Professional *Standards*

COPYRIGHTED MATERIAL

This section defines the new International Professional Practices Framework – 2017 (new IPPF of 2017) issued in January 2017 and serves as a strong orientation to the new CIA Exam's Professional *Standards*, all of which are effective in January 2019.

It presents a detailed discussion of four Attribute *Standards*, such as 1000, 1100, 1200, and 1300 series, and one Performance *Standard*, such as 2100 series. The only reason for putting all the relevant Professional *Standards* in one place in this section is to provide a solid mind-print of the *Standards* in the first reading. Later, study the specific *Standards* in this section as they apply to each domain for an in-depth understanding of the *Standards*. In addition to the *Standards*, three important topics, Risks to Internal Audit Activity, Auditing Metrics and Key Performance Indicators, and Three Lines of Defense, are presented. Listing all the relevant *Standards* in one place is a great convenience to students in serving as a memory jogger.

Note that the *Standards* should be studied together with the theoretical subject matter presented in Domains 1 through 6, as follows.

Standards: 1000 and 1010 ⟶ Domain 1

Standards: 1100, 1110, 1111, 1112, 1120, and 1130 ⟶ Domain 2

Standards: 1200, 1210, 1220, and 1230 ⟶ Domain 3

Standards: 1300, 1310, 1311, 1312, 1320, 1321, and 1322 ⟶ Domain 4

Standards: 2100, 2110, 2120, and 2130 ⟶ Domain 5

Standards: 1220 ⟶ Domain 6

Note that this section does not contain any sample practice questions at the end because such questions are included in their respective domains in this book (i.e., Domains 1 through 6). With respect to the CIA Exam, cognitive levels are labeled as proficient level and basic level. These cognitive levels suggest that more time and effort should be spent in studying and mastering the subject matter covered in the topics labeled as the proficient level. Comparatively less time and effort should be spent on the topics labeled as the basic level.

International Standards for the Professional Practice of Internal Auditing Copyright © 2017 by The Institute of Internal Auditors, Inc. ("The IIA"). All rights reserved.

i.1 New IPPF Defined

The new International Professional Practices Framework – 2017 (new IPPF of 2017) is the conceptual framework that organizes the authoritative guidance promulgated by The Institute of Internal Auditors (IIA). Authoritative guidance is composed of two categories: mandatory guidance and recommended guidance.

The mission of internal audit describes internal audit's primary purpose and overarching goal. Achievement of the mission is supported by the new IPPF of 2017, including the mandatory guidance elements of the Core Principles for the Professional Practice of Internal Auditing (Core Principles), the Definition of Internal Auditing (Definition), the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing* (*Standards*). The IPPF also includes recommended guidance with elements of implementation guidance and supplemental guidance.

Mission = Purpose + Goals + Objectives

Authoritative Guidance = Mandatory Guidance + Recommended Guidance

Mandatory Guidance = Core Principles + Definition + Code of Ethics + *Standards*

Recommended Guidance = Implementation Guidance + Supplemental Guidance.

New IPPF = Mission + Mandatory Guidance + Recommended Guidance

i.2 Introduction to the IIA's *Standards*

A ***Standard*** is a professional pronouncement promulgated by the IIA's Internal Audit Standards Board (IASB) that delineates the requirements for performing a broad range of internal audit activities and for evaluating internal audit performance.

Internal auditing is conducted in diverse legal and cultural environments; for organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. Examples of these environments where audits are conducted include private sector, public sector, for-profit organizations, and not-for-profit organizations operating at the local, city, state, regional, province, national, and continent level. While differences may affect the practice of internal auditing in each environment, conformance with the Institute of Internal Auditor's (IIA's) *International Standards for the Professional Practice of Internal Auditing – 2017* (*Standards – 2017*) is essential in meeting the responsibilities of internal auditors and the internal audit activity.

The purpose of the *Standards* is to:

- Guide adherence with the mandatory elements of the International Professional Practices Framework (IPPF-2017).
- Provide a framework for performing and promoting a broad range of value-added internal auditing service.
- Establish the basis for the evaluation of internal audit performance.
- Foster improved organizational processes and operations.

The *Standards* are a set of principles-based, mandatory requirements consisting of:

- Statements of core requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance that is internationally applicable at organizational and individual levels.
- Interpretations clarifying terms or concepts within the *Standards*.

The *Standards*, together with the Code of Ethics, encompass all mandatory elements of the IPPF; therefore, conformance with the Code of Ethics and the *Standards* demonstrates conformance with all mandatory elements of the IPPF.

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. Furthermore, 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.

The *Standards* comprise two main categories: Attribute *Standards* and Performance *Standards*. Implementation *Standards* expand on the Attribute *Standards* and Performance *Standards* by providing the requirements applicable to assurance services or consulting services.

- **Attribute *Standards*** address the characteristics of organizations and parties performing internal audit activities.
- **Performance *Standards*** describe the nature of internal audit activities and provide criteria against which the performance of these services can be evaluated.

Both Attribute *Standards* and Performance *Standards* apply to all internal audit services.

The *Standards* apply to individual internal auditors and the internal audit activity. All internal auditors are accountable for conforming with the *Standards* related to individual objectivity, proficiency, and due professional care and the *Standards* relevant to the performance of their job responsibilities. Chief audit executives (CAEs) are additionally accountable for the internal audit activity's overall conformance with the *Standards*.

If internal auditors or the internal audit activity is prohibited by law or regulation from conformance with certain parts of the *Standards*, conformance with all other parts of the *Standards* and appropriate disclosures are needed.

If the *Standards* are used in conjunction with requirements issued by other authoritative bodies, internal audit communications may also cite the use of other requirements, as appropriate. In such a case, if the internal audit activity indicates conformance with the *Standards* and inconsistencies exist between the *Standards* and other requirements, internal auditors and the internal audit activity must conform to the *Standards* and may conform with the other requirements if such requirements are more restrictive.

Mandatory Guidance versus Recommended Guidance

The IIA offers two major types of guidance to the internal auditing profession—mandatory guidance and recommended guidance—which are the scope of authoritative guidance.

Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The ultimate goal is to have a framework where conformance with the Code of Ethics and the *Standards* achieves conformance with the Core Principles. Conformance with the principles set forth in mandatory guidance is required and essential for the professional practice of internal auditing.

Specifically, mandatory guidance covers attribute standards and performance standards. Attribute *Standards* address the characteristics of organizations and parties performing internal audit activities. Performance *Standards* describe the nature of internal audit activities and provide criteria against which the performance of these services can be evaluated.

Recommended guidance (nonmandatory guidance) addresses implementation guidance and supplemental guidance. These guides are 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*.

Implementation guidance is designed to assist both internal auditors and internal audit activities to enhance their ability to achieve conformance with the *Standards.* Specifically, implementation guides assist internal auditors in applying the *Standards*, and they expand on the Attribute *Standards* and Performance *Standards*. They collectively address internal audit's approach, methodologies, and consideration, but do not detail processes or procedures.

Supplemental guidance provides detailed guidance for conducting internal audit activities. These include topical areas, sector-specific issues, as well as processes and procedures, tools and techniques, programs, step-by-step approaches, and examples of deliverables. Specifically, supplemental guides include several types of practice guides, such as global technology audit guides, guides to the assessment of information technology (IT) risks, and general-purpose practice guides.

Mandatory Guidance = Attribute *Standards* + Performance *Standards*
Recommended Guidance = Implementation Guidance + Supplemental Guidance

i.3 IIA's International *Standards*

This section presents four Attribute *Standards*, the 1000, 1100, 1200, and 1300 series, and one Performance *Standard*, the 2100 series. These *Standards* and their substandards include the following.

1000—Purpose, Authority, and Responsibility

1010—Recognizing Mandatory Guidance in the Internal Audit Charter

1100—Independence and Objectivity

1110—Organizational Independence

1111—Direct Interaction with the Board

1112—Chief Audit Executive Roles Beyond Internal Auditing

1120—Individual Objectivity

1130—Impairment to Independence or Objectivity

1200—Proficiency and Due Professional Care

1210—Proficiency

1220—Due Professional Care

1230—Continuing Professional Development

1300—Quality Assurance and Improvement Program

1310—Requirements of the Quality Assurance and Improvement Program

1311—Internal Assessments

1312—External Assessments

1320—Reporting on the Quality Assurance and Improvement Program

1321—Use of "Conforms to the *International Standards for the Professional Practice of Internal Auditing*"

1322—Disclosure of Nonconformance

2100—Nature of Work

2110—Governance

2120—Risk Management

2130—Control

Note that *Standard* 1112—Chief Audit Executive Roles Beyond Internal Auditing—is a new *Standard* added in 2017 to recognize the evolving nature of the CAE's roles and responsibilities. While *Standard* 1112 does not promote multiple roles for the CAE, it suggests situations where an organization's board may require a CAE to undertake new roles or additional responsibilities that fall outside of internal audit (i.e., nonaudit work). *Standard* 1112 was added to ensure that there are safeguards in place when this situation occurs.

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 (CAE) 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 CAE'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.

1000—Implementation Guide

Establishing a scope for implementation work consists of developing an audit charter, including coordination and consultation between the CAE, internal legal counsel, external consulting counsel, board of directors (board), and senior management (senior managers). Note that the board and senior management together can set the **tone at the top** for others to follow and can express the **voice of the top** for others to hear. The CAE can use the IIA's model charter or the industry format (e.g., retail or healthcare) as a template to create an initial (draft) and a final audit charter document.

Initial Draft ⟶ Board Review ⟶ Final Draft ⟶ Board Approval ⟶ Final Document

Considerations for implementation include developing an internal audit charter with a standard format and using essential elements. A draft version of the charter document can contain these sections:

- Introduction
- Authority
- Organization and reporting structure (functional reporting to the board and administrative reporting to the chief executive officer (CEO)
- Independence and objectivity (either in fact or appearance)
- Responsibilities (audit work and nonaudit work)
- Quality assurance and improvement
- Approval signatures

The board needs to confirm that the draft accurately describes the agreed-upon role and expectations and later accepts it. Then the CAE presents the charter document during a board meeting for discussion and approval, including future (periodic) review and reaffirmation schedule going forward.

Considerations for demonstrating conformance require the following output documents:

- Minutes of the board meetings listing the initial discussions and final presentations of the audit charter
- The board's meeting minutes showing a standby annual agenda item to discuss, update, and approve the charter document as needed

Requiring a familiarity with the related Standards includes:

- Recognizing mandatory guidance in the internal audit charter (*Standard* 1010)

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.

1010—Implementation Guide

Establishing a scope for implementation work includes determining all the input documents required and understanding their purpose before developing or revising the internal audit charter document. These input documents include:

- Mission of internal audit
- Core Principles
- Code of Ethics
- *Standards*
- Definition of internal auditing

The Core Principles, Code of Ethics, *Standards*, and definition are part of mandatory guidance, which in turn, when combined with the mission, become the mandatory elements of the new IIA's International Professional Practices Framework (new IPPF).

Mission = Purpose + Goals + Objectives

Mandatory Guidance = Core Principles + Code of Ethics + *Standards* + Definition

New IPPF = Mission + Mandatory Guidance

Considerations for implementation include the CAE discussing the internal audit charter with senior management and the board and how the audit charter recognizes the mandatory elements. After the charter has been adopted, the CAE monitors the charter for any changes that may require updates during the next charter review.

Considerations for demonstrating conformance are evidenced in the written and approved charter that recognizes the mandatory elements of the IPPF. In addition, board's meeting minutes documented during the initial review and periodic reviews are considered adequate.

Requiring a familiarity with the related Standards includes:

- Purpose, authority, and responsibility (*Standard* 1000)

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.

1100—Implementation Guide

Establishing a scope for implementation work requires defining terms such as *independence* and *objectivity*. Because there is confusion between these two terms, some individuals may treat independence as a proxy for objectivity, which is not right within the context of the *Standards*. **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. **Objectivity** requires that internal auditors do not subordinate their judgment on audit matters to others.

Considerations for implementation include how the CAE's reporting lines and responsibilities are established. Several approaches follow to ensure independence and to curb objectivity impairment.

- A direct **functional reporting** line to the board (i.e., audit committee) is good because it provides the CAE a direct access to the board for sensitive matters and elevates the CAE's organizational status in the company. The board members in the audit committee can establish safeguards (i.e., oversight activities) when they feel that the CAE's objectivity is impaired.
- An **administrative reporting** to a senior manager or the CEO is good because it provides authority to perform audit work without impediments. The IIA recommends that the CAE report to the CEO. This approach implies that the CAE should not report to an accounting controller, an IT manager, a business division head, or a mid-level manager because the CAE would perform audit work in their business functions. Senior managers can establish safeguards (i.e., oversight activities) when they feel that the CAE's objectivity is impaired.
- Preferred reporting lines are:
  - CAE's functional reporting to the board
  - CAE's administrative reporting to a senior manager or the CEO

Many CAEs have issued an internal audit policy manual or handbook to describe expectations and requirements for an internal auditor's unbiased mindsets. The contents of the policy manual can include:

- A list of objectivity-impairing or threat-creating situations and scenarios with approaches to avoid or address them. These situations include self-interest, self-review, conflict, familiarity, bias, and undue influence.
- A requirement that internal auditors discuss their objectivity concerns with their audit manager or the CAE for advice.
- A requirement where each internal auditor periodically reports and discloses conflict-of-interest situations.
- A requirement that all internal auditors go through training classes or workshops to understand the objectivity-impairing or threat-creating scenarios in order to avoid conflicts.

Many CAEs are conducting client-satisfaction feedback surveys from audit clients after audit work is completed. These surveys have advantages and disadvantages. An advantage is that the

survey results build a stronger relationship between auditors and audit clients, which represents a good business practice.

A disadvantage is that the survey results could negatively affect an auditor's performance evaluation ratings and compensation benefits. This means that reporting negative audit findings could result in low satisfaction ratings, which in turn lower the auditor's compensation benefits. The reverse is also true, requiring a balancing act on the part of the CAE.

Considerations for demonstrating conformance include internal audit charter, organization chart, internal audit policy manual, training records, and conflict-of-interest disclosure forms.

Requiring a familiarity with the related Standards includes:

- Organizational independence (*Standard* 1110)
- Direct interaction with the board (*Standard* 1111)
- CAE roles beyond internal auditing (*Standard* 1112)
- Individual objectivity (*Standard* 1120)
- Impairment to independence and objectivity (*Standard* 1130)

Risks to Internal Audit Activity—*Standard* 1100

Similar to other functions, the internal audit function is a risk-prone activity, as there is no function in an organization that is risk resistant. Risks to internal audit activities fall into three broad categories: audit failure risks, false assurance risks, and reputation risks.

Audit Failure Risks

In addition to control breakdowns and fraud occurrences, the internal audit activity itself could be a contributing factor to audit failures due to auditors' own doing. This means auditors showing negligence in performing their professional work, not following their professional standards, not identifying high-risk auditable areas during the planning of individual audits, not paying attention to fraud alerts and red flags, not doing the right audits at the right time, wasting resources on doing the wrong audits at the wrong time, and not delivering a quality audit product.

Seven *specific causes leading to audit failure risks* include failure to:

1. Design effective internal audit procedures to test the "real" risks and the right controls.
2. Evaluate both the design adequacy and the control effectiveness as part of internal audit procedures.
3. Provide adequate internal audit supervision.
4. Exercise professional skepticism and judgment.
5. Undertake extended internal audit procedures related to negative findings or control deficiencies.
6. Communicate fraud suspicions to the right people at the right time.
7. Assign competent auditors to perform complex audit engagements.

Six *remedies to address audit failure risks* include:

1. Periodic review of the audit universe and audit plan.
2. Effective audit planning process and audit design of the system of internal controls.

Risks to Internal Audit Activity— *Standard* 1100 *(Continued)*

3. Escalation procedures within the internal audit activity indicating when and what types of issues to escalate to which level of the audit management hierarchy.
4. Ensuring that high-risk audit engagements are staffed with auditors possessing a combination of right experience, knowledge, skills, competencies, or talents (i.e., right mix of audit resources with a blend of hard skills and soft skills).
5. Ensuring that lead auditors have strong project management skills to complete an audit engagement on time and within the budget.
6. Implementing an effective quality assurance and improvement program (QAIP) to conduct internal assessments and external assessments.

False Assurance Risks

False assurance is a level of confidence or assurance based on perceptions or assumptions, not based on facts. False assurance risks result when auditors are unknowingly overselling or underperforming themselves and making empty promises to audit clients who take those promises very seriously and who make auditors accountable for what they promised. Simply put, false assurances result from what was said, when it was said, and how it was said. Examples of empty promises or false assurances that could raise an **expectation gap** include: "We will take care of it," "We will help you, don't worry about it," "I will talk to my audit management and let me see what I can do for you."

Four *specific causes leading to false assurance risks* include:

1. Not keeping the proper mental distance between auditors and audit clients.
2. Not monitoring an auditor's independence and objectivity issues.
3. Not clearly defining and documenting the auditor's roles and responsibilities (**role gap**) when business units request the audit staff's help in implementing a new computer system project in the accounting department or analyzing the customer service department's problems with product warranty and guarantee claims (**loaned audit resources**).
4. Not communicating scope inclusions (what is covered, in scope) and scope exclusions (what is not covered, out of scope) in the auditor's work when conducting risk assessments, developing internal audit plans, and performing internal audit engagements (**expectation gap**).

Auditors need to realize that a role gap and an expectation gap may exist in the minds of audit clients.

Auditors' Role Gap = Audit Clients' Perceived Role of Auditors – Auditors' Actual Role

Auditors' Expectation Gap = Audit Clients' Expected Deliverables – Auditors' Actual Deliverables

Loaned audit resources can create false assurance risks, in part due to the expectation gap.

Four *remedies to address the false assurance risks* include:

1. Communicating frequently and clearly to all affected parties about the auditor's role, professional mission and mandate, and adherence to the professional *Standards*.
2. Communicating scope inclusions and exclusions in every audit engagement project.
3. Documenting "project risk" information at the beginning of a project by describing the types and sources of risks a project is facing, including its risk immunity levels (risk resistant or risk prone) and risk sensitivity levels (sensitive or insensitive).
4. Installing a "project acceptance" process at the beginning of a project where auditors document their specific roles and project outcomes and deliverables, the types of project risks being handled, the types of audit talent and competencies required or available, and auditor independence.

Reputation Risks

Reputation risks primarily deal with positive or negative impressions or images of auditors in the eyes of audit clients. A positive image can take many years to earn, whereas it takes very little time to earn a

negative image due to one high-profile and high-impact adverse event. Both audit failure risks and false assurance risks in combination can result in reputation risks, as they are interconnected.

Reputation Risks = Audit Failure Risks + False Assurance Risks

For example, when auditors are assigned to a business function to assist its day-to-day work due to that function's staff shortages or to participate in a special project taking considerable duration (say three to six months), these **loaned resources** of auditors can create false assurance situations and reputation risks. This is because nonauditors think that auditors are highly experienced and highly knowledgeable people who carry a strong "brand" name for perfection and excellence and that they never make mistakes or have mishaps. When something goes wrong in auditor-assisted work, auditors are the first ones to be blamed for problems because they are outsiders and are assumed to do perfect work, and to know everything (or should know everything). Loaned audit resources can be found in accounting, finance, treasury, corporate tax, insurance, and loss prevention departments.

Three *specific causes leading to reputation risks* include:

1. Using auditors as loaned resources to other business functions, whether short term or long term.
2. Auditors' behavior and performance as loaned resources in other business functions and the impressions and images they leave on employees and managers of those business functions.
3. The inability of auditors to understand, protect, and maintain their own strong audit "brand" name (goodwill), leading to credibility issues (**credibility gaps**). A clear connection among the reputation, role, expectation, and credibility gap can be seen:

Reputation Gap = Role Gap + Expectation Gap + Credibility Gap

Eight *remedies to address the reputation risks* include:

1. Training all internal auditors about the scope and nature of false assurances, reputation risks, and brand-name protections.
2. Educating auditors in that each auditor is a source for creating audit failures, false assurances, and reputation risks. The same auditor can be a source for eliminating such failures and risks.
3. Conducting an assessment of the internal audit department by outsiders, similar to what internal auditors do at an internal audit client location.
4. Maintaining an **audit incident log** describing all the audit failures, false assurances, and reputation issues and not revealing the auditors' names and locations.
5. Posting, publicizing, and notifying every internal auditor about the **lessons learned** from recent observations and experiences regarding audit failures, false assurances, and reputation risks.
6. Installing a **suggestion box** system within the internal audit department for improving or removing audit failures, false assurances, and reputation risks.
7. Selecting internal auditors for job rotational assignments in nonaudit functions (job rotations) based on a careful blend of **hard skills** and **soft skills** they possess and those auditors that can protect internal audit's brand reputation.

Note that CAEs must be open-minded (transparent), forward-thinking, and proactive in nature to maintain an audit incident log, similar to a security incident log maintained in the IT function. Security incident logs document all data security breaches and cyberattacks that occur on data files and websites respectively.

Audit Risk Components

Audit risk is the overall risk of audit work and is composed of five individual risks: inherent risk, control risk, materiality risk, detection risk, and fraud risk. We added other terms related to audit risk such as systemic risk, sampling risk, nonsampling risk, and evidence risk, and internal audit risk to provide a comprehensive list of risks. Exhibit i.1 summarizes a number of audit-related risk types with brief descriptions.

Risks to Internal Audit Activity— *Standard* 1100 *(Continued)*

EXHIBIT i.1 A Summary of Audit-Related Risk Types

Risk Type	Description
Audit risk	Audit risk is the risk that the auditor may unknowingly fail to appropriately modify his or her opinion on financial statements that are materially misstated. It is also defined as the risk that an auditor may fail to detect a significant error or weakness during an examination. Audit risk = Inherent risk × Control risk × Materiality risk × Detection risk × Fraud risk
Inherent risk	Inherent risk is the susceptibility of a management assertion to a material misstatement, assuming that there are no related internal control structure policies or procedures. Inherent risk – Materiality risk + Control risk (i.e., lack of controls)
Systemic risk	Systemic risk is same as the inherent risk. Systemic risk is a built-in risk and is common to and natural in most activities.
Control risk	Control risk is the risk that a material misstatement in a management assertion will not be prevented or detected on a timely basis by the entity's internal control structure policies or procedures. Control risk = Design effectiveness + Control operational efficiency
Materiality risk	Materiality risk is the risk of material misstatement of financial statements where the risk is significant. An auditor using judgment assesses the inherent risk and control risk either individually or collectively. The higher the management's assertion levels, the greater the need for extended audit procedures. Materiality risk = Inherent risk + Control risk Note that materiality risk and detection risk together are used in determining substantive audit procedures.
Detection risk	Detection risk is the risk that the auditor will not detect a material misstatement present in a management assertion. Detection risk = Effectiveness of audit procedures + Application of audit procedures Note that detection risk and materiality risk together are used in determining substantive audit procedures.
Fraud risk	The auditor determines the risks of material fraud occurring concurrently with the consideration of inherent risk and control risk. The scope of fraud includes fraudulent financial reporting, misappropriation of assets, and material misstatement of financial statements. Fraud risk = Inherent risk + Control risk
Audit assurance risk	Audit assurance equals 100% minus the percentage of allowable audit risk. Audit assurance risk is the complement of audit risk. The auditor determines the level of assurance to use based on judgment. For example, when an auditor states that he has 95% audit assurance that the financial statements are not materially misstated, he means that he allowed for a 5% audit risk (100 – 95 = 5). Audit assurance of 95% = 100% – 5%. Note that the audit assurance level is not the same as the confidence level because the former is related to an auditor's judgment and the latter is related to an individual sample.

Risk Type	Description
Sampling risk	The risk that the auditor's conclusion based on a sample might differ from the conclusion that would be reached by applying the test in the same way to the entire population. For tests of controls, sampling risk is the risk of assessing control risk either too low or too high. For substantive testing, sampling risk is the risk of incorrect acceptance or the risk of incorrect rejection. Usually the smaller the sample size, the larger the sampling risk will be.
Nonsampling risk	Nonsampling risk occurs even if the entire population is tested and is due to errors in auditor judgment, such as (1) use of inappropriate audit procedures, (2) incorrectly applying appropriate audit procedures, (3) misreading of sampling test results, and (4) not recognizing errors during sampling. This risk can be controlled with better audit planning and supervision. Auditors can use nonsampling selections to test controls through inquiry, observation, and walk-through procedures.
Evidence risk	Evidence risk occurs when an auditor collects incorrect, insufficient, irrelevant, inappropriate, and unreliable evidence that does not fit the audit scope and objectives. Evidence can be physical and/or digital. Moreover, the auditor-collected evidence could be rejected in a court of law when it does not meet the court's requirements.
Audit failure risk (internal audit)	Audit failure risk means that auditors show negligence in performing their professional work; do not follow their Professional *Standards*; do not identify high-risk auditable areas during the planning of individual audits; do not pay attention to fraud alerts and red flags; do not do the right audits at the right time; waste resources on doing the wrong audits at the wrong time; and do not deliver a quality audit product.
Audit false assurance risk (internal audit)	Audit false assurance risk results from what was said, when it was said, and how it was said by auditors to audit clients.
Audit reputation risk (internal audit)	Audit reputation risk is a combined audit failure risk and audit false assurance risk resulting in the reputation risk.
Total internal audit risk	Total internal audit risk = Audit failure risk + Audit false assurance risk + Audit reputation risk

1110—Organizational Independence

The chief audit executive (CAE) must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The CAE must confirm to the board, at least annually, the organizational independence of the internal audit activity.

Interpretation: *Organizational independence is effectively achieved when the CAE 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 CAE on the internal audit activity's performance relative to its plan and other matters.
- Approving decisions regarding the appointment and removal of the CAE.
- Approving the remuneration of the CAE.
- Making appropriate inquiries of management and the CAE to determine whether there is 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.

1110—Implementation Guide

Establishing a scope for implementation work includes considering the organizational placement, supervisory oversight, regulatory requirements, and reporting lines of internal audit activity to ensure organizational independence. The internal audit charter shows the organizational placement and reporting lines. Assuring organizational independence is a shared understanding of internal audit's responsibility, authority, and expectations among the CAE, senior managers, and board members.

Considerations for implementation include determining the correct organizational placement and reporting lines for the internal audit activity. It consists of two types of reporting structures: functional and administrative.

1. A **functional reporting** line to the board (i.e., audit committee) provides direct access for sensitive matters and enables sufficient organizational status to conduct internal audit work. The board provides functional oversight because it approves the audit charter, audit plan, audit budget and resource plan, and hiring and removal of the CAE, including performance evaluation and compensation benefits for the CAE. In return, the CAE is required to provide periodic performance updates and quarterly meetings with the board with agreed-upon agenda. The CAE also discusses key audit findings, impairments to audit independence, and other matters of concern to the board.
2. An **administrative reporting** line to senior management or the CEO provides authority and status to fulfill audit responsibilities. The CAE would not report to an accounting controller, an accounting manager, or a mid-level functional manager because they are not senior-level positions. Audit independence cannot be assured with low-level positions.

   Functional Reporting ⟶ Board of Directors ⟶ "Solid" Line of Reporting

   Administrative Reporting ⟶ Senior Managers or the CEO ⟶ "Dotted" Line of Reporting

Considerations for demonstrating conformance include several documents such as the internal audit charter, the audit committee charter, the CAE's job description and his performance evaluation results, the internal audit policy manual, board's periodic reports, and the board's meeting minutes and agenda. In addition, documentation showing who interviewed the CAE when hiring indicates the final person making the CAE's hiring decision. External auditors should not make such a final decision in hiring the CAE. Only the internal management and the board should make that final decision.

Requiring a familiarity with the related Standards includes:

- Independence and objectivity (*Standard* 1100)
- Direct interaction with the board (*Standard* 1111)
- CAE roles beyond internal auditing (*Standard* 1112)
- Individual objectivity (*Standard* 1120)
- Impairment to independence and objectivity (*Standard* 1130)

1111—Direct Interaction with the Board

The chief audit executive (CAE) must communicate and interact directly with the board.

1111—Implementation Guide

Establishing a scope for implementation work highlights the need for a functional reporting relationship with the board to ensure a direct and open communication with the entire board or individual members of the board.

Considerations for implementation require the CAE to participate in audit committee meetings and/or the full board meetings. The CAE can contact the chair or any member of the board through in-person meetings or by phone calls either prior to scheduled meetings or routinely during the year to ensure a direct and open communication. If the CAE does not have direct access to or functional reporting to the board, the CAE can show the related IIA's *Standards* entitled Independence and Objectivity and Organizational Independence to the board as external evidence and authority requiring a direct access.

Considerations for demonstrating conformance can be shown with board meeting agendas and minutes and the CAE's calendar listing the scheduled meetings. In addition, a policy requiring the CAE to meet privately with the board periodically should be documented in the board's charter or the audit committee's charter.

Requiring a familiarity with the related Standards includes:

- Independence and objectivity (*Standard* 1100)
- Organizational independence (*Standard* 1110)
- Chief audit executive roles beyond internal auditing (*Standard* 1112)
- Individual objectivity (*Standard* 1120)
- Impairment to independence and objectivity (*Standard* 1130)

1112—Chief Audit Executive Roles Beyond Internal Auditing

Where the chief audit executive (CAE) 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 CAE 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.

1112—Implementation Guide

Usually the scope of internal audit work is confined to conducting routine and planned internal audits within the organization where audit independence and objectivity can be maintained and assured. However, there will be occasions where the board can ask the CAE to perform specific roles in nonaudit work for which management is normally responsible which could impair audit independence and objectivity because the work is not routine internal audit work. The reason for the board asking the CAE to perform nonaudit work is due to lack of resources (employees and budgets) in other functional departments to perform such roles or due to presence of special skills, talent, and expertise only available in the audit department.

Nonaudit Work ⟶ Management ⟶ CAE (before the work is performed)

Nonaudit Work ⟶ CAE ⟶ Management (after the work is performed)

Five examples of these unusual, specific roles in nonaudit work assigned to the internal audit include:

1. Fulfilling new regulatory compliance requirements with needed policies, procedures, controls, and risk management activities, which cannot be fulfilled today.
2. Performing risk management processes and activities for acquisition of new businesses.
3. Assuming greater responsibilities for designing, developing, and implementing risk management controls and compliance with them.
4. Working in loss prevention, insurance, accounting, corporate taxes, finance, and treasury departments.
5. Fulfilling (filling in) sudden changes that occurred in key management positions (e.g., promotion, demotion, termination, resignation, or death).

Establishing a scope for implementation work requires the IIA's Mission Statement, Code of Ethics, Core Principles, *Standards* (dealing with audit independence and auditor objectivity), internal audit charter, audit committee charter, and organization's general policies. If the CAE's specific role falls outside of internal auditing, the CAE should report to senior management and the board about potential impairments to independence and objectivity, risks associated with the proposed role, and control safeguards needed to mitigate those risks.

Considerations for implementation include establishing safeguards such as board oversight activities to protect the CAE's independence and objectivity and hiring an outsourced assurance provider when the CAE's objectivity is impaired due to previous duties performed beyond internal auditing.

The scope and nature of nonaudit roles and responsibilities assigned to the internal auditing could be short term (temporary) or long term (ongoing). A transition plan is required when the CAE is transferring the temporary (short-term) nonaudit work back to management showing timelines and resources needed. Ongoing (long-term) nonaudit work requires changes to the audit charter and safeguards to control the CAE's independence and objectivity.

Short Term ⟶ Transition Plan Required ⟶ No Change to Audit Charter Required

Long Term ⟶ No Transition Plan Required ⟶ Change to Audit Charter Required with Safeguards Established to Protect Independence and Objectivity

Considerations for demonstrating conformance include proper documentation of safeguards to protect the CAE's independence and objectivity. The type of documentation can include organization's general policies, code of ethics, audit committee charter, audit mission statement, audit charter, transition plans, minutes of board meetings, reports from outsourced assurance providers, surveys of audit clients, and reports of external assessments performed by an independent assessor.

Requiring a familiarity with the related Standards includes:

- Independence and objectivity (*Standard* 1100)
- Organizational independence (*Standard* 1110)
- Direct interaction with the board (*Standard* 1111)
- Individual objectivity (*Standard* 1120)
- Impairment to independence and objectivity (*Standard* 1130)
- Purpose, authority, and responsibility (*Standard* 1000)
- External assessments (*Standard* 1312)

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.*

1120—Implementation Guide

An internal auditor's objectivity is recognized or enhanced when he or she avoids conflict-of-interest situations and is related to whether the auditor has an impartial and unbiased mind-set. Objectivity is personal to the auditor based on trust and confidence placed on him or her by others. A conflict-of-interest situation can arise based on the appearance of impropriety, and it can occur even when the auditor did not commit unethical or illegal acts.

Presence of Objectivity ⟶ Showing Impartiality and Exhibiting Unbiased Mind-set

Lack of Objectivity ⟶ Showing Partiality and Exhibiting Biased Mind-set

Establishing a scope for implementation work requires a review of an organization's general policies related to employee performance evaluation and compensation, internal audit's policies, conflict-of-interest policies, and auditor training policies. All these policies taken as a whole can provide a working environment where conflict-of-interest situations can arise or hinder.

Considerations for implementation require an understanding of conflict-of-interest situations that could undermine an auditor's objectivity and avoiding those situations. Examples of such situations include auditing (1) a business function where an auditor previously and recently worked as an employee, (2) a family member or a close friend who is in charge of or working in a business function, and (3) a business function with prior positive experiences (i.e., auditor friendly). Situations also include not auditing a business function with prior negative experiences (i.e., auditor unfriendly).

Internal auditors are required to discuss, report, or disclose to an internal audit manager or the CAE (1) current objectivity concerns, (2) potential objectivity concerns, and (3) potential conflicts or threats that can occur. A common practice is to require that all auditors sign an annual statement indicating that no potential threats exist and acknowledging any known potential threats.

Disclosure Requirements = No Known Current Conflicts + No Known Future Threats

Considerations for demonstrating conformance include internal audit policies, auditor training records, examples of conflict-of-interest situations, signed acknowledgment forms disclosing existence and nonexistence of conflicts, and engagement workpapers showing the audit team assigned to an audit. These workpapers can be compared to auditor employment records and auditor-signed acknowledgment forms to determine the presence or absence of conflict-of-interest conditions.

Requiring a familiarity with the related Standards includes:

- Independence and objectivity (*Standard* 1100)
- Organizational independence (*Standard* 1110)
- Direct interaction with the board (*Standard* 1111)
- Chief audit executive roles beyond internal auditing (*Standard* 1112)
- Impairment to independence and objectivity (*Standard* 1130)

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 whom 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 CAE'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 CAE 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.

1130—Implementation Guide

Establishing a scope for implementation work includes an internal audit policy manual or handbook describing a discussion of organizational independence and internal auditor objectivity, the nature of impairments (real or perceived), and how internal auditors should handle potential impairments. The CAE will discuss these impairments with the board and senior management.

Considerations for implementation include understanding of various impairment situations, such as self-imposed, self-interest, self-review, self-bias, familiarity, or undue influence—all leading to conflicts of interest, scope limitations, resource limitations, or placing unnecessary and deliberate restrictions on access to records, personnel, or properties. The CAE needs to disclose the real impairments (now) or after-the-fact (later) impairments to the board and senior management for resolution.

Examples leading to an internal audit activity's (organizational) independence impairments include:

- The internal audit's annual budget is insufficient to fulfill its responsibilities.
- The CAE does not report functionally to the board or does not communicate or interact directly with the board.
- The CAE reports administratively to the chief financial officer (CFO), chief accounting officer (CAO), or lower-level management in finance and accounting functions and when the CAE audits those functions.
- The CAE manages more than the internal audit function, such as risk management, loss prevention, or insurance functions, and the CAE audits those functions.

Examples leading to an internal auditor's objectivity impairments include:

- The auditor is assigned to audit a business function that employs the auditor's relative or a close friend, or the auditor has previously worked in the same business function.
- The auditor does not apply professional skepticism and assumes that a business function must have mitigated risks because this function has received a positive audit opinion in previous audits or this function is being managed by a good manager who happens to be the auditor's friend.
- The auditor is influenced by a supervisor or manager during audit scope establishment and audit engagement instead of using his own judgment and experience and without proper justification (say *Standards* or best practices).

Considerations for demonstrating conformance include the following output documents:

- Internal audit's policy and procedure manual describing how to handle conflicts and impairment situations and how to report or communicate them
- Board meeting minutes discussing impairments
- Memos to files, emails, or reports documenting the discussions of impairments

Requiring a familiarity with the related Standards includes:

- Independence and objectivity (*Standard* 1100)
- Organizational independence (*Standard* 1110)
- Direct interaction with the board (*Standard* 1111)
- Chief audit executive roles beyond internal auditing (*Standard* 1112)
- Individual objectivity (*Standard* 1120)
- Communication and approval (*Standard* 2020)
- Errors and omissions (*Standard* 2421)

1200—Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

1200—Implementation Guide

All professionals, such as doctors, lawyers, and accountants, need to be proficient (expert) in what work they do for a society or for a business entity with utmost care and attention. *Proficiency* refers to knowledge, skills, abilities (KSAs), experiences, talents, or competencies. Proficiency or professionalism asks a basic question: Is he or she qualified to do the assigned job? Due professional care is a legal concept referring to discipline without gross negligence. Due care asks a basic question: Can he or she show diligence and exercise professional judgment similar to peers? The same requirements of professionalism and due care that are used during audit planning, staffing, and supervising specific audit engagements apply to internal auditors.

Establishing a scope for implementation work includes the following input documents:

- Internal audit charter
- Internal audit plan
- Internal audit's policies and procedures, which incorporate the IIA's Mandatory Guidance of the IPPF, signed and acknowledged by auditors

Considerations for implementation include:

- Compliance with the IIA's Code of Ethics by signing an annual declaration document
- Compliance with the organization's Code of Conduct by signing an annual declaration document
- Compliance with the IIA's Global Internal Audit Competency Framework
- Adherence to benchmarks and best practices established in the industry

The CAE can use the above criteria and others when creating job descriptions, developing skills inventory, and when recruiting, training, and assigning auditors to an audit engagement. Here, the CAE's goal is to keep the competencies of internal auditors current and sufficient, thus making them competent at all times and for all audit engagements.

Considerations for demonstrating conformance include the following output documents:

- Internal audit plan and individual audit engagement plans are matched to determine the competencies required with the competencies available. Any **competency gaps** must be addressed in a timely manner prior to assigning auditors to specific and individual audits.

  Competency Gap = Competencies Required – Competencies Available

- Internal audit's policies and procedures by signing an annual declaration document.
- The IIA's Code of Ethics and the organization's Code of Conduct by signing an annual declaration document.
- Audit engagement workpapers showing an individual auditor's professionalism and due care and showing an audit supervisor's professionalism and due care.
- Feedback and survey results from audit client showing the proficiency and due professional care exhibited by individual internal auditors assigned to audit engagements.
- Reports from independent external assessors indicating that internal audit engagements are performed with proficiency and due professional care. These assessors perform a review of the internal audit activity's quality assurance and improvement program. Here, the key point is to determine whether individual audit engagements were conducted with greater proficiency and due professional care.

Requiring a familiarity with the related Standards includes:

- Proficiency (*Standard* 1210)
- Due professional care (*Standard* 1220)
- Continuing professional development (*Standard* 1230)
- Policies and procedures (*Standard* 2040)

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 provide 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 IIA and other appropriate professional organizations.*

1210.A1—The CAE 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 IT auditing.

1210.C1—The CAE 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.

1210—Implementation Guide

Establishing a scope for implementation work requires that the CAE is responsible for ensuring the **collective proficiency** of the internal audit activity after understanding the core competencies required by the IIA's Global Internal Audit Competency Framework. This framework defines the core competencies. Here, *collective audit proficiency* means:

Proficiency of Auditor 1 + Proficiency of Auditor 2 + Proficiency of Auditor *N*

Considerations for implementation include:

- Developing competency assessments tools or skills assessment tools based on the IIA's Global Internal Audit Competency Framework as input into auditors' job descriptions and recruitment materials.
- Identifying skills gaps or competency gaps lacking proper mix of KSAs to fulfill the internal audit plan.

  Competency Gaps = Competencies Required − Competencies Available

- Knowing that competency gaps lead to audit coverage gaps, which can be removed through proper hiring, training, and outsourcing.

  Audit Coverage Gaps = Coverage Required − Coverage Completed

- Encouraging professional development of auditors through on-the-job training, attending seminars and conferences, and acquiring professional certifications, which require continuing professional development programs.
- Requiring all auditors to keep abreast of current trends and emerging issues in the industry in which they work and their impact on the internal audit profession. This proficiency can be acquired through reading whitepapers and research studies, subscribing to the industry's newsletters and services, attending in-person seminars, and participating in online seminars (webinars).
- Supervising each audit engagement to ensure quality of audit work, achievement of audit objectives, and audit staff development. There is a direct relationship between the proficiency of auditors and the extent of supervision required, meaning highly proficient and competent auditors require less supervision and vice versa.

- Surveying or interviewing the audit client after an audit engagement is completed to assess the level of proficiencies and competencies exhibited by the engagement audit staff in order to determine whether current audit objectives have been achieved. This input can be used to tailor future audit engagements.

Considerations for demonstrating conformance include the following output documents:

- An auditor's proficiency is evidenced through resumes or curriculum vitae, certifications, and continuing professional development courses, which can be used to develop skills inventory of auditors.
- An auditor's performance is reviewed and evaluated after completing an audit engagement, combined with feedback from post-engagement surveys and interviews of audit clients.
- An internal audit plan showing resource requirements, such as time budget, staff budget, and travel budget.
- An assurance map showing qualifications of service providers on which the internal audit activity relies for assurance.
- A report from internal assessment of the internal audit activity.

Requiring a familiarity with the related Standards includes:

- Proficiency (*Standard* 1200)
- Due professional care (*Standard* 1220)
- Continuing professional development (*Standard* 1230)
- Resource management (*Standard* 2030)
- Coordination and reliance (*Standard* 2050)
- Engagement resource allocation (*Standard* 2230)
- Engagement supervision (*Standard* 2340)

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.

1220—Implementation Guide

Establishing a scope for implementation work includes the following requirements:

- Internal auditors acquiring the necessary education, experience, certifications, training, and continuing education to increase the level of skills and expertise so they can perform their work with due professional care
- Internal auditors understanding and applying the Mandatory Guidance of the IIA's IPPF and the IIA's Global Internal Audit Competency Framework
- Internal auditors understanding and conforming to the IIA's Code of Ethics and the organization's Code of Conduct and signing those documents for acknowledgment

Considerations for implementation require an understanding and exercising of due professional care at three different levels:

1. *Due professional care at the individual auditor level* (personal level) involves (a) considering the possibility of significant errors, fraud, and noncompliance; (b) conducting audit examinations and verifications to the same extent as would a reasonably prudent and competent auditor in the same or similar circumstances; and (c) providing a reasonable assurance, not an absolute assurance, that noncompliance or irregularities do not exist. Due professional care does not imply infallibility.

   Due Professional Care looks for Errors, Fraud, Irregularities, and Noncompliances

2. *Due professional care at the audit engagement level* (audit assignment level) involves (a) understanding the objectives and scope of the engagement, knowing the competencies required to conduct the audit work, and understanding any policies and procedures of the internal audit activity and the organization; (b) supervisory review of the engagement workpapers, audit results, and audit conclusions to be reported; (c) providing supervisory feedback to auditors who conducted the engagement; and (d) soliciting post-engagement surveys from audit clients.

   Due Professional Care Focuses on Objectives, Scope, Competencies, and Reviews

3. *Due professional care at the internal audit activity level* (audit department level) involves the CAE (a) assuming overall responsibility that due professional care is applied, developing measurement tools (e.g., conducting self-assessment exercises and analyzing metrics and key performance indicators [KPIs]); (b) assessing the performance of individual auditors as individuals and the internal audit activity as a whole through internal and external assessments; and (c) evaluating individual auditors through peer reviews, supervisory

feedbacks, audit client surveys, and other audit stakeholder feedbacks, representing a 360-degree review.

Auditor Evaluation = Peer Reviews + Supervisor's Feedback + Audit Client Surveys + Stakeholder's Feedback = 360-Degree Reviews

Considerations for demonstrating conformance can be achieved through the following output documents:

- Audit engagement plan, work programs, and workpapers
- Auditor's performance review reports
- Supervisory reviews of engagement work as documented in workpapers
- Post-engagement feedback from supervisors to auditors
- Feedback from audit clients through surveys, interviews, and memos
- Auditor's signing the IIA's Code of Ethics and the organization's Code of Conduct documents
- Reports from internal and external assessments of the internal audit activity as part of the quality assurance and improvement program

Requiring a familiarity with the related Standards includes:

- Proficiency (*Standard* 1200)
- Proficiency (*Standard* 1210)
- Continuing professional development (*Standard* 1230)
- Engagement supervision (*Standard* 2340)
- Quality assurance and improvement program (*Standard* 1300)
- Requirements of the quality assurance and improvement program (*Standard* 1310)
- Internal assessments (*Standard* 1311)
- External assessments (*Standard* 1312)

1230—Continuing Professional Development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

1230—Implementation Guide

An internal auditor's long-term career goals and plans will shape the auditor's continuing professional development (CPD) plans. The CPD plan is a part of auditor's professional development plan (PDP). An auditor's CPD plan and PDP plan must be aligned with the CAE's career plans developed for that auditor.

Establishing a scope for implementation work needs the following input documents:

- Job descriptions stating job requirements for auditors
- Training policies and professional education requirements of a profession, organization, or industry

- Conformance with the Mandatory Guidance of the IIA's IPPF
- Self-assessments based on the IIA's Global Internal Audit Competency Framework or any other benchmarks
- A CPD plan that considers the internal audit's policies, auditors' training schedules, and the audit staff's surveys and feedbacks

Considerations for implementation include:

- An auditor's self-assessment tool becomes a basis for the auditor's PDP.
- The scope of an auditor's PDP plan can include on-the-job training, coaching, mentoring, job rotation, internal and external training programs (e.g., conferences and seminars), educational programs (e.g., online and offline courses, webinars, self-study programs, and research projects), professional certifications, and volunteering with professional associations and organizations.

  Job Rotation = Moving from Audit Function to Nonaudit Function

  Reverse Job Rotation = Moving from Nonaudit Function to Audit Function
- An auditor's PDP becomes the basis for the auditor's KPIs that could be incorporated into supervisory reviews, audit-client surveys, and annual performance reviews.
- An internal audit department's training and development policies support CPD in terms of number of hours of training (say 40 hours), which can be benchmarked with other internal audit departments.
- An auditor's PDP must be aligned or synchronized with that of the CAE's CPD plan.
- An auditor's business acumen can be measured or assessed through audit-client surveys and feedbacks, supervisor comments, and peer observations.
- An auditor can keep his or her knowledge, skills, and abilities (KSAs) current with guidance from the IIA's *Standards*, research publications, best practices, procedures, and techniques.
- An auditor can subscribe to newsfeeds or notification services related to the audit profession and industry-specific news.
- An auditor can acquire two types of proficiency: required proficiency and enhanced proficiency.

Required Proficiency = Continuing Education Credit Hours + Professional Certifications + Certificates of Completion

Enhanced Proficiency = On the Job Training Coaching + Job Rotation Mentoring + Internal and/or External Training

Considerations for demonstrating conformance require the following output documents:

- Self-assessment reports and benchmark studies
- Professional development and training plans
- Paying for membership dues and magazine subscriptions
- Evidence of completed training and educational programs with a proof of continuing education credits, certificates of completion, certificates of attendance, professional certifications, and college-level credits
- CPD plans for each auditor developed from the internal audit's policies, training schedules, and surveys and feedbacks from audit staff

Requiring a familiarity with the related Standards includes:

- Proficiency (*Standard* 1200)
- Proficiency (*Standard* 1210)
- Due professional care (*Standard* 1220)

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

1300—Implementation Guide

Establishing a scope for implementation work includes:

- Assurance engagements as stated in the Mandatory Guidance of the IIA's IPPF
- Consulting engagements as stated in the Mandatory Guidance of the IIA's IPPF
- Internal audit activity operations
- QAIP sources that include audit literature reviews, audit research studies, and best practices in the internal audit profession
- QAIP scope that includes both internal assessments and external assessments of the internal audit activity

Considerations for implementation include:

- Conforming to QAIP means conforming to the IIA's *Standards*, applying the Code of Ethics, and aligning with the definition of internal auditing and core principles.
- Each individual audit engagement is not required to conform to the IIA's *Standards.*
- Each individual audit engagement should conform to an established audit methodology primarily and by default with the *Standards*. Moreover, the audit methodology should be uniformly and consistently applied to all individual audit engagements.
- The audit methodology promotes continuous gradual improvement of the audit activity.

Considerations for demonstrating conformance can be found in the following output documents:

- The CAE's documents describing the QAIP itself
- The CAE's communication of QAIP results with the board and senior management about its findings, corrective actions plans, and corrective actions already taken
- Reports from external assessments provided by independent and qualified assessors
- Board's meeting minutes showing discussions and presentations made to the board and senior management

Requiring a familiarity with the related Standards includes:

- Requirements of the quality assurance and improvement program (*Standard* 1310)
- Internal assessments (*Standard* 1311)
- External assessments (*Standard* 1312)
- Reporting on the quality assurance and improvement program (*Standard* 1320)
- Use of "conforms with the international standards for the professional practice of internal auditing" (*Standard* 1321)
- Disclosure of nonconformance (*Standard* 1322)

1310—Requirements of the Quality Assurance and Improvement Program

The quality assurance and improvement program must include both internal and external assessments.

1310—Implementation Guide

Establishing a scope for implementation work includes:

- Audit QAIP coverage includes both internal assessments and external assessments where these assessments add value to the internal audit activity first and organization's stakeholders next.
- Internal assessments consist of rigorous and comprehensive processes; continuous supervision and testing of assurance and consulting work; and periodic validation of conformance with the IIA's *Standards* and the Code of Ethics. A report is issued to identify areas for improvement.
- External assessments are provided by an external and independent assessor or team of assessors to conclude whether the internal audit activity conforms to the IIA's *Standards* and the Code of Ethics. A report is issued to identify areas for improvement.
- The CAE conducts ongoing and continuous measurements and analyses using audit metrics and KPIs.
- The CAE monitors the outcomes of the internal and external assessments and develops and implements action plans related to any identified improvements through the QAIP.

Considerations for implementation include:

- Internal assessments consist of ongoing monitoring and periodic self-assessments in that order.
- Ongoing monitoring is achieved primarily through continuous activities such as engagement planning and supervision, standardized work programs and practices, standardized workpaper development procedures and sign-offs, and workpaper and report reviews. Continuous monitoring is related to delivering quality audits on an engagement-by-engagement basis.
- Periodic self-assessments are conducted internally to validate that ongoing monitoring is operating effectively and to assess whether the internal audit activity is in conformance with the IIA's *Standards* and the Code of Ethics. This conformance in turn also achieves alignment with the definition of internal auditing and the core principles.

Internal Assessments = Ongoing Monitoring + Periodic Self-Assessments

Ongoing monitoring is done first.

Periodic self-assessment is done next.

- External assessments are conducted at least once every five years by an independent and external assessor or a team from outside the audit function and outside the audit organization.
- A self-assessment may be performed in lieu of a full external assessment, provided it is validated by a qualified, independent, competent, and professional external assessor. Under these conditions, the scope of a self-assessment is the same as that of a full external assessment.

  An original self-assessment can be performed onsite by an internal assessor or by an external assessor.

  A self-assessment must be validated onsite by a separate independent external assessor regardless of who performed the original self-assessment.
- The goal of internal assessments and external assessments is the same: to determine whether an internal audit activity conforms to the IIA's *Standards* and the Code of Ethics.

Considerations for demonstrating conformance include the following output documents:

- Minutes of board meetings where internal external assessment plans and results were discussed.
- A request for services (RFSs) document that shows how the external assessors are vetted (screened), selected, and hired to do the external assessment work. This document combined with a benchmarking report demonstrates the exercise of due diligence on the part of the internal audit activity.
- Documents showing how internal assessments are conducted with review scope, approach plan, workpapers, and reports containing recommendations for improvement. These documents are accompanied by audit metrics and KPIs.
- Documents showing how external assessments are conducted with a report containing conclusions as to the degree of conformance (e.g., 85%); recommendations to improve internal audit quality, efficiency, and effectiveness; and corrective action plans required.

Requiring a familiarity with the related Standards includes:

- Quality assurance and improvement program (*Standard* 1300)
- Internal assessments (*Standard* 1311)
- External assessments (*Standard* 1312)
- Reporting on the quality assurance and improvement program (*Standard* 1320)
- Use of "conforms with the international standards for the professional practice of internal auditing" (*Standard* 1321)
- Disclosure of nonconformance (*Standard* 1322)

Audit Metrics and Key Performance Indicators—*Standard* 1310

Internal audit activity is a function requiring a measurement of its performance similar to other functions in an organization. Audit metrics and KPIs are self-checks for internal auditors to measure and manage progress of their own performance levels. Audit metrics and KPIs can be organized, structured, and monitored in terms of management KPIs, operational KPIs, strategic KPIs, professional KPIs, financial KPIs, and board-level KPIs.

Management KPIs

- Time to complete an audit engagement in hours or days (time to audit in hours or days)
- Average time to complete an audit engagement in hours or days (average time to audit in hours or days)
- Elapsed time between the audit fieldwork completion and audit report issuance (Longer time periods require improvements.)
- Average time to issue audit reports in days or weeks (This measures how much time was taken to issue an audit report after an audit engagement was completed.)
- Time since the last audit (in years) (This actual time should be compared with the planned audit cycle time, and proper actions should be taken.)
- Elapsed time between the audits (in years) (This actual time should be compared with the planned audit cycle time, and proper actions should be taken.)
- Time to take corrective actions by audit client management regarding audit recommendations (Longer time periods require audit monitoring and follow-up.)
- The longest time an auditor's job is open for months, quarters, and years
- The shortest time an auditor's job is open for months, quarters, and years

Operational KPIs

- Percentage of the annual audit plan completed (Higher percentage indicates successful audits while lower percentages indicate unsuccessful audits, where the latter results in residual risks.)
- Percentage of actual risks addressed, assured, or covered to the total number of risks discovered or uncovered (The difference results in an assurance gap.)
- Percentage of audit reports issued as scheduled or planned (This shows that the audit activity can deliver its reports on time and that it is disciplined in doing so.)
- Percentage of follow-up audits conducted as scheduled or planned (This indicates auditors' lack of seriousness and shows that auditors are there just to make recommendations and that they are not serious about whether they help the organization that they work for. It is a sign of disservice to the organization.)
- Percentage of recommendations implemented resulting from internal assessments and external assessments regarding internal audit activity's QAIP

Strategic KPIs

- Percentage of audit recommendations accepted by audit clients at a point in time (This indicates the usefulness [benefit] of audit recommendation to audit clients.)
- Percentage of audit recommendations rejected by audit clients at a point in time (This indicates the nonuse (no benefit) of audit recommendation to audit clients.)
- Percentage of audit recommendations implemented after they are accepted by audit clients at a point in time (This indicates that audit recommendations are practical and useful.)

- Percentage of unimplementable audit recommendations after they were accepted by audit clients at a point in time (This indicates that audit recommendations are theoretical in nature with no practical benefits.)
- Percentage of significant audit recommendations (vital few of 20/80 or 80/20 rule) to the total number of audit recommendations made in a year (This indicates that internal auditors are clearly adding and enhancing value to their organization.)
- Percentage of insignificant audit recommendations (trivial many of 20/80 rule) to the total number of audit recommendations made in a year (This indicates that internal auditors are not adding value to their organization.)
- Percentage of audit recommendations accepted and remaining open at a point in time (This indicates that audit clients have not decided to implement the recommendations for some reason.)
- Percentage of audit recommendations that were closed at a point in time (This indicates that audit clients have fully implemented the auditors' recommendations to the auditors' full satisfaction.)
- Overall audit client satisfaction rate (This is an aggregated measure of satisfaction-related information received from audit clients and other stakeholders through surveys, feedback, one-on-one meetings and interviews, memos, emails, and reports. This satisfaction rate is expressed in terms of a percentage.)

Professional KPIs

- Percentage of auditors certified in internal auditing with the CIA designation
- Percentage of auditors with audit-related multiple certifications
- Average number of professional certifications held by auditors
- Average number of continuing professional development (CPD) hours earned in a year by auditors
- Average number of years of auditor work experience in internal auditing
- Percentage of technology auditors to nontechnology auditors
- Average turnover of audit staff in a year

Financial KPIs

- Percentage of audits completed over budget
- Percentage of audits completed under budget
- Variance analysis between budgeted hours and actual hours

Board-Level KPIs

- Percentage of independent directors to total board members (The goal should be a higher percentage than in the industry.)
- Percentage of a company's executives on the board to total board members (The goal should be a smaller percentage than in the industry.)
- Percentage of shadow directors to total board members (The goal should be a zero percentage because shadow directors—for example, outsiders such as lobbyists, activists, friends, family members, consultants, and majority shareholders—can exercise greater pressure on and influence over the board.)
- Percentage of nonexecutive directors to risk management committee members (The goal should be a higher percentage because executive directors such as the CEO, CFO, and chief risk officer [CRO] can exercise greater influence on the risk committee, which is not good for the company.)

Audit Metrics and Key Performance Indicators— *Standard* 1310 *(Continued)*

- Percentage of independent directors to audit committee members (The goal should be a higher percentage because the audit committee oversees the entire financial reporting process and coordinates between internal auditors and external auditors, which is a major responsibility. The audit committee should not oversee the risk management and regulatory compliance functions as they are the responsibilities of senior management [executives].)
- Percentage of female directors to total board members (The goal should be a comparable percentage in the industry and nation's data.)
- Percentage of directors with little or no compensation or remuneration paid (The goal should be a zero percentage because it follows the simple principle of no money, no work. Two outcomes are possible here: say on pay and no pay, no say. Without comparable compensation and remuneration, directors are hired just for their name only to act as a rubber stamp for the CEO, directors simply become routine box checkers in their work, and they have no strong voice [or no teeth] in the board's work and decisions.)
- Percentage of board-level qualitative metrics to the total number of board-level metrics (Total metrics include both qualitative metrics and quantitative metrics, which should be given equal importance. Examples of quantitative metrics include (1) sales, revenues, profits, market share, and company stock prices year over year; and (2) earnings per share, return on investment, return on assets, return on equity, and return on capital. Examples of qualitative metrics include employee low morale, negative comments posted on social media by unhappy customers, cyberrisks, supply-chain risks, product recall risks, public relations risks, and customer dissatisfaction risks.)

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.

1311—Implementation Guide

Establishing a scope for implementation work requires the following considerations:

- The scope of internal assessments includes both ongoing monitoring and periodic self-assessments with different focus. The difference in scope and focus is shown next:

  Ongoing monitoring takes a narrow scope and focuses on conformance with performance standards at the individual audit engagement level.

Periodic self-assessments take a broad scope and focus on conformance with all *Standards* (Attribute and Performance *Standards*) at the internal audit activity level.

- Both ongoing monitoring and periodic self-assessments require constant measuring, monitoring, and reporting of audit metrics and audit KPIs.
- All internal assessments must conform to the IIA's *Standards* and the Code of Ethics.
- Internal assessments focus on continuous improvement of the internal audit activity.
- The IIA's Quality Assessment Manual for the Internal Audit Activity or other guidelines and tools can help in conducting internal assessments.
- The relation between internal assessments and external assessments:

  Internal assessments are done first.

  External assessments are done last.

  Internal assessments support external assessments.

Considerations for implementation include:

- Ongoing monitoring occurs routinely throughout the year with the implementation of standard work practices such as audit supervision, audit planning, audit program, workpaper reviews, and audit reports.
- During ongoing monitoring, checklists or automation tools can be used to ensure compliance with established practices and procedures and to ensure consistency in the application of performance standards.
- Ongoing monitoring requires feedback from audit clients immediately after an audit engagement, semiannually, or annually to determine how efficiently and effectively the internal audit work was performed during the engagement.
- Ongoing monitoring delivers quality audit results on an engagement-by-engagement basis.
- Periodic self-assessments are conducted by senior members of the internal audit activity, Certified Internal Auditors (CIAs), and competent internal audit professionals working in nonaudit departments of the same organization. These members can form a team with extensive experience and knowledge with IIA's IPPF, consisting of *Standards* and Code of Ethics. Conducting post-engagement reviews or analyzing metrics and KPIs can support the periodic self-assessment.
- A periodic self-assessment should be performed shortly before the external assessment to reduce the time and effort required to complete the external assessment.
- Audit metrics and KPIs should be measured during self-assessments and internal assessments.
- Results of ongoing monitoring and periodic self-assessments should be reported to the board at least annually.

Considerations for demonstrating conformance include the following output documents:

- Completed checklists that support workpapers reviews
- Submitted survey results from audit clients and other stakeholders
- Audit metrics and KPIs showing the efficiency and effectiveness of the internal audit activity

- Completed periodic self-assessments showing the scope and focus of work
- Internal assessment results presented to the board and senior management with corrective action plans and corrective actions taken
- Board meeting minutes

Requiring a familiarity with the related Standards includes:

- Quality assurance and improvement program (*Standard* 1300)
- Requirements of the quality assurance and improvement program (*Standard* 1310)
- External assessments (*Standard* 1312)
- Reporting on the quality assurance and improvement program (*Standard* 1320)
- Use of "conforms with the international standards for the professional practice of internal auditing" (*Standard* 1321)
- Disclosure of nonconformance (*Standard* 1322)
- Policies and procedures (*Standard* 2040)
- Engagement planning (*Standard* 2200)
- Performing the engagement (*Standard* 2300)
- Engagement supervision (*Standard* 2340)
- Communicating results (*Standard* 2400)

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 CAE 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 CAE should encourage board oversight in the external assessment to reduce perceived or potential conflicts of interest.

1312—Implementation Guide

Establishing a scope for implementation work includes:

- External assessments are required at least once every five years or more frequently by an independent and competent external assessor, either individually or a team, coming from outside the organization. Reasons for conducting assessments more frequently include changes in senior management, shorter business cycles, new CAE, changes in the audit policies and procedures, merger of two or more audit departments, and significant audit staff turnover.
- The goal of the external assessor is to validate that an internal audit activity conforms to the IIA's *Standards* and the Code of Ethics.
- The external assessor must be hired through an acquisition policy such as submitting an RFSs document followed by bidding and evaluation practices.
- The CAE must ensure that the external assessor will not impair independence, will maintain objectivity, and will be free of conflict-of-interest situations.
- The relation between internal assessments and external assessments is shown next:

  Internal assessments are done first.

  External assessments are done last.

  Internal assessments support external assessments.

Considerations for implementation include:

- Two approaches to external assessments include (1) a full external assessment and (2) a self-assessment with independent external validation (SAIV). These two approaches will have the same comprehensiveness in terms of scope and size, as they evaluate the audit's conformance with the IIA's *Standards* and Code of Ethics.
- A full external assessment addresses: (1) the level of conformance with the IIA's *Standards* and Code of Ethics as evidenced from the audit charter, plans, policies, procedures, practices, and regulatory requirements; (2) the efficiency and effectiveness of the internal audit activity through a review of audit processes, QAIP requirements, and the audit staff's knowledge, experience, and expertise; and (3) the extent to which the audit activity adds value to the stakeholders and meets the expectations of senior management, operations management, and functional management.
- The work of SAIV is conducted by a qualified internal auditor first and later validated by a qualified external assessor. The work is conducted onsite.

  SAIV = Qualified Internal Auditor for Onsite Self-Assessment
  + Qualified External Assessor for Onsite Validation

- External assessors must be competent in the professional practice of internal auditing (i.e., knowledge of IPPF's Mandatory Guidance and *Standards*) and must be knowledgeable in the external quality assessment process.
- External assessors must have work experience at the audit management level (i.e., CAE or similar), must have received the CIA designation, and must have received the IIA's quality assessment training course or similar training.

- The external assessment team may consist of specialists (e.g., risk analysts, IT auditors, statisticians, scientists, engineers, and actuaries) to provide assistance to the team members. Each team member does not need to possess all of the preferred competencies; rather, the team as a whole should possess the necessary competencies to deliver the best results.
- The external assessors, either individually or a team, must be objective. This means that they should be free from actual, potential, or perceived conflict-of-interest situations that could impair objectivity.
- The external assessors must be independent of the internal audit activity (audit department). They are not independent if they were: (1) recent previous employees of the internal audit department; (2) employees from another department of the organization (nonaudit department); (3) employees from a related organization, such as a parent company, an affiliate group, or a business division; or (4) reciprocal peer assessments between two audit departments. However, reciprocal peer assessments among three or more audit departments are considered independent.

Considerations for demonstrating conformance include the following output documents:

- A report from the external assessor describing observations and recommendations to management in order to improve the internal audit quality, efficiency, and effectiveness
- Minutes of a board meeting documenting the assessment results with action plans for improvement
- A benchmarking report showing how the external assessor was screened, selected, and hired (a vetting process) through an RFSs document that demonstrates the audit's commitment to a due diligence process (Note that the vetting process does not apply to guest auditors, who are borrowed auditors and employed in a nonaudit department of the same organization as that of the internal audit department.)

Requiring a familiarity with the related Standards includes:

- Quality assurance and improvement program (*Standard* 1300)
- Requirements of the quality assurance and improvement program (*Standard* 1310)
- Internal assessments (*Standard* 1311)
- Reporting on the quality assurance and improvement program (*Standard* 1320)
- Use of "conforms with the international standards for the professional practice of internal auditing" (*Standard* 1321)
- Disclosure of nonconformance (*Standard* 1322)

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 CAE 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.*

1320—Implementation Guide

Establishing a scope for implementation work requires the following considerations:

- The CAE establishes the minimum criteria for conducting internal assessments and external assessments and communicates them to the board and senior management.
- The CAE is aware of previous internal and external assessments with their rating scales.
- The CAE is familiar with the IIA's *Standards* and Code of Ethics.

Considerations for implementation include four core elements:

1. Scope and frequency of both internal assessments and external assessments

   Internal assessments are done at least every year for large-size audit departments.

   Internal assessments are done at least every two years for small-size audit departments.

   External assessments are done at least every five years or more frequently.

   Ongoing monitoring, a part of internal assessments, requires a reporting of audit metrics and KPIs.

2. Qualifications and independence of the assessor(s) or assessment team

   Both internal assessors and external assessors must be qualified and competent to do their work.

   External assessors must be independent and objective from the audit activity in that they do not have actual, potential, or perceived conflicts of interests.

3. Conclusions of assessors

   External assessors express their opinions or conclusions on the results of their work.

   External assessors indicate the degree of conformance with the IIA's *Standards*, whether for each standard and/or a series or group of standards, with a rating scale.

   The conformance rating scale includes three types: (1) generally conforms (a top rating of conformance with the audit charter, polices, practices, processes, and *Standards*), (2) partially conforms (a middle rating of deviations from the *Standard*s that do not preclude the audit activity from fulfilling its responsibilities), and (3) does not conform (a bottom rating of significant deficiencies that have a serious impact or that can preclude the audit activity from adequately fulfilling its responsibilities).

4. Corrective action plans that have been completed or yet to be completed

   The CAE reports the results of external assessments to the board and senior management at two different times: immediately after the assessment work was done and before

the corrective actions were taken on recommendations and immediately after all the recommendations have been corrected.

The CAE adds the external assessor's recommendations to the ongoing monitoring processes on a proactive basis.

Considerations for demonstrating conformance include the following output documents:

- Board meeting minutes showing the CAE's discussions with the board and senior management about the scope, objectives, and frequency of both internal assessments and external assessments
- Procurement or acquisition documents showing how the external assessors are carefully screened, selected, and hired (i.e., vetted)
- Reports from internal assessments and external assessments with conclusions and recommendations

Requiring a familiarity with the related Standards includes:

- Quality assurance and improvement program (*Standard* 1300)
- Requirements of the quality assurance and improvement program (*Standard* 1310)
- Internal assessments (*Standard* 1311)
- External assessments (*Standard* 1312)
- Use of "conforms with the international standards for the professional practice of internal auditing" (*Standard* 1321)
- Disclosure of nonconformance (*Standard* 1322)
- Recognizing mandatory guidance in the internal audit charter (*Standard* 1010)
- Policies and procedures (*Standard* 2040)

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.*

1321—Implementation Guide

This *Standard* discusses the scenarios and situations under which a conformance statement can be used, whether it is a partial conformance with one or more *Standards* or a full conformance with all *Standards*. Here, conformance addresses both the IIA's *Standards* and the Code of Ethics. Note that external auditors are required to state that all of their attestation engagements and financial statement audits are conducted in conformance with the Generally Accepted Auditing Standards. On the other hand, internal auditors have specific conditions to meet prior to stating that their internal audit work conforms to the IIA's *Standards* and Code of Ethics.

Conformance = Internal Assessments and External Assessments
Nonconformance = No Internal Assessments and No External Assessments
Nonconformance = Internal Assessments without External Assessments

Establishing a scope for implementation work requires:

- The CAE is required to have a full and clear understanding of the QAIP requirements.
- The CAE reviews the results from recent internal assessments and external assessments.
- The CAE learns the expectations of the board about conformance to the IIA's *Standards*, educates board members about the scope and nature of such *Standards*, and explains to board members what it means to conform or not conform to those *Standards.*

Considerations for implementation include an understanding of the following scenarios:

- It is a nonconformance when the results of either the current internal assessment or the most recent external assessment do not conform to the IIA's *Standards* and Code of Ethics.
- It is a nonconformance when the age of the internal audit activity is five years or more and it did not complete an external assessment.
- It is a nonconformance when the internal audit activity did not conduct an internal assessment according to its published frequency and that a completed external assessment did not validate the internal assessment.
- It is a nonconformance when the external assessment was not done every five years and it requires that the internal audit activity must not use a statement that it is in conformance until the external assessment is completed and that it supports conformance with the IIA's *Standards* and Code of Ethics.
- It is a nonconformance when the external assessment concludes that the internal audit activity was not in compliance. Then the audit activity must immediately discontinue using a conformance statement until all the nonconformance items are corrected based on the next external assessment with full validation.
- Nonconformance becomes conformance after full validation by external assessors.
- It is a conformance when the age of the internal audit activity is less than five years and the recent self-assessment (a part of internal assessment) report stated that it was in compliance with the IIA's *Standards* and Code of Ethics.

Considerations for demonstrating conformance include the following output documents:

- Reports from internal assessments and external assessments with clear conclusions whether the internal audit activity has achieved conformance with the IIA's *Standards*
- Engagement plans, notifications, and schedules for internal and external assessments
- Internal audit charter
- Internal audit policies and procedures manual
- QAIP manual
- Board meeting minutes showing the CAE's communications with the board about the internal and external assessments and their results

Requiring a familiarity with the related Standards includes:

- Quality assurance and improvement program (*Standard* 1300)
- Requirements of the quality assurance and improvement program (*Standard* 1310)
- Internal assessments (*Standard* 1311)
- External assessments (*Standard* 1312)
- Reporting on the quality assurance and improvement program (*Standard* 1320)
- Disclosure of nonconformance (*Standard* 1322)

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.

1322—Implementation Guide

This *Standard* discusses the disclosures required when an internal audit activity does not conform to the IIA's *Standards* and Code of Ethics and presents the impact of nonconformance on the overall scope or operation of the internal audit activity. This *Standard* presents examples of such nonconformances.

Establishing a scope for implementation work requires:

- The CAE is required to have a full and clear understanding of the QAIP requirements.
- The CAE reviews the results from recent internal assessments and external assessments.
- The CAE learns the expectations of the board about conformance to the IIA's *Standards* and Code of Ethics, educates board members about the scope and nature of such *Standards* and Ethics, and explains what it means to conform or not conform to those *Standards* and Ethics.

Considerations for implementation include:

- The CAE is required to communicate annually to the board and senior management about the results of internal and external assessments and the level of conformance with the IIA's *Standards* and Ethics. This communication is necessary to uncover impairments to independence or objectivity, audit scope restrictions or limitations, and resource limitations for auditors and audit clients.
- Examples of nonconformances include: (1) when the internal audit activity did not conduct external assessment at least once every five years; (2) when an internal auditor did not meet individual objectivity requirements during an audit engagement; (3) when an audit engagement did not have auditors possessing collective knowledge, skills, and experiences; and (4) when the CAE and managers and supervisors failed to consider risk when developing the audit plan.
- The CAE should be able to quantify (how much) the impact of nonconformance on the internal audit activity in fulfilling its responsibilities such as providing reliable assurance and consulting services, completing the audit plan, and addressing high-risk audit areas.

Considerations for demonstrating conformance require the following output documents:

- Board meeting minutes showing the impact of nonconformance with the *Standards* and ethics
- Private meetings with the audit committee
- One-on-one meeting with the board chair
- Memos or emails to senior management and the board

Requiring a familiarity with the related Standards includes:

- Quality assurance and improvement program (*Standard* 1300)
- Requirements of the quality assurance and improvement program (*Standard* 1310)
- Internal assessments (*Standard* 1311)
- External assessments (*Standard* 1312)
- Reporting on the quality assurance and improvement program (*Standard* 1320)
- Use of "conforms with the international standards for the professional practice of internal auditing" (*Standard* 1321)
- Individual objectivity (*Standard* 1120)
- Proficiency (*Standard* 1210)
- Planning (*Standard* 2010)

The IIA's Three Lines of Defense Model—*Standard* 1322

Similar to information systems security requiring multiple layers of defense (i.e., security controls using defense-in-depth and defense-in-breadth concepts) to protect technology assets (e.g., computers, networks, and mobile devices), organizations need three lines of defense (three layers of defense) to protect and preserve human assets (e.g., employees, customers, suppliers, vendors, visitors, and contractors), tangible assets (e.g., buildings, inventory, plant, and equipment), intangible assets (e.g., copyrights, trademarks, service marks, and patents), financial assets (e.g., cash, stocks, and bonds), and information assets (e.g., data, plans, policies, procedures, and practices). The scope of the three-lines-of-defense model applies to risk management and control activities and processes. The nature of this model includes vigilant employees observing people and things for unusual and strange behavior, manual control procedures, automated control procedures, and daily work rules and practices.

The idea behind the three-lines-of-defense model is that:

- If the first line of defense does not work for some reason, then the second line of defense comes into play to protect and preserve the assets.
- If the first line and second lines of defense do not work for some reason, the third line of defense (last line of defense) should work in protecting and preserving the assets.

The concept behind the three-lines-of-defense model is that two hands are stronger than one hand and that multiple lines of defense provide a much stronger support and protection than a single line of defense. This model can be installed at two levels: organization level and internal audit level.

THE IIA'S THREE LINES OF DEFENSE MODEL— *STANDARD* 1322 *(Continued)*

Organization Level: Three Lines of Defense

Examples of organization-level three-lines-of-defense follow. Although not officially and explicitly defined, outside auditors, such as external auditors, bank examiners, and regulatory auditors, can be treated and recognized as providing fourth-line-of-defense services.

First line of defense	Operational and functional management working in manufacturing, marketing, merchandising, procurement, IT, human resources, accounting, loss prevention, finance, and operations departments. This first defense is a form of initial exercise of controls through management controls and internal control measures. This defense is provided by risk owners and managers who own, manage, and oversee risks. These risk owners implement corrective actions to address process weaknesses and control deficiencies.
Second line of defense	Employees working in compliance function, health and safety department, customer service department, technical support group, environmental management, IT security analysts, physical security guards, legal staff, risk analysts, financial control analysts, product quality inspectors, internal quality assurance providers, and external quality assurance providers. This second defense is a form of intermediary exercise of controls and provides risk control and compliance.
Third line of defense	Internal auditors, physical security guards, fraud specialists, public relations officers, insurance claims adjusters, and corporate gatekeepers (e.g., accountants, auditors, and attorneys). This third defense is a form of final exercise of controls and provides risk assurance.
Fourth line of defense	Although not officially and explicitly defined, outside auditors, such as external auditors, bank examiners, and regulatory auditors, can be treated and recognized as providing fourth-line-of-defense services. These outside auditors can be asked to provide a separate and comprehensive review of an organization's risk management framework and practices (e.g., enterprise risk management), to assess the adequacy of the three lines of defense, and to report their review results to senior management, the board, and shareholders.

Both the second and third lines of defense provide oversight and/or assurance services over risk management. The key difference between the second and third lines is the concepts of independence and objectivity of internal auditors.[1]

Responsibilities may become blurred across internal audit function and second-line-of-defense functions when internal auditors are asked to assume second-line-of-defense activities due to their special skills and talents. Examples of these assumed activities include new regulatory requirements (e.g., assistance in training and implementation of Sarbanes-Oxley Act of 2002), change in business (e.g., entry into new markets, new products, and new lines of business), resource constraints (internal auditors are requested to fill the staffing and management gap), and efficiency in performing compliance and risk management functions better than the others.

[1] IIA, *Internal Audit and the Second Line of Defense, IPPF's Supplemental Guidance, Practice Guide* (January 2016), www.theiia.org.

Where safeguards to maintain internal audit's independence and objectivity are not possible, the responsibility for performing the second-line-of-defense activities should be reassigned to an internal nonaudit function or outsourced externally to a third-party provider. Moreover, the second-line-of-defense activities performed by internal audit should be referenced in the audit's charter document and/or included in the board update report issued at least annually by the internal audit department.

Internal auditors should avoid activities that compromise their independence and objectivity, including:

- Setting the risk appetite levels
- Owning, managing, and overseeing risks
- Assuming responsibilities for accounting, business development, and other first-line-of-defense functions
- Making risk-response decisions on the organization's management's behalf
- Implementing or assuming accountability for risk management or governance processes
- Providing assurance on second-line-of-defense activities performed by internal auditors

Audit Level: Three Lines of Defense

Similar to the three lines of defense found at an organization level, internal audit activity has three lines or layers of defense within its own department or function.

First line of defense	Staff auditor who is assigned to an audit engagement (engagement auditor), who developed the audit program, who prepared audit workpapers, and who drafted the initial audit reports can act as the first line of defense. Sign-off letters received from the engagement auditor after completing the audit work support and strengthen the audit work.
Second line of defense	In-charge auditor or lead auditor who reviewed the audit program, workpapers, and audit reports to confirm adherence to the audit plan, objectives, and scope can act as the second line of defense. Sign-offs received from the in-charge auditor or lead auditor support and strengthen the audit work completed.
Third line of defense	Audit supervisor or manager who reviewed the audit plan, audit program, workpapers, and audit reports to confirm adherence to the IIA's Standards, including the audit quality assurance standards, can act as the third line of defense. Sign-offs received from the audit supervisor or manager support and strengthen the audit work completed. Note that the audit supervisors and managers should act as the last line of defense (last resort) because there is no one after them to protect and defend the audit work.

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.

2100—Implementation Guide

Establishing a scope for implementation work includes:

- The CAE should possess **business acumen** in understanding the concepts and principles of organizational governance, risk management, and control. Business acumen is a collective knowledge and understanding of business mission and vision; business objectives and goals; business strategies and plans; regulatory and legal requirements; and competitors' strategies and plans. This understanding can help the CAE in evaluating the effectiveness and efficiency of governance, risk management, and control (GRC) processes in the organization.
- The CAE and staff understand that the full scope and nature of internal audit work consists of improving the GRC processes.

  Scope and Nature of Audit Work = Governance Processes + Risk Management Processes + Control Processes

- Internal auditors, supervisors, and managers need to apply their knowledge, experience, and best practices in the GRC processes to proactively highlight observed operational weaknesses and control breakdowns and make recommendations for improvement.
- The board is responsible for guiding the governance processes whereas senior management is accountable for leading risk management and control processes.

  Board ⟶ Governance Processes

  Senior Management ⟶ Risk Management and Control Processes

- The CAE will review and understand the board's charter and the audit committee's charter to understand the scope and nature of their duties, responsibilities, and accountabilities.
- The CAE will review and become familiar with the key organizational structures and roles of the chairman of the board, CEO, and other C-level executives such as CFO, chief information officer, and CRO.

Considerations for implementation include the following;

- Whereas the board is responsible for governance processes and senior management is accountable for risk management and control processes, the CAE is responsible for providing objective assurance and consulting services related to the GRC processes and to improve such processes.

  Board ⟶ Governance

  Senior Management ⟶ Risk Management and Control

  Chief Audit Executive ⟶ Governance, Risk Management, and Control

- The CAE can assess the risks associated with the GRC processes only after assessing the maturity level of the GRC processes, maturity level of the organization's culture, and seniority of the individuals managing the GRC processes. Maturity levels can be either high (mature) or low (immature).
- A **fit-gap analysis** can be performed showing maturity or immaturity of GRC processes, as follows:

  Mature GRC Processes + Mature Organization's Culture + Mature Senior Managers = Fit

  Mature GRC Processes + Immature Organization's Culture + Mature Senior Managers = Gap

Mature GRC Processes + Mature Risk Management + Mature Controls = Fit
Mature GRC Processes + Mature Risk Management + Immature Controls = Gap
Mature GRC Processes + Immature Risk Management + Mature Controls = Gap
Immature GRC Processes + Mature Risk Management + Mature Controls = Gap

- The CAE can seek guidance from an established framework that senior management uses in guiding the risk assessment. Examples of these frameworks include the Committee of Sponsoring Organizations of the Treadway Commission's internal control (COSO's Internal Control) and COSO's enterprise risk management framework (COSO-ERM), the King Report on Corporate Governance, or International Standards Organization (ISO) 31000 for risk management. If the organization does not use any framework to guide the GRC processes, the CAE should recommend an appropriate framework for adaptation.
- The CAE assesses how her organization promotes business ethics and values, both internally within the organization and externally with its business partners. This assessment covers a review of mission, vision, and value statements; a code of conduct; hiring and training processes; an antifraud and whistleblowing policy; and a hotline and investigation process. Surveys and interviews can be used to measure whether the organization's efforts result in sufficient awareness of its ethical standards and values.
- The CAE ensures that his organization is effective in employee performance management and accountability matters. This scope covers a review of policies and processes related to employee compensation, objective setting (management by objective, MBO), performance evaluations, organization's KPIs, and incentive plans (bonuses and perks to management). This review can disclose unacceptable behavior of employees and management or excessive risk taking by management, which can be contrary to the organization's strategic objectives.
- The CAE appraises how her organization communicates risk and control information to employees and nonemployees. Internal reports, newsletters, memos and emails, staff meeting minutes, surveys, interviews, and audit assurance and consulting engagements all can be used to appraise the effectiveness of communicating risk and control information to all parties.
- The CAE assesses his organization's ability to coordinate governance activities and communicate governance information among various parties such as internal auditors, external auditors, audit committee, risk committee, and governance committee.
- The CAE can provide consulting services, as a preferred approach, when governance issues are known or the governance process is immature because consulting services provide recommendations for improvement of governance processes.
- The CAE can assign senior-level internal auditors to attend and observe meetings of governance-related bodies and advise them on an ongoing basis. This assignment is an example of continuous monitoring methods for the internal audit activity.
- The CAE understands that a review of his organization's governance processes must be based on a broad focus with a comprehensive scope due to its pervasive nature, not a narrow focus with a limited scope.
- The broad focus takes into account: (1) previous internal audit reports; (2) results of management assessments (e.g., compliance inspections, quality audits, and control self-assessments); (3) results of external assurance providers (e.g., legal investigators, government auditor general offices, called the Office of the Inspector General), public accounting firms, and reports from regulators; (4) results from the work of internal assurance providers or

second-line-of-defense functions, such as health and safety, compliance, and quality; and (5) adverse incidents, such as natural disasters, manmade disasters, website hacking, data breaches, and computer glitches and crashes.

Considerations for demonstrating conformance require the following output documents:

- Internal audit charter describing the internal audit activity's roles and responsibilities related to the GRC processes
- Internal audit plans showing the audit schedules in performing the GRC processes
- Board meeting minutes discussing the GRC processes among the CAE, board, and senior management
- Audit engagement plans and reports showing a risk-based approach to audit the GRC processes

Requiring a familiarity with the related Standards includes:

- Governance (*Standard* 2110)
- Risk management (*Standard* 2120)
- Control (*Standard* 2130)

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.

2110—Implementation Guide

Establishing a scope for implementation work requires the following:

- The CAE must understand the definition of **governance** as the combination of processes and structures implemented by the board of directors to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.
- The CAE becomes familiar with the globally accepted governance frameworks and models (e.g., COSO, U.S. Business Roundtable, National Association of Corporate Directors

[NACD], and global governance models). The CAE understands that the effectiveness of these frameworks and models depends on the size, complexity, life cycle, maturity level, stakeholder structure, and legal and regulatory requirements in which the organization operates.

Larger organizations are found to have stronger governance mechanisms.

Smaller organizations are found to have weaker governance mechanisms.

- The CAE understands that GRC processes are highly interrelated:

  Effective governance activities consider risk.

  Risk management relies on effective governance.

  Effective governance relies on internal controls.

  Effective governance requires tone at the top, voice of the top, risk culture, risk appetite, risk tolerance, risk maturity, risk sensitivity, oversight of risk management, and organization's culture.

- The CAE recognizes that the two most important items in a board's risk management activities are risk appetite and risk tolerance.
- The CAE reviews the board's charter, audit committee's charter, and the board meeting agendas and minutes to understand the role of the board in establishing strategic and operational decision-making framework. Note that the board members are not guarantors of governance activity; instead, they are overseers, custodians, loyalists, stewards, protectors, fiduciaries, caretakers, shepherds, gatekeepers, defenders, and guardians.
- The CAE reviews and evaluates the amount and frequency of compensation and remuneration paid to board members using the "contract for services" document. The CAE determines if these compensations and remunerations are reasonable and comparable in the industry. The effectiveness of a board's function is directly related to members' compensation and remuneration amounts, meaning lower or no compensation and remuneration amounts can lead to ineffective boards. The same logic applies to a board's incentive programs, which include bonuses, stock options, termination and retirement packages, and perks.
- The CAE interviews with the C-level executives to gain a detailed understanding of specific governance processes and activities. These executives include chief governance officer, chief compliance officer, chief ethics officer, chief risk officer, and chief people officer (human resources). Consulting with the organization's independent external auditor is a good practice in this area.
- The CAE understands the key requirements of good governance include two parties, such as the board and the CEO. Both parties must be good for good governance to exist. The following relationships can apply based on specific conditions.

Good Board + Good CEO = Good Governance
Bad Board + Good CEO = Bad Governance
Good Board + Bad CEO = Bad Governance
Bad Board + Bad CEO = Worse Governance

Considerations for implementation need:

- The CAE identifies the organization's higher-risk governance processes, which are addressed through assurance and consulting engagements described in the final audit plan.

- The CAE is responsible for assessing and making recommendations to improve the organization's overall governance processes.
- The CAE reviews past audit reports and board meeting minutes and interviews the department-level heads, such as functional managers and senior managers, to find out what governance processes led to strategic and operational decisions.
- The CAE learns how the organization conducts its annual risk assessment exercise and how it provides oversight of its risk management processes and control activities. In this regard, the CAE can interview key risk management personnel in the C-level executive suite, such as chief compliance officer, chief risk officer, and CFO.

Considerations for demonstrating conformance require the following output documents:

- Board meeting minutes and materials showing that the board is actively monitoring the performance, compensation, and incentive packages offered to senior-level executives
- Signed ethics statements from senior-level executives and business partners to show their commitment to maintaining business ethics and values and to eliminating conflict-of-interest situations
- Internal audit reports issued related to governance from assurance-based engagements and consulting-based recommendations to improve the governance processes

Requiring a familiarity with the related Standards includes:

- Nature of work (*Standard* 2100)
- Risk management (*Standard* 2120)
- Control (*Standard* 2130)
- Governance frameworks and models (e.g., COSO, U.S. Business Roundtable, NACD, and global governance models)

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.

2120 Implementation Guide

Establishing a scope for implementation work requires:

- The CAE and staff must understand the definitions of risk management, risk, risk culture, risk attitude, risk appetite, risk tolerance, risk sensitivity, risk maturity, and risk immunity.
- The following highlights the relationships among risk attitude, risk appetite, risk tolerance, and risk sensitivity.

  Risk Taker = High-Risk Appetite = High Tolerance to Risk = Risk Insensitive
  Risk Averter = Low-Risk Appetite = High Intolerance to Risk = Risk Sensitive

- There is a built-in conflict when the internal auditor who is making audit recommendations is a risk taker and the audit client who is receiving these audit recommendations is a risk averter. Under these conditions, the audit client's acceptance of recommendations will be low (i.e., low risk appetite).
- The CAE and staff must understand the various types of risks the organization can face, including strategic, financial, operational, pure, hazard, speculative, legal, regulatory, and reputation risks.
- Internal auditors, supervisors, and managers need to know how their organization's management identifies, assesses, and provides oversight for risks before they evaluate the management's risk assessment processes.
- Internal auditors' assessment of risk considers their organization's size, complexity, life cycle, maturity, stakeholder structure, and legal and competitive environment, including new risks resulting from recent changes in the organization's environment. Examples of these changes include new laws and regulations, new management staff, new organization

structure, new processes (manual and automated), new computer systems, new markets and products, and new business entities through mergers and acquisitions.

- Total risks facing an organization are the summation of risks assessed by the organization's management and risks assessed by the internal auditors.

  Total Risks = Management-Assessed Risks + Auditor-Assessed Risks

  Management assesses risks first.

  Auditors assess risks next.

  The CAE integrates both management-assessed risks and auditor-assessed risks.

- Internal auditors must understand the relationships among risks, returns, and controls as follows:

  Risks and returns move in the same direction, meaning that higher risks yield higher returns and lower risks give lower returns.

  Risks and controls move in the same direction, meaning that higher risks need higher levels of controls and lower risks require lower levels of controls.

- Internal auditors evaluate risk management processes during assurance and consulting reviews related to a specific business area, function, system, or process. They identify significant risks arising from major threats or vulnerabilities. Both the board and senior management should treat vulnerabilities as a test of their leadership; a challenge to their traditions, customs, beliefs, and values; an opportunity for their company's growth, progress, and success; and a strategic move to beat their competitors.

- The CAE reviews and evaluates the senior management's incentive programs in place and their relation to risk management activities that management undertakes. Incentive programs can take several forms, such as promotions, bonuses, stock options, perks, and termination and retirement packages.

  There should be a match between a company management's risk-taking approaches, a company's stated risk appetite levels, and a company's incentive programs established for the management. In addition, there should be a match between a company's risk policy and risk appetite; otherwise, a risk policy gap can occur. This is because strong incentives encourage excessive risk taking at the expense of company's risk policy and its stakeholders, which is not good. Incentives need to be risk adjusted or risk corrected when the actual outcomes are less than the planned or expected outcomes.

  Risk Policy = Risk Appetite

  Aggressive risk appetite implies aggressive risk policy.

  Risk Policy Gap = Risk Policy – Risk Appetite

- The CAE should ascertain whether the CRO or equivalent is computing value-at-risk (VAR). VAR is an estimate of the maximum amount of loss that can occur in a given time period (e.g., one year) and at a given confidence level (e.g., 95%). Risk appetite is directly related to the VAR amount, meaning that the higher the risk appetite, the larger the amount of VAR, implying more value is at risk. The VAR amount can be computed using the Monte Carlo simulation method.

- The CAE and staff recognizes and promotes that a company management with high regard for compliance with laws, rules, and regulations will have a high, positive reputation in the business community and society.

- Senior managers and functional managers must carefully consider the appropriate balance between controls and risks in their functions, programs, and operations. To emphasize, too many controls can result in an inefficient and ineffective organization; managers must ensure an appropriate balance between the strength of controls and the relative risk associated with particular functions, programs, and operations**. The benefits of controls should outweigh the costs of controls.** Managers should consider both qualitative and quantitative factors when analyzing costs against benefits.

Considerations for implementation include:

- Risk assessment is of two types: one done by the management of the organization (management's risk assessment) and the other one done by the internal audit activity of the same organization (auditor's risk assessment). Any gaps between the management's risk assessment and the auditor's risk assessment should be identified and reported to the board and senior management. A **fit-gap analysis** indicates what fits and what does not fit (gap).

  Risk Fit-Gap Analyses = Management's Risk Assessment – Auditor's Risk Assessment

  - The CAE and staff can use an established risk management framework, such as COSO-ERM or the ISO 31000 Standard, to assist them in risk identification and risk reduction.
  - The CAE understands management's risk environment, such as risk appetite, risk tolerance, and risk culture (risk profiles), through conversations with the board and senior management.
  - The CAE evaluates management's risk responses after alerting managers to new emerging risks due to changes and old risks that were not adequately mitigated (not remedied or not fixed). Examples of these risk responses include accept, pursue, transfer, mitigate, avoid, reject, or reduce.
  - A risk exists when management has accepted a level of risk that may be unacceptable to the organization. The CAE should discuss this matter with senior management first and with the board next only after senior management fails to offer a risk mitigation strategy. When senior management offers a risk mitigation plan, the internal audit activity can evaluate the adequacy and timeliness of remedial actions (establishing controls) taken through reviews of control designs, testing of controls, and monitoring of control procedures.

    A risk exists when controls do not mitigate or do not limit that risk.

    A risk does not exist when controls mitigate or limit that risk.

- An organization's management faces its own risks, such as failed business strategies; poor execution of strategic plans; unethical incentive programs at the expense of customers, suppliers, and employees' goodwill; questionable business practices; underestimating or miscalculating competitors' moves and actions; and ignoring compliance with government's laws, rules, and regulations.
- Just as an organization's management faces its own risks, internal auditors face their own risks arising from the nature of the audit work performed (audit-related risks). Examples of audit-related risks include audit failure risk, false assurance risks, and reputation risks. The CAE should ensure that corrective actions are taken for audit-related risks.

Considerations for demonstrating conformance include the following output documents:

- Internal audit charter documenting the auditor's roles and responsibilities related to risk management

- Internal audit plan showing the risk management audit schedules with timelines and staff resources assigned
- Board meeting minutes discussing risk management audit's conclusions and recommendations with the board and senior management
- Audit committee meeting notes discussing risk management audit's conclusions and recommendations with members of the audit committee
- A report showing fit-gap analysis of risk management
- Meeting notes from discussions with special task forces (e.g., employee wages and benefits) and special committees (e.g., finance committee)

Requiring a familiarity with the related Standards includes:

- Nature of work (*Standard* 2100)
- Governance (*Standard* 2110)
- Control (*Standard* 2130)
- Communicating the acceptance of risks (*Standard* 2600)
- Risk management frameworks such as COSO-ERM and ISO 31000

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

2130.C1—Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

2130—Implementation Guide

- The CAE and staff must understand the definitions of control**,** control concepts, control processes, and control environment.
- **Control** is any positive or negative 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 accomplished.
- Several **control concepts** exist, including controls by motivation dimension, controls by action dimension, controls by time dimension, and controls by function dimension.

Controls by motivation dimension include positive controls and negative controls. Positive controls will increase the motivation levels of employees, making them more sincere, honest, efficient (productive), and effective (achieving goals) in their work. Examples of positive controls include bonuses, incentives, promotions, praises, recognition, and wage increases. Negative controls will decrease the motivation levels of employees, making them less sincere, honest, efficient (productive), and effective (achieving goals) in their work. Examples of negative controls include punishments, demotions, disciplinary actions, threats, criticism, and wage decreases.

Controls by action dimension include feedforward controls, concurrent controls, and feedback controls. A feedforward control is a proactive control based on strategies, budgets, and plans. Examples include error prevention, inspection of incoming materials and products, employee training and development, operating budget, and capital budget. A concurrent control is a current control that is repeated daily and ongoing. Examples include supervision, monitoring, on-the-job training, employee or machine work scheduling, and completing assigned work activities and tasks. A feedback control is a reactive control used to evaluate past activity to improve future performance. It measures actual performance against a standard to ensure that a defined result is achieved. Examples include surveys from customers, employees, and suppliers and variance analysis from budgets.

Controls by time dimension include pre-controls (proactive controls), current controls (ongoing controls), and post-controls (reactive controls).

Controls by function dimension include preventive controls, detective controls, and corrective controls. Preventive controls are actions taken to deter undesirable events, such as errors, irregularities, and fraud, from occurring. Examples include policies, procedures, directives, standards, circulars, regulations, guidelines, and segregation of duties. Detective controls are actions taken to detect undesirable events that have occurred. The installation of detective controls is necessary to provide feedback on the effectiveness of preventive controls. Examples include reviews, comparisons, bank reconciliations, receivable and payable reconciliations, and physical counts. Corrective controls are actions taken to correct undesirable events that have occurred. They fix both detected and reported errors. Examples include correction procedures, documentation, control reports, and exception reports.

The following is a relationship among controls by action dimension, controls by time dimension, and controls by function dimension.

Feedforward Controls ⟶ Proactive Controls ⟶ Pre-Controls ⟶ Preventive Controls

Concurrent Controls ⟶ Ongoing Controls ⟶ Current Controls ⟶ Detective Controls

Feedback Controls ⟶ Reactive Controls ⟶ Post-Controls ⟶ Corrective Controls

- **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.
- The **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 six essential elements:

  1. Integrity and ethical values
  2. Management's philosophy and operating style

3. Organizational culture
4. Assignment of authority and responsibility
5. Human resource policies and practices
6. Competence of personnel such as auditors and nonauditors

The control environment is enhanced when a tone at the top or voice of the top promotes a high culture of ethical behavior and a low tolerance for noncompliance with laws, rules, and regulations.

Proper Control Environment = High Culture of Ethical Behavior
+ Low Tolerance for Noncompliance with Laws, Rules, and Regulations

An organization's control environment consists of developing and implementing business controls, which can be classified as hard controls and soft controls.

- *Hard controls* are formal, tangible, objective, and much easier to measure and evaluate than the soft controls. Examples of hard controls include budgets, dual controls, written approvals, reconciliations, authorization levels, verifications, and segregation of duties. Soft controls are informal, intangible, subjective, and difficult to measure and evaluate. Tools to evaluate hard controls include flowcharts, system narratives, testing, and counting. Higher-level managers and executives need more depth in soft skills and soft controls and less depth in hard skills and hard controls. Lower-level managers and executives need more depth in hard skills and hard controls and less depth in soft skills and soft controls.
- *Soft controls* are informal, intangible, subjective, and much harder to measure and evaluate than the hard controls. Examples of soft controls include an organization's ethical climate, integrity, values, culture, vision, people's behaviors and attitudes, commitment to competence, tone at the top, management philosophy, management's operating style, level of understanding and commitment, and communication. Tools to evaluate soft controls include self-assessments, questionnaires, interviews, workshops, and role playing. Higher-level managers and executives need more depth in soft skills and soft controls and less depth in hard skills and hard controls. Lower-level managers and executives need more depth in hard skills and hard controls and less depth in soft skills and soft controls.

Establishing a scope for implementation work includes:

- The CAE and staff must understand the critical risks that could inhibit the organization's ability to achieve its objectives and the controls that have been implemented to mitigate such risks to an acceptable level. The following is a relationship between risks and controls.

  Business strategies, plans, and policies are designed into controls.

  Business controls are built into daily procedures and practices.

  Business events and transactions create risks.

  Controls mitigate risks to an acceptable level of risk tolerance.

- The CAE and staff must be familiar with globally recognized, comprehensive control frameworks such as *Internal Control–Integrated Framework*, issued by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

- A management control policy can state that: (1) senior management oversees the establishment, administration, and assessment of the organization's control system; (2) functional management is responsible for the design and assessment of controls within their operating areas; and (3) the internal audit management is responsible for evaluating the effectiveness of the control processes in place at a point in time.
- The CAE and staff must understand the five relationships between controls and risks:
  1. Standards, regardless of their source, and regulatory guidelines are developed based on best practices, which eventually become "controls" for auditors.
  2. Controls can manage current risks only and cannot predict future risks.
  3. Controls cannot always provide reasonable assurance that risks are being managed effectively due to built-in control weaknesses, control overrides, and control breakdowns.
  4. Controls must address root causes of problems and risks, not just symptoms.
  5. Internal auditors should focus on significant risks and provide reasonable assurance on the management of such risks using the Pareto principle and the rule of 80/20.

Considerations for implementation require:

- Controls are designed to mitigate risks at three levels of an organization: at the entity level (e.g., a retail company level), at an activity level (e.g., customer order processing at the retailer), and at the transaction level (e.g., a customer buying and paying for goods and services from a retailer).
- Internal auditors must assess the effectiveness of controls by using a **risk and control matrix**, which shows how controls are used to manage risks and whether controls are effective or ineffective. Prior to developing this matrix, auditors gather information through interviews of management; review of organizational plans, policies, and processes; and use of walk-throughs, surveys, internal control questionnaires, checklists, narratives, and flowcharts. After gathering such information, auditors evaluate the adequacy of control design and test the effectiveness of controls using inspections, confirmations, continuous auditing, data analytics (e.g., ratio analysis and trend analysis), and audit metrics.
- Internal auditors must evaluate the efficiency of controls through a **cost-benefit analysis**, meaning costs should not exceed benefits.
- Internal auditors must assess whether the level of a control is appropriate for the risk it mitigates. A **risk and control map** can help auditors to document the relationship between risks and controls. Possible outcomes from the risk and control mapping follow:

  Some high risks are undercontrolled (open to fraud, threats, and vulnerabilities).

  Some low risks are overcontrolled (waste of resources, delays in operations).

  Some risks are not controlled at all (open to fraud, threats, and exposures).

  Some controls are not needed (waste of resources, delays in operations).

  Some controls do not address any risks (waste of resources, open to threats).

  Some weak controls are overdesigned (waste of resources, delays in operations).

  Some strong controls are underdesigned (open to fraud, threats, and vulnerabilities).

  Some simple controls are overcomplicated (waste of resources, delays in operations).

Some complex controls are oversimplified (open to fraud, threats, and vulnerabilities).

Some controls and risks have no relationship (mismatch of design and function).

- The CAE promotes a **continuous improvement program** in maintaining effective controls with control evaluations using a control framework for uniformity and consistency. He may recommend the implementation of a control framework if one is not already in place. Specific actions include (1) training nonauditors in controls, control concepts, control processes, and a positive control environment; (2) encouraging nonauditors to self-monitor controls; (3) facilitating control and risk assessment sessions; and (4) educating management and nonauditors in the purposes and consequences of control efficiency, control effectiveness, control deficiencies, control breakdowns, control overrides, and control requirements.

Considerations for demonstrating conformance require the following output documents:

- Risk and control matrices
- Risk and control maps
- Narrative descriptions of walk-throughs
- Results of surveys, interviews, and meetings with management and nonmanagement
- Standard operating manual showing continuous improvements of controls
- Internal audit plans, work programs, workpapers, reports showing control evaluations, control testing, and control assessment exercises

Requiring a familiarity with the related Standards includes:

- Nature of work (*Standard* 2100)
- Governance (*Standard* 2110)
- Risk management (*Standard* 2120)
- Control framework
- COSO—Internal Control
- SOX 2002
- Cadbury Report