

# Part 1: The Internal Audit Activity's Role in Governance, Risk, and Control

## Table of Contents

<b>Part 1 Overview</b> .....	1-1
<b>Section 1: Comply with The IIA's Attribute Standards</b> .....	1-3
Section Introduction .....	1-3
Topic 1: Define Purpose, Authority, and Responsibility of the Internal Audit Activity (Level P)...	1-10
Topic 2: Maintain Independence and Objectivity (Level P) .....	1-19
Topic 3: Determine Availability of Required Knowledge, Skills, and Competencies (Level P).....	1-27
Topic 4: Develop and/or Procure Necessary Knowledge, Skills, and Competencies Collectively Required by Internal Audit Activity (Level P).....	1-34
Topic 5: Exercise Due Professional Care (Level P) .....	1-39
Topic 6: Promote Continuing Professional Development (Level P).....	1-43
Topic 7: Promote Quality Assurance and Improvement of the Internal Audit Activity (Level P)....	1-47
Topic 8: Abide By and Promote Compliance With The IIA's Code of Ethics (Level P) .....	1-56
<b>Section 2: Risk and Control Knowledge Elements</b> .....	1-60
Section Introduction .....	1-60
Topic 1: Risk and Control Terminology (Level P).....	1-61
Topic 2: Risk Elements (Level P) .....	1-64
Topic 3: Control Elements (Level P).....	1-67
<b>Section 3: Establish a Risk-based Plan to Determine the Priorities of the Internal Audit Activity</b> .....	1-73
Section Introduction .....	1-73
Topic 1: Establish a Framework for Assessing Risk (Level P).....	1-74
Topic 2: Use of the Framework (Level P).....	1-75
Topic 3: Identify Internal Audit Resource Requirements (Level P).....	1-84
Topic 4: Coordinate the Internal Audit Activity's Efforts (Level P).....	1-84
Topic 5: Select Engagements (Level P) .....	1-88
<b>Section 4: Plan Engagements</b> .....	1-90
Section Introduction .....	1-90
Topic 1: Initiate Preliminary Communication with Engagement Client (Level P).....	1-93

*Part 1: The Internal Audit Activity's Role in Governance, Risk, and Control*

Topic 2: Conduct a Preliminary Survey of the Area of Engagement (Level P) ..... 1-95

Topic 3: Complete a Detailed Risk Assessment of the Area  
(Prioritize or Evaluate Risk/Control Factors) (Level P) ..... 1-115

Topic 4: Coordinate Audit Engagement Efforts (Level P)..... 1-119

Topic 5: Establish/Refine Engagement Objectives and  
Identify/Finalize the Scope of Engagement (Level P) ..... 1-121

Topic 6: Identify or Develop Criteria for Assurance Engagements  
(Criteria Against Which to Audit) (Level P) ..... 1-125

Topic 7: Consider the Potential for Fraud When Planning an Engagement (Level P)..... 1-126

Topic 8: Determine Engagement Procedures (Level P) ..... 1-131

Topic 9: Determine the Level of Staff and Resources Needed for the Engagement (Level P) ..... 1-134

Topic 10: Establish Adequate Planning and Supervision of the Engagement (Level P)..... 1-136

Topic 11: Prepare Engagement Work Program (Level P)..... 1-138

**Section 5: The Nature of Internal Audit Work in Risk**

**Management, Control, and Governance**..... 1-142

Section Introduction ..... 1-143

Topic 1: Risk Management (Level P) ..... 1-147

Topic 2: Internal Control (Levels A and P)..... 1-179

Topic 3: Governance (Levels A and P) ..... 1-205

Topic 4: Related Topics (Level P)..... 1-222

**Bibliography** ..... 1-244

**Index** ..... 1-249



# Part 1 Overview

Welcome to Part 1 of *The IIA's CIA Learning System*.

An internal audit is the process of reviewing the effectiveness and efficiency of operations; compliance with laws, regulations, policies, and procedures; achievement of operational/organizational objectives; reliability of information; and safeguarding of assets. Individuals employed in an internal audit activity are typically employees of an organization. However, there are alternative arrangements to staff an internal audit department through outsourcing arrangements.

Distinctions between internal audit and other review functions include:

- **Compliance**

Compliance reviews are conducted to strictly test adherence to laws, regulations, standards, and policies and procedures. These reviews typically serve to determine whether or not an organization is adhering to a specified regulation, etc., and the results are reported as such. Compliance audits do not consider the effectiveness and efficiency of business processes. Typically, specialized individuals, some with legal backgrounds, conduct these reviews.

- **External auditors/financial auditors**

These auditors provide an attestation solely on the financial reports and statements generated by an organization. While these auditors focus on the accuracy of reported information, they also review the related controls over the financial information. These auditors are governed by the American Institute of Certified Public Accountants (AICPA) Generally Accepted Auditing Standards (GAAS) standards.

- **Regulators**

These auditors work for regulating bodies (e.g., Financial Industry Regulatory Authority [FINRA], U.S. Securities and Exchange Commission [SEC], Options Clearing Corporation [OCC]) and review compliance with specific regulations. They perform compliance reviews of corporations or agencies that are regulated by the specified regulating body.

- **Government audit**

Government auditors typically work for the departments, ministries, or agencies of a government and focus on compliance with program requirements, performance audits, budget reviews, and management audits.

# Section 1: Comply with The IIA's Attribute Standards

*This section is designed to help you:*

- *Recognize the longevity of the auditing profession.*
- *Define internal auditing.*
- *Explain the International Professional Practices Framework categories of guidance.*
- *Explain how the purpose, authority, and responsibility for an internal audit activity is documented, communicated, and approved.*
- *Explain independence and objectivity and how to maintain both during an internal audit activity.*
- *Identify and describe the required knowledge, skills, and competencies for an internal audit activity and how an organization develops and/or procures them.*
- *Explain how to exercise due professional care in an internal audit activity.*
- *Describe the importance of professional development and formal certification for internal auditors.*
- *Describe elements of a quality assurance and improvement program.*
- *Describe compliance with The IIA Code of Ethics.*

*The Certified Internal Auditor (CIA) exam questions based on content from this section make up approximately 15% to 25% of the total number of questions for Part 1. All topics are covered at the “P—Proficiency” level, meaning that you are responsible not only for comprehension and recall of information but also for higher-level mastery, including application, analysis, synthesis, and evaluation.*

## Section Introduction

The profession of auditing has a rich and storied past. The earliest accounts of auditing date back to the Mesopotamian civilization, where marks were used to record ship cargos and verify financial transactions. In ancient Rome, the term “audit” originated from the Latin word *auditus*, “a hearing,” referring to the hearing of oral evidence as one official would verify records with those of another.

Internal auditing evolved through the years, gaining recognition from executives and organization leaders and altering the focus of internal audit efforts to respond to the changing needs of the global environment. The profession has evolved from focusing on financial information, compliance

reviews, information technology, operational processes, and risk and controls. Today, internal auditing focuses on a combination of the above items through integrated audits and compliance reviews.

Throughout the centuries, auditors have continued to pursue the truth, control transactions, and prevent or detect fraudulent acts. Today, internal audits are independent, unbiased fact-finding exercises that provide verifiable information to management or outside interests.

## Internal auditing defined

According to The Institute of Internal Auditors (The IIA), “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 risk management, control, and governance processes.”

Internal auditing is performed by professionals with an in-depth understanding of the business culture, systems, and processes. Internal audit activities may be performed by people within the organization or from outside the organization.

Effective internal auditors serve as an organization’s corporate conscience and advisors for operational efficiency, internal control, and risk management. They also educate and make recommendations to management and the board of directors (and/or other governance oversight bodies) to support the organization in meeting its goals and objectives. In fulfilling these responsibilities, internal auditors must demonstrate professionalism, objectivity, knowledge, integrity, and leadership.

## The internal auditing landscape and the International Professional Practices Framework

To help internal auditors ensure the highest-quality internal audit results in widely diverse environments, The IIA has developed and maintains a full range of guidance for practitioners through an International Professional Practices Framework (IPPF). The International Professional Practices Framework is defined as the “conceptual framework that organizes the authoritative guidance promulgated by The IIA. Authoritative guidance comprises two categories: (1) mandatory and (2) endorsed and strongly recommended.

The IPPF also includes a *Standards* Glossary. In the *Standards* Glossary **internal auditing** is defined as “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 risk management, control, and governance processes.”

Further, the *Standards* Glossary defines the use of the words “must” and “should” in the following manner.

- **Must:** The *Standards* use the word “must” to specify an unconditional requirement.
- **Should:** The *Standards* use the word “should” where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

The framework consists of the following mandatory, advisory, and practical categories of guidance.

- The Code of Ethics and the *International Standards for the Professional Practice of Internal Auditing (Standards)*
- Practice Advisories (PAs)
- Practice Guides
- Position Papers
- Definition of internal auditing
- Glossary

The Practice Advisories and Practice Guides are intended for the use of IIA members. They are available at The IIA's Web site and are password-protected. The full International Professional Practices Framework is available in a printed version, known familiarly, and for reasons obvious to those who have seen it, as “The Red Book.” It can be ordered online. While the book includes all aspects of the framework—Code of Ethics, *Standards*, and Practice Advisories—it is not necessarily as up-to-date as the online version, which is subject to continuous review, revision, and addition. Internal auditors should be sure they are familiar with the most current version of the framework available at The IIA's Web site. Position papers are also posted on The IIA's Web site.

**The Code of Ethics and the International Standards for the Professional Practice of Internal Auditing**

Compliance with the Code of Ethics and the *Standards* is mandatory for all members of The IIA and all Certified Internal Auditors (CIAs).

An overview of the *Standards* follows in this introduction and subsequent topics. The Code of Ethics is discussed in detail in Topic 8 of this section, “Abide By and Promote Compliance With The IIA Code of Ethics.”

### **Purpose of the *Standards***

The purpose of the *Standards* is to:

- Delineate basic principles that represent the practice of internal auditing as it should be.
- Provide a framework for performing and promoting a broad range of value-added internal audit activities.
- Establish the basis for the evaluation of internal audit performance.
- Foster improved organizational processes and operations.

The *Standards* employ terms that have been given specific meanings. Whenever these terms are defined in this module, they are identified as being from the *Standards* Glossary.

### **Categories of *Standards***

The *Standards* consist of Attribute Standards, Performance Standards, and Implementation Standards.

- **Attribute Standards** address the characteristics of organizations and parties performing internal audit activities. Attribute Standards apply to all internal audit services and internal auditors individually.

The following are examples of Attribute Standards.

- **Attribute Standard 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 Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

- **Attribute Standard 1100—Independence and Objectivity**

The internal audit activity should be independent, and internal auditors should be objective in performing their work.

- **Performance Standards** describe the nature of internal audit activities and provide criteria against which the performance of these services can be evaluated. Similar to Attribute Standards,

Performance Standards apply to all internal audit services as well as internal auditors.

The following are examples of Performance Standards.

- **Performance Standard 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.
- **Performance Standard 2100—Nature of Work**  
The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Implementation Standards** expand Attribute and Performance Standards and how they apply to specific types of assurance or consulting engagements. The *Standards* Glossary defines an engagement as “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.”

Implementation Standards ultimately may deal with industry-specific, regional, or specialty types of auditing services.

Implementation Standards can be recognized by their unique format. For example, 1000.A1 and 1000.C1 are the Implementation Standards related to Attribute Standard 1000, whereby the “A” indicates an assurance engagement standard and “C” indicates a consulting engagement.

There is one set of Attribute and Performance Standards. However, there are multiple sets of Implementation Standards that apply to each of the two major types of internal audit activity: assurance services and consulting services.

Exhibit 1-1 compares assurance services and consulting services.

**Exhibit 1-1: Assurance Services and Consulting Services**

Type	Assurance Services	Consulting Services
<b>Definition</b>	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. ( <i>Standards Glossary</i> ),	Advisory and related client service activities, the nature and scope of which are agreed to by the client and which 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. ( <i>Standards Glossary</i> ).
<b>Parties involved</b>	The internal auditor determines the nature and scope of the assurance engagement. Typically, three parties are involved in assurance services. <ul style="list-style-type: none"> <li>• The person or group directly involved with the process, system, or other subject matter (the process owner)</li> <li>• The person or group making the assessment (the internal auditor)</li> <li>• The person or group using the assessment (the user)</li> </ul>	Consulting services generally involve two parties. <ul style="list-style-type: none"> <li>• The person or group offering the advice (the internal auditor)</li> <li>• The person or group seeking and receiving the advice (the engagement client)</li> </ul>
<b>Scope of activities</b>	The internal auditor determines the nature and scope.	The client determines the nature and scope with agreement from the auditor.
<b>Deliverable</b>	An assessment, opinion, or conclusion of the assurance engagement result is communicated.	Advise, counsel, and add value to an organization's governance, risk management, and control processes.

If laws or regulations prohibit internal auditors from complying with certain parts of the *Standards*, appropriate disclosures should be made. Internal auditors should comply with all other parts of the *Standards*.

Internal or external, an audit activity is intended to provide assurance that internal controls in place are adequate to mitigate the risks and that organizational goals and objectives are met.

**Practice Advisories**

Practice Advisories are IIA-endorsed guidance on best practices for performance of the *Standards*; they are nonmandatory. They may help to interpret the *Standards* or to apply the *Standards* to specific internal auditing environments. Some Practice Advisories are applicable to all internal auditors; others address the needs of a specific industry, audit specialty, or geographic area.

Practice Advisories address approach, methodology, and considerations but NOT detailed processes and procedures. They provide concise and timely guidance to assist internal auditors in applying the Code of Ethics and *Standards* and promoting good practices. Practice Advisories include practices relating to international, country, or industry specific issues; specific types of engagements; and legal or regulatory issues.

Practice Advisories have ongoing updates and changes to provide new best practices to conform with the requirements of the *Standards*. All Practice Advisories are submitted to a formal review process by The IIA's Professional Issues Committee or other group designated by the Guidance Planning Committee. Practice Advisories are posted on The IIA's Web site.

### **Practice Guides**

Practice Guides are another form of guidance provided by The IIA to help internal auditors incorporate the *Standards* in their practice. According to the Preface to the framework, this category of guidance provides “detailed guidance for conducting internal audit activities” and “includes detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, including examples of deliverables.”

### **Position Papers**

Position Papers are IIA statements to assist a wide range of interested parties, including those not in the internal audit profession, in understanding significant governance, risk, or control issues and delineating the related roles and responsibilities of the internal audit profession.

### **Supporting endeavors**

To help implement the International Professional Practices Framework guidance, internal auditors perform ongoing internal quality assessments and are required to undergo independent external quality assessments to validate conformance to the *Standards*. They may also receive individual auditor certifications.

There are many reasons to obtain an official IIA certification designation. Whether it's the hallmark designation of internal audit—the Certified Internal Auditor® (CIA®) designation—or one of three specialty industry certifications, obtaining a certification is professionalism defined. The IIA's CIA Learning System you are now reading is an example of IIA certification preparation materials.

Used in combination, all of these professional endeavors help individual auditors and the organizations they serve to succeed together.