage contributions by employees
- Regular surveys of employees, suppliers, and customers to determine the state of the ethical climate
- Regular reviews of the processes that undermine the ethical culture
- Regular reference and background checks

Study Unit 3, Subunit 5, has a summary of an assurance engagement focused on auditing organizational culture.

# 6.3 Roles of Internal Auditors in Governance

## Internal Audit Function

Understanding the role of the internal audit function begins with understanding the nature of governance in a specific organization.

Governance has a range of definitions depending on the circumstances.

- The CAE should work with the board and senior management to determine how governance should be defined for audit purposes.

**Principle 9 Plan Strategically** states that the CAE plans strategically to position the internal audit function to fulfill its mandate and achieve long-term success.

Planning strategically requires the CAE to understand the internal audit mandate and the organization's governance, risk management, and control processes. A properly resourced and positioned internal audit function develops and implements a strategy to support the organization's success. The CAE also creates and implements methodologies to guide the internal audit function and develop the internal audit plan.

According to **Standard 9.1 Understanding Governance, Risk Management, and Control Processes**, to understand governance processes, the CAE must consider how the organization

- Establishes strategic objectives and makes strategic and operational decisions
- Oversees risk management and control
- Promotes an ethical culture
- Delivers effective performance management and accountability
- Structures its management and operating functions
- Communicates risk and control information throughout the organization
- Coordinates activities and communications among the board, internal and external providers of assurance services, and management

## Implementation

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

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

The CAE should be well-informed about leading governance principles, globally accepted governance frameworks and models, and professional guidance specific to the organization's industry and sector.

With this understanding, the CAE needs to determine whether any of these practices are in place within the organization and evaluate how advanced its governance processes are. How governance is organized and practiced can be influenced by specific traits of the organization, including its nature, scale, complexity, framework, the level of development of its processes, and applicable laws or regulations.

The CAE may examine the documents generated by the board and its committees. Examination helps the CAE to comprehend how the board contributes to managing the organization effectively, particularly in making important strategic and operational choices.

The CAE may interview persons who have important positions in the various facets of the governance processes. These interactions may familiarize the CAE with the organization's governance processes and evaluations. The CAE also may read reports or findings from past governance reviews, especially those that raised specific issues.

## Internal Audit and Governance

A clear understanding of how the organization is managed, how it handles risks, and how it controls its operations allows the CAE to choose, and assess the importance of, internal audit services that may improve the organization's success. These activities support the internal audit strategy and planning.

Governance experts typically view it as a dynamic process, not a fixed system.

Governance rules differ depending on the type of organization and applicable laws. For instance, these can include public companies, non-profit organizations, government bodies, private firms, and stock markets.

Effective governance is shaped by several factors, including

- The organization's size, complexity, and stage of its development
- The makeup of its stakeholders
- The legal and cultural context in which it operates

The main role of internal auditing is to assess and enhance governance practices.

Internal auditors have a special role that allows them to scrutinize and evaluate governance practices without being influenced by the organization.

The board and senior management need a shared understanding of the nature of governance. Internal auditors need to be familiar with governance processes and how they interact with risk management and control measures.

Internal auditors evaluate how well governance processes are designed and how effectively they work in practice. They also offer suggestions for enhancing these processes.

Internal auditors also may advise the board to perform self-evaluations of its governance practices. An audit plan needs to be created by analyzing risks that address governance processes and their controls.

This plan should emphasize any governance processes that present higher risk. Furthermore, if the board or top management asks for an evaluation, an assessment of relevant processes or risk areas may need to be included in the audit plan.

With respect to governance processes, the audit plan

- Specifies the nature of the procedures;
- Identifies the processes; and
- States the types of evaluations, such as those for risks and means of reducing risks.

The CAE should keep the following points in mind when planning evaluations of governance:

- The audit needs to examine the safeguards in governance processes intended to stop or identify conditions that could harm the organization.
- Safeguards within processes may be crucial in handling various risks. For instance, the rules outlined in the code of conduct may help manage risks related to compliance and fraud.
- If other audits evaluate safeguards, the auditor may use their findings to inform the work.

Evaluating governance usually relies on multiple audits. The internal auditor’s decision process may include

- Examinations of particular processes,
- Governance concerns resulting from audits not specifically addressing governance,
- Findings from other assurance providers, and/or
- Any details about negative events that point to chances for enhancing governance.

Given control weaknesses or if the governance process is not well-developed, the CAE may apply different procedures for strengthening control or improving governance using advisory services.

Other roles of internal auditors in governance include the following:

- Obtain the board's approval of the internal audit charter
- Communicate the plan of engagements
- Report significant audit issues
- Communicate key performance indicators to the board on a regular basis
- Discuss areas of significant risk
- Support the board in organization-wide risk assessment
- Review the positioning of the internal audit function within the risk management framework of the organization
- Monitor compliance with the corporate code of conduct or business practices
- Report on the effectiveness of the control framework
- Assess the ethical climate of the board and the organization
- Conduct a follow-up and report on management's response to regulatory body reviews or the external audit
- Assess the adequacy of the performance measurement system and achievement of organizational objectives
- Support a culture of fraud awareness and encourage the reporting of improprieties

## Governance System Maturity

The role of the internal audit function and the advice given by it depend on the maturity of the governance system.

- In a **less mature** system, the internal audit function emphasizes compliance with policies, procedures, laws, etc. It also addresses the basic risks to the organization.
- In a **more mature** system, the internal audit function's emphasis is on optimizing structure and practices.
- As the internal audit function becomes more sophisticated, it transitions from only auditing for compliance purposes to auditing **and** adding value to the organization by suggesting how to optimize the organization's operations.