DOMAIN 1

Mandatory Guidance (35–45%)

1.1 Definition of Internal Auditing

The globally accepted definition of internal auditing states the fundamental purpose, nature, and scope of internal auditing:

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

1.2 International Standards

Internal auditing is conducted in diverse legal and cultural environments; within organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. While differences may affect the practice of internal auditing in each environment, conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* (*Standards*) is essential in meeting the responsibilities of internal auditors and the internal audit activity.

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 standards issued by other authoritative bodies, internal audit communications may also cite the use of other standards, as appropriate. In such a case, if inconsistencies exist between the *Standards* and other standards, internal auditors and the internal audit activity must conform with the *Standards* and may conform with the other standards if they are more restrictive.

The purpose of the *Standards* is to:

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

The *Standards* are principles-focused, mandatory requirements consisting of:

- Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance that are internationally applicable at organizational and individual levels.
- Interpretations that clarify terms or concepts within the Statements.

The *Standards* employ terms that have been given specific meanings that are included in the Glossary. Specifically, the *Standards* use the word "must" to specify an unconditional requirement and the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

It is necessary to consider the Statements and their Interpretations as well as the specific meanings from the Glossary to understand and apply the *Standards* correctly.

The structure of the *Standards* is divided between Attribute and Performance *Standards*. **Attribute *Standards*** address the attributes of organizations and individuals performing internal auditing (numbered from 1000 to 1322). **Performance *Standards*** describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured (numbered from 2000 to 2600). The Attribute and Performance *Standards* are also provided to apply to all internal audit services.

Implementation *Standards* are also provided to expand on the Attribute and Performance *Standards*, by providing the requirements applicable to assurance (A) or consulting (C) activities.

Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusions regarding an entity, operation, function, process, system, or other subject matter. The nature and scope of the assurance engagement are determined by the internal auditor. Generally there are three parties involved in assurance services: (1) the person or group directly involved with the entity, operation, function, process, system, or other subject matter—the process owner; (2) the person or group making the assessment—the internal auditor; and (3) the person or group using the assessment—the user.

Consulting services are advisory in nature and generally are performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Consulting services generally involve two parties: (1) the person or group offering the advice—the internal auditor; and (2) the person or group seeking and receiving the advice—the engagement client. When performing consulting services, the internal auditor should maintain objectivity and not assume management responsibility.

(a) Attribute Standards (1000 to 1322)

1000—Purpose, Authority, and Responsibility

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the definition of Internal auditing, the Code of Ethics, and the *Standards*. The chief audit executive (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.

Practice Advisory 1000-1: Internal Audit Charter

1. Providing a formal, written internal audit charter is critical in managing the internal audit activity. The internal audit charter provides a recognized statement for review and acceptance by management and for approval, as documented in the minutes, by the board. It also facilitates a periodic assessment of the adequacy of the internal audit activity's purpose, authority, and responsibility, which establishes the role of the internal audit activity. If a question should arise, the internal audit charter provides a formal, written agreement with management and the board about the organization's internal audit activity.

2. The CAE is responsible for periodically assessing whether the internal audit activity's purpose, authority, and responsibility, as defined in the internal audit charter, continue to be adequate to enable the activity to accomplish its objectives. The CAE is also responsible for communicating the result of this assessment to senior management and the board.

1010–Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter

The mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* must be recognized in the internal audit charter. The CAE should discuss the definition of internal auditing, the Code of Ethics, and the *Standards* with senior management and the board.

No Practice Advisory for Standard 1010

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 CAE 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.

No Practice Advisory for Standard 1100

1110–Organizational Independence

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

1110.A1–The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

Practice Advisory 1110-1: Organizational Independence

1. Support from senior management and the board assists the internal audit activity in gaining the cooperation of engagement clients and performing their work free from interference.

2. The CAE, reporting functionally to the board and administratively to the organization's chief executive officer (CEO), facilitates organizational independence. At a minimum, the CAE needs to report to an individual in the organization with sufficient authority to promote independence and to ensure broad audit coverage, adequate consideration of engagement communications, and appropriate action on engagement recommendations.

3. Functional reporting to the board typically involves the board:

- ☐ Approving the internal audit activity's overall charter.
- ☐ Approving the internal audit risk assessment and related audit plan.
- ☐ Receiving communications from the CAE on the results of the internal audit activities or other matters that the CAE determines are necessary, including private meetings with the CAE without management present, as well as annual confirmation of the internal audit activity's organizational independence.

- Approving all decisions regarding the performance evaluation, appointment, or removal of the CAE.
- Approving the annual compensation and salary adjustment of the CAE.
- Making appropriate inquiries of management and the CAE to determine whether there is audit scope or budgetary limitations that impede the ability of the internal audit activity to execute its responsibilities.

4. Administrative reporting is the reporting relationship within the organization's management structure that facilitates the day-to-day operations of the internal audit activity. Administrative reporting typically includes:

- Budgeting and management accounting.
- Human resource administration, including personnel evaluations and compensation.
- Internal communications and information flows.
- Administration of the internal audit activity's policies and procedures.

1111–Direct Interaction with the Board

The CAE must communicate and interact directly with the board.

Practice Advisory 1111-1: Board Interaction

1. Direct communication occurs when the CAE regularly attends and participates in board meetings that relate to the board's oversight responsibilities for auditing, financial reporting, organizational governance, and control. The CAE's attendance and participation at these meetings provide an opportunity to be apprised of strategic business and operational developments and to raise high-level risk, systems, procedures, or control issues at an early stage. Meeting attendance also provides an opportunity to exchange information concerning the internal audit activity's plans and activities and to keep each other informed on any other matters of mutual interest.

2. Such communication and interaction also occurs when the CAE meets privately with the board, at least annually.

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.*

Practice Advisory 1120-1: Individual Objectivity

1. "Individual objectivity" means the internal auditors perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Internal auditors are not to be placed in situations that could impair their ability to make objective professional judgments.

2. Individual objectivity involves the CAE organizing staff assignments that prevent potential and actual conflict of interest and bias, periodically obtaining information from the internal audit staff concerning potential conflict of interest and bias, and, when practicable, rotating internal audit staff assignments periodically.

3. Review of internal audit work results before the related engagement communications are released assists in providing reasonable assurance that the work was performed objectively.

4. The internal auditor's objectivity is not adversely affected when the auditor recommends standards of control for systems or reviews procedures before they are implemented. The auditor's objectivity is considered to be impaired if the auditor designs, installs, drafts procedures for, or operates such systems.

5. The occasional performance of non-audit work by the internal auditor, with full disclosure in the reporting process, would not necessarily impair objectivity. However, it would require careful consideration by management and the internal auditor to avoid adversely affecting the internal auditor's objectivity.

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 on the impairment.

Interpretation: *"Impairment to organizational independence and individual objectivity" may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.*

The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent on 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 he or she 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.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.

Practice Advisory 1130-1: Impairment to Independence or Objectivity

1. Internal auditors are to report to the CAE any situations in which an actual or potential impairment to independence or objectivity may reasonably be inferred or if they have questions about whether a situation constitutes an impairment to objectivity or independence. If the CAE determines that impairment exists or may be inferred, he or she needs to reassign the auditor(s).

2. A scope limitation is a restriction placed on the internal audit activity that precludes the activity from accomplishing its objectives and plans. Among other things, a scope limitation may restrict the:

- Scope defined in the internal audit charter.
- Internal audit activity's access to records, personnel, and physical properties relevant to the performance of engagements.
- Approved engagement work schedule.

- Performance of necessary engagement procedures.
- Approved staffing plan and financial budget.

3. A scope limitation, along with its potential effect, needs to be communicated, preferably in writing, to the board. The CAE needs to consider whether it is appropriate to inform the board regarding scope limitations that were previously communicated to and accepted by the board. This may be necessary particularly when there have been organization, board, senior management, or other changes.

4. Internal auditors are not to accept fees, gifts, or entertainment from an employee, client, customer, supplier, or business associate that may create the appearance that the auditors' objectivity has been impaired. The appearance that objectivity has been impaired may apply to current and future engagements conducted by the auditors. The status of engagements is not to be considered as justification for receiving fees, gifts, or entertainment. The receipt of promotional items (such as pens, calendars, or samples) that are available to employees and the general public and have minimal value do not hinder internal auditors' professional judgments. Internal auditors are to report immediately to their supervisors the offer of all material fees or gifts.

Practice Advisory 1130.A1-1: Assessing Operations for Which Internal Auditors Were Previously Responsible

1. Persons transferred to, or temporarily engaged by, the internal audit activity should not be assigned to audit those activities they previously performed or for which they had management responsibility until at least one year has elapsed. Such assignments are presumed to impair objectivity, and additional consideration should be exercised when supervising the engagement work and communicating engagement results.

Practice Advisory 1130.A2-1: Internal Audit's Responsibility for Other (Non-Audit) Functions

1. Internal auditors are not to accept responsibility for non-audit functions or duties that are subject to periodic internal audit assessments. If they have this responsibility, then they are not functioning as internal auditors.

2. When the internal audit activity, CAE, or individual internal auditor is responsible for, or management is considering assigning, an operational responsibility that the internal audit activity might audit, the internal auditor's independence and objectivity may be impaired. At a minimum, the CAE needs to consider the next factors in assessing the impact on independence and objectivity:

- Requirements of the Code of Ethics and the *Standards*.
- Expectations of stakeholders, who may include the shareholders, board of directors, management, legislative bodies, public entities, regulatory bodies, and public interest groups.
- Allowances and/or restrictions contained in the internal audit charter.
- Disclosures required by the *Standards*.
- Audit coverage of the activities or responsibilities undertaken by the internal auditor.
- Significance of the operational function to the organization (in terms of revenue, expenses, reputation, and influence).
- Length or duration of the assignment and scope of responsibility.
- Adequacy of separation of duties.
- Whether there is any history or other evidence that the internal auditor's objectivity may be at risk.

3. If the internal audit charter contains specific restrictions or limiting language regarding the assignment of non-audit functions to the internal auditor, then disclosure and discussion

with management of such restrictions is necessary. If management insists on such an assignment, then disclosure and discussion of this matter with the board is necessary. If the internal audit charter is silent on this matter, the guidance noted in the points listed below are to be considered. All the points noted below are subordinate to the language of the internal audit charter.

4. When the internal audit activity accepts operational responsibilities and that operation is part of the internal audit plan, the CAE needs to:

- Minimize the impairment to objectivity by using a contracted, third-party entity or external auditors to complete audits of those areas reporting to the CAE.
- Confirm that individuals with operational responsibility for those areas reporting to the CAE do not participate in internal audits of the operation.
- Ensure that internal auditors conducting the assurance engagement of those areas reporting to the CAE are supervised by, and report the results of the assessment, to senior management and the board.
- Disclose the operational responsibilities of the internal auditor for the function, the significance of the operation to the organization (in terms of revenue, expenses, or other pertinent information), and the relationship of those who audited the function.

5. The auditor's operational responsibilities need to be disclosed in the related audit report of those areas reporting to the CAE and in the internal auditor's standard communication to the board. Results of the internal audit may also be discussed with management and/or other appropriate stakeholders. Impairment disclosure does not negate the requirement that assurance engagements for functions over which the CAE has responsibility need to be overseen by a party outside the internal audit activity.

1200–Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

Practice Advisory 1200-1: Proficiency and Due Professional Care

1. Proficiency and due professional care are the responsibility of the CAE and each internal auditor. As such, the CAE ensures that persons assigned to each engagement collectively possess the necessary knowledge, skills, and other competencies to conduct the engagement appropriately.

2. Due professional care includes conforming with the Code of Ethics and, as appropriate, the organization's code of conduct as well as the codes of conduct for other professional designations the internal auditors may hold. The Code of Ethics extends beyond the definition of internal auditing to include two essential components:

- Principles that are relevant to the profession and practice of internal auditing: integrity, objectivity, confidentiality, and competency.
- Rules of conduct that describe behavioral norms expected of internal auditors. These rules are an aid to interpreting the principles into practical applications and are intended to guide the ethical conduct of internal auditors.

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: "*Knowledge, skills, and other competencies***" *is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor (CIA) designation and other designations offered by The Institute of Internal Auditors (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 (IT) 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.

Practice Advisory 1210-1: Proficiency

1. The knowledge, skills, and other competencies referred to in the standard include:
   - Proficiency in applying internal audit standards, procedures, and techniques in performing engagements. "Proficiency" means the ability to apply knowledge to situations likely to be encountered and to deal with them appropriately without extensive recourse to technical research and assistance.
   - Proficiency in accounting principles and techniques if internal auditors work extensively with financial records and reports.
   - Knowledge to identify the indicators of fraud.
   - Knowledge of key IT risks and controls and available technology-based audit techniques.
   - An understanding of management principles to recognize and evaluate the materiality and significance of deviations from good business practices. "An understanding" means the ability to apply broad knowledge to situations likely to be encountered, to recognize significant deviations, and to be able to carry out the research necessary to arrive at reasonable solutions.
   - An appreciation of the fundamentals of business subjects such as accounting, economics, commercial law, taxation, finance, quantitative methods, IT, risk management, and fraud. "An appreciation" means the ability to recognize the existence of problems or potential problems and to identify the additional research to be undertaken or the assistance to be obtained.
   - Skills in dealing with people, understanding human relations, and maintaining satisfactory relationships with engagement clients.
   - Skills in oral and written communications to clearly and effectively convey such matters as engagement objectives, evaluations, conclusions, and recommendations.

2. Suitable criteria of education and experience for filling internal audit positions is established by the CAE, who gives due consideration to the scope of work and level of responsibility and obtains reasonable assurance as to each prospective auditor's qualifications and proficiency.

3. The internal audit activity needs to collectively possess the knowledge, skills, and other competencies essential to the practice of the profession within the organization. Performing an annual analysis of an internal audit activity's knowledge, skills, and other competencies helps identify areas of opportunity that can be addressed by continuing professional development, recruiting, or co-sourcing.

4. Continuing professional development is essential to help ensure internal audit staff remains proficient.

5. The CAE may obtain assistance from experts outside the internal audit activity to support or complement areas where the internal audit activity is not sufficiently proficient.

Practice Advisory 1210.A1-1: Obtaining External Service Providers to Support or Complement the Internal Audit Activity

1. Each member of the internal audit activity need not be qualified in all disciplines. The internal audit activity may use external service providers or internal resources that are qualified in disciplines such as accounting, auditing, economics, finance, statistics, IT, engineering, taxation, law, environmental affairs, and other areas as needed to meet the internal audit activity's responsibilities.

2. An external service provider is a person or firm, independent of the organization, who has special knowledge, skill, and experience in a particular discipline. External service providers include actuaries, accountants, appraisers, culture or language experts, environmental specialists, fraud investigators, lawyers, engineers, geologists, security specialists, statisticians, IT specialists, the organization's external auditors, and other audit organizations. An external service provider may be engaged by the board, senior management, or the CAE.

3. External service providers may be used by the internal audit activity in connection with, among other things:

- Achievement of the objectives in the engagement work schedule.
- Audit activities where a specialized skill and knowledge are needed, such as IT, statistics, taxes, or language translations.
- Valuations of assets, such as land and buildings, works of art, precious gems, investments, and complex financial instruments.
- Determination of quantities or physical condition of certain assets, such as mineral and petroleum reserves.
- Measuring the work completed and to be completed on contracts in progress.
- Fraud and security investigations.
- Determination of amounts by using specialized methods, such as actuarial determinations of employee benefit obligations.
- Interpretation of legal, technical, and regulatory requirements.
- Evaluation of the internal audit activity's quality assurance and improvement program in conformance with the *Standards*.
- Mergers and acquisitions.
- Consulting on risk management and other matters.

4. When the CAE intends to use and rely on the work of an external service provider, the CAE needs to consider the competence, independence, and objectivity of the external service provider as it relates to the particular assignment to be performed. The assessment of competency, independence, and objectivity is also needed when the external service provider is selected by senior management or the board, and the CAE intends to use and rely on the external service provider's work. When the selection is made by others and the CAE's assessment indicates that he or she should not use and rely on the work of the external service provider, communication of such results is needed to senior management or the board, as appropriate.

5. The CAE determines that the external service provider possesses the necessary knowledge, skills, and other competencies to perform the engagement by considering:

- Professional certification, license, or other recognition of the external service provider's competence in the relevant discipline.
- Membership of the external service provider in an appropriate professional organization and adherence to that organization's code of ethics.
- The reputation of the external service provider. This may include contacting others familiar with the external service provider's work.
- The external service provider's experience in the type of work being considered.
- The extent of education and training received by the external service provider in disciplines that pertain to the particular engagement.
- The external service provider's knowledge and experience in the industry in which the organization operates.

6. The CAE needs to assess the relationship of the external service provider to the organization and to the internal audit activity to ensure that independence and objectivity are maintained throughout the engagement. In performing the assessment, the CAE verifies that there are no financial, organizational, or personal relationships that will prevent the external service provider from rendering impartial and unbiased judgments and opinions when performing or reporting on the engagement.

7. The CAE assesses the independence and objectivity of the external service provider by considering:

- The financial interest the external service provider may have in the organization.
- The personal or professional affiliation the external service provider may have to the board, senior management, or others within the organization.
- The relationship the external service provider may have had with the organization or the activities being reviewed.
- The extent of other ongoing services the external service provider may be performing for the organization.
- Compensation or other incentives that the external service provider may have.

8. If the external service provider is also the organization's external auditor and the nature of the engagement is extended audit services, the CAE needs to ascertain that work performed does not impair the external auditor's independence. "Extended audit services" refer to those services beyond the requirements of audit standards generally accepted by external auditors. If the organization's external auditors act or appear to act as members of senior management, management, or as employees of the organization, then their independence is impaired. Additionally, external auditors may provide the organization with other services, such as tax and

consulting. Independence needs to be assessed in relation to the full range of services provided to the organization.

9. To ascertain that the scope of work is adequate for the purposes of the internal audit activity, the CAE obtains sufficient information regarding the scope of the external service provider's work. It may be prudent to document these and other matters in an engagement letter or contract. To accomplish this, the CAE reviews the next items with the external service provider:

- Objectives and scope of work including deliverables and time frames.
- Specific matters expected to be covered in the engagement communications.
- Access to relevant records, personnel, and physical properties.
- Information regarding assumptions and procedures to be employed.
- Ownership and custody of engagement working papers, if applicable.
- Confidentiality and restrictions on information obtained during the engagement.
- Where applicable, conformance with the *Standards* and the internal audit activity's standards for working practices.

10. In reviewing the work of an external service provider, the CAE evaluates the adequacy of work performed, which includes sufficiency of information obtained to afford a reasonable basis for the conclusions reached and the resolution of exceptions or other unusual matters.

11. When the CAE issues engagement communications and an external service provider was used, the CAE may, as appropriate, refer to such services provided. The external service provider needs to be informed, and, if appropriate, concurrence should be obtained before making such reference in engagement communications.

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.

Practice Advisory 1220-1: Due Professional Care

1. Due professional care calls for the application of the care and skill expected of a reasonably prudent and competent internal auditor in the same or similar circumstances. Due professional care is therefore appropriate to the complexities of the engagement being performed. Exercising due professional care involves internal auditors being alert to the possibility of fraud, intentional wrongdoing, errors and omissions, inefficiency, waste, ineffectiveness, and conflicts of interest as well as being alert to those conditions and activities where irregularities are most likely to occur. This also involves internal auditors identifying inadequate controls and recommending improvements to promote conformance with acceptable procedures and practices.

2. Due professional care implies reasonable care and competence, not infallibility or extraordinary performance. As such, due professional care requires the internal auditor to conduct examinations and verifications to a reasonable extent. Accordingly, internal auditors cannot give absolute assurance that noncompliance or irregularities do not exist. Nevertheless, the possibility of material irregularities or noncompliance needs to be considered whenever an internal auditor undertakes an internal audit assignment.

1220.A1–Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.

- Adequacy and effectiveness of governance, risk management, and control processes.
- Probability of significant errors, fraud, or noncompliance.
- Cost of assurance in relation to potential benefits.

1220.A2–In exercising due professional care, internal auditors must consider the use of technology-based audit and other data analysis techniques**.**

1220.A3–Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

1220.C1–Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results.
- Relative complexity and extent of work needed to achieve the engagement's objectives.
- Cost of the consulting engagement in relation to potential benefits.

1230–Continuing Professional Development

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

Practice Advisory 1230-1: Continuing Professional Development

1. Internal auditors are responsible for continuing their education to enhance and maintain their proficiency. Internal auditors need to stay informed about improvements and current developments in internal audit standards, procedures, and techniques, including the IIA's *International Professional Practices Framework* guidance. Continuing professional education (CPE) may be obtained through membership, participation, and volunteering in professional organizations, such as the IIA; attendance at conferences, seminars, and in-house training programs; completion of college and self-study courses; and involvement in research projects.

2. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certification, such as the Certified Internal Auditor (CIA) designation, other designations offered by the IIA, and additional designations related to internal auditing.

3. Internal auditors are encouraged to pursue CPE (related to their organization's activities and industry) to maintain their proficiency with regard to the governance, risk, and control processes of their unique organization.

4. Internal auditors who perform specialized audit and consulting work—such as IT, tax, actuarial, or systems design—may undertake specialized CPE to allow them to perform their internal audit work with proficiency.

5. Internal auditors with professional certifications are responsible for obtaining sufficient CPE to satisfy requirements related to the professional certification held.

6. Internal auditors not currently holding appropriate certifications are encouraged to pursue an educational program and/or individual study to obtain professional certification.

1300–Quality Assurance and Improvement Program

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

Interpretation: *A QAIP is designed to enable an evaluation of the internal audit activity's conformance with the definition of internal auditing and 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.*

Practice Advisory 1300-1: Quality Assurance and Improvement Program

1. The CAE is responsible for establishing an internal audit activity whose scope of work includes the activities in the *Standards* and in the definition of internal auditing. To ensure that this occurs, Standard 1300 requires that the CAE develop and maintain a QAIP.

2. The CAE is accountable for implementing processes designed to provide reasonable assurance to the various stakeholders that the internal audit activity:

- Performs in accordance with the internal audit charter, which is consistent with the definition of internal auditing, the Code of Ethics, and the *Standards*.
- Operates in an effective and efficient manner.
- Is perceived by those stakeholders as adding value and improving the organization's operations.

These processes include appropriate supervision, periodic internal assessments and ongoing monitoring of quality assurance, and periodic external assessments.

3. The QAIP needs to be sufficiently comprehensive to encompass all aspects of operation and management of an internal audit activity, as found in the definition of internal auditing, the Code of Ethics, the *Standards*, and best practices of the profession. The QAIP process is performed by or under direct supervision of the CAE. Except in small internal audit activities, the CAE would usually delegate most QAIP responsibilities to subordinates. In large or complex environments (e.g., numerous business units and/or locations), the CAE establishes a formal QAIP function—headed by an internal audit executive—independent of the audit and consulting segments of the internal audit activity. This executive (and limited staff) administers and monitors the activities needed for a successful QAIP.

1310–Requirements of the Quality Assurance and Improvement Program

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

Practice Advisory 1310-1: Requirements of the Quality Assurance and Improvement Program

1. A QAIP is an ongoing and periodic assessment of the entire spectrum of audit and consulting work performed by the internal audit activity. These ongoing and periodic assessments are composed of rigorous, comprehensive processes; continuous supervision and testing of internal audit and consulting work; and periodic validations of conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*. This also includes ongoing measurements and analyses of performance metrics (e.g., internal audit plan accomplishment, cycle time, recommendations accepted, and customer satisfaction). If the assessments' results indicate areas for improvement by the internal audit activity, the CAE will implement the improvements through the QAIP.

2. Assessments evaluate and conclude on the quality of the internal audit activity and lead to recommendations for appropriate improvements. QAIPs include an evaluation of:

- Conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*, including timely corrective actions to remedy any significant instances of nonconformance.

- Adequacy of the internal audit activity's charter, goals, objectives, policies, and procedures.
- Contribution to the organization's governance, risk management, and control processes.
- Compliance with applicable laws, regulations, and government or industry standards.
- Effectiveness of continuous improvement activities and adoption of best practices.
- The extent to which the internal audit activity adds value and improves the organization's operations.

3. The QAIP efforts also include follow-up on recommendations involving appropriate and timely modification of resources, technology, processes, and procedures.

4. To provide accountability and transparency, the CAE communicates the results of external and, as appropriate, internal quality program assessments to the various stakeholders of the activity (such as senior management, the board, and external auditors). At least annually, the CAE reports to senior management and the board on the quality program efforts and results.

1311–Internal Assessments

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity.
- Periodic reviews performed through self-assessment or 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 definition of internal auditing, the Code of Ethics, and the* Standards*.*

Periodic reviews are assessments conducted to evaluate conformance with the definition of internal auditing, 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.

Practice Advisory 1311-1: Internal Assessments

1. The processes and tools used in ongoing internal assessments include:
   - Engagement supervision;
   - Checklists and procedures (e.g., in an audit and procedures manual) are being followed;
   - Feedback from audit customers and other stakeholders;
   - Selective peer reviews of working papers by staff not involved in the respective audits;
   - Project budgets, timekeeping systems, audit plan completion, and cost recoveries; and/or
   - Analyses of other performance metrics (such as cycle time and recommendations accepted).

2. Conclusions are developed as to the quality of ongoing performance, and follow-up action is taken to ensure that appropriate improvements are implemented.

3. The IIA's *Quality Assessment Manual*, or a comparable set of guidance and tools, should serve as the basis for periodic internal assessments.

4. Periodic internal assessments may:
   - Include more in-depth interviews and surveys of stakeholder groups.
   - Be performed by members of the internal audit activity (self-assessment).
   - Be performed by CIAs or other competent audit professionals currently assigned elsewhere in the organization.
   - Encompass a combination of self-assessment and preparation of materials subsequently reviewed by CIAs or other competent audit professionals.
   - Include benchmarking of the internal audit activity's practices and performance metrics against relevant best practices of the internal audit profession.

5. A periodic internal assessment performed within a short time before an external assessment can serve to facilitate and reduce the cost of the external assessment. If the periodic internal assessment is performed by a qualified, independent external reviewer or review team, the assessment results should not communicate any assurances on the outcome of the subsequent external quality assessment. The report may offer suggestions and recommendations to enhance the internal audit activities' practices. If the external assessment takes the form of a self-assessment with independent validation, the periodic internal assessment can serve as the self-assessment portion of this process.

6. Conclusions are developed as to quality of performance, and appropriate action are initiated to achieve improvements and conformity to the *Standards*, as necessary.

7. The CAE establishes a structure for reporting results of internal assessments that maintains appropriate credibility and objectivity. Generally, those assigned responsibility for conducting ongoing and periodic reviews report to the CAE while performing the reviews and communicate results directly to the CAE.

8. At least annually, the CAE reports the results of internal assessments, necessary action plans, and their successful implementation to senior management and the board.

1312–External Assessments

External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The CAE must discuss with the board:

- The need for more frequent external assessments.
- The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.

Interpretation: *A qualified reviewer or review 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 a review 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 a reviewer or review team demonstrates sufficient competence to be qualified.*

An "independent reviewer or review team" means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs.

Practice Advisory 1312-1: External Assessments

1. External assessments cover the entire spectrum of audit and consulting work performed by the internal audit activity and should not be limited to assessing its quality assurance and improvement program. To achieve optimum benefits from an external assessment, the scope of work should include benchmarking, identification, and reporting of leading practices that could assist the internal audit activity in becoming more efficient and/or effective. This can be accomplished in two ways: through (a) a full external assessment by a qualified, independent external reviewer or review team or (b) a comprehensive internal self-assessment with independent validation by a qualified, independent external reviewer or review team. Nonetheless, the CAE is to ensure that the scope clearly states the expected deliverables of the external assessment in each case.

2. External assessments of an internal audit activity contain an expressed opinion as to the entire spectrum of assurance and consulting work performed (or that should have been performed based on the internal audit charter) by the internal audit activity, including its conformance with the definition of internal auditing, the Code of Ethics, and the *Standards* and, as appropriate, includes recommendations for improvement. Apart from conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*, the scope of the assessment is adjusted at the discretion of the CAE, senior management, or the board. These assessments can have considerable value to the CAE and other members of the internal audit activity, especially when benchmarking and best practices are shared.

3. On completion of the review, a formal communication is to be given to senior management and the board.

4. There are two approaches to external assessments. The first approach is a full external assessment conducted by a qualified, independent external reviewer or review team. This approach involves an outside team of competent professionals under the leadership of an experienced and professional project manager. The second approach involves the use of a qualified, independent external reviewer or review team to conduct an independent validation of the internal self-assessment and a report completed by the internal audit activity**.** Independent external reviewers should be well versed in leading internal audit practices.

5. Individuals who perform the external assessment are free from any obligation to, or interest in, the organization whose internal audit activity is the subject of the external assessment or the personnel of such organization. Particular matters relating to independence, which are to be considered by the CAE in consultation with the board, in selecting a qualified, independent external reviewer or review team, include:

- Any real or apparent conflict of interest of firms that provide:
  - The external audit of financial statements.
  - Significant consulting services in the areas of governance, risk management, financial reporting, internal control, and other related areas.
  - Assistance to the internal audit activity. The significance and amount of work performed by the professional service provider is to be considered in the deliberation.
- Any real or apparent conflict of interest of former employees of the organization who would perform the assessment. Consideration should be given to the length of time the individual has been independent of the organization.
- Individuals who perform the assessment are independent of the organization whose internal audit activity is the subject of the assessment and do not have any real or apparent conflict of interest. "Independent of the organization" means not a part of, or under the control of, the organization to which the internal audit activity belongs. In the selection

of a qualified, independent external reviewer or review team, consideration is to be given to any real or apparent conflict of interest the reviewer may have due to present or past relationships with the organization or its internal audit activity, including the reviewer's participation in internal quality assessments.

- Individuals in another department of the subject organization or in a related organization, although organizationally separate from the internal audit activity, are not considered independent for purposes of conducting an external assessment. A related organization may be a parent organization; an affiliate in the same group of entities; or an entity with regular oversight, supervision, or quality assurance responsibilities with respect to the subject organization.
- Real or apparent conflict involving peer review arrangements. Peer review arrangements among three or more organizations (e.g., within an industry or other affinity group, regional association, or other group of organizations—except as precluded by the "related organization" definition in the previous point) may be structured in a manner that alleviates independence concerns, but care must be taken to ensure that the issue of independence does not arise. Peer reviews between two organizations would not pass the independence test.
- To overcome concerns regarding the appearance or reality of impairment of independence in instances such as those discussed in this section, one or more independent individuals could be part of the external assessment team to independently validate the work of that external assessment team.

6. Integrity requires the reviewer to be honest and candid within the constraints of confidentiality. Service and the public trust should not be subordinated to personal gain and advantage. Objectivity is a state of mind and a quality that lends value to a reviewer's services. The principle of objectivity imposes the obligation to be impartial, intellectually honest, and free of conflict of interest.

7. Performing and communicating the results of an external assessment require the exercise of professional judgment. Accordingly, an individual serving as an external reviewer should:

- Be a competent, CIA professional who possesses current, in-depth knowledge of the *Standards*.
- Be well versed in the best practices of the profession.
- Have at least three years of recent experience in the practice of internal auditing or related consulting at a management level.

Leaders of independent review teams and external reviewers who independently validate the results of the self-assessment should have an additional level of competence and experience gained from working previously as team members on an external quality assessment, successful completion of the IIA's quality assessment training course or similar training, and CAE or comparable senior internal audit management experience.

8. The reviewer should possess relevant technical expertise and industry experience. Individuals with expertise in other specialized areas may assist the team. For example, specialists in enterprise risk management, IT auditing, statistical sampling, operations monitoring systems, or control self-assessment may participate in certain segments of the assessment.

9. The CAE involves senior management and the board in determining the approach and selection of an external quality assessment provider.

10. The external assessment consists of a broad scope of coverage that includes the following elements of the internal audit activity:

- Conformance with the definition of internal auditing; the Code of Ethics; and the *Standards*; and the internal audit activity's charter, plans, policies, procedures, practices, and applicable legislative and regulatory requirements.
- Expectations of the internal audit activity expressed by the board, senior management, and operational managers.
- Integration of the internal audit activity into the organization's governance process, including the relationships between and among the key groups involved in the process.
- Tools and techniques employed by the internal audit activity.
- Mix of knowledge, experience, and disciplines within the staff, including staff focus on process improvement.
- Determination as to whether the internal audit activity adds value and improves the organization's operations.

11. The preliminary results of the review are discussed with the CAE during and at the conclusion of the assessment process. Final results are communicated to the CAE or other official who authorized the review for the organization, preferably with copies sent directly to appropriate members of senior management and the board.

12. The communication includes:

- An opinion on the internal audit activity's conformance with the definition of internal auditing, the Code of Ethics, and the *Standards* based on a structured rating process. The term "conformance" means the practices of the internal audit activity, taken as a whole, satisfy the requirements of the definition of internal auditing, the Code of Ethics, and the *Standards*. Similarly, "nonconformance" means the impact and severity of the deficiencies in the practices of the internal audit activity are so significant they impair the internal audit activity's ability to discharge its responsibilities. The degree of "partial conformance" with the definition of internal auditing, the Code of Ethics, and/or individual *Standards*, if relevant to the overall opinion, should also be expressed in the report on the independent assessment. The expression of an opinion on the results of the external assessment requires the application of sound business judgment, integrity, and due professional care.
- An assessment and evaluation of the use of best practices, both those observed during the assessment and others potentially applicable to the activity.
- Recommendations for improvement, where appropriate.
- Responses from the CAE that include an action plan and implementation dates.

13. To provide accountability and transparency, the CAE communicates the results of external quality assessments, including specifics of planned remedial actions for significant issues and subsequent information as to accomplishment of those planned actions, to the various stakeholders of the activity, such as senior management, the board, and external auditors.

Practice Advisory 1312-2: External Assessments: Self-Assessment with Independent Validation

1. An external assessment by a qualified, independent reviewer or review team may be troublesome for smaller internal audit activities, or there may be circumstances in other organizations where a full external assessment by an independent team is not deemed appropriate or necessary. For example, the internal audit activity may (a) be in an industry subject to extensive regulation and/or supervision, (b) be otherwise subject to extensive external oversight and direction relating

to governance and internal controls, (c) have been recently subjected to external review(s) and/or consulting services in which there was extensive benchmarking with best practices, or (d) in the judgment of the CAE, the benefits of self-assessment for staff development and the strength of the internal quality assurance and improvement program currently outweigh the benefits of a quality assessment by an external team.

2. A self-assessment with independent (external) validation includes:

- A comprehensive and fully documented self-assessment process, which emulates the external assessment process, at least with respect to evaluation of conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*.
- An independent, on-site validation by a qualified, independent reviewer.
- Economical time and resource requirements—for example, the primary focus would be on conformance with the *Standards*.
- Limited attention to other areas—such as benchmarking, review and consultation as to employment of leading practices, and interviews with senior and operating management—may be reduced. However, the information produced by these parts of the assessment is one of the benefits of an external assessment.

3. The same guidance and criteria as set forth in Practice Advisory 1312-1 would apply for a self-assessment with independent validation.

4. A team under the direction of the CAE performs and fully documents the self-assessment process. A draft report, similar to that for an external assessment, is prepared including the CAE's judgment on conformance with the *Standards*.

5. A qualified, independent reviewer or review team performs sufficient tests of the self-assessment so as to validate the results and express the indicated level of the activity's conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*. The independent validation follows the process outlined in the IIA's *Quality Assessment Manual* or a similar comprehensive process.

6. As part of the independent validation, the independent external reviewer—upon completion of a rigorous review of the self-assessment team's evaluation of conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*:

- Reviews the draft report and attempts to reconcile unresolved issues (if any).
- If in agreement with the opinion of conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*, adds wording (as needed) to the report, concurring with the self-assessment process and opinion and—to the extent deemed appropriate—with the report's findings, conclusions, and recommendations.
- If not in agreement with the evaluation, adds dissenting wording to the report, specifying the points of disagreement with it and—to the extent deemed appropriate—with the significant findings, conclusions, recommendations, and opinions in the report.
- Alternatively, may prepare a separate independent validation report—concurring or expressing disagreement as outlined above—to accompany the report of the self-assessment.

7. The final report(s) of the self-assessment with independent validation is signed by the self-assessment team and the qualified, independent external reviewer(s) and issued by the CAE to senior management and the board.

8. To provide accountability and transparency, the CAE communicates the results of external quality assessments—including specifics of planned remedial actions for significant issues and subsequent information as to accomplishment of those planned actions—with the various stakeholders of the activity, such as senior management, the board, and external auditors.

1320–Reporting on the Quality Assurance and Improvement Program

The CAE must communicate the results of the QAIP to senior management and the board.

Interpretation: *The form, content, and frequency of communicating the results of the QAIP 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 definition of internal auditing, 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 reviewer's or review team's assessment with respect to the degree of conformance.*

No Practice Advisory for Standard 1320

1321–Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"

The CAE may state that the internal audit activity conforms with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the QAIP support this statement.

Interpretation: *The internal audit activity conforms with the* Standards *when it achieves the outcomes described in the definition of internal auditing, Code of Ethics, and* Standards*.*

The results of the QAIP 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.

Practice Advisory 1321-1: Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"

1. Ongoing monitoring and external and internal assessments of an internal audit activity are performed to evaluate and express an opinion as to the internal audit activity's conformance with the definition of internal auditing, the Code of Ethics, and the *Standards* and, as appropriate, should include recommendations for improvement.

2. The phrase to be used may be "in conformance with the *Standards*" or "in conformity to the *Standards*." To use one of these phrases, an external assessment is required at least once during each five-year period, along with ongoing monitoring and periodic internal assessments, and these activities need to have concluded that the internal audit activity is in conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*. Initial use of the conformance phrase is not appropriate until an external review has demonstrated that the internal audit activity is in conformance with the definition of internal auditing, the Code of Ethics, and the *Standards*.

3. The CAE is responsible for disclosing instances of nonconformance that impact the overall scope or operation of the internal audit activity, including failure to obtain an external assessment within a five-year period, to senior management and the board.

4. Before the internal audit activity's use of the conformance phrase, any instances of nonconformance that have been disclosed by a quality assessment (internal or external) which impair the internal audit activity's ability to discharge its responsibilities needs to be adequately remedied. In addition, the following are needed:

- Remedial actions need to be documented and reported to the relevant assessor(s) to obtain concurrence that the nonconformance has been adequately remedied.
- Remedial actions and agreement of the relevant assessor(s) therewith need to be reported to senior management and the board.

1322–Disclosure of Nonconformance

When nonconformance with the definition of internal auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the CAE must disclose the nonconformance and the impact to senior management and the board.

No Practice Advisory for Standard 1322

(b) Performance Standards (2000 to 2600)

2000–Managing the Internal Audit Activity

The CAE must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation: *The internal audit activity is effectively managed when:*

- *The results of the internal audit activity's work achieve the purpose and responsibility included in the internal audit charter.*
- *The internal audit activity conforms with the definition of internal auditing and the* Standards.
- *The individuals who are part of the internal audit activity demonstrate conformance with the Code of Ethics and the* Standards.

The internal audit activity adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.

No Practice Advisory for Standard 2000

2010–Planning

The CAE must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation: *The CAE is responsible for developing a risk-based plan. The CAE takes into account the organization's risk management framework, including using* ***risk appetite*** *levels set by management for the different activities or parts of the organization. If a framework does not exist, the CAE uses his or her own judgment of risks after consultation with senior management and the board.*

2010.A1–The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2–The CAE must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

2010.C1–The CAE should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures

1. In developing the internal audit activity's audit plan, many CAEs find it useful to first develop or update the audit universe. The audit universe is a list of all the possible audits that could be performed. The CAE may obtain input on the audit universe from senior management and the board.

2. The audit universe can include components from the organization's strategic plan. By incorporating components of the organization's strategic plan, the audit universe will consider and reflect the business's overall objectives. Strategic plans also likely reflect the organization's attitude toward risk and the degree of difficulty to achieving planned objectives. The audit universe will normally be influenced by the results of the risk management process. The organization's strategic plan considers the environment in which the organization operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

3. The CAE prepares the internal audit activity's audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization. Key audit objectives are usually to provide senior management and the board with assurance and information to help them accomplish the organization's objectives, including an assessment of the effectiveness of management's risk management activities.

4. The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus. It is advisable to assess the audit universe on at least an annual basis to ensure that it reflects the most current strategies and direction of the organization. In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the organization's business, operations, programs, systems, and controls.

5. Audit work schedules are based on, among other factors, an assessment of risk and exposures. Prioritizing is needed to make decisions for applying resources. A variety of risk models exist to assist the CAE. Most risk models use risk factors such as impact, likelihood, materiality, asset liquidity, management competence, quality of and adherence to internal controls, degree of change or stability, timing and results of last audit engagement, complexity, and employee and government relations.

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

1. Risk management is a critical part of providing sound governance that touches all the organization's activities. Many organizations are moving to adopt consistent and holistic risk management approaches that should, ideally, be fully integrated into the management of the organization. Risk management applies at all levels—enterprise, function, and business unit—of the organization. Management typically uses a risk management framework to conduct the assessment and document the assessment results.

2. An effective risk management process can assist in identifying key controls related to significant inherent risks. Enterprise risk management (ERM) is a term in common use. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission defines "ERM" as "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Implementation of controls is one common method

management can use to manage risk within its risk appetite. Internal auditors audit the key controls and provide assurance on the management of significant risks.

3. The IIA *Standards* defines "control" as "any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved."

4. Two fundamental risk concepts are inherent risk and residual risk (also known as current risk). Financial/external auditors have long had a concept of inherent risk that can be summarized as the susceptibility of information or data to a material misstatement, assuming that there are no related mitigating controls. The *Standards* define "residual risk" as "the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk." "Current risk" is often defined as the risk managed within existing controls or control systems.

5. "Key controls" can be defined as controls or groups of controls that help to reduce an otherwise unacceptable risk to a tolerable level. Controls can be most readily conceived as organizational processes that exist to address risks. In an effective risk management process (with adequate documentation), the key controls can be readily identified from the difference between inherent and residual risk across all affected systems that are relied on to reduce the rating of significant risks. If a rating has not been given to inherent risk, the internal auditor estimates the inherent risk rating. When identifying key controls (and assuming the internal auditor has concluded that the risk management process is mature and reliable), the internal auditor would look for:

- Individual risk factors where there is a significant reduction from inherent to residual risk (particularly if the inherent risk was very high). This highlights controls that are important to the organization.
- Controls that serve to mitigate a large number of risks.

6. Internal audit planning needs to make use of the organizational risk management process, where one has been developed. In planning an engagement, the internal auditor considers the significant risks of the activity and the means by which management mitigates the risk to an acceptable level. The internal auditor uses risk assessment techniques in developing the internal audit activity's plan and in determining priorities for allocating internal audit resources. Risk assessment is used to examine auditable units and select areas for review to include in the internal audit activity's plan that have the greatest risk exposure.

7. Internal auditors may not be qualified to review every risk category and the ERM process in the organization (e.g., internal audits of workplace health and safety, environmental auditing, or complex financial instruments). The CAE ensures that internal auditors with specialized expertise or external service providers are used appropriately.

8. Risk management processes and systems are set up differently throughout the world. The maturity level of the organization related to risk management varies among organizations. Where organizations have a centralized risk management activity, the role of this activity includes coordinating with management regarding its continuous review of the internal control structure and updating the structure according to evolving risk appetites. The risk management processes in use in different parts of the world might have different logic, structures, and terminology. Internal auditors therefore make an assessment of the organization's risk management process and determine what parts can be used in developing the internal audit activity's plan and what parts can be used for planning individual internal audit assignments.

9. Factors the internal auditor considers when developing the internal audit plan include:

- Inherent risks. Are they identified and assessed?
- Residual risks. Are they identified and assessed?

- Mitigating controls, contingency plans, and monitoring activities. Are they linked to the individual events and/or risks?
- Risk registers. Are they systematic, completed, and accurate?
- Documentation. Are the risks and activities documented?

In addition, the internal auditor coordinates with other assurance providers and considers planned reliance on their work. Refer to the IIA's *Practice Advisory 2050-2: Assurance Maps*.

10. The internal audit charter normally requires the internal audit activity to focus on areas of high risk, including both inherent and residual risk. The internal audit activity needs to identify areas of high inherent risk, high residual risks, and the key control systems on which the organization is most reliant. If the internal audit activity identifies areas of unacceptable residual risk, management needs to be notified so that the risk can be addressed. The internal auditor will, as a result of conducting a strategic audit planning process, be able to identify different kinds of activities to include in the internal audit activity's plan, including:

- Control reviews/assurance activities, where the internal auditor reviews the adequacy and efficiency of the control systems and provides assurance that the controls are working and the risks are effectively managed.
- Inquiry activities, where organizational management has an unacceptable level of uncertainty about the controls related to a business activity or identified risk area and the internal auditor performs procedures to gain a better understanding of the residual risk.
- Consulting activities, where the internal auditor advises organizational management in the development of the control systems to mitigate unacceptable current risks.

Internal auditors also try to identify unnecessary, redundant, excessive, or complex controls that inefficiently reduce risk. In these cases, the cost of the control may be greater than the benefit realized, and therefore there is an opportunity for efficiency gains in the design of the control.

11. To ensure that relevant risks are identified, the approach to risk identification is systematic and clearly documented. Documentation can range from the use of a spreadsheet in small organizations to vendor-supplied software in more sophisticated organizations. The crucial element is that the risk management framework is documented in its entirety.

12. The documentation of risk management in an organization can be at various levels below the strategic level of the risk management process. Many organizations have developed **risk registers** that document risks below the strategic level, providing documentation of significant risks in an area and related inherent and residual risk ratings, key controls, and mitigating factors. An alignment exercise can then be undertaken to identify more direct links between risk "categories" and "aspects" described in the risk registers and, where applicable, the items already included in the audit universe documented by the internal audit activity.

13. Some organizations may identify several high (or higher) inherent risk areas. While these risks may warrant the internal audit activity's attention, it is not always possible to review all of them. Where the risk register shows a high, or above, ranking for inherent risk in a particular area, and the residual risk remains largely unchanged and no action by management or the internal audit activity is planned, the CAE reports those areas separately to the board with details of the risk analysis and reasons for the lack of, or ineffectiveness of, internal controls.

14. A selection of audits of lower-risk-level business units or branches need to periodically be included in the internal audit activity's plan to give them coverage and confirm that their risks have not changed. Also, the internal audit activity establishes a method for prioritizing outstanding risks not yet subject to an internal audit.

15. An internal audit activity's plan will normally focus on:

- Unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately.
- Control systems on which the organization is most reliant.
- Areas where the differential is great between inherent risk and residual risk.
- Areas where the inherent risk is very high.

16. When planning individual internal audits, the internal auditor identifies and assesses risks relevant to the area under review.

2020–Communication and Approval

The CAE must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The CAE must also communicate the impact of resource limitations.

Practice Advisory 2020-1: Communication and Approval

1. The CAE will submit annually to senior management and the board for review and approval a summary of the internal audit plan, work schedule, staffing plan, and financial budget. This summary will inform senior management and the board of the scope of internal audit work and of any limitations placed on that scope. The CAE will also submit all significant interim changes for approval and information.

2. The approved engagement work schedule, staffing plan, and financial budget, along with all significant interim changes, are to contain sufficient information to enable senior management and the board to ascertain whether the internal audit activity's objectives and plans support those of the organization and the board and are consistent with the internal audit charter.

2030–Resource Management

The CAE must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Interpretation: *"Appropriate" refers to the mix of knowledge, skills, and other competencies needed to perform the plan. "Sufficient" refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.*

Practice Advisory 2030-1: Resource Management

1. The CAE is primarily responsible for the sufficiency and management of internal audit resources in a manner that ensures the fulfillment of internal audit's responsibilities, as detailed in the internal audit charter. This includes effective communication of resource needs and reporting of status to senior management and the board. Internal audit resources may include employees, external service providers, financial support, and technology-based audit techniques. Ensuring the adequacy of internal audit resources is ultimately a responsibility of the organization's senior management and board; the CAE should assist them in discharging this responsibility.

2. The skills, capabilities, and technical knowledge of the internal audit staff are to be appropriate for the planned activities. The CAE will conduct a periodic skills assessment or inventory to determine the specific skills required to perform the internal audit activities. The skills assessment

is based on and considers the various needs identified in the risk assessment and audit plan. This includes assessments of technical knowledge, language skills, business acumen, fraud detection and prevention competency, and accounting and audit expertise.

3. Internal audit resources need to be sufficient to execute the audit activities in the breadth, depth, and timeliness expected by senior management and the board, as stated in the internal audit charter. Resource planning considerations include the audit universe, relevant risk levels, the internal audit plan, coverage expectations, and an estimate of unanticipated activities.

4. The CAE also ensures that resources are deployed effectively. This includes assigning auditors who are competent and qualified for specific assignments. It also includes developing a resourcing approach and organizational structure appropriate for the business structure, risk profile, and geographical dispersion of the organization.

5. From an overall resource management standpoint, the CAE considers succession planning, staff evaluation and development programs, and other human resource disciplines. The CAE also addresses the resourcing needs of the internal audit activity, whether those skills are present within the internal audit activity itself or not. Other approaches to addressing resource needs include external service providers, employees from other departments within the organization, or specialized consultants.

6. Because of the critical nature of resources, the CAE maintains ongoing communications and dialog with senior management and the board on the adequacy of resources for the internal audit activity. The CAE periodically presents a summary of status and adequacy of resources to senior management and the board. To that end, the CAE develops appropriate metrics, goals, and objectives to monitor the overall adequacy of resources. This can include comparisons of resources to the internal audit plan, the impact of temporary shortages or vacancies, educational and training activities, and changes to specific skill needs based on changes in the organization's business, operations, programs, systems, and controls.

2040–Policies and Procedures

The CAE must establish policies and procedures to guide the internal audit activity.

Interpretation: *The form and content of policies and procedures are dependent on the size and structure of the internal audit activity and the complexity of its work.*

Practice Advisory 2040-1: Policies and Procedures

1. The CAE develops policies and procedures. Formal administrative and technical audit manuals may not be needed by all internal audit activities. A small internal audit activity may be managed informally. Its audit staff may be directed and controlled through daily, close supervision and memoranda that state policies and procedures to be followed. In a large internal audit activity, more formal and comprehensive policies and procedures are essential to guide the internal audit staff in the execution of the internal audit plan.

2050–Coordination

The CAE should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

Practice Advisory 2050-1: Coordination

1. Oversight of the work of external auditors, including coordination with the internal audit activity, is the responsibility of the board. Coordination of internal and external audit work is the responsibility of the CAE. The CAE obtains the support of the board to coordinate audit work effectively.

2. Organizations may use the work of external auditors to provide assurance related to activities within the scope of internal auditing. In these cases, the CAE takes the steps necessary to understand the work performed by the external auditors, including:

- The nature, extent, and timing of work planned by external auditors, to be satisfied that the external auditors' planned work, in conjunction with the internal auditors' planned work, satisfies the requirements of Standard 2100.
- The external auditor's assessment of risk and materiality.
- The external auditors' techniques, methods, and terminology to enable the CAE to (a) coordinate internal and external auditing work; (b) evaluate, for purposes of reliance, the external auditors' work; and (c) communicate effectively with external auditors.
- Access to the external auditors' programs and working papers, to be satisfied that the external auditors' work can be relied upon for internal audit purposes. Internal auditors are responsible for respecting the confidentiality of those programs and working papers.

3. External auditors may rely on the work of the internal audit activity in performing their work. In this case, the CAE needs to provide sufficient information to enable external auditors to understand the internal auditors' techniques, methods, and terminology to facilitate reliance by external auditors on work performed. Access to the internal auditors' programs and working papers is provided to external auditors in order for external auditors to be satisfied as to the acceptability for external audit purposes of relying on the internal auditors' work.

4. It may be efficient for internal and external auditors to use similar techniques, methods, and terminology to coordinate their work effectively and to rely on the work of one another.

5. Planned audit activities of internal and external auditors need to be discussed to ensure that audit coverage is coordinated and duplicate efforts are minimized where possible. Sufficient meetings are to be scheduled during the audit process to ensure coordination of audit work and efficient and timely completion of audit activities and to determine whether observations and recommendations from work performed to date require that the scope of planned work be adjusted.

6. The internal audit activity's final communications, management's responses to those communications, and subsequent follow-up reviews are to be made available to external auditors. These communications assist external auditors in determining and adjusting the scope and timing of their work. In addition, internal auditors need access to the external auditors' presentation materials and management letters. Matters discussed in presentation materials and included in management letters need to be understood by the CAE and used as input to internal auditors in planning the areas to emphasize in future internal audit work. After review of management letters and initiation of any needed corrective action by appropriate members of senior management and the board, the CAE ensures that appropriate follow-up and corrective actions have been taken.

7. The CAE is responsible for regular evaluations of the coordination between internal and external auditors. Such evaluations may also include assessments of the overall efficiency and effectiveness of internal and external audit activities, including aggregate audit cost. The CAE communicates the results of these evaluations to senior management and the board, including relevant comments about the performance of external auditors.

Practice Advisory 2050-2: Assurance Maps

1. One of the key responsibilities of the board is to gain assurance that processes are operating within the parameters it has established to achieve the defined objectives. It is necessary to determine whether risk management processes are working effectively and whether key or business-critical risks are being managed to an acceptable level.

2. Increased focus on the roles and responsibilities of senior management and boards has prompted many organizations to place a greater emphasis on assurance activities. The *Standards* Glossary defines "assurance" as "an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization." The board will use multiple sources to gain reliable assurance. Assurance from management is fundamental and should be complemented by the provision of objective assurance from internal audit and other third parties. Risk managers, internal auditors, and compliance practitioners are asking: "Who does what and why?" Boards in particular are beginning to question who is providing assurance, where the delineation between the functions is, and if there are any overlaps.

3. There are fundamentally three classes of assurance providers, differentiated by the stakeholders they serve, their level of independence from the activities over which they provide assurance, and the robustness of that assurance.

a. Those who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management- designated assurance personnel.

b. Those who report to the board, including internal audit.

c. Those who report to external stakeholders (external audit assurance), which is a role traditionally fulfilled by the independent/statutory auditor.

The level of assurance desired, and who should provide that assurance, will vary depending on the risk.

4. There are many assurance providers for an organization. These include

- Line management and employees. (Management provides assurance as a first line of defense over the risks and controls for which they are responsible.)
- Senior management.
- Internal and external auditors.
- Compliance.
- Quality assurance.
- Risk management.
- Environmental auditors.
- Workplace health and safety auditors.
- Government performance auditors.
- Financial reporting review teams.
- Subcommittees of the board (e.g., audit, actuarial, credit, governance).
- External assurance providers, including surveys, specialist reviews (health and safety), etc.

5. The internal audit activity will normally provide assurance over the entire organization, including risk management processes (both their design and operating effectiveness), management of those risks classified as "key" (including the effectiveness of the controls and other responses to them), and verification of the reliability and appropriateness of the risk assessment and reporting of the risk and control status.

6. With responsibility for assurance activities traditionally being shared among management, internal audit, risk management, and compliance, it is important that assurance activities are

coordinated to ensure that resources are used in the most efficient and effective way. Many organizations operate with traditional (and separate) internal audit, risk, and compliance activities. It is common for organizations to have a number of separate groups performing different risk management, compliance, and assurance functions independently of one another. Without effective coordination and reporting, work can be duplicated or key risks may be missed or misjudged.

7. While many organizations monitor the activities of internal audit, risk, and compliance, not all view all their activities in a holistic way. An assurance mapping exercise involves mapping assurance coverage against the key risks in an organization. This process allows an organization to identify and address any gaps in the risk management process and gives stakeholders comfort that risks are being managed and reported on and that regulatory and legal obligations are being met. Organizations will benefit from a streamlined approach, which ensures the information is available to management about the risks they face and how the risks are being addressed. The mapping is done across the organization to understand where the overall risk and assurance roles and accountabilities reside. The aim is to ensure that there is a comprehensive risk and assurance process with no duplicated effort or potential gaps.

8. Often an organization will have defined the significant risk categories that make up its risk management framework. In such cases, the **assurance map** would be based on the structure of this framework. For example, an assurance map could have these columns:

- Significant risk category
- Management role responsible for the risk (risk owner)
- Inherent risk rating
- Residual risk rating
- External audit coverage
- Internal audit coverage
- Other assurance provider coverage

In this example, the CAE would populate the internal audit coverage column with recent coverage. Often each significant risk has a risk owner or a person responsible for coordinating assurance activities for that risk; that person would populate the other assurance provider coverage column. Each significant unit within an organization could have its own assurance map. Alternatively, the internal audit activity may play a coordinating role in developing and completing the organization's assurance map.

9. Once the assurance map for the organization has been completed, significant risks with inadequate assurance coverage, or areas of duplicated assurance coverage, can be identified. Senior management and the board need to consider changes in assurance coverage for these risks. The internal audit activity needs to consider areas of inadequate coverage when developing the internal audit plan.

10. It is the responsibility of the CAE to understand the independent assurance requirements of the board and the organization and to clarify the role the internal audit activity fills and the level of assurance it provides. The board needs to be confident that the overall assurance process is adequate and sufficiently robust to validate that the risks of the organization are being managed and reported on effectively.

11. The board needs to receive information about assurance activities, both implemented and planned, in regard to each category of risk. The internal audit activity and other assurance providers offer the board the appropriate level of assurance for the nature and levels of risk that exist in the organization under the respective categories.

12. In organizations requiring an overall opinion from the CAE, the CAE needs to understand the nature, scope, and extent of the integrated assurance map to consider the work of other assurance providers (and rely on it as appropriate) before presenting an overall opinion on the organization's governance, risk management, and control processes. The IIA's Practice Guide titled *Formulating and Expressing Internal Audit Opinions* provides additional guidance.

13. In instances where the organization does not expect an overall opinion, the CAE can act as the coordinator of assurance providers to ensure that there are either no gaps in assurance or the gaps are known and accepted. The CAE reports on any lack of input/involvement/ oversight/assurance over other assurance providers. If the CAE believes that the assurance coverage is inadequate or ineffective, senior management and the board need to be advised accordingly.

14. The CAE is directed by Standard 2050 to coordinate activities with other assurance providers; the use of an assurance map will help achieve this. Assurance maps offer an effective way of communicating this coordination.

Practice Advisory 2050-3: Relying on the Work of Other Assurance Providers

1. The internal auditor may rely on or use the work of other internal or external assurance providers in providing governance, risk management, and control assurance to the board. Internal assurance providers could include company functions such as compliance, information security, quality, and labor health and safety as well as management monitoring activities. External assurance providers could include external auditors, joint venture partners, specialist reviews, or third-party audit firms, including those providing reports in accordance with *International Standard on Assurance Engagements 3402: Assurance Reports on Controls at a Service Organization*.

2. The decision to rely on the work of other assurance providers can be made for a variety of reasons, including to address areas that fall outside of the competence of the internal audit activity, to gain knowledge transfer from other assurance providers, or to efficiently enhance coverage of risk beyond the internal audit plan.

3. An internal audit charter and/or engagement letter should specify that the internal audit activity have access to the work of other internal and external assurance providers.

4. Where the internal auditor is hiring the assurance provider, the auditor should document engagement expectations in a contract or agreement. Minimum expectations should be provided for the nature and ownership of deliverables, methods/techniques, the nature of procedures and data/information to be used, progress reports/supervision to ensure the work is adequate, and reporting requirements.

5. If management within the organization provides the contracting of, and direction to, a third-party assurance provider, the internal auditor should be satisfied that the instruction is appropriate, understood, and executed.

6. The internal auditor should consider the independence and objectivity of the other assurance providers when considering whether to rely on or use their work. If an assurance provider is hired by and/or is under the direction of management instead of internal auditing, the impact of this arrangement on the assurance provider's independence and objectivity should be evaluated.

7. The internal auditor should assess the competencies and qualifications of the provider performing the assurance work. Examples of competency include verifying that the assurer holds appropriate professional experience and qualifications, has a current registration with the relevant professional body or institute, and has a reputation for competency and integrity in the sector.

8. The internal auditor should consider the other assurance provider's elements of practice to have reasonable assurance the findings are based on sufficient, reliable, relevant, and useful information, as required by *Standard 2310: Identifying Information*. Standard 2310 must be met by the CAE regardless of the degree to which the work of other assurance providers is used.

9. The internal auditor should ensure that the work of the other assurance provider is appropriately planned, supervised, documented, and reviewed. The auditor should consider whether the

audit evidence is appropriate and sufficient to determine the extent of use and reliance on the work of the other assurance providers. Based on an assessment of the work of the other assurance provider, additional work or test procedures may be needed to gain appropriate and sufficient audit evidence. The internal auditor should be satisfied, based on knowledge of the business, environment, techniques, and information used by the assurance provider, that the findings appear to be reasonable.

10. The level of reliance that can be placed on another assurance provider will be impacted by the factors mentioned earlier: independence, objectivity, competencies, elements of practice, adequacy of execution of audit work, and sufficiency of audit evidence to support the given level of assurance. As the risk or significance of the activity reviewed by the other assurance provider increases, the internal auditor should gather more information on these factors and may need to obtain additional audit evidence to supplement the work done by the other assurance provider. To increase the level of reliance on the results, the internal audit activity may retest results of the other assurance provider.

11. The internal auditor should incorporate the assurance provider's results into the overall report of assurance that the internal auditor reports to the board or other key stakeholders. Significant issues raised by the other assurance provider can be incorporated in detail or summarized in internal audit reports. The internal auditor should include reference to other assurance providers where reports rely on such information.

12. Follow-up is a process by which internal auditors evaluate the adequacy, effectiveness, and timeliness of actions taken by management on reported observations and recommendations, including those made by other assurance providers. In reviewing actions taken to address recommendations made by other assurance providers, the internal auditor should determine whether management has implemented the recommendations or assumed the risk of not implementing them.

13. Significant findings from other assurance providers should be considered in the assurance and communications internal auditing is providing the organization. In addition, results of work performed by others may impact the internal audit risk assessment as to whether the findings impact the evaluation of risk and the level of audit work necessary in response to that risk.

14. In evaluating the effectiveness of, and contributing to the improvement of, risk management processes (*Standard 2120: Risk Management*), the internal audit activity may review the processes of these internal assurance providers, including company functions such as compliance, information security, quality, and labor health and safety as well as management monitoring activities. There should be coverage of risk areas by internal auditing, but when another assurance function exists, the internal audit activity may review the performance of that process rather than duplicate the detailed specific work of that other function.

15. Assessment from the other assurance provider on significant risks should be reported to relevant areas of the organization to be included in considerations regarding the organization's risk management framework and assurance map. See *Practice Advisory 2050-2: Assurance Maps*.

2060–Reporting to Senior Management and the Board

The CAE must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

Interpretation: *The frequency and content of reporting are determined in discussion with senior management and the board and depend on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management or the board.*

Practice Advisory 2060-1: Reporting to Senior Management and the Board

1. The purpose of reporting is to provide assurance to senior management and the board regarding governance processes (Standard 2110), risk management (Standard 2120), and control

(Standard 2130). Standard 1111 states: "The CAE must communicate and interact directly with the board."

2. The CAE should agree with the board about the frequency and nature of reporting on the internal audit activity's charter (e.g., purpose, authority, and responsibility) and performance. Performance reporting should be relative to the most recently approved plan to inform senior management and the board of significant deviations from the approved audit plan, staffing plans, and financial budgets; reasons for the deviations; and action needed or taken. Standard 1320 states: "The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board."

3. Significant risk exposures and control issues are those conditions that, according to the CAE's judgment, could adversely affect the organization and its ability to achieve its strategic, financial reporting, operational, and compliance objectives. Significant issues may carry unacceptable exposure to internal and external risks, including conditions related to control weaknesses, fraud, irregularities, illegal acts, errors, inefficiency, waste, ineffectiveness, conflicts of interest, and financial viability.

4. Senior management and the board make decisions on the appropriate action to be taken regarding significant issues. They may decide to assume the risk of not correcting the reported condition because of cost or other considerations. Senior management should inform the board of decisions about all significant issues raised by internal auditing.

5. When the CAE believes that senior management has accepted a level of risk that the organization considers unacceptable, the CAE must discuss the matter with senior management as stated in Standard 2600. The CAE should understand management's basis for the decision, identify the cause of any disagreement, and determine whether management has the authority to accept the risk. Disagreements may relate to risk likelihood and potential exposure, understanding of risk appetite, cost, and level of control. Preferably, the CAE should resolve the disagreement with senior management.

6. If the CAE and senior management cannot reach an agreement, Standard 2600 directs the CAE to inform the board. If possible, the CAE and management should make a joint presentation about the conflicting positions. For financial reporting matters, CAEs should consider discussing these issues with the external auditors in a timely manner.

2070–External Service Provider and Organizational Responsibility for Internal Auditing

When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.

Interpretation: *This responsibility is demonstrated through the QAIP, which assesses conformance with the definition of internal auditing, the Code of Ethics, and the* Standards.

No Practice Advisory for Standard 2070

2100–Nature of Work

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

No Practice Advisory for Standard 2100

2110–Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- 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, 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 IT governance of the organization supports the organization's strategies and objectives.

Practice Advisory 2110-1: Governance: Definition

1. The role of internal auditing as noted in the definition of internal auditing includes the responsibility to evaluate and improve governance processes as part of the assurance function.

2. The term "governance" has a range of definitions, depending on a variety of environmental, structural, and cultural circumstances as well as legal frameworks. The *Standards* define "governance" as "the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives." The CAE may use a different definition for audit purposes when the organization has adopted a different governance framework or model.

3. Globally, there are a variety of governance models that have been published by other organizations and legal and regulatory bodies. For example, the Organisation for Economic Co-operation and Development defines "governance" as "a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance provides the structure through which the objectives of the company are set and the means of attaining those objectives and monitoring performance are determined." The Australian Securities Exchange Corporate Governance Council defines "governance" as "the system by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed, and how performance is optimized." In most instances, there is an indication that governance is a process or system and is not static. What distinguishes the approach in the *Standards* is the specific emphasis on the board and its governance activities.

4. The frameworks and requirements for governance vary according to organization type and regulatory jurisdictions. Examples include publicly traded companies, not-for-profit organizations, associations, government or quasi-government entities, academic institutions, private companies, commissions, and stock exchanges.

5. How an organization designs and practices the principles of effective governance also vary depending on the size, complexity, and life cycle maturity of the organization, its stakeholder structure, legal and cultural requirements, and so on.

6. As a consequence of the variation in the design and structure of governance, the CAE should work with the board and the executive management team, as appropriate, to determine how governance should be defined for audit purposes.

7. Internal auditing is integral to the organization's governance framework. The unique position of internal auditors within the organization enables them to observe and formally assess the governance structure, its design, and its operational effectiveness while remaining independent.

8. The relationship among governance, risk management, and internal control should be considered. This item is addressed in Practice Advisory 2110-2. Practice Advisory 2110-3 discusses assessing governance.

Practice Advisory 2110-2: Governance: Relationship with Risk and Control

1. The *Standards* define "governance" as "the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives."

2. Governance does not exist as a set of distinct and separate processes and structures. Rather, there are relationships among governance, risk management, and internal controls.

3. Effective governance activities consider risk when setting strategy. Conversely, risk management relies on effective governance (e.g., tone at the top, risk appetite and tolerance, risk culture, and the oversight of risk management).

4. Effective governance relies on internal controls and communication to the board on the effectiveness of those controls.

5. Control and risk also are related, as "control" is defined as "any action taken by management, the board, and other parties to manage risk and increase the likelihood that established goals will be achieved."

6. The CAE should consider these relationships in planning assessments of governance processes:

- An audit should address those controls in governance processes that are designed to prevent or detect events that could have a negative impact on the achievement of organizational strategies, goals, and objectives; operational efficiency and effectiveness; financial reporting; or compliance with applicable laws and regulations. (See Practice Advisory 2110-3.)
- Controls within governance processes are often significant in managing multiple risks across the organization. For example, controls around the code of conduct may be relied on to manage compliance risks, fraud risks, and so on. This aggregation effect should be considered when developing the scope of an audit of governance processes.
- If other audits assess controls in governance processes (e.g., audits of controls over financial reporting, risk management processes, or compliance), the auditor should consider relying on the results of those audits.

Practice Advisory 2110-3: Governance—Assessments

1. Internal auditors can act in a number of different capacities in assessing and contributing to the improvement of governance practices. Typically, internal auditors provide independent, objective assessments of the design and operating effectiveness of the organization's governance processes. They also may provide consulting services and advice on ways to improve those processes. In some cases, internal auditors may be called on to facilitate board self-assessments of governance practices.

2. As noted in *Practice Advisory 2110-1: Governance: Definition*, the definition of governance for audit purposes should be agreed on with the board and executive management, as appropriate. In addition, the internal auditor should understand the organization's governance processes and the relationships among governance, risk, and control (refer to *Practice Advisory 2110-2: Governance: Relationship with Risk and Control*).

3. The audit plan should be developed based on an assessment of risks to the organization. All governance processes should be considered in the risk assessment. The plan should include the higher-risk governance processes, and inclusion of an assessment of processes or risk areas

where the board or executive management has requested work be performed should be considered. The plan should define the nature of the work to be performed, the governance processes to be addressed, and the nature of the assessments that will be made (i.e., macro—considering the entire governance framework, or micro—considering specific risks, processes, or activities, or some combination of both).

4. When there are known control issues or the governance process is not mature, the CAE could consider different methods for improving the control or governance processes through consulting services instead of, or in addition to, formal assessments.

5. Internal audit assessments regarding governance processes are likely to be based on information obtained from numerous audit assignments over time. The internal auditor should consider:

- The results of audits of specific governance processes (e.g., the whistleblower process, the strategy management process).
- Governance issues arising from audits that are not specifically focused on governance (e.g., audits of the risk management process, internal control over financial reporting, fraud risks).
- The results of other internal and external assurance providers' work (e.g., a firm engaged by the general counsel to review the investigation process). Refer to *Practice Advisory 2050: Coordination.*
- Other information on governance issues, such as adverse incidents indicating an opportunity to improve governance processes.

6. *During the planning, evaluating, and reporting phases,* the internal auditor should be sensitive to the potential nature and ramifications of the results and ensure appropriate communications with the board and executive management. The internal auditor should consider consulting legal counsel both before initiating the audit and before finalizing the report.

7. The internal audit activity is an essential part of the governance process. The board and executive management should be able to rely on the QAIP of the internal audit activity in conjunction with external quality assessments performed in accordance with the *Standards* for assurance on its effectiveness.

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:

- 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.

Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes

1. Risk management is a key responsibility of senior management and the board. To achieve its business objectives, management ensures that sound risk management processes are in place and functioning. Boards have an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective. In this role, boards may direct the internal audit activity to assist them by examining, evaluating, reporting, and/or recommending improvements to the adequacy and effectiveness of management's risk processes.

2. Management and the board are responsible for their organization's risk management and control processes. However, internal auditors acting in a consulting role can assist the organization in identifying, evaluating, and implementing risk management methodologies and controls to address those risks.

3. In situations where the organization does not have formal risk management processes, the CAE formally discusses with management and the board their obligations to understand, manage, and monitor risks within the organization and the need to satisfy themselves that there are processes operating within the organization, even if informal, that provide the appropriate level of visibility into the key risks and how they are being managed and monitored.

4. The CAE is to obtain an understanding of senior management's and the board's expectations of the internal audit activity in the organization's risk management process. This understanding is then codified in the charters of the internal audit activity and the board. Internal auditing's responsibilities are to be coordinated among all groups and individuals within the organization's risk management process. The role of internal audit in the risk management process of an organization can change over time and may encompass:

- No role.
- Auditing the risk management process as part of the internal audit plan.
- Active, continuous support and involvement in the risk management process such as participation on oversight committees, monitoring activities, and status reporting.
- Managing and coordinating the risk management process.

5. Ultimately, senior management and the board are charged with determining the role of internal auditing in the risk management process. Their view on internal auditing's role is likely to be determined by factors such as the culture of the organization, ability of the internal audit staff, and local conditions and customs of the country. However, taking on management's responsibility regarding the risk management process and the potential threat to internal audit's independence requires a full discussion and board approval.

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

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

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

8. Internal auditors need to obtain sufficient and appropriate evidence to determine that the key objectives of the risk management processes are being met to form an opinion on the adequacy of risk management processes. In gathering such evidence, the internal auditor might consider these audit procedures:

- Research and review current developments, trends, industry information related to the business conducted by the organization, and other appropriate sources of information to determine risks and exposures that may affect the organization and related control procedures used to address, monitor, and reassess those risks.
- Review corporate policies and board minutes to determine the organization's business strategies, risk management philosophy and methodology, appetite for risk, and acceptance of risks.
- Review previous risk evaluation reports issued by management, internal auditors, external auditors, and any other sources.
- Conduct interviews with line and senior management to determine business unit objectives, related risks, and management's risk mitigation and control monitoring activities.
- Assimilate information to independently evaluate the effectiveness of risk mitigation, monitoring, and communication of risks and associated control activities.
- Assess the appropriateness of reporting lines for risk monitoring activities.
- Review the adequacy and timeliness of reporting on risk management results.
- Review the completeness of management's risk analysis and actions taken to remedy issues raised by risk management processes, and suggest improvements.
- Determine the effectiveness of management's self-assessment processes through observations, direct tests of control and monitoring procedures, testing the accuracy of information used in monitoring activities, and other appropriate techniques.
- Review risk-related issues that may indicate weakness in risk management practices and, as appropriate, discuss with senior management and the board. If the auditor believes

that management has accepted a level of risk that is inconsistent with the organization's risk management strategy and policies or that he or she deems unacceptable to the organization, the auditor should refer to Standard 2600 and related guidance for additional direction.

Practice Advisory 2120-2: Managing the Risk of the Internal Audit Activity

1. The role and importance of internal auditing has grown tremendously, and the expectations of key stakeholders (e.g., board, executive management) continue to expand. Internal audit activities have broad mandates to cover financial, operational, IT, legal/regulatory, and strategic risks. At the same time, many internal audit activities face challenges related to the availability of qualified personnel in the global labor markets, increased compensation costs, and high demand for specialized resources (e.g., information systems, fraud, derivatives, and taxes). The combination of these factors results in a high level of risk for an internal audit activity. As a result, CAEs need to consider the risks related to their internal audit activities and the achievement of their objectives.

2. The internal audit activity is not immune to risks. It needs to take the necessary steps to ensure that it is managing its own risks.

3. Risks to internal audit activities fall into three broad categories: audit failure, false assurance, and reputation risks. The following discussion highlights the key attributes related to these risks and some steps an internal audit activity may consider to better manage them.

4. Every organization will experience control breakdowns. Often when controls fail or frauds occur, someone will ask: "Where were the internal auditors?" The internal audit activity could be a contributing factor due to:

- Not following the *Standards*.
- An inappropriate QAIP (Standard 1300), including procedures to monitor auditor independence and objectivity.
- Lack of an effective risk assessment process to identify key audit areas during the strategic risk assessment as well as areas of high risk during the planning of individual audits—as a result, failure to do the right audits and/or time wasted on the wrong audits.
- Failure to design effective internal audit procedures to test the "real" risks and the right controls.
- Failure to evaluate both the design adequacy and the control effectiveness as part of internal audit procedures.
- Use of audit teams that do not have the appropriate level of competence based on experience or knowledge of high-risk areas.
- Failure to exercise heightened professional skepticism and extended internal audit procedures related to findings or control deficiencies.
- Failure of adequate internal audit supervision.
- Making the wrong decision when there was some evidence of fraud—for example, "It's probably not material" or "We don't have the time or resources to deal with this issue."
- Failure to communicate suspicions to the right people.
- Failure to report adequately.

5. Internal audit failures may not only be embarrassing for internal audit activities; they can also expose an organization to significant risk. While there is no absolute assurance that audit

failures will not occur, an internal audit activity can implement the following practices to mitigate such risk:

- **QAIP.** It is critical for every internal audit activity to implement an effective QAIP.
- **Periodic review of the audit universe.** Review the methodology to determine the completeness of the audit universe by routinely evaluating the organization's dynamic risk profile.
- **Periodic review of the audit plan.** Review the current audit plan to assess which assignments may be of higher risk. By flagging the higher-risk assignments, management of the internal audit activity has better visibility and may spend more time understanding the approach to the critical assignments.
- **Effective planning.** There is no substitute for effective audit planning. A thorough planning process that includes updating relevant facts about the client and the performance of an effective risk assessment can significantly reduce the risks of audit failure. In addition, understanding the scope of the assignment and the internal audit procedures to be performed are important elements of the planning process, which will reduce the risks of audit failure. Building internal audit activity management checkpoints into the process and obtaining approval of any deviation from the agreed-on plan is also key.
- **Effective audit design.** In most cases, a fair amount of time is spent understanding and analyzing the design of the system of internal controls to determine whether it provides adequate control prior to the start of testing for effectiveness. This provides a firm basis for internal audit comments that address root causes, which sometimes can be the result of poor control design, rather than addressing symptoms. It will also reduce the chance for audit failure by identifying missing controls.
- **Effective management review and escalation procedures.** Internal audit management's involvement in the internal audit process (i.e., before the report draft) plays an important part in mitigating the risk of audit failure. This involvement might include work paper reviews, real-time discussions related to findings, or a closing meeting. By including management of the internal audit activity in the internal audit process, potential issues may be identified and assessed earlier in the assignment. In addition, an internal audit activity may have guidance procedures outlining when and what types of issues to escalate to which level of internal auditing management.
- **Proper resource allocation.** It is important to assign the right staff to each internal audit engagement. It is especially important when planning a higher-risk or a very technical engagement. Making sure the appropriate competencies are available on the team can play a significant role in reducing the risk of audit failure. In addition to the right competencies, it is important to ensure the appropriate level of experience is on the team, including strong project management skills for those leading an internal audit engagement.

6. An internal audit activity may unknowingly provide some level of false assurance. "False assurance" is a level of confidence or assurance based on perceptions or assumptions rather than fact. In many cases, the mere fact that the internal audit activity is involved in a matter may create some level of false assurance.

7. The use of internal audit resources in assisting the organization to identify and evaluate significant exposures to risk needs to be clearly defined for projects other than internal audits. For example, an internal audit activity was asked by a business unit to provide some "resources" to assist with the implementation of a new enterprise-wide computer system. The business unit

deployed these resources to support some of the testing of the new system. Subsequent to the deployment, an error in the design of the system resulted in a restatement of the financial statements. When asked how this happened, the business unit responded by saying that the internal audit activity had been involved in the process and had not identified the matter. Involvement of internal auditors created a level of false assurance that was not consistent with their actual role in the project.

8. While there is no way to mitigate all of the risk of false assurance, an internal audit activity can proactively manage its risk in this area. Frequent and clear communication is a key strategy to manage false assurance. Other leading practices include:

- Proactively communicate the role and the mandate of the internal audit activity to the audit committee, senior management, and other key stakeholders.
- Clearly communicate what is covered in the risk assessment, internal audit plan, and internal audit engagement. Also explicitly communicate what is not in the scope of the risk assessment and internal audit plan.
- Have a "project acceptance" process to assess the level of risk related to each project and internal audit's role in the project. The assessment may consider the scope of the project, the role of the internal audit activity, the reporting expectations, the competencies required, and the independence of internal auditors.

9. If internal auditors are used to augment the staffing of a project or initiative, document their role and scope of their involvement as well as future objectivity and independence issues rather than using internal auditors as "loaned" resources, which may create false assurance. The credible reputation of an internal audit activity is an essential part of its effectiveness. Internal audit activities that are viewed with high regard are able to attract talented professionals and are highly valued by their organizations. Maintaining a strong "brand" is paramount to the internal audit activity's success and ability to contribute to the organization. In most cases, the internal audit activity's brand has been built over several years through consistent, high-quality work. Unfortunately, this brand can be destroyed instantly by one high-profile, adverse event.

10. For example, an internal audit activity could be highly regarded with several of the key financial executives having had rotational assignments as internal auditors, which was viewed as a training ground for future executives. A string of significant restatements and regulatory investigations, however, would impact the reputation of the internal audit activity. The audit committee and the board might ask if the internal audit activity has the right talent and QAIP to support the organization.

11. In another example, during an audit of the human resource function, the internal auditors may discover that background checks were not being reviewed appropriately. The discovery that newly hired internal auditors did not have the appropriate education background, while others had been involved in criminal activity, could seriously impact the credibility of the internal audit activity.

12. Situations like these are not only embarrassing; they also damage the efficacy of the internal audit activity. Protecting the reputation and the brand of the internal audit activity is important not only to the internal audit activity but to the entire organization. It is important that the internal audit activity consider what types of risks it faces that could impact its reputation and develop mitigation strategies to address these risks.

13. Some practices to protect the reputation include:

- Implement a strong QAIP over all processes in the internal audit activity, including human resources and hiring.
- Periodically perform a risk assessment for the internal audit activity to identify potential risks that might impact its brand.

- Reinforce code of conduct and ethical behavior standards, including the IIA's Code of Ethics to internal auditors.
- Ensure that the internal audit activity is in compliance with all applicable company policies and practices.

14. To the extent that an internal audit activity experiences an event outlined above, the CAE needs to review the nature of the event and gain an understanding of the root causes. This analysis provides insight into the potential changes to be considered in the internal audit process or control environment to mitigate future occurrences.

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:

- 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.

Practice Advisory 2130-1: Assessing the Adequacy of Control Processes

1. An organization establishes and maintains effective risk management and control processes. The purpose of control processes is to support the organization in the management of risks and the achievement of its established and communicated objectives. The control processes are expected to ensure, among other things, that:

- Financial and operational information is reliable and possesses integrity.
- Operations are performed efficiently and achieve established objectives.
- Assets are safeguarded.
- Actions and decisions of the organization are in compliance with laws, regulations, and contracts.

2. Senior management's role is to oversee the establishment, administration, and assessment of the system of risk management and control processes. Among the responsibilities of the organization's line managers is the assessment of the control processes in their respective areas. Internal auditors provide varying degrees of assurance about the effectiveness of the risk management and control processes in select activities and functions of the organization.

3. The CAE forms an overall opinion about the adequacy and effectiveness of the control processes. The expression of such an opinion by the CAE will be based on sufficient audit evidence obtained through the completion of audits and, where appropriate, reliance on the work of other assurance providers. The CAE communicates the opinion to senior management and the board.

4. The CAE develops a proposed internal audit plan to obtain sufficient evidence to evaluate the effectiveness of the control processes. The plan includes audit engagements and/or other procedures to obtain sufficient, appropriate audit evidence about all major operating units and business functions to be assessed as well as a review of the major control processes operating across the organization. The plan should be flexible so that adjustments may be made during the year as a result of changes in management strategies, external conditions, major risk areas, or revised expectations about achieving the organization's objectives.

5. The audit plan gives special consideration to those operations most affected by recent or unexpected changes. Changes in circumstances can result, for example, from marketplace or investment conditions, acquisitions and divestitures, organizational restructuring, new systems, and new ventures.

6. In determining the expected audit coverage for the proposed audit plan, the CAE considers relevant work performed by others who provide assurances to senior management (e.g., reliance by the CAE on the work of corporate compliance officers). The CAE's audit plan also considers audit work completed by the external auditor and management's own assessments of its risk management process, controls, and quality improvement processes.

7. The CAE should evaluate the breadth of coverage of the proposed audit plan to determine whether the scope is sufficient to enable the expression of an opinion about the organization's risk management and control processes. The CAE should inform senior management and the board of any gaps in audit coverage that would prevent the expression of an opinion on all aspects of these processes.

8. A key challenge for the internal audit activity is to evaluate the effectiveness of the organization's control processes based on the aggregation of many individual assessments. Those assessments are largely gained from internal audit engagements, reviews of management's self-assessments, and other assurance providers' work. As the engagements progress, internal auditors communicate, on a timely basis, the findings to the appropriate levels of management so prompt action can be taken to correct or mitigate the consequences of discovered control discrepancies or weaknesses.

9. In evaluating the overall effectiveness of the organization's control processes, the CAE considers whether:

- Significant discrepancies or weaknesses were discovered.
- Corrections or improvements were made after the discoveries.
- The discoveries and their potential consequences lead to a conclusion that a pervasive condition exists resulting in an unacceptable level of risk.

10. The existence of a significant discrepancy or weakness does not necessarily lead to the judgment that it is pervasive and poses an unacceptable risk. The internal auditor considers the nature and extent of risk exposure as well as the level of potential consequences in determining whether the effectiveness of the control processes are jeopardized and unacceptable risks exist.

11. The CAE's report on the organization's control processes is normally presented **once a year** to senior management and the board. The report states the critical role played by the control processes in the achievement of the organization's objectives. The report also describes the nature and extent of the work performed by the internal audit activity and the nature and extent of reliance on other assurance providers in formulating the opinion.

Practice Advisory 2130.A1-1: Information Reliability and Integrity

1. Internal auditors determine whether senior management and the board have a clear understanding that information reliability and integrity is a management responsibility. This responsibility includes all critical information of the organization regardless of how the information is stored. Information reliability and integrity includes accuracy, completeness, and security.

2. The CAE determines whether the internal audit activity possesses, or has access to, competent audit resources to evaluate information reliability and integrity and associated risk exposures. This includes both internal and external risk exposures, and exposures relating to the organization's relationships with outside entities.

3. The CAE determines whether information reliability and integrity breaches and conditions that might represent a threat to the organization will promptly be made known to senior management, the board, and the internal audit activity.

4. Internal auditors assess the effectiveness of preventive, detective, and mitigation measures against past attacks, as appropriate, and future attempts or incidents deemed likely to occur. Internal auditors determine whether the board has been appropriately informed of threats, incidents, vulnerabilities exploited, and corrective measures.

5. Internal auditors periodically assess the organization's information reliability and integrity practices and recommend, as appropriate, enhancements to, or implementation of, new controls and safeguards. Such assessments can be either conducted as separate stand-alone engagements or integrated into other audits or engagements conducted as part of the internal audit plan. The nature of the engagement will determine the most appropriate reporting process to senior management and the board.

Practice Advisory 2130-A1-2: Evaluating an Organization's Privacy Framework

1. The failure to protect personal information with appropriate controls can have significant consequences for an organization. The failure could damage the reputation of individuals and/or the organization and expose an organization to risks that include legal liability and diminished consumer and/or employee trust.

2. Privacy definitions vary widely depending on the culture, political environment, and legislative framework of the countries in which the organization operates. Risks associated with the privacy of information encompass personal privacy (physical and psychological); privacy of space (freedom from surveillance); privacy of communication (freedom from monitoring); and privacy of information (collection, use, and disclosure of personal information by others). "Personal information" generally refers to information associated with a specific individual or that has identifying characteristics that, when combined with other information, can then be associated with a specific individual. It can include any factual or subjective information—recorded or not—in any form of media. Personal information can include:

- Name, address, identification numbers, family relationships.
- Employee files, evaluations, comments, social status, or disciplinary actions.
- Credit records, income, financial status.
- Medical status.

3. Effective control over the protection of personal information is an essential component of the governance, risk management, and control processes of an organization. The board is ultimately accountable for identifying the principal risks to the organization and implementing appropriate control processes to mitigate those risks. Doing so includes establishing the necessary privacy framework for the organization and monitoring its implementation.

4. The internal audit activity can contribute to good governance and risk management by assessing the adequacy of management's identification of risks related to its privacy objectives and the adequacy of the controls established to mitigate those risks to an acceptable level. The internal auditor is well positioned to evaluate the privacy framework in his or her organization and identify the significant risks as well as the appropriate recommendations for mitigation.

5. The internal audit activity identifies the types and appropriateness of information gathered by the organization that is deemed personal or private, the collection methodology used, and

whether the organization's use of that information is in accordance with its intended use and applicable legislation.

6. Given the highly technical and legal nature of privacy issues, the internal audit activity needs appropriate knowledge and competence to conduct an assessment of the risks and controls of the organization's privacy framework.

7. In conducting such an evaluation of the management of the organization's privacy framework, the internal auditor:

- Considers the laws, regulations, and policies relating to privacy in the jurisdictions where the organization operates.
- Liaises with in-house legal counsel to determine the exact nature of laws, regulations, and other standards and practices applicable to the organization and the country/countries in which it operates.
- Liaises with IT specialists to determine that information security and data protection controls are in place and regularly reviewed and assessed for appropriateness.
- Considers the level or maturity of the organization's privacy practices. Depending on the level, the internal auditor may have differing roles. The auditor may facilitate the development and implementation of the privacy program, evaluate management's privacy risk assessment to determine the needs and risk exposures of the organization, or provide assurance on the effectiveness of the privacy policies, practices, and controls across the organization. If the internal auditor assumes any responsibility for developing and implementing a privacy program, his or her independence will be impaired.

2200–Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

Practice Advisory 2200-1: Engagement Planning

1. The internal auditor plans and conducts the engagement, with supervisory review and approval. Prior to the engagement's commencement, the internal auditor prepares an engagement program that:

- States the objectives of the engagement.
- Identifies technical requirements, objectives, risks, processes, and transactions that are to be examined.
- States the nature and extent of testing required.
- Documents the internal auditor's procedures for collecting, analyzing, interpreting, and documenting information during the engagement.
- Is modified, as appropriate, during the engagement with the approval of the CAE or his or her designee.

2. The CAE should require a level of formality and documentation (e.g., of the results of planning meetings, risk assessment procedures, level of detail in the work program, etc.) that is appropriate to the organization. Factors to consider would include:

- Whether the work performed and/or the results of the engagement will be relied on by others (e.g., external auditors, regulators, or management).
- Whether the work relates to matters that may be involved in potential or current litigation.

- The experience level of the internal audit staff and the level of direct supervision required.
- Whether the project is staffed internally, by guest auditors, or by external service providers.
- The project's complexity and scope.
- The size of the internal audit activity.
- The value of documentation (e.g., whether it will be used in subsequent years).

3. The internal auditor determines the other engagement requirements, such as the period covered and estimated completion dates. The internal auditor also considers the final engagement communication format. Planning at this stage facilitates the communication process at the engagement's completion.

4. The internal auditor informs those in management who need to know about the engagement, conducts meetings with management responsible for the activity under review, summarizes and distributes the discussions and any conclusions reached from the meetings, and retains the documentation in the engagement working papers. Topics of discussion may include:

- Planned engagement objectives and scope of work.
- The resources and timing of engagement work.
- Key factors affecting business conditions and operations of the areas being reviewed, including recent changes in internal and external environment.
- Concerns or requests from management.

5. The CAE determines how, when, and to whom engagement results will be communicated. The internal auditor documents this and communicates it to management, to the extent deemed appropriate, during the planning phase of the engagement. The internal auditor communicates to management subsequent changes that affect the timing or reporting of engagement results.

Practice Advisory 2200-2: Using a Top-Down, Risk-Based Approach to Identify the Controls to Be Assessed in an Internal Audit Engagement

1. Read this practice advisory in conjunction with *Practice Advisories 2010-2: Using the Risk Management Process in Internal Audit Planning*, *2210-1: Engagement Objectives*, and *2210.A1-1: Risk Assessment in Engagement Planning* and the Practice Guide *GAIT for Business and IT Risk* (*GAIT-R*).

2. This practice advisory assumes that the objectives for the internal audit engagement have been determined and the risks to be addressed have been identified in the internal audit planning process. It provides guidance on the use of a top-down, risk-based approach to identify and include in the internal audit scope (per Standard 2220) the key controls relied on to manage the risks.

3. "Top-down" refers to basing the scope definition on the more significant risks to the organization. This is in contrast to developing the scope based on the risks at a specific location, which may not be significant to the organization as a whole. A top-down approach ensures that internal auditing is focused, as noted in Practice Advisory 2010-2, on "providing assurance on the management of significant risks."

4. A system of internal control typically includes both manual and automated controls. (Note that this applies to controls at every level—entity, business process, and IT general controls—and in every layer of the control framework; e.g., activities in the control environment, monitoring, or risk assessment layers may also be automated.) Both types of controls need to be assessed to determine whether business risks are effectively managed. In particular, the internal auditor needs to assess whether there is an appropriate combination of controls, including those related to IT, to mitigate business risks within organizational tolerances. The internal auditor

needs to consider including procedures to assess and confirm that risk tolerances are current and appropriate.

5. The internal audit scope needs to include all the controls required to provide reasonable assurance that the risks are effectively managed (subject to the comments in paragraph 9 below). These controls are referred to as key controls—those necessary to manage risk associated with a critical business objective. Only the key controls need to be assessed, although the internal auditor can choose to include an assessment of nonkey controls (e.g., redundant, duplicative controls) if there is value to the business in providing such assurance. The internal auditor may also discuss with management whether the nonkey controls are required.

6. Note that where the organization has a mature and effective risk management program, the key controls relied on to manage each risk will have been identified. In these cases, the internal auditor needs to assess whether management's identification and assessment of the key controls is adequate.

7. The key controls can be in the form of:

- Entity-level controls (e.g., employees are trained and take a test to confirm their understanding of the code of conduct). The entity-level controls may be manual, fully automated, or partly automated.
- Manual controls within a business process (e.g., the performance of a physical inventory).
- Fully automated controls within a business process (e.g., matching or updating accounts in the general ledger).
- Partly automated controls within a business process (also called hybrid or IT-dependent controls), where an otherwise manual control relies on application functionality, such as an exception report. If an error in that functionality would not be detected, the entire control could be ineffective. For example, a key control to detect duplicate payments might include the review of a system-generated report. The manual part of the control would not ensure that the report is complete. Therefore, the application functionality that generated the report should be in scope.

The internal auditor may use other methods or frameworks, as long as all the key controls relied on to manage the risks are identified and assessed, including manual controls, automated controls, and controls within IT general control processes.

8. Fully and partly automated controls—whether at the entity level or within a business process—generally rely on the proper design and effective operation of IT general controls. *GAIT-R* discusses the recommended process for identifying key IT general controls.

9. The assessment of key controls may be performed in a single, integrated internal audit engagement or in a combination of internal audit engagements. For example, one internal audit engagement may address the key controls performed by business process users, while another covers the key IT general controls, and a third assesses related controls that operate at the entity level. This is common where the same controls (especially those at the entity level or within IT general controls) are relied on for more than one risk area.

10. As noted in paragraph 5, before providing an opinion on the effective management of the risks covered by the internal audit scope, it is necessary to assess the combination of all key controls. Even if multiple internal audit engagements are performed, each addressing some key controls, the internal auditor needs to include in the scope of at least one internal audit engagement an assessment of the design of the key controls as a whole (i.e., across all the related internal audit engagements) and whether it is sufficient to manage risks within organizational tolerances.

11. If the internal audit scope (considering other internal audit engagements as discussed in paragraph 9) includes some, but not all, key controls required to manage the targeted risks, a scope limitation should be considered and clearly communicated in the internal audit notification and final report.

2201–Planning Considerations

In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity, its objectives, resources, and operations, and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model.
- The opportunities for making significant improvements to the activity's risk management and control processes.

2201.A1–When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

2201.C1–Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

No Practice Advisory for Standard 2201

2210–Engagement Objectives

Objectives must be established for each engagement.

2210.A1–Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

2210.A2–Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

2210.A3–Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.

2210.C1–Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed on with the client.

2210.C2–Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

Practice Advisory 2210-1: Engagement Objectives

1. Internal auditors establish engagement objectives to address the risks associated with the activity under review. For planned engagements, the objectives proceed and align to those initially identified during the risk assessment process from which the internal audit plan is derived. For unplanned engagements, the objectives are established prior to the start of the engagement and are designed to address the specific issue that prompted the engagement.

2. The risk assessment during the engagement's planning phase is used to further define the initial objectives and identify other significant areas of concern.

3. After identifying the risks, the auditor determines the procedures to be performed and the scope (nature, timing, and extent) of those procedures. Engagement procedures performed in appropriate scope are the means to derive conclusions related to the engagement objectives.

Practice Advisory 2210.A1-1: Risk Assessment in Engagement Planning

1. Internal auditors consider management's assessment of risks relevant to the activity under review. The internal auditor also considers:

- The reliability of management's assessment of risk.
- Management's process for monitoring, reporting, and resolving risk and control issues.
- Management's reporting of events that exceeded the limits of the organization's risk appetite and management's response to those reports.
- Risks in related activities relevant to the activity under review.

2. Internal auditors obtain or update background information about the activities to be reviewed to determine the impact on the engagement objectives and scope.

3. If appropriate, internal auditors conduct a survey to become familiar with the activities, risks, and controls to identify areas for engagement emphasis and to invite comments and suggestions from engagement clients.

4. Internal auditors summarize the results from the reviews of management's assessment of risk, the background information, and any survey work. The summary includes:

- Significant engagement issues and reasons for pursuing them in more depth.
- Engagement objectives and procedures.
- Methodologies to be used, such as technology-based audit and sampling techniques.
- Potential critical control points, control deficiencies, and/or excess controls.
- When applicable, reasons for not continuing the engagement or for significantly modifying engagement objectives.

2220–Engagement Scope

The established scope must be sufficient to satisfy the objectives of the engagement.

2220.A1–The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

2220.A2–If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

2220.C1–In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-on objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

2220.C2–During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

No Practice Advisory for Standard 2220

2230–Engagement Resource Allocation

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

Practice Advisory 2230-1: Engagement Resource Allocation

1. Internal auditors consider the following when determining the appropriateness and sufficiency of resources:

- The number and experience level of the internal audit staff.
- Knowledge, skills, and other competencies of the internal audit staff when selecting internal auditors for the engagement.
- Availability of external resources where additional knowledge and competencies are required.
- Training needs of internal auditors as each engagement assignment serves as a basis for meeting the internal audit activity's developmental needs.

2240–Engagement Work Program

Internal auditors must develop and document work programs that achieve the engagement objectives.

2240.A1–Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

2240.C1–Work programs for consulting engagements may vary in form and content, depending on the nature of the engagement.

Practice Advisory 2240-1: Engagement Work Program

1. Internal auditors develop and obtain documented approval of work programs before commencing the internal audit engagement. The work program includes methodologies to be used, such as technology-based audit and sampling techniques.

2. The process of collecting, analyzing, interpreting, and documenting information is to be supervised to provide reasonable assurance that engagement objectives are met and that the internal auditor's objectivity is maintained.

2300–Performing the Engagement

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

Practice Advisory 2300-1: Use of Personal Information in Conducting Engagements

1. Internal auditors need to consider concerns relating to the protection of personally identifiable information gathered during audit engagements as advances in IT and communications continue to present privacy risks and threats. Privacy controls are legal requirements in many jurisdictions.

2. "Personal information" generally refers to data associated with a specific individual or data that have identifying characteristics that may be combined with other information. It includes any factual or subjective information, recorded or not, in any form or media. Personal information includes:

- Name, address, identification numbers, income, blood type.
- Evaluations, social status, disciplinary actions.
- Employee files and credit and loan records.
- Employee health and medical data.

3. In many jurisdictions, laws require organizations to identify the purposes for which personal information is collected at or before the time of collection. These laws also prohibit using and disclosing personal information for purposes other than those for which it was collected except with the individual's consent or as required by law.

4. It is important that internal auditors understand and comply with all laws regarding the use of personal information in their jurisdiction and in those jurisdictions where their organizations conduct business.

5. It may be inappropriate, and in some cases illegal, to access, retrieve, review, manipulate, or use personal information in conducting certain internal audit engagements. If the internal auditor accesses personal information, it may be necessary to develop procedures to safeguard this information. For example, the internal auditor may decide not to record personal information in engagement records in some situations.

6. The internal auditor may seek advice from legal counsel before beginning audit work if there are questions or concerns about access to personal information.

2310–Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Interpretation: *Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Reliable information is the best attainable information through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organization meet its goals.*

No Practice Advisory for Standard 2310

2320–Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

Practice Advisory 2320-1: Analytical Procedures

1. Internal auditors may use analytical procedures to obtain audit evidence. Analytical procedures involve studying and comparing relationships among both financial and nonfinancial information. The application of analytical procedures is based on the premise that, in the absence of known conditions to the contrary, relationships among information may reasonably be expected to exist and continue. Examples of contrary conditions include unusual or nonrecurring transactions or events; accounting, organizational, operational, environmental, and technological changes; inefficiencies; ineffectiveness; errors; fraud; or illegal acts.

2. Analytical procedures often provide the internal auditor with an efficient and effective means of obtaining evidence. The assessment results from comparing information with expectations identified or developed by the internal auditor. Analytical procedures are useful in identifying:

- Unexpected differences.
- The absence of differences when they are expected.
- Potential errors.
- Potential fraud or illegal acts.
- Other unusual or nonrecurring transactions or events.

3. Analytical audit procedures include:

- Comparing current period information with expectations based on similar information for prior periods as well as budgets or forecasts.
- Studying relationships between financial and appropriate nonfinancial information (e.g., recorded payroll expense compared to changes in average number of employees).
- Studying relationships among elements of information (e.g., fluctuation in recorded interest expense compared to changes in related debt balances).
- Comparing information with expectations based on similar information for other organizational units as well as for the industry in which the organization operates.

4. Internal auditors may perform analytical procedures using monetary amounts, physical quantities, ratios, or percentages. Specific analytical procedures include ratio, trend, and regression analysis; reasonableness tests; period-to-period comparisons; comparisons with budgets; forecasts; and external economic information. Analytical procedures assist internal auditors in identifying conditions that may require additional audit procedures. An internal auditor uses analytical procedures in planning the engagement in accordance with the guidelines contained in Standard 2200.

5. Internal auditors may use analytical procedures to generate evidence during the audit engagement. When determining the extent of analytical procedures, the internal auditor considers the:

- Significance of the area being audited.
- Assessment of risk management in the area being audited.
- Adequacy of the internal control system.
- Availability and reliability of financial and nonfinancial information.

- Precision with which the results of analytical audit procedures can be predicted.
- Availability and comparability of information regarding the industry in which the organization operates.
- Extent to which other procedures provide evidence.

6. When analytical audit procedures identify unexpected results or relationships, the internal auditor evaluates such results or relationships. This evaluation includes determining whether the difference from expectations could be a result of fraud, error, or a change in conditions. The auditor may ask management about the reasons for the difference and would corroborate management's explanation, for example, by modifying expectations and recalculating the difference or by applying other audit procedures. In particular, the internal auditor needs to be satisfied that the explanation considers both the direction of the change (e.g., sales decreased) and the amount of the difference (e.g., sales decreased by 10%). Unexplained results or relationships from applying analytical procedures may be indicative of a significant problem (e.g., a potential error, fraud, or illegal act). Results or relationships that are not adequately explained may indicate a situation to be communicated to senior management and the board in accordance with Standard 2060. Depending on the circumstances, the internal auditor may recommend appropriate action.

2330–Documenting Information

Internal auditors must document relevant information to support the conclusions and engagement results.

2330.A1–The CAE must control access to engagement records. The CAE must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

2330.A2–The CAE must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2330.C1–The CAE must develop policies governing the custody and retention of consulting engagement records as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

Practice Advisory 2330-1: Documenting Information

1. Internal auditors prepare working papers. Working papers document the information obtained, the analyses made, and the support for the conclusions and engagement results. Internal audit management reviews the prepared working papers.

2. Engagement working papers generally:

- Aid in the planning, performance, and review of engagements.
- Provide the principal support for engagement results.
- Document whether engagement objectives were achieved.
- Support the accuracy and completeness of the work performed.
- Provide a basis for the internal audit activity's QAIP.
- Facilitate third-party reviews.

3. The organization, design, and content of engagement working papers depend on the engagement's nature and objectives and the organization's needs. Engagement working papers document all aspects of the engagement process from planning to communicating results. The internal audit activity determines the media used to document and store working papers.

4. The CAE establishes working paper policies for the various types of engagements performed. Standardized engagement working papers, such as questionnaires and audit programs, may improve the engagement's efficiency and facilitate the delegation of engagement work. Engagement working papers may be categorized as permanent or carry-forward engagement files that contain information of continuing importance.

Practice Advisory 2330.A1-1: Control of Engagement Records

1. Internal audit engagement records include reports, supporting documentation, review notes, and correspondence, regardless of storage media. Engagement records or working papers are the property of the organization. The internal audit activity controls engagement working papers and provides access to authorized personnel only.

2. Internal auditors may educate management and the board about access to engagement records by external parties. Policies relating to access to engagement records, handling of access requests, and procedures to be followed when an engagement warrants an investigation need to be reviewed by the board.

3. Internal audit policies explain who in the organization is responsible for ensuring the control and security of the activity's records, which internal or external parties can be granted access to engagement records, and how requests for access to those records need to be handled. These policies will vary depending on the nature of the organization, practices followed in the industry, and access privileges established by law.

4. Management and other members of the organization may request access to all or specific engagement working papers. Such access may be necessary to substantiate or explain engagement observations and recommendations or for other business purposes. The CAE approves these requests.

5. The CAE approves access to engagement working papers by external auditors.

6. There are circumstances in which parties outside the organization, other than external auditors, request access to engagement working papers and reports. Prior to releasing the documentation, the CAE obtains the approval of senior management and/or legal counsel, as appropriate.

7. Potentially, internal audit records that are not specifically protected may be accessed in legal proceedings. Legal requirements vary significantly in different jurisdictions. When there is a specific request for engagement records in relation to a legal proceeding, the CAE works closely with legal counsel in deciding what to provide.

Practice Advisory 2330.A1-2: Granting Access to Engagement Records

Caution: Internal auditors are encouraged to consult legal counsel in matters involving legal issues as requirements may vary significantly in different jurisdictions. The guidance contained in this Practice Advisory is based primarily on the legal systems that protect information and work performed for, or communicated to, an engaged attorney (i.e., attorney–client privilege), such as the legal system in the United States of America. Practice Advisory 2400-1 discusses attorney–client privilege.

1. Internal audit engagement records include reports, supporting documentation, review notes, and correspondence, regardless of storage media. Engagement records are generally produced under the presumption that their contents are confidential and may contain a mix of facts and opinions. However, those who are not familiar with the organization or its internal audit process may misunderstand those facts and opinions. Outside parties may seek access to engagement

records in different types of proceedings, including criminal prosecutions, civil litigation, tax audits, regulatory reviews, government contract reviews, and reviews by self-regulatory organizations. Most of an organization's records that are not protected by the attorney–client privilege may be accessible in criminal proceedings. In noncriminal proceedings, the issue of access is less clear and may vary according to the jurisdiction of the organization.

2. Explicit practices of the internal audit activity may increase the control of access to engagement records.

3. The internal audit activity may address access to, and control of, internal audit records regardless of the media used for storage.

4. The internal audit activity's policies should cover what to include in engagement records and specify the content and format of the engagement records and how internal auditors handle resolved review notes. The policies also should specify how long internal audit records are to be retained. The CAE, when specifying the length of retention for engagement records, should consider the organization's needs as well as legal requirements.

5. The internal audit activity's policies may document who in the organization is responsible for the control and security of internal audit records, who can be granted access to engagement records, and how requests for access to those records are to be handled. These policies depend on the practices followed in the organization's industry or legal jurisdiction. The CAE should be aware of changing practices in the industry and changing legal precedents. When developing policies, the CAE should consider who may seek access to internal audit records.

6. The policy granting access to engagement records may also address processes:

- For resolving access issues.
- For educating the internal audit staff concerning the risks and issues regarding access to their work products.
- To determine who may seek access to the work product in the future.

7. The CAE also may educate senior management and the board about the risks of access to engagement records. The board may review policies relating to who can be granted access to engagement records and how those requests are to be handled. The specific policies will vary depending on the nature of the organization and the access privileges that have been established by law.

8. When furnishing engagement records, the CAE usually:

- Provides only the specific documents as directed by legal counsel or policies. These usually exclude documents covered by attorney–client privilege. Documents that reveal attorneys' thought processes or strategies will usually be privileged and not subject to forced disclosure.
- Releases documents in a form where they cannot be changed (e.g., as an image rather than in word processing format). For paper documents, the CAE releases copies and keeps the originals.
- Labels each document as confidential and places a notation that secondary distribution is not permitted without permission.

Practice Advisory 2330.A2-1: Retention of Records

1. Engagement record retention requirements vary among jurisdictions and legal environments.

2. The CAE develops a written retention policy that meets organizational needs and legal requirements of the jurisdictions within which the organization operates.

3. The record retention policy needs to include appropriate arrangements for the retention of records related to engagements performed by external service providers.

2340–Engagement Supervision

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

Interpretation: *The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The CAE has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.*

Practice Advisory 2340-1: Engagement Supervision

1. The CAE or designee provides appropriate engagement supervision. Supervision is a process that begins with planning and continues throughout the engagement. The process includes:

- Ensuring that designated auditors collectively possess the required knowledge, skills, and other competencies to perform the engagement.
- Providing appropriate instructions during the planning of the engagement and approving the engagement program.
- Ensuring that the approved engagement program is completed unless changes are justified and authorized.
- Determining that engagement working papers adequately support engagement observations, conclusions, and recommendations.
- Ensuring that engagement communications are accurate, objective, clear, concise, constructive, and timely.
- Ensuring that engagement objectives are met.
- Providing opportunities for developing internal auditors' knowledge, skills, and other competencies.

2. The CAE is responsible for all internal audit engagements, whether performed by or for the internal audit activity, and all significant professional judgments made throughout the engagement. The CAE also adopts suitable means to ensure this responsibility is met. "Suitable" means include policies and procedures designed to:

- Minimize the risk that internal auditors or others performing work for the internal audit activity make professional judgments or take other actions that are inconsistent with the CAE's professional judgment such that the engagement is impacted adversely.
- Resolve differences in professional judgment between the CAE and internal audit staff over significant issues relating to the engagement. Such means may include discussion of pertinent facts, further inquiry or research, and documentation and disposition of the differing viewpoints in engagement working papers. In instances of a difference in professional judgment over an ethical issue, suitable means may include referral of the issue to those individuals in the organization having responsibility over ethical matters.

3. All engagement working papers are reviewed to ensure they support engagement communications and necessary audit procedures are performed. Evidence of supervisory review consists of the reviewer initialing and dating each working paper after it is reviewed. Other techniques that

provide evidence of supervisory review include completing an engagement working paper review checklist; preparing a memorandum specifying the nature, extent, and results of the review; or evaluating and accepting reviews within the working paper software.

4. Reviewers can make a written record (i.e., review notes) of questions arising from the review process. When clearing review notes, care needs to be taken to ensure working papers provide adequate evidence that questions raised during the review are resolved. Alternatives with respect to disposition of review notes are to:

- Retain the review notes as a record of the reviewer's questions raised, the steps taken in their resolution, and the results of those steps.
- Discard the review notes after the questions raised are resolved and the appropriate engagement working papers are amended to provide the information requested.

5. Engagement supervision also allows for training and development of staff and performance evaluation.

2400–Communicating Results

Internal auditors must communicate the results of engagements.

Practice Advisory 2400-1: Legal Considerations in Communicating Results

Caution: Internal auditors are encouraged to consult legal counsel in matters involving legal issues as requirements may vary significantly in different jurisdictions. The guidance contained in this Practice Advisory is based primarily on the legal systems that protect information and work performed for, or communicated to, an engaged attorney (i.e., attorney–client privilege), such as the legal system in the United States of America. Practice Advisory 2400-1 discusses attorney–client privilege.

1. The internal auditor needs to exercise caution when communicating noncompliance with laws, regulations, and other legal issues. Developing policies and procedures regarding the handling of those matters as well as a close working relationship with other appropriate areas (e.g., legal counsel and compliance) is strongly encouraged.

2. The internal auditor gathers evidence, makes analytical judgments, reports results, and determines whether management has taken appropriate corrective action. The internal auditor's need to prepare engagement records may conflict with legal counsel's desire to not leave discoverable evidence that could harm the organization's position in legal matters. For example, even if an internal auditor gathers and evaluates information properly, the facts and analyses disclosed may negatively impact the organization from a legal perspective. Proper planning and policy making—including role definition and methods of communication—are essential so that a sudden revelation does not place the internal auditor and legal counsel at odds with one another. Both parties need to foster an ethical and preventive perspective throughout the organization by sensitizing and educating management about the established policies.

3. A communication made between "privileged persons"—in confidence and for the purpose of seeking, obtaining, or providing legal assistance for the client—is necessary to protect the attorney–client privilege. This privilege, which is primarily used to protect communications with attorneys, can also apply to communications with third parties working with an attorney.

4. Some courts have recognized a privilege of critical self-analysis that shields self-critical materials (e.g., audit work products) from discovery. In general, the recognition of this privilege is premised on the belief that the confidentiality of the self-analysis in these instances outweighs the valued public interest.

5. Privilege usually applies when:

- The information results from a self-critical analysis undertaken by the party asserting the privilege.
- The public has a strong interest in preserving the free flow of the information contained in the critical analysis.
- The information is of the type whose flow would be curtailed if discovery were allowed.

6. Self-evaluative privileges are less likely to be available when a government agency—rather than a party involved in a private legal matter—seeks out the documents. Presumably this reluctance results from recognition of the government's stronger interest in enforcing the law.

7. Documents intended to be protected under the work-product doctrine usually need to be:

- Some type of work product (e.g., memo and computer program).
- Prepared in anticipation of litigation.
- Completed by someone working at the direction of an attorney.

8. Documents prepared and delivered to the attorney before the attorney–client relationship is established are not generally protected by the attorney–client privilege.

2410–Criteria for Communicating

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

> **2410.A1**–Final communication of engagement results must, where appropriate, contain the internal auditors' opinion and/or conclusions. When issued, an opinion or conclusion must take account of the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

Interpretation: *Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the engagement results and their significance.*

> **2410.A2**–Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.
>
> **2410.A3**–When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.
>
> **2410.C1**–Communication of the progress and results of consulting engagements will vary in form and content depending on the nature of the engagement and the needs of the client.

Practice Advisory 2410-1: Communication Criteria

1. Although the format and content of the final engagement communications varies by organization or type of engagement, they are to contain, at a minimum, the purpose, scope, and results of the engagement.

2. Final engagement communications may include background information and summaries. Background information may identify the organizational units and activities reviewed and

provide explanatory information. It may also include the status of observations, conclusions, and recommendations from prior reports and an indication of whether the report covers a scheduled engagement or is responding to a request. Summaries are balanced representations of the communication's content.

3. Purpose statements describe the engagement objectives and may inform the reader why the engagement was conducted and what it was expected to achieve.

4. Scope statements identify the audited activities and may include supportive information such as time period reviewed and related activities not reviewed to delineate the boundaries of the engagement. They may describe the nature and extent of engagement work performed.

5. Results include observations, conclusions, opinions, recommendations, and action plans.

6. Observations are pertinent statements of fact. The internal auditor communicates those observations necessary to support or prevent misunderstanding of his or her conclusions and recommendations. The internal auditor may communicate less significant observations or recommendations informally.

7. Engagement observations and recommendations emerge by a process of comparing criteria (the correct state) with condition (the current state). Whether there is a difference or not, the internal auditor has a foundation on which to build the report. When conditions meet the criteria, communication of satisfactory performance may be appropriate. Observations and recommendations are based on the following attributes:

- **Criteria.** The standards, measures, or expectations used in making an evaluation and/or verification (the correct state).
- **Condition.** The factual evidence that the internal auditor found in the course of the examination (the current state).
- **Cause.** The reason for the difference between expected and actual conditions.
- **Effect.** The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the impact of the difference). In determining the degree of risk or exposure, internal auditors consider the effect their engagement observations and recommendations may have on the organization's operations and financial statements.

Observations and recommendations can include engagement client accomplishments, related issues, and supportive information.

8. Conclusions and opinions are the internal auditor's evaluations of the effects of the observations and recommendations on the activities reviewed. They usually put the observations and recommendations in perspective based on their overall implications. Clearly identify any engagement conclusions in the engagement report. Conclusions may encompass the entire scope of an engagement or specific aspects. They may cover, but are not limited to, whether operating or program objectives and goals conform to those of the organization, whether the organization's objectives and goals are being met, and whether the activity under review is functioning as intended. An opinion may include an overall assessment of controls or may be limited to specific controls or aspects of the engagement.

9. The internal auditor may communicate recommendations for improvements, acknowledgments of satisfactory performance, and corrective actions. Recommendations are based on the internal auditor's observations and conclusions. They call for action to correct existing conditions or improve operations and may suggest approaches to correcting or enhancing performance as a guide for management in achieving desired results. Recommendations can be general or specific. For example, under some circumstances, the internal auditor may recommend a general course of

action and specific suggestions for implementation. In other circumstances, the internal auditor may suggest further investigation or study.

10. The internal auditor may communicate engagement client accomplishments, in terms of improvements since the last engagement or the establishment of a well-controlled operation. This information may be necessary to fairly present the existing conditions and to provide perspective and balance to the engagement final communications.

11. The internal auditor may communicate the engagement client's views about the internal auditor's conclusions, opinions, or recommendations.

12. As part of the internal auditor's discussions with the engagement client, the internal auditor obtains agreement on the results of the engagement and on any necessary plan of action to improve operations. If the internal auditor and engagement client disagree about the engagement results, the engagement communications state both positions and the reasons for the disagreement. The engagement client's written comments may be included as an appendix to the engagement report, in the body of the report, or in a cover letter.

13. Certain information is not appropriate for disclosure to all report recipients because it is privileged, proprietary, or related to improper or illegal acts. Disclose such information in a separate report. Distribute the report to the board if the conditions being reported involve senior management.

14. Interim reports are written or oral and may be transmitted formally or informally. Use interim reports to communicate information that requires immediate attention, to communicate a change in engagement scope for the activity under review, or to keep management informed of engagement progress when engagements extend over a long period. The use of interim reports does not diminish or eliminate the need for a final report.

15. A signed report is issued after the engagement's completion. Summary reports highlighting engagement results are appropriate for levels of management above the engagement client and can be issued separately from or in conjunction with the final report. The term "signed" means the authorized internal auditor's name is manually or electronically signed in the report or on a cover letter. The CAE determines which internal auditor is authorized to sign the report. If engagement reports are distributed by electronic means, a signed version of the report is kept on file by the internal audit activity.

2420–Quality of Communications

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

Interpretation: *Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.*

Practice Advisory 2420-1: Quality of Communications

1. Gather, evaluate, and summarize data and evidence with care and precision.

2. Derive and express observations, conclusions, and recommendations without prejudice, partisanship, personal interests, and the undue influence of others.

3. Improve clarity by avoiding unnecessary technical language and providing all significant and relevant information in context.
4. Develop communications with the objective of making each element meaningful but succinct.
5. Adopt a useful, positive, and well-meaning content and tone that focuses on the organization's objectives.
6. Ensure communication is consistent with the organization's style and culture.
7. Plan the timing of the presentation of engagement results to avoid undue delay.

2421–Errors and Omissions

If a final communication contains a significant error or omission, the CAE must communicate corrected information to all parties who received the original communication.

No Practice Advisory for Standard 2421

2430–Use of "Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*"

Internal auditors may report that their engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*" only if the results of the QAIP support the statement.

No Practice Advisory for Standard 2430

2431–Engagement Disclosure of Nonconformance

When nonconformance with the definition of internal auditing, the Code of Ethics, or the *Standards* impacts a specific engagement, communication of the results must disclose the:

- Principle or rule of conduct of the Code of Ethics or *Standard(s)* with which full conformance was not achieved.
- Reason(s) for nonconformance.
- Impact of nonconformance on the engagement and the communicated engagement results.

No Practice Advisory for Standard 2431

2440–Disseminating Results

The CAE must communicate results to the appropriate parties.

Interpretation: *The CAE or designee reviews and approves the final engagement communication before issuance and decides to whom and how it will be disseminated.*

2440.A1–The CAE is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2–If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization, the CAE must:

- Assess the potential risk to the organization.
- Consult with senior management and/or legal counsel as appropriate.
- Control dissemination by restricting the use of the results.

2440.C1–The CAE is responsible for communicating the final results of consulting engagements to clients.

2440.C2–During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

Practice Advisory 2440-1: Disseminating Results

1. Internal auditors discuss conclusions and recommendations with appropriate levels of management before the CAE issues the final engagement communications. This is usually accomplished during the course of the engagement and/or at postengagement meetings (i.e., exit meetings).
2. Another technique is for the management of the audited activity to review draft engagement issues, observations, and recommendations. These discussions and reviews help avoid misunderstandings or misinterpretations of fact by providing the opportunity for the engagement client to clarify specific items and express views about the observations, conclusions, and recommendations.
3. The level of participants in the discussions and reviews varies by organization and nature of the report; they generally include those individuals who are knowledgeable regarding detailed operations and those who can authorize the implementation of corrective action.
4. The CAE distributes the final engagement communication to the management of the audited activity and to those members of the organization who can ensure engagement results are given due consideration and take corrective action or ensure that corrective action is taken. Where appropriate, the CAE may send a summary communication to higher-level members in the organization. Where required by the internal audit charter or organizational policy, the CAE also communicates to other interested or affected parties such as external auditors and the board.

Practice Advisory 2440-2: Communicating Sensitive Information Within and Outside the Chain of Command

1. Internal auditors often come into possession of critically sensitive information that is substantial to the organization and poses significant potential consequences. This information may relate to exposures, threats, uncertainties, fraud, waste and mismanagement, illegal activities, abuse of power, misconduct that endangers public health or safety, or other wrongdoings. Furthermore, these matters may adversely impact the organization's reputation, image, competitiveness, success, viability, market values, investments and intangible assets, or earnings.
2. Once the internal auditor has deemed the new information substantial and credible, he or she would normally communicate the information—in a timely manner—to senior management and the board in accordance with Standard 2060 and Practice Advisory 2060-1. This communication typically would follow the normal chain of command for the internal auditor.
3. If the CAE, after those discussions, concludes that senior management is exposing the organization to an unacceptable risk and is not taking appropriate action, he or she needs to present the information and the differences of opinion to the board in accordance with Standard 2600.

4. The typical chain-of-command communication scenario may be accelerated for certain types of sensitive occurrences because of laws, regulations, or common practices. For example, in the case of evidence of fraudulent financial reporting by an organization with publicly traded securities, local regulations may prescribe that the board be immediately informed of the circumstances surrounding the possibility of misleading financial reports even though senior management and the CAE may agree on which actions need to be taken. Laws and regulations in some jurisdictions specify that the board should be informed of discoveries of criminal, securities, food, drugs, or pollution laws violations as well as other illegal acts, such as bribery or improper payments to government officials or to suppliers or customers.

5. In some situations, an internal auditor may face the dilemma of considering whether to communicate the information to persons outside the normal chain of command or even outside the organization. This communication is commonly referred to as whistleblowing. The act of disclosing adverse information to someone within the organization but outside the internal auditor's normal chain of command is considered internal whistleblowing, while disclosing adverse information to a government agency or other authority outside the organization is considered external whistleblowing.

6. Most whistleblowers disclose sensitive information internally, even if outside the normal chain of command, if they trust the organization's policies and mechanisms to investigate allegations of illegal or other improper activity and to take appropriate action. However, some persons possessing sensitive information may decide to take the information outside the organization if they fear retribution from their employer or fellow employees, doubt that the issue will be properly investigated, believe that it will be concealed, or possess evidence about an illegal or improper activity that jeopardizes the health, safety, or well-being of people in the organization or community.

7. In a case where internal whistleblowing is elected as an option, an internal auditor must evaluate alternative ways of communicating the risk he or she sees to persons or groups outside the normal chain of command. Because of risks and ramifications associated with these approaches, the internal auditor needs to proceed with caution in evaluating the evidence and reasonableness of his or her conclusions as well as in examining the merits and disadvantages of each potential action. Taking this action may be appropriate if it will result in responsible action by persons in senior management or the board.

8. Many jurisdictions have laws or regulations requiring public servants with knowledge of illegal or unethical acts to inform an inspector general, other public official, or ombudsman. Some laws pertaining to whistleblowing actions protect citizens if they come forward to disclose specific types of improper activities. The activities listed in these laws and regulations include:

- Criminal offenses and other failures to comply with legal obligations.
- Acts that are considered miscarriages of justice.
- Acts that endanger the health, safety, or well-being of individuals.
- Acts that damage the environment.
- Activities that conceal or cover up any of the above activities.

Some jurisdictions offer no guidance or protection or offer protection only to public (i.e., government) employees.

9. The internal auditor should be aware of the laws and regulations of the various jurisdictions in which the organization operates. Legal counsel familiar with the legal aspects of whistleblowing can assist internal auditors confronted with this issue. The internal auditor should always obtain legal advice if he or she is uncertain of the legal requirements or consequences of engaging in internal or external whistleblowing.

10. Many professional associations hold their members accountable for disclosing illegal or unethical activities. A distinguishing mark of a profession is its acceptance of broad responsibilities to the public and its protection of the general welfare. In addition to examining the legal requirements, IIA members and all certified internal auditors must follow the requirements presented in the IIA's Code of Ethics.

11. An internal auditor has a professional duty and an ethical responsibility to carefully evaluate all evidence and the reasonableness of his or her conclusions and decide whether further actions are needed to protect the organization's interests and stakeholders, the outside community, or the institutions of society. Also, the auditor will need to consider the duty of confidentiality imposed by the IIA's Code of Ethics to respect the value and ownership of information and avoid disclosing it without appropriate authority unless there is a legal or professional obligation to do so. During this evaluation process, the auditor may seek the advice of legal counsel and, if appropriate, other experts. Those discussions may be helpful in providing a different perspective on the circumstances as well as offering opinions about the potential impact and consequences of possible actions. The manner in which the internal auditor seeks to resolve this type of complex and sensitive situation may lead to reprisals and potential liability.

12. Ultimately, the internal auditor makes a professional decision about his or her obligations to the employer. The decision to communicate outside the normal chain of command needs to be based on a well-informed opinion that the wrongdoing is supported by substantial, credible evidence and that a legal or regulatory imperative, or a professional or ethical obligation, requires further action.

Practice Advisory 2440.A2-1: Communications Outside the Organization

1. The internal audit activity's charter, the board's charter, organizational policies, or the engagement agreement may contain guidance related to reporting information outside the organization. If such guidance does not exist, the CAE may facilitate adoption of appropriate policies that may include:

- Authorization required for reporting information outside the organization.
- Process for seeking approval to report information outside the organization.
- Guidelines for permissible and nonpermissible information that may be reported.
- Outside persons authorized to receive information and the types of information they may receive.
- Related privacy regulations, regulatory requirements, and legal considerations for reporting information outside the organization.
- Nature of assurances, advice, recommendations, opinions, guidance, and other information that may be included in communicating information outside the organization.

2. Requests can relate to information that already exists (e.g., a previously issued internal audit report) as well as for information to be created or determined, which results in a new internal audit engagement or report. If the request relates to information or a report that already exists, the internal auditor needs to determine whether it is suitable for dissemination outside the organization.

3. In certain situations, it may be possible to create a special-purpose report based on an existing report or information to make the report suitable for dissemination outside the organization.

4. Some matters to consider when reporting information outside the organization include:

- Usefulness of a written agreement with the intended recipient concerning the information to be reported and the internal auditor's responsibilities.

- Identification of information providers, sources, report signers, recipients, and related persons to the disseminated report or information.
- Identification of objectives, scope, and procedures to be performed in generating applicable information.
- Nature of report or other communication, including opinions, inclusion or exclusion of recommendations, disclaimers, limitations, and type of assurance or assertions to be provided.
- Copyright issues, intended use of the information, and limitations on further distribution or sharing of the information.

5. If the internal auditor discovers information reportable to senior management or the board while conducting engagements that require dissemination of information outside the organization, the CAE needs to provide suitable communication to the board.

2450–Overall Opinions. When an overall opinion is issued, it must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

Interpretation: *The communication will identify:*

- *The scope, including the time period to which the opinion pertains.*
- *Scope limitations.*
- *Consideration of all related projects including the reliance on other assurance providers.*
- *The risk or control framework or other criteria used as a basis for the overall opinion.*
- *The overall opinion, judgment, or conclusion reached.*

The reasons for an unfavorable overall opinion must be stated.

No Practice Advisory for Standard 2450

2500–Monitoring Progress

The CAE must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1–The CAE must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1–The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

Practice Advisory 2500-1: Monitoring Progress

1. To effectively monitor the disposition of results, the CAE establishes procedures to include:
   - The time frame within which management's response to the engagement observations and recommendations is required.
   - Evaluation of management's response.

- Verification of the response (if appropriate).
- Performance of a follow-up engagement (if appropriate).
- A communications process that escalates unsatisfactory responses/actions, including the assumption of risk, to the appropriate levels of senior management or the board.

2. If certain reported observations and recommendations are significant enough to require immediate action by management or the board, the internal audit activity monitors actions taken until the observation is corrected or the recommendation implemented.

3. The internal audit activity may effectively monitor progress by:

- Addressing engagement observations and recommendations to appropriate levels of management responsible for taking action.
- Receiving and evaluating management responses and proposed action plan to engagement observations and recommendations during the engagement or within a reasonable time period after the engagement results are communicated. Responses are more useful if they include sufficient information for the CAE to evaluate the adequacy and timeliness of proposed actions.
- Receiving periodic updates from management to evaluate the status of its efforts to correct observations and/or implement recommendations.
- Receiving and evaluating information from other organizational units assigned responsibility for follow-up or corrective actions.
- Reporting to senior management and/or the board on the status of responses to engagement observations and recommendations.

Practice Advisory 2500.A1-1: Follow-up Process

1. Internal auditors determine whether management has taken action or implemented the recommendation. The internal auditor determines whether the desired results were achieved or if senior management or the board has assumed the risk of not taking action or implementing the recommendation.

2. Follow-up is a process by which internal auditors evaluate the adequacy, effectiveness, and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others. This process also includes determining whether senior management and/or the board have assumed the risk of not taking corrective action on reported observations.

3. The internal audit activity's charter should define the responsibility for follow-up. The CAE determines the nature, timing, and extent of follow-up, considering the following factors:

- Significance of the reported observation or recommendation.
- Degree of effort and cost needed to correct the reported condition.
- Impact that may result should the corrective action fail.
- Complexity of the corrective action.
- Time period involved.

4. The CAE is responsible for scheduling follow-up activities as part of developing engagement work schedules. Scheduling of follow-up is based on the risk and exposure involved as well as the degree of difficulty and the significance of timing in implementing corrective action.

5. Where the CAE judges that management's oral or written response indicates that action taken is sufficient when weighed against the relative importance of the observation or recommendation, internal auditors may follow up as part of the next engagement.

6. Internal auditors ascertain whether actions taken on observations and recommendations remedy the underlying conditions. Follow-up activities should be appropriately documented.

2600–Resolution of Senior Management's Acceptance of Risks

When the CAE believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the CAE must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the CAE must report the matter to the board for resolution.

No Practice Advisory for Standard 2600

1.3 Code of Ethics

(a) Introduction to the Code of Ethics

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

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

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

The Institute's Code of Ethics extends beyond the definition of internal auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing.
2. Rules of conduct that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

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

(b) Applicability and Enforcement of the Code of Ethics

This Code of Ethics applies to both entities and individuals that perform internal audit services.

For IIA members and recipients of or candidates for IIA professional certifications, breaches of the Code of Ethics will be evaluated and administered according to the Institute's Bylaws and

Administrative Directives. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

(c) Code of Ethics

(i) Principles

Internal auditors are expected to apply and uphold the following principles:

1. **Integrity.** The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
2. **Objectivity.** Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments
3. **Confidentiality.** Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.
4. **Competency.** Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

(ii) Rules of Conduct

1. **Integrity.** Internal auditors:
   - **1.1.** Shall perform their work with honesty, diligence, and responsibility.
   - **1.2.** Shall observe the law and make disclosures expected by the law and the profession.
   - **1.3.** Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
   - **1.4.** Shall respect and contribute to the legitimate and ethical objectives of the organization.
2. **Objectivity.** Internal auditors:
   - **2.1.** Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
   - **2.2.** Shall not accept anything that may impair or be presumed to impair their professional judgment.
   - **2.3.** Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.
3. **Confidentiality.** Internal auditors:
   - **3.1.** Shall be prudent in the use and protection of information acquired in the course of their duties.
   - **3.2.** Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. **Competency.** Internal auditors:

   4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.

   4.2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

   4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.