



The Institute of
**Internal
Auditors**

Global Internal Audit Standards

2023 Draft for Public Comment

Global Internal Audit Standards – 2023 Draft for Public Comment

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Table of Contents

- Introduction to the Global Internal Audit Standards3
- Glossary5
- I. Purpose of Internal Auditing 10
- II. Ethics and Professionalism..... 11
- III. Governing the Internal Audit Function..... 33
- IV. Managing the Internal Audit Function..... 59
- V. Performing Internal Audit Services 102

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Introduction to the Global Internal Audit Standards

The Global Internal Audit Standards provide requirements and recommendations to guide the professional practice of quality internal auditing globally. The Standards also establish a basis for evaluating the performance of internal audit services.

Structure of the Standards

The Global Internal Audit Standards contains:

- Principles: broad descriptions of a basic assumption or rule summarizing a group of requirements and recommendations that follow.
- Standards:
 - Requirements for the professional practice of internal auditing.
 - Considerations:
 - Implementation: common and preferred practices for implementing the requirements.
 - Evidence of Conformance: examples of recommended ways to demonstrate that the requirements of the Standards have been implemented.

The Standards are organized into five domains related by a common theme:

- I. Purpose of Internal Auditing.
- II. Ethics and Professionalism.
- III. Governing the Internal Audit Function.
- IV. Managing the Internal Audit Function.
- V. Performing Internal Audit Services.

Applicability of the Standards

Global Internal Audit Standards set forth essential requirements and recommendations for the professional practice of internal auditing globally. The Standards apply to any individual or function that provides internal audit services; for organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. The Standards apply whether internal auditors are employees of the organization, contracted with an external service provider, or a combination of both.

The Standards apply to individual internal auditors and the internal audit function. All internal auditors are accountable for conforming with the principles and standards in the Ethics and Professionalism domain as well as the principles and standards relevant to performing their job responsibilities. Chief audit executives are additionally accountable for the internal audit function's overall conformance with the Standards.

If internal auditors or the internal audit function 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 required.

If the Standards are used in conjunction with requirements issued by other authoritative bodies, internal audit communications must also cite the use of other requirements, as appropriate. However, conformance with the Standards is expected.

How to Use the Standards

The Requirements sections of the Standards use the word “must” to specify unconditional requirements. The Considerations for Implementation sections of the Standards use the word “should” to specify preferred practices and the word “may” to specify optional practices to implement the Requirements.

The Standards use certain terms as defined specifically in its glossary. To understand and apply the Standards correctly, it is necessary to understand and adopt the specific meanings and usage of the terms as described in the glossary.

Standard-setting Process

The IIA is committed to setting standards in the public interest, which includes an extensive, ongoing process undertaken by the International Internal Audit Standards Board and overseen by the IPPF Oversight Council. The Standards Board engages in a due process that includes soliciting stakeholder input when drafting and revising the content of the Global Internal Audit Standards. The process includes posting a draft for worldwide public comment on The IIA’s public-facing website before the Standards are finalized and issued. The draft is distributed to all IIA affiliates and translated into several languages; translations are also posted on The IIA’s website. The IPPF Oversight Council is an independent oversight group that evaluates and advises on the standard-setting process to promote inclusiveness and transparency, which ultimately serves the public interest.

PUBLIC EXPOSURE DRAFT
DO NOT REPLY

Glossary

activity under review – The subject of an internal audit engagement. Examples include an area, entity, operation, function, process, or system.

advisory services – Services including advisory engagements and other advisory activities typically undertaken at the request of senior management, the board, or the management of an activity. The nature and scope of advisory services are subject to agreement with the party requesting the services. Examples of advisory engagements include internal auditors providing advice on the development and implementation of new policies and the design of processes and systems. Other advisory activities include internal auditors providing facilitation and training.

assurance – Statement intended to give confidence about conditions compared to criteria.

assurance services – Services through which internal auditors perform objective assessments to provide statements about conditions compared to established criteria. Such statements are intended to give stakeholders confidence about an organization's governance, risk management, and control processes. Examples of assurance services include financial, performance, compliance, and technology engagements.

board – Highest-level body charged with governance, such as a:

- Board of directors or a committee or another body to which the board of directors has delegated certain functions (for example, an audit committee).
- Nonexecutive/supervisory board in an organization that has more than one governing body.
- Board of governors or trustees.
- Group of elected officials or political appointees.

If a board does not exist, the word “board” refers to a group or person charged with governance of an organization (for example, some public sector entities and smaller private sector organizations may rely on the head of the organization or the senior management team to act as the highest-level governing body).

chief audit executive – Leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services. The specific job title and/or responsibilities may vary across organizations. For example, titles such as "general auditor," "head of internal audit," "chief internal auditor," "internal audit director," and "inspector general" may be used for "chief audit executive" roles.

Code of Ethics – Principles and standards in the Ethics and Professionalism domain of the Global Internal Audit Standards are considered to be internal auditors' Code of Ethics; adherence to these principles and standards is synonymous to adherence to a professional code of ethics.

competency – Knowledge, skills, and abilities.

compliance – Adherence to laws, regulations, contracts, policies, procedures, or other requirements.

condition – Existing state of the activity under review.

conflict of interest – A situation, activity, or relationship that may influence, or appear to influence, the internal auditor to make professional judgments or take actions that are not in the best interest of the organization.

Considerations for Evidence of Conformance – a section of the Global Internal Audit Standards that provides examples of ways to show that the requirements of each standard have been implemented.

Considerations for Implementation – a section of the Global Internal Audit Standards that provides common and preferred practices for implementing the requirements of each standard.

control – 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.

control processes – The policies, procedures, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance.

criteria – Measurable specifications of the desired state of the activity under review (also called "evaluation criteria").

effect – Risk encountered because the condition differs from the criteria.

engagement – A specific internal audit assignment or project that includes multiple tasks or activities designed to accomplish a specific set of related objectives. See also "assurance services" and "advisory services."

engagement conclusion – Internal auditors' professional judgment about the overall significance of the engagement's findings when viewed together.

engagement objectives – Statements that articulate the purpose of the engagement and describe the specific goals to be achieved.

engagement planning – Process during which internal auditors gather information, assess, and prioritize risks relevant to the activity under review, and establish the engagement objectives and scope, identify evaluation criteria, and create a work program for an internal audit engagement.

engagement supervisor – An internal auditor responsible for supervising an internal audit engagement, which may include reviewing and approving the engagement work program, workpapers, final communication, and performance as well as training and assisting internal auditors. The chief audit executive may be the engagement supervisor or may delegate such responsibilities.

engagement work program – A document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools needed to perform the tasks, and the internal auditors assigned to perform the tasks. The work program is based on information obtained during engagement planning.

external service provider – Resource from outside the organization that provides relevant knowledge, skills, experience, and/or tools to support internal audit services.

finding – In an engagement, the determination that a significant risk exists in the activity under review, based on the difference between the evaluation criteria and the condition of the activity. Examples include errors, irregularities, illegal acts, or potential opportunities for improving efficiency or effectiveness.

fraud – Any act characterized by deceit, concealment, or violation of trust perpetrated by individuals or organizations to secure personal or business advantage.

governance – 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.

impact – The result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the entity's strategy or business objectives.

independence – The freedom from conditions that impair the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner.

inherent risk – The combination of internal and external risk factors in their pure, uncontrolled state, or the gross risk that exists, assuming there are no controls in place.

integrity – Behaving in a manner that can withstand scrutiny by peers and others. It involves fair dealing, truthfulness, and having the courage to act appropriately, even when facing pressure to do otherwise or when doing so might create potential adverse personal or organizational consequences.

internal audit charter – A formal document that defines the internal audit function's mandate and other requirements.

internal audit function – A professional individual or group responsible for providing an organization with assurance and advisory services.

internal audit mandate – The internal audit function's authority, role, and responsibilities.

internal audit manual – The chief audit executive's documentation of the methodologies (policies, processes, and procedures) to guide and direct internal auditors within the internal audit function.

internal audit plan – A document, created by the chief audit executive, that identifies the engagements and other internal audit services that will be provided during a given period of time. The plan should be dynamic, reflecting timely responses to organizational changes.

internal auditing – An independent, objective assurance and advisory 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 governance, risk management, and control processes.

International Professional Practices Framework – The IIA's conceptual framework of authoritative standards and guidance.

likelihood – The possibility that a given event will occur.

may – As used in the Considerations for Implementation of the Global Internal Audit Standards, the word "may" describes optional practices to implement the Requirements.

methodologies – Policies, processes, and procedures established by the chief audit executive to guide the internal audit function and enhance its effectiveness.

must – The Global Internal Audit Standards use the word "must" to specify an unconditional requirement.

objectivity – An unbiased mental attitude that allows internal auditors to make professional judgments, fulfill their responsibilities, and achieve the Purpose of Internal Auditing without compromise.

outsourcing – Contracting with an independent external service provider of internal audit services. Fully outsourcing a function refers to contracting the entire internal audit function, and partially outsourcing (also called "cosourcing") indicates that only a portion of the services are outsourced.

Principles – Statements that describe the essential elements of internal auditing and serve as the foundation for the Global Internal Audit Standards.

professional skepticism – Questioning and critically assessing the reliability of information.

public sector – Governments and all publicly controlled or publicly funded agencies, enterprises, and other entities that deliver public programs, goods, or services.

quality assurance and improvement program – A program established by the chief audit executive to evaluate and ensure the internal audit function conforms with the Global Internal Audit Standards, achieves performance objectives, and pursues continuous improvement. The program includes internal and external assessments.

residual risk – The portion of inherent risk that remains after management executes its controls (also called "net risk").

results of internal audit services – Outcomes, such as engagement conclusions, themes (such as effective practices or root causes), and conclusions at the level of the business unit or organization.

risk – The possibility that events will occur and affect the achievement of strategy and business objectives.

risk and control matrix – A tool that facilitates the performance of internal auditing. It typically links business objectives, risks, control processes, and key information to support the internal audit process.

risk appetite – The types and amount of risk that an organization is willing to accept in the pursuit of its strategies and business objectives. Risk appetite takes into consideration the amount of risk that the organization consciously accepts after balancing the cost and benefits of implementing controls.

risk assessment – The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed in terms of impact and likelihood.

risk management – A process to assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

risk tolerance – Boundaries of acceptable variation in performance related to achieving business objectives.

root cause – Core issue or underlying reason for the difference between the criteria and the condition of an activity under review.

senior management – The highest level of management of an organization.

should – As used in the Considerations for Implementation of the Global Internal Audit Standards, the word "should" describes practices that are preferred but not required.

significance – The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives. When referring to risk, significance is often measured as a combination of impact and likelihood.

stakeholder – A party with a direct or indirect interest in an entity's activities and outcomes. Examples of an organization's stakeholders include its employees, customers, vendors, and shareholders; regulatory agencies; and financial institutions. Examples of the internal audit function's stakeholders include the organization's board, management, employees, customers, and vendors; external auditors; and regulatory agencies. The public may also be a stakeholder.

standard – A professional pronouncement promulgated by the International Internal Audit Standards Board that delineates the:

- Requirements for the professional practice of internal auditing.
- Considerations for Implementation.
- Considerations for Evidence of Conformance.

workpapers – Documentation of the internal audit work done when planning and performing engagements, which provides the supporting information and evidence that serves as the basis of the engagement findings and conclusions.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

I. Purpose of Internal Auditing

The purpose statement is intended to assist internal auditors and internal audit stakeholders in understanding the value of internal auditing and articulating the value of internal auditing.

Purpose Statement

Internal auditing enhances the organization's success by providing the board and management with objective assurance and advice.

Internal auditing strengthens the organization's:

- Value creation, protection, and sustainability.
- Governance, risk management, and control processes.
- Decision-making and oversight.
- Reputation and credibility with its stakeholders.
- Ability to serve the public interest.

Internal auditing is most effective when:

- It is performed by qualified internal auditors in conformance with the Global Internal Audit Standards, which are set in the public interest.
- The internal audit function is independently positioned with direct accountability to the board.
- Internal auditors are free from bias and undue influence and committed to making objective assessments.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

II. Ethics and Professionalism

The ethics and professionalism principles and standards comprise internal auditors' code of ethics. They outline the behavioral expectations of professional internal auditors, including chief audit executives, as well as individuals and entities that provide internal audit services. Adherence to these principles and standards instills trust in the profession of internal auditing, creates an ethical culture within the internal audit function, and provides the basis for reliance on internal auditors' work and judgment.

"Internal auditors" refers to recipients of or candidates for IIA professional certifications and all IIA members, including those who are members of IIA affiliates and chapters. Internal auditors are required to conform with the standards of ethics and professionalism. If internal auditors are expected to abide by other codes of conduct, such as their organization's code of ethics, they still must adhere to the principles and standards of ethics and professionalism contained herein. The fact that a particular behavior is not mentioned in these principles and standards does not preclude it from being considered unacceptable or discreditable.

Principle 1 Demonstrate Integrity

Internal auditors demonstrate integrity in their work and behavior.

Integrity is behaving in a manner that can withstand scrutiny by peers and others. It involves fair dealing, truthfulness, and having the courage to act appropriately, even when facing pressure to do otherwise or when doing so might create potential adverse personal or organizational consequences. In simple terms, internal auditors are expected to tell the truth and do the right thing, even when it is uncomfortable or difficult.

Integrity is the foundation of the other principles of ethics and professionalism, including objectivity, competency, due professional care, and confidentiality. The integrity of internal auditors is essential to establishing trust and earning respect.

Standard 1.1 Honesty and Courage

Requirements

Internal auditors must perform their work with honesty and courage.

Internal auditors must be truthful, accurate, clear, open, and respectful in all professional relationships and communications. Internal auditors must not make false, misleading, or deceptive statements, nor conceal or omit findings or other pertinent information from engagement communications. Internal auditors must disclose all material facts known to them that if not disclosed could affect the organization's ability to make well-informed decisions.

Internal auditors must exhibit courage by communicating truthfully and taking appropriate action, even when confronted by dilemmas and difficult situations. Internal auditors must treat others professionally and respectfully, even when expressing skepticism or offering an opposing viewpoint.

The chief audit executive must maintain a work environment where internal auditors feel supported when expressing legitimate, evidence-based findings, conclusions, and recommendations, whether favorable or unfavorable.

Considerations for Implementation and Evidence of Conformance

Implementation

Annually, internal auditors should obtain at least two hours of continuing professional education on ethics to enhance their awareness and understanding of their ethical responsibilities. The chief audit executive should ensure that internal auditors have opportunities to receive this training. The chief audit executive may also emphasize the importance of integrity by providing internal auditors with training that demonstrates integrity and other ethical principles in action; for example, discussing situations that require making ethical choices.

Effective management of the internal audit function includes proper engagement supervision and periodic reviews of internal auditors' performance, which provides opportunities for internal auditors and their supervisors to discuss how integrity may be challenged and applied in real situations. For example, when approving work programs or reviewing engagement workpapers, an engagement supervisor may provide appropriate guidance to help internal auditors address potential or encountered situations that could pose a threat to their integrity.

Public Sector

Internal auditors in the public sector should always protect the public interest and should display courage when providing findings, recommendations, and conclusions.

Evidence of Conformance

- Training plan that includes annual ethics training for all internal auditors.
- Sign-in sheets, training schedules, certificates of completion, or other documents that evidence internal auditors' attendance or participation in ethics training.

Standard 1.2 Organization's Ethical Expectations

Requirements

Internal auditors must respect and contribute to the legitimate and ethical expectations of the organization.

Internal auditors must understand and meet the organization's ethical expectations and be able to recognize conduct that is contrary to those expectations. Internal auditors must encourage and promote an ethics-based culture in the organization.

Internal auditors must assess and make recommendations to improve the organization's objectives, policies, and processes for promoting appropriate ethics and values. If internal auditors identify behavior within the organization that is inconsistent with the organization's ethical expectations, they must report the concern according to the policies established by the chief audit executive.

Considerations for Implementation and Evidence of Conformance

Implementation

The internal audit plan should include assessments of the organization's ethics-related risks to determine whether existing policies, processes, and other controls adequately and effectively address these risks. For example, the organization's policies may specify the criteria and process for communicating about and handling ethics-related issues, the parties that should receive the communication, and the protocol for escalating unresolved issues. The chief audit executive also should determine a methodology for addressing ethical issues and discuss the methodology with senior management and the board to ensure alignment of the approaches.

Internal auditors should consider ethics-related risks and controls during individual engagements. If internal auditors identify behavior within the organization that is inconsistent with the organization's ethical expectations, they should follow methodology and communicate issues internally, according to the methodology established by the chief audit executive, which takes into account the organization's policies and processes.

If internal auditors determine that senior management violated the organization's ethical expectations — whether documented in a code of conduct, code of ethics, or otherwise — the chief audit executive should report this concern to the board. If an ethics-related concern involves the chairman of the board, the chief audit executive should report the concern to the entire board. Internal auditors should follow up on any ethics-related issues involving senior management or the board and validate that appropriate actions were taken to address the concern.

Evidence of Conformance

- Records of internal auditors' participation in workshops, training events, or meetings where ethical expectations and issues were discussed.
- Forms, signed by individual internal auditors, acknowledging their understanding and commitment to follow ethics policies and processes of the organization.
- A documented assessment of the organization's ethics policies and processes.
- Documentation demonstrating that ethical issues were effectively communicated to senior management, the board, and regulators in accordance with the organization's policies and relevant laws and regulations.

Standard 1.3 Legal and Professional Behavior

Requirements

Internal auditors must not engage in or be a party to any activity that is illegal or discreditable to the organization or the profession of internal auditing. Internal auditors must not engage in or be a party to any activity that may harm the organization or its employees.

Internal auditors must understand and abide by the laws and regulations relevant to the industry and jurisdictions in which the organization operates, including making disclosures as required. If internal auditors identify legal or regulatory violations, they must report such incidents to individuals or entities that have the authority to take appropriate action, as specified in laws, regulations, and internal audit policies.

Considerations for Implementation and Evidence of Conformance

Implementation

The chief audit executive should develop and implement a methodology to ensure that internal auditors abide by laws and regulations relevant to the industry and jurisdictions in which the organization operates. The methodology should specify the actions internal auditors are expected to take in response to any legal or regulatory violations, including the established procedure for validating that the actions address the violation adequately.

The chief audit executive should establish methodologies to ensure that internal auditors are properly supervised, conform with the Global Internal Audit Standards, and behave in alignment with ethical and professional values. Examples of discreditable behaviors include but are not limited to:

- Bullying, harassment, or discrimination.
- Failing to accept responsibility for mistakes.
- Intentionally issuing false reports or communications or allowing or encouraging others to do so, including minimizing, concealing, or omitting internal audit findings, conclusions, or ratings from engagement reports or overall assessments.
- Lying, deceiving, or intentionally misleading others, including misrepresenting one's competency or qualifications (such as claiming to hold a certification or displaying credentials when the designation is expired or inactive, has been revoked, or was never earned).
- Making disparaging comments about the organization, fellow employees, or its stakeholders, among coworkers or in a public forum.
- Performing internal audit services with undeclared impairments to objectivity or independence.
- Soliciting or disclosing confidential information without proper authorization.
- Stating that the internal audit function is operating in conformance with the Global Internal Audit Standards when the assertion is not supported.
- Overlooking illegal activities that the organization may tolerate or condone.

Evidence of Conformance

- Records of internal auditors' participation in training on laws, regulations, and/or professional behavior.
- Forms, signed by individual internal auditors, acknowledging their understanding of and commitment to act in accordance with relevant legal and professional expectations.
- Documented methodologies for handling illegal or discreditable behavior among internal auditors and legal or regulatory violations by individuals within the organization.
- Supervisory review notes in workpapers or documentation of conversations between internal auditors and their supervisors that address concerns about illegal or unprofessional actions.

Principle 2 Maintain Objectivity

Internal auditors maintain an impartial and unbiased attitude when performing internal audit services and making decisions.

Objectivity is an unbiased mental attitude that allows internal auditors to make professional judgments, fulfill their responsibilities, and achieve the Purpose of Internal Auditing without compromise. An independently positioned internal audit function supports internal auditors' ability to maintain objectivity.

Standard 2.1 Individual Objectivity

Requirements

Internal auditors must maintain professional objectivity when performing all aspects of internal audit services. Professional objectivity requires internal auditors to apply an impartial and unbiased mindset and make judgments based on balanced assessments of all relevant circumstances.

Internal auditors must be aware of and manage potential biases, including but not limited to:

- Self-review bias – lack of critical perspective when reviewing one's own work, which may lead to overlooking mistakes or shortcomings.
- Familiarity bias – making assumptions based on past experiences, which may compromise professional skepticism.
- Prejudice or unconscious bias – misinterpretation of information including predisposed ideas about culture, ethnicity, gender, ideology, race, or other characteristics that may unduly influence judgments.

The chief audit executive must provide policies, procedures, and training to support and promote objectivity. Internal auditors must understand the expectations relevant to their responsibilities and apply the policies and procedures.

Considerations for Implementation and Evidence of Conformance

Implementation

Making objective assessments requires an impartial mindset, free from bias and undue influence, which is essential to providing objective assurance and advice to senior management and the board. Internal auditors should develop their awareness of the ways in which situations, activities, and relationships may affect their ability to be objective.

Internal auditors also should consider the human tendency or inclination to misinterpret information, make assumptions and mistakes, and ignore or overlook information in a way that unduly influences their judgments and decisions and impairs their ability to evaluate information and evidence objectively.

Objectivity means internal auditors perform their work without compromise or subordination of judgment to others. The Global Internal Audit Standards, along with the policies and training established by the chief audit executive, support objectivity by providing requirements, procedures, and guidance that set forth a systematic and disciplined approach for gathering and evaluating information to provide a balanced assessment of the activity under review. Training may help internal auditors to better understand objectivity-impairing scenarios and how best to address them.

Annually, internal auditors should sign an attestation form, confirming their awareness of the importance of objectivity, understanding of relevant policies and procedures, and obligation to disclose any potential impairments.

Evidence of Conformance

- References in the internal audit charter to internal auditors' responsibility for maintaining objectivity.
- Policies and procedures related to objectivity.
- Records of objectivity training planned and completed, including list of participants.
- Attestation forms, confirming internal auditors' awareness of the importance of objectivity and obligation to disclose any potential impairments.
- Documented disclosures of potential conflicts of interest or other impairments to objectivity.
- Notes from supervisory reviews and mentoring of internal auditors.

Standard 2.2 Safeguarding Objectivity

Requirements

Internal auditors must recognize and avoid or mitigate actual, potential, and perceived impairments to objectivity.

Internal auditors must avoid:

- Accepting any tangible or intangible item, such as a gift, reward, or favor, that may impair or be presumed to impair objectivity.
- Conflicts of interest, including situations, activities, and relationships that may:
 - Oppose, compete with, or be contrary to the interests of the organization.
 - Create the potential for financial or other personal gain.
 - Be established to protect oneself from potential or actual loss or harm.
 - Be nepotistic or provide favoritism to certain individuals.

Internal auditors must not be unduly influenced by their own interests or the interests of others, including senior management or others in a position of authority, or by the political environment or other aspects of their surroundings.

When performing internal audit services:

- Internal auditors must not provide assurance over an activity for which, within the past year, they provided advisory services, had significant responsibility, or were able to exert significant influence. Given the same circumstances, internal auditors may perform an advisory engagement only if they disclose the circumstances to the requester of the advisory services before accepting the engagement. After providing such disclosure, internal auditors may accept the advisory engagement.
- A qualified and competent internal auditor must supervise internal audit engagements and review engagement documentation. When internal auditors perform an assurance engagement in an area for which the chief audit executive has responsibility, the engagement supervision must be overseen by a qualified, independent party.

The chief audit executive must establish policies and procedures to address impairments to objectivity. Internal auditors must discuss impairments with the chief audit executive or a designee and take appropriate actions according to relevant policies and procedures.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Impairments to objectivity are situations, activities, and relationships that may influence internal auditors' judgments and decisions in a way that may change internal audit findings and conclusions. Standard 2.2 Safeguarding Objectivity specifies types of situations, activities, and relationships from which internal auditors must refrain to maintain an impartial and unbiased mindset. Impairments to objectivity may exist, in fact or appearance, even when they are unintended. Impairments to objectivity may be perceived by others, even when no impairment has occurred in fact. Internal auditors should apply judgment regarding additional circumstances that may impair or be presumed to impair objectivity.

Conflicts of interest are situations in which an internal auditor has a competing professional or personal interest that may make it difficult to fulfill internal audit duties impartially. Conflicts of interest may create the appearance of impropriety that can undermine the confidence in an internal auditor, the internal audit function, and the internal audit profession, even if no unethical or improper acts result.

The internal audit function's policies and procedures should specify the expectations and requirements for internal auditors related to:

- Receiving gifts, favors, and rewards.
- Identifying situations that may impair objectivity.
- Responding appropriately upon becoming aware of an impairment.

Most organizations have a policy related to the acceptance of gifts, rewards, and favors, such as a policy limiting the value of gifts that can be accepted. Because of the importance of objectivity in the practice of internal auditing, the chief audit executive may have a policy that is more restrictive than that of the organization. Internal auditors should follow the more restrictive policy and carefully consider whether accepting a gift, reward, or favor could be perceived to affect their judgment or be given in exchange for producing favorable internal audit findings, conclusions, or results.

The policies of the organization and/or the internal audit function may prohibit specific activities or relationships that could create conflicts of interest. Activities to be avoided may include fraternizing outside of work with the organization's employees, management, third-party suppliers, and vendors. Internal auditors should avoid close personal relationships and relationships involving financial ties, such as investments, that could represent conflicts of interest, whether in fact or appearance.

The chief audit executive should take precautions to reduce the potential impairments to objectivity that may result from the design of performance evaluations and compensation arrangements, bonuses, and incentives.

Examples of compensation arrangements that could impair objectivity include:

- Basing performance evaluations and compensation primarily on surveys of or input from the management of the activity under review.
- Measuring performance against the number of findings identified during engagements, the revenue growth of the activity under review, or the cost savings or job eliminations imposed upon the activity under review.
- Allowing management to provide indirect compensation in the form of gifts and gratuities.

Internal auditors should apply their understanding of objectivity and relevant policies and procedures to evaluate whether any situations, activities, or relationships may impair or may be presumed to impair their objectivity. The perceptions of other people should be considered.

The requirements in Standard 2.2 Safeguarding Objectivity for staffing and supervising engagements are intended to ensure that the internal auditors assigned to an engagement were not recently responsible for any aspect of the activity under review, which could bias their view, give them a vested interest in a particular outcome, or create the perception or appearance that their objectivity is impaired. For each engagement, the

internal auditors performing and supervising the engagement should be independent from the activity under review.

When planning resources for an engagement, the chief audit executive or a designated supervisor should discuss the engagement with internal auditors to identify any current or potential impairments to objectivity. The discussion should include consideration of any impairments previously disclosed.

As part of the process for supervising engagements, workpapers are reviewed to ensure findings and conclusions are adequately supported. Engagement supervision also provides opportunities for more experienced internal auditors to provide feedback and mentoring regarding potential objectivity concerns. (See also Standard 12.3 Ensuring and Improving Engagement Performance and Standard 13.5 Engagement Resources.)

If an impairment is unavoidable, it should be disclosed and mitigated as described in Standard 2.3 Disclosing Impairments to Objectivity.

Public Sector

If public sector internal auditors have potential impairments related to an advisory engagement, laws and regulations may require them to ensure that the person(s) requesting the advisory engagement understands the potential impairment and accepts the responsibility for the findings, recommendations, and conclusions. Additionally, internal auditors may be required to disclose potential impairments in the final engagement communication.

Evidence of Conformance

- Policies and procedures for identifying potential impairments and necessary safeguards.
- Records of objectivity training.
- Notes from supervisory reviews.
- Attestation forms.
- Compensation plan.
- Minutes of board meetings where impairments to objectivity were discussed.
- Documentation disclosing impairments to objectivity.
- Plans showing alternative provisions to fulfill the internal audit plan activities where impairments to objectivity were unavoidable.
- Sources of feedback on the perception of the chief audit executive's objectivity, such as surveys of the internal audit function's stakeholders.
- Results of external quality assessments performed by an independent assessor.

Standard 2.3 Disclosing Impairments to Objectivity

Requirements

If objectivity is impaired, in fact or appearance, the details of the impairment must be disclosed to the appropriate parties before internal audit services are performed.

If internal auditors become aware of an impairment that may affect their objectivity, they must disclose the impairment to the chief audit executive or a designated supervisor. If the chief audit executive determines that an impairment is affecting an internal auditor's ability to perform duties objectively, the chief audit executive must

discuss the impairment with management of the activity under review, senior management, and/or the board and determine the appropriate actions to resolve the situation.

If an impairment that affects the reliability or perceived reliability of the engagement findings, recommendations, and/or conclusions is discovered after an engagement has been completed, the chief audit executive must discuss the concern with the management of the activity under review, senior management, the board, and/or other affected stakeholders and determine the appropriate actions to resolve the situation. (See also Standard 11.4 Errors and Omissions.)

If the objectivity of the chief audit executive is impaired in fact or appearance, the chief audit executive must disclose the impairment to the board. (See also Standard 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications and Standard 7.3 Safeguarding Independence.)

Considerations for Implementation and Evidence of Conformance

Implementation

The requirements for disclosing impairments to objectivity are typically defined in internal audit policies and procedures and describe the actions to be taken to address each impairment to objectivity. The general approach to disclosing and mitigating impairments to objectivity is typically determined by the chief audit executive in agreement with senior management and the board.

If an impairment to objectivity cannot be avoided, the chief audit executive may consider options to mitigate the impairment, including:

- Reassigning internal auditors to remove the impaired auditor from the engagement.
- Rescheduling an engagement to ensure it is properly staffed.
- Adjusting the scope of an engagement.
- Outsourcing the performance or supervision of the engagement.

When a concern arises during engagement planning that relates solely to the perception of an impairment, the chief audit executive may choose to discuss the concern with management of the activity under review and/or senior management, explain why the risk exposure is minimal and how it will be managed, and document the discussion.

If the chief audit executive or other internal auditors are asked to assume roles or responsibilities beyond internal auditing, the chief audit executive should speak with senior management and the board about the reporting relationships, responsibilities, and expectations related to the role. During such a discussion, the chief audit executive should emphasize the IIA standards related to objectivity, the potential impairments to objectivity that the proposed role and responsibilities may pose, and the safeguards necessary to mitigate the impairments. (See also Standard 6.1 Internal Audit Mandate; 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications; Standard 7.3 Safeguarding Independence; and Standard 9.3 Internal Audit Charter.)

Evidence of Conformance

- Internal audit policies and procedures about disclosing objectivity impairments.
- Documentation disclosing the presence or affirming the absence of objectivity impairments.
- Records of communicating the disclosure and of receipt and response and/or approval of appropriate parties.

Principle 3 Demonstrate Competency

Internal auditors apply the knowledge, skills, and abilities to fulfill their roles and responsibilities successfully.

Demonstrating competency requires developing and applying the knowledge, skills, and abilities to provide internal audit services. This includes internal auditors advancing their understanding of business, management, and technology; as well as economic, environmental, legal, political, and social contexts.

Standard 3.1 Competency

Requirements

Internal auditors must possess or obtain the knowledge, skills, and abilities to perform their responsibilities successfully.

Internal auditors must engage only in those services for which they have or can attain the necessary competencies. Each internal auditor is responsible for continually developing and applying the competencies necessary to fulfill their professional responsibilities.

For internal auditors, being competent requires possessing and demonstrating knowledge, skills, and abilities relevant to:

- The IIA's Global Internal Audit Standards and current internal audit practices.
- Supervision, leadership, communication, and collaboration.
- Governance, risk management, and control processes.
- Business functions, such as financial management and information technology, and pervasive risks, such as fraud.
- Industry-specific laws, regulations, and practices.
- Tools and techniques for gathering, analyzing, and evaluating data.
- Current activities, trends, and emerging issues.

Additionally, the chief audit executive must ensure the internal audit function collectively possesses the competencies to perform the internal audit services described in the internal audit charter or must make arrangements to obtain the necessary competencies. (See also Standard 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications and Standard 10.2 Human Resource Management.)

Considerations for Implementation and Evidence of Conformance

Implementation

Internal auditors at all levels of their careers should:

- Obtain appropriate professional designations, such as the Certified Internal Auditor designation and other certifications and credentials offered by The IIA and other professional organizations.
- Identify opportunities for improvement and competencies that need development, based on feedback provided by stakeholders, peers, and supervisors.
- Be trained not only on internal audit methodologies but also on specific business activities relevant to the organization for which the internal auditors are providing services. For example, an internal auditor providing internal audit services to an investment company should be trained in business processes related to investment companies. Training opportunities may include enrolling in courses, working with a mentor, or being assigned new tasks under supervision during an engagement.

To ensure the internal audit function collectively possesses the competencies to perform the internal audit services, chief audit executives should:

- Maintain an inventory of internal auditors' competencies to be utilized when assigning work, identifying training needs, and recruiting internal auditors to fill open positions.
- Participate in reviewing the performance of individual internal auditors annually.
- Identify areas in which the competencies of the internal audit function should be improved.
- Encourage internal auditors' intellectual curiosity and invest in training and other opportunities to improve internal audit performance.
- Understand the competencies of other providers of assurance and advisory services and consider relying upon those providers as a source of additional or specialty competencies not available within the internal audit function.
- Consider contracting with an independent, external service provider when the internal audit function collectively does not possess the competencies to perform requested services.
- Effectively implement a quality assurance and improvement program.

Evidence of Conformance

- An inventory or other documentation listing the certifications, education, experience, work history, and other qualifications of internal auditors.
- Internal auditors' self-assessments of their competencies and plans for professional development.
- Documentation of internal auditors' completion of continuing professional education, such as courses, conference sessions, workshops, and seminars.
- The chief audit executive's documented reviews of internal auditors' performance.
- Documented supervisory reviews of engagements, post-engagement surveys completed by internal audit stakeholders, and other forms of feedback indicating competencies exhibited by individual internal auditors and the internal audit function as a whole.
- The results of internal and external quality assessments.
- Relevant documentation the chief audit executive has completed to resource the internal audit plan, including an inventory of competencies necessary to fulfill the plan, an analysis of resource gaps, and the identification of the training and budget necessary to fill the gaps.
- Documentation such as an assurance map that indicates the competencies of other providers of assurance and advisory services upon which the internal audit function may rely.

Standard 3.2 Continuing Professional Development

Requirements

Internal auditors must maintain and continuously develop their competencies to improve the effectiveness and quality of internal audit services.

Internal auditors must enhance their knowledge, skills, and abilities by completing at least 20 hours of continuing professional education annually. Practicing internal auditors who have attained professional internal audit certifications must keep their certifications current by fulfilling any additional requirements for continuing professional education.

Considerations for Implementation and Evidence of Conformance

Implementation

By completing a minimum of 20 hours of continuing professional education annually, internal auditors keep their knowledge current and deepen their understanding of relevant topics so that they can improve the effectiveness and quality of internal audit services. Internal auditors should focus on opportunities to learn about emerging topics, risks, trends, and changes that may affect the organizations for which they work and the internal audit profession. Professionals with credentials, such as the Certified Internal Auditor, should be aware of additional requirements for maintaining their credentials. Failing to fulfill such requirements may result in consequences, including jeopardizing internal auditors' permission to use the credentials.

As part of the required continuing professional education, The IIA requires holders of its certifications to complete ethics training annually. While this requirement is linked specifically to IIA certifications, all internal audit professionals should obtain ethics-focused continuing professional education or training on a regular basis.

While the chief audit executive is responsible for providing opportunities for education and training for the internal audit function as a whole, internal auditors ultimately are responsible for developing their competencies and should seek opportunities to learn. For example, internal auditors may ask to be assigned to engagements involving processes or areas of the organization with which they are unfamiliar or have had limited experience. Internal auditors should also seek and welcome opportunities for mentorship and robust guidance from supervisors, who provide feedback and suggestions and share their experience and insights.

Internal auditors may subscribe to news services and newsletters to stay abreast of current developments in the internal audit profession and industries relevant to the organizations for which they work. The chief audit executive may also attend or recommend online or in-person seminars to the internal audit staff. Periodically, the chief audit executive may schedule internal staff training events to introduce new technology or changes in internal audit practices.

Professional development initiatives should include a regular review and assessment of internal auditors' career paths and needs for professional development. The chief audit executive should ensure plans and budgets for training reflect a balance between investing in developing the competencies of the internal audit function as a whole and providing internal auditors with opportunities to achieve their individual goals to grow professionally.

Evidence of Conformance

- Documented plans for training events and other continuing professional education.
- Records of internal auditors' completed continuing professional education and credentials obtained.
- Internal auditors' performance reviews and/or plans for professional development.
- Evidence of active involvement in The IIA and other relevant professional organizations, such as volunteer service and attendance at professional conferences.

Principle 4 Exercise Due Professional Care

Internal auditors apply due professional care in planning and performing internal audit services.

The standards that embody exercising due professional care require:

- Conformance with the Global Internal Audit Standards.
- Consideration of the nature, circumstances, and requirements of the work to be performed.
- Application of professional skepticism to critically assess and question information.

Due professional care requires planning and performing internal audit services with the diligence, judgment, and skepticism possessed by other reasonably prudent and competent internal auditors. When exercising due professional care, internal auditors perform in the best interests of those receiving internal audit services but are not expected to be infallible.

Standard 4.1 Conformance with Global Internal Audit Standards

Requirements

Internal auditors must plan and perform internal audit services in accordance with the Global Internal Audit Standards.

The internal audit function's methodologies must be established, documented, and maintained in alignment with the Standards. Internal auditors must follow the Standards and the internal audit function's methodologies when planning and performing internal audit services and when communicating internal audit findings, recommendations, conclusions, and other results.

If laws or regulations prohibit internal auditors or the internal audit function from conforming with any part of the Standards, conformance with all other parts of the Standards is required and appropriate disclosures must be made.

If inconsistencies exist between the Standards and requirements issued by other authoritative bodies, internal auditors and the internal audit function must conform with the Standards and may conform with the other requirements if such requirements are more restrictive.

Considerations for Implementation and Evidence of Conformance

Implementation

The chief audit executive should review the Standards annually and update internal audit function's methodologies to ensure alignment between both resources.

The chief audit executive or a designated engagement supervisor should ensure that engagement work programs align with the requirements of the Standards and that internal audit engagements are conducted in accordance with the Standards' requirements.

If internal auditors are unable to conform with a standard when performing an internal audit engagement, they should discuss with the chief audit executive or a designated supervisor the reason for the nonconformance and the effect of the nonconformance on the engagement. Standard 8.3 Quality, Standard 12.1 Internal Quality Assessment, and Standard 15.1 Final Engagement Communication provide additional requirements related to communicating about conformance and nonconformance with the Standards.

Evidence of Conformance

- Documentation of the internal audit function's methodologies and notes indicating the most recent update.
- Statements of conformance with the Standards and disclosures of nonconformance with the Standards in final engagement communications and communications with senior management and the board.
- Documentation referencing the law or regulation with which internal auditors were required to comply that prevented their conformance with the Standards.
- Documentation referencing other authoritative requirements to which the internal audit function adheres in addition to the Standards.
- Results of the quality assurance and improvement program.

Standard 4.2 Due Professional Care

Requirements

Internal auditors must exercise due professional care by taking into account the nature, circumstances, and requirements of the services to be provided, including:

- The organization's strategy and objectives.
- The best interests of those for whom internal audit services are provided and other stakeholders.
- Adequacy and effectiveness of governance, risk management, and control processes.
- Cost in relation to potential benefits of the internal audit services to be performed.
- Extent and timeliness of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of risks to the activity under review.
- Probability of significant errors, fraud, noncompliance, and other risks that might affect objectives, operations, or resources.
- Use of appropriate techniques, tools, and technology.

Considerations for Implementation and Evidence of Conformance

Implementation

To perform services with due professional care requires that internal auditors consider and understand the Purpose of Internal Auditing and the nature of the internal audit services to be provided. Internal auditors should start by understanding the internal audit charter, the chief audit executive's internal audit plan, and the circumstances that helped determine which engagements are included in the plan. When planning and performing internal audit services, internal auditors also take into account the best interests of the organization's customers and other stakeholders (including the public) affected by the organization's actions. Such interests include stakeholders' expectations (such as fair and honest business practices), needs (such as safety), and potential exposure to underlying risks that may not be obviously related to the organization's strategy and objectives.

Relevant circumstances include the organization's strategy and objectives and the adequacy and effectiveness of the organization's governance, risk management, and control processes. The chief audit executive takes these circumstances into account when performing the risk assessment on which the internal audit plan is based. Additionally, internal auditors consider these circumstances in relation to an activity under review in an engagement. Internal auditors exercise due professional care by approaching the internal audit services to be provided with this basis of understanding.

At the earliest stages of planning internal audit services, internal auditors communicate with the management of the activity under review and gather information to determine the engagement objectives and scope. (See also Standard 13.1 Engagement Communication and Standard 13.2 Engagement Risk Assessment). When prioritizing the risks relevant to the organization or the activity under review, due professional care requires taking into account the probability of significant errors made by management, noncompliance with laws and regulations, fraud, and other risks that might affect the operations or resources of the organization or activity under review, which in turn affect the achievement of objectives.

The complexity, materiality, and significance of risks being evaluated is relative. A risk may not be material or significant to the organization as a whole but may be material or significant in an engagement or to an activity under review. Thus, understanding the complexity, materiality, and significance in context is necessary for properly assessing relevant risks and determining which risks should be prioritized for further evaluation.

Due professional care also requires weighing the costs (such as resource requirements) of the internal audit services against the benefits that may result. For example, if the controls in an activity under review are not adequately designed, the benefits of fully evaluating the effectiveness of those controls are not likely to be worth the costs. Internal auditors seek to provide the most value or benefit for the organization's investment in internal audit services. Additionally, thorough planning requires internal auditors to consider the techniques, tools, and technology and the extent and timeliness of work that will be needed to achieve the engagement objectives most efficiently. Internal auditors, especially the chief audit executive, should consider the use of data analysis software and other technology that support the review and evaluation processes.

Although not directly required as part of Standard 4.2 Due Professional Care, due professional care is ensured when engagements are properly supervised and a quality assurance and improvement program is implemented. (See 8.4 External Quality Assessment, Standard 12.1 Internal Quality Assessment, Standard 12.2 Performance Measurement, and Standard 12.3 Ensuring and Improving Engagement Performance.)

Evidence of Conformance

- Planning notes documenting the strategy and objectives of the organization and activity under review.
- Documented assessments of governance, risk management, and control processes.
- Notes showing assessment of risks including errors, noncompliance, and fraud.
- Notes from meetings or discussions of potential costs and benefits of internal audit services to be performed as well as extent and timeliness of engagement work.
- Workpapers indicating supervisory review of engagements.
- Internal auditors' performance reviews.
- Notes from meetings, training, or other discussion of due professional care.
- Feedback from stakeholders solicited through surveys or other tools.
- Internal and external assessments performed as part of the internal audit function's quality assurance and improvement program.

Standard 4.3 Professional Skepticism

Requirements

Internal auditors must exercise professional skepticism when planning and performing internal audit services.

To exercise professional skepticism, internal auditors must:

- Maintain an attitude that includes a questioning mind.
- Critically assess the reliability of information.
- Be straightforward and honest when raising concerns and asking questions about inconsistent information.
- Seek additional evidence to make a judgment about information and statements that might be incomplete, inconsistent, false, or misleading.

Considerations for Implementation and Evidence of Conformance

Implementation

Professional skepticism enables internal auditors to make objective judgments based on facts, information, and logic, rather than trust or belief. Skepticism is the attitude of always questioning or doubting the validity and truthfulness of claims, statements, and other information. Auditors apply professional skepticism when they seek evidence to support and validate statements by management, rather than simply trusting the information presented as true or genuine without question or doubt. Professional skepticism requires curiosity and the willingness to explore beyond the surface level of a given topic.

When performing internal audit engagements, internal auditors apply professional skepticism to gather relevant, reliable, and sufficient information and to analyze and evaluate the information. If internal auditors determine that information is incomplete, inconsistent, false, or misleading, they should perform additional analyses to identify the correct and complete information and produce evidence to support engagement findings, recommendations, and conclusions. Additional validation is provided by the review and approval of workpapers and/or engagement communications by the chief audit executive or a designated engagement supervisor.

Chief audit executives should help internal auditors build their competency related to professional skepticism. Workshops and other training opportunities can help internal auditors develop and learn to apply professional skepticism and understand the importance of avoiding bias and maintaining an open and curious mindset. Internal auditors can learn to recognize information that is inconsistent, incomplete, false, and/or misleading. Additionally, chief audit executives should set expectations regarding the amount of time appropriate to invest in seeking evidence within the engagement's time constraints.

Evidence of Conformance

- Records of relevant training planned and completed, including list of participants.
- Workpapers identifying an internal auditor's approach to evaluate and validate information gathered during an engagement.
- Documentation of false or misleading information as an engagement finding.
- Workpapers and engagement communication, reviewed and signed or initialed by the engagement supervisor.

Principle 5 Maintain Confidentiality

Internal auditors use and protect information appropriately.

Internal auditors receive information that may be confidential, proprietary, and/or personally identifiable. This includes information in physical and digital form as well as oral communication, such as formal or informal meeting discussions. Internal auditors respect the value and ownership of information they receive by using it only for approved purposes and protecting it from unintended access or disclosure, internally and externally.

Standard 5.1 Use of Information

Requirements

Internal auditors must follow the policies and procedures of the organization and the internal audit function when using information to perform internal audit services.

Internal auditors must collect and document only the information required to perform the assigned internal audit engagement or services. The information must be used only for approved purposes.

Internal auditors must not use information for personal gain or in a manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

Considerations for Implementation and Evidence of Conformance

Implementation

The policies and procedures of the organization and the internal audit function govern internal auditors' handling and use of information. The chief audit executive should discuss with internal auditors the policies, procedures, and expectations related to the appropriate use of information to which they have access. The chief audit executive may require internal auditors to acknowledge their understanding through signed attestations or other formats.

Internal auditors often have access to information that is confidential, proprietary, and/or personally identifiable. The inappropriate use of such information could have unintended consequences, such as reputational damage and violations of laws and regulations.

Templates for work programs or engagement workpapers should include reminders about the authorized use of information. Electronic formats may contain automated controls that require internal auditors to acknowledge such reminders before they are able to access and complete their documentation.

Internal auditors should not use insider financial, strategic, or operational knowledge or other organizational information for personal gain. For example, information obtained as the result of providing internal audit services should not be used, sold, or released to others to inform decisions to purchase or sell stock or to create a competitive product. Internal auditors should not access information unless it is relevant to the internal audit services being provided.

Evidence of Conformance

- Documentation of relevant policies, procedures, and training related to the proper use of information.
- Minutes from meetings during which the appropriate use of information was discussed.
- Attendance records of training on use of information, acknowledging understanding of relevant policies, procedures, laws, and regulations.
- Performance reviews demonstrating that policies and procedures related to the use of information have been followed.
- Effectively designed and operating controls over access to information.

Standard 5.2 Protection of Information

Requirements

Internal auditors must be aware of their responsibilities for protecting information and act in a manner demonstrating respect for the confidentiality, privacy, and ownership of information acquired when performing internal audit services or as the result of professional relationships.

Internal auditors must understand and abide by the laws and regulations related to confidentiality, information security, and information privacy for the jurisdictions in which their organization operates. Additionally, internal auditors must follow the policies and procedures of their organization and internal audit function governing:

- Custody, retention, and disposal of engagement records.
- Release of engagement records to internal and external parties.
- Handling of access to, or copies of, confidential information when it is no longer needed.

Internal auditors must not disclose confidential information to unauthorized parties unless there is a legal or professional responsibility to do so. This applies even if internal auditors change roles within the organization or leave the organization.

Internal auditors must be alert to the possibility of inadvertent breach, exposure, or disclosure of information, including in a social environment or to an associate or family member.

The chief audit executive must ensure that the internal audit function and individuals assisting the internal audit function follow the same protection requirements.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The information acquired, used, and produced by the internal audit function is protected by laws, regulations, and the policies and procedures of the organization and the internal audit function. Laws, regulations, policies, and procedures generally cover physical and digital security and access, retention, and disposal of information.

The chief audit executive should consult with legal counsel to better understand the impact of legal and regulatory requirements and protections (for example, legal privilege or attorney-client privilege). The organization's policies and procedures may require that specific authorities review and approve business information before external release.

Information can be protected from intentional or unintentional disclosure through controls such as data encryption, email distribution, restrictions on the use of social media, and restrictions on physical access to the information. When internal auditors no longer need access to such data, digital permissions should be revoked and printed copies should be handled according to established policies and procedures.

One example of information typically protected from disclosure is personally identifiable information (for example, individual salaries and records of reprimands or personnel problems discussed with supervisors and human resource personnel). Access to such information is often restricted or monitored through physical and/or information system controls, including password protection and encryption of data.

The chief audit executive should periodically assess and confirm internal auditors' needs for access to information and whether access controls are working effectively.

Public Sector

Internal auditors in the public sector must understand and comply with any jurisdictional requirements regarding disclosures of information.

Evidence of Conformance

- Documentation demonstrating application of relevant policies, processes, and procedures relating to control of access, custody, retention, and disposal of engagement records, release of engagement records to internal and external parties, and handling of confidential information when it is no longer needed.
- Documentation regarding the implementation of mechanisms that restrict access and mitigate the risk of circumventing or otherwise violating these controls.
- Attendance records of training on protection of information, acknowledging understanding of confidentiality and relevant policies, procedures, laws, and regulations.
- Performance reviews demonstrating that policies and procedures related to the protection and disclosure of information have been followed.
- Documentation of restrictions on the distribution of workpapers and final communications.
- Documented authorization of all disclosures and approved distribution lists.
- Records of disclosures required by law or regulation or approved by legal counsel, if applicable, and by senior management and the board.
- Signed acknowledgment attesting that internal audit engagement-related information has been kept confidential.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

III. Governing the Internal Audit Function

Certain governance arrangements are essential to enable the internal audit function to be effective. This domain outlines the board's responsibilities to authorize the internal audit function, ensure its independent positioning, and oversee its performance. While the chief audit executive has responsibilities to communicate effectively and provide the board with information, the board also has a role and responsibilities that are key to the internal audit function's ability to fulfill the Purpose of Internal Auditing. The standards in this domain indicate the responsibilities of the chief audit executive and the board as well as those responsibilities that are accomplished jointly.

The Global Internal Audit Standards use the term "board" to refer to the highest-level body charged with governance, such as:

- A board of directors, a committee, or another body to which the board of directors has delegated certain functions (for example, an audit committee).
- A nonexecutive/supervisory board in an organization that has more than one governing body.
- A board of governors or trustees.
- A group of elected officials or political appointees.

If a board does not exist, the word "board" refers to a group or person charged with governance of an organization (for example, some public sector entities or small private sector organizations may rely on the head of the organization or the senior management team to act as the highest-level governing body).

The responsibilities of the board as described in the Standards apply whether the internal audit function comprises employees of the organization or is contracted with an external service provider. The chief audit executive's responsibilities are performed by an individual designated by the board, whether the individual is an employee of the organization or a person employed by an external service provider. The board retains the responsibility to ensure the internal audit function conforms with the Standards.

Principle 6 Authorized by the Board

The board establishes, approves, and supports the authority, role, and responsibilities of the internal audit function.

The authority, role, and responsibilities of the internal audit function are defined in the internal audit mandate. The mandate empowers the internal audit function to enhance the organization's success by providing senior management and the board with objective assurance and advice. The internal audit function carries out the mandate by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes throughout the organization.

Standard 6.1 Internal Audit Mandate

Requirements

Board Responsibilities

The board must approve the internal audit mandate, which defines the internal audit function's authority, role, and responsibilities and specifies the scope and types of internal audit services.

To understand and support a mandate that establishes the basis for an effective internal audit function, the board must consider information provided by the chief audit executive.

The board must review the internal audit mandate at least annually to consider changes affecting the organization, such as the employment of a new chief audit executive or changes in the type, severity, and interdependencies of risks to the organization.

Chief Audit Executive Responsibilities

The chief audit executive must provide the board with the information necessary to establish the internal audit mandate. This information includes the Global Internal Audit Standards related to governing the internal audit function, the potential scope and types of internal audit services, and other responsibilities common to internal audit functions.

To help the board determine the scope and types of internal audit services, the chief audit executive must collaborate with other internal and external assurance providers and with regulators, if applicable, to ensure a mutual understanding of each other's roles and responsibilities. This mutual understanding should be shared with the board.

Joint Responsibilities

The board and the chief audit executive must discuss and agree upon the internal audit function's mandate. The chief audit executive must document the agreed-upon internal audit mandate in an internal audit charter, which is approved by the board.

At least annually, the board and the chief audit executive must discuss the internal audit mandate and the charter to assess whether the authority, role, and responsibilities continue to enable the internal audit function to accomplish its objectives. The chief audit executive must document any changes in a revised internal audit charter. The board must approve changes to the mandate and the charter. (See also Standard 9.3 Internal Audit Charter.)

Considerations for Implementation and Evidence of Conformance

Implementation

Board Practices

Examples of information the board should understand to determine the internal audit mandate include:

- The overall Purpose of Internal Auditing, as defined in the Standards.
- The Principles of internal auditing, identified in the Standards.
- The opportunities for the internal audit function to add value and contribute to organizational success.
- Leading practices for an internal audit function's authority, role, and responsibilities.
- Relevant jurisdictional laws and regulations.

With this understanding, the board and the chief audit executive should then discuss the expectations for the internal audit function and establish the appropriate authority, role, and responsibilities.

Given the wide-reaching purview of the internal audit function, the board should recognize and promote organizational acceptance of the value of the internal audit function's assurance and advice in supporting opportunities for management to create and protect value.

If changes in the organization or circumstances warrant, the internal audit mandate and charter may require review and updating more frequently than once per year. In such cases, discussions should occur as warranted, rather than waiting for the required annual discussion.

Chief Audit Executive Practices

The chief audit executive assists the board in its considerations of an appropriate internal audit mandate by advising the board about the characteristics of an effective internal audit function. To do this, the chief audit executive shares knowledge about the Standards, any relevant jurisdictional laws and regulations, and the results of research into the leading activities and practices of internal audit functions.

The chief audit executive should participate in the coordination of the organization's assurance providers and advise the board regarding how other functions within the organization may contribute to the internal audit mandate. By helping the board understand the roles and responsibilities of other internal and external assurance providers and regulators, the chief audit executive may provide clarity about an appropriate internal audit mandate.

Before gaining board approval, the chief audit executive should review the proposed internal audit charter with senior management to ensure they understand and support the board's expectations.

Joint Practices

The chief audit executive may provide the board with recommended examples, templates, or other guidance on the components of an internal audit charter to help determine the appropriate content and format.

The internal audit charter may also reference any applicable laws and regulations supporting the internal audit function's mandate. For example, regulations or stock exchange listing requirements may apply to the internal audit function.

The chief audit executive should review with senior management the proposed internal audit mandate and charter, as well as any updates, to ensure understanding and support of the board's expectations.

The chief audit executive should ensure that review of the internal audit charter is included on the board agenda at least annually.

Public Sector

The mandate in the public sector may require the internal audit function to be accountable and transparent to the public and conduct its work in the public interest.

The internal audit mandate may be specified in a governing document, such as in law or regulation, which may serve as the internal audit charter. As a result, an annual review of the mandate may not be warranted. If the law or regulation does not cover all aspects typically expressed in the mandate and charter, the chief audit executive should develop and document the additional specifications for review and approval by the board.

In the public sector, the chief audit executive may be appointed or elected and must be aware of the unique requirements related to reporting relationships.

Evidence of Conformance

- Minutes of board meetings during which the mandate was discussed and approved.
- Minutes of board meetings during which the changes to the mandate were discussed and approved as necessary.
- Board meeting agenda and/or minutes featuring annual review of mandate.
- Documentation that the chief audit executive reviewed the internal audit charter annually.
- An internal audit charter with date and evidence of version control.
- Minutes of board meetings acknowledging approval of the charter and subsequent changes.

Standard 6.2 Board Support

Requirements

Board Responsibilities

The board must support the internal audit function, ensuring its recognition throughout the organization.

The board must ensure the internal audit function has unrestricted access to the data, records, and other information as well as the personnel and physical properties necessary to fulfill the internal audit mandate.

The board must support the chief audit executive through regular, direct communications.

The board demonstrates its support by:

- Establishing and approving the internal audit mandate.
- Ensuring the chief audit executive reports to a level within the organization that allows the internal audit function to fulfill the internal audit mandate.
- Approving the internal audit charter, internal audit plan, budget, and resource plan.

- Making appropriate inquiries of senior management and the chief audit executive to determine whether any restrictions on the internal audit function's scope, access, authority, or resources limit the function's ability to carry out its responsibilities effectively.
- Meeting as necessary with the chief audit executive in sessions without senior management present.

Chief Audit Executive Responsibilities

The chief audit executive must provide the board with information it needs to support and ensure recognition of the internal audit mandate throughout the organization.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Board Practices

A meeting between the board and the chief audit executive without management present at least quarterly is a leading governance practice. Such a meeting often occurs as a private, or closed, session following a normally scheduled board meeting. The board also should have calls or other informal discussions with the chief audit executive between official meetings to demonstrate its ongoing support and to keep apprised of the internal audit function's progress.

The board should ensure the chief audit executive reports administratively to an individual in the organization who is able to support the internal audit function's pursuit of the mandate. Ideally, this individual should be the chief executive officer or equivalent.

The board should understand the internal audit function's needs for access to data, records, and other information as well as personnel and physical properties. Periodically, the board should evaluate whether any access, scope, or resource limitations are impairing the internal audit function's ability to perform services and fulfill the internal audit mandate. If the chief audit executive reports encountering barriers, the board should demonstrate support by communicating with senior management, as needed.

Chief Audit Executive Practices

The chief audit executive should advise the board regarding ways to demonstrate its support for the internal audit function. The chief audit executive should also inform the board about any restrictions impeding the internal audit function's ability to perform services and fulfill the internal audit mandate.

Joint Practices

The types of information and the level of detail to be communicated by the chief audit executive to the board should be agreed upon by both parties.

Public Sector

In the public sector, the board may have no direct authority to approve the internal audit function's budget and/or resource plan. In cases where senior management requests the budget from a budgetary authority outside the organization, the board should advocate for internal audit resources that are sufficient to fulfill the internal audit mandate.

In the public sector, the chief audit executive must be aware that policies or jurisdictional laws or regulations (such as those related to public records) may prohibit or limit informal discussions and/or establish rules for private sessions with the board, such as limiting them to specific topics, to ensure public integrity.

Evidence of Conformance

- Minutes of board meetings indicating board review and approval of the internal audit charter, internal audit plan, internal audit budget, and resource plan.
- Records indicating timely, informative communications between the chief audit executive and the board.
- Documentation of the agreement with the board on the nature and levels of information to be provided by the chief audit executive.
- Minutes or other documentation of communication between the board and senior management in which the internal audit function's unrestricted access was discussed.
- A jointly agreed-upon matrix or similar documentation showing what information should be communicated by the chief audit executive to the board.
- Documentation of discussion of access to the data, records, personnel, and physical properties required to perform internal audit services.

Principle 7 Positioned Independently

The board establishes and protects the internal audit function's independence.

The board is responsible for ensuring the independence of the internal audit function. Independence is defined as the freedom from conditions that impair the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner. Independence is established through accountability to the board, access to relevant resources, and freedom from interference. The internal audit function is only able to achieve the Purpose of Internal Auditing fully when the chief audit executive reports directly to the board and is positioned at a level within the organization that enables the internal audit function to perform its services and responsibilities without interference.

Standard 7.1 Organizational Independence

Requirements

Board Responsibilities

To enable the internal audit function to fulfill its mandate, the board must establish a direct reporting relationship with the chief audit executive and the internal audit function.

As part of a direct reporting relationship, the board must:

- Approve and/or participate in decisions regarding the appointment, removal, performance evaluation, and remuneration of the chief audit executive.
- Provide the chief audit executive with opportunities to discuss significant and sensitive matters with the board, including meetings without senior management present.
- Ensure that the chief audit executive is positioned at a level that enables internal audit services and responsibilities to be performed without interference from any level of management and provides the organizational authority and status to bring matters directly to senior management and/or the board and to escalate matters to the board when necessary.
- Ensure that the internal audit function is free from interference when determining its scope, performing internal audit engagements, and communicating results.

Chief Audit Executive Responsibilities

At least annually, the chief audit executive must confirm to the board the organizational independence of the internal audit function. This includes communicating incidents where independence may have been impaired and the actions or safeguards employed to address the impairment. (See also 7.3 Safeguarding Independence.)

Joint Responsibilities

The chief audit executive must document in the internal audit charter the reporting relationships and organizational placement, as determined by the board. The board must approve the internal audit charter.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Board Practices

The chief audit executive's reporting relationships and the organizational placement of the internal audit function are not determined solely by the chief audit executive. Typically, the board, senior management, and the chief audit executive discuss the reporting relationships that best enable the internal audit function to fulfill its mandate.

Internal auditing is most effective when the internal audit function is directly accountable to the board (also known as "functionally reporting to the board" or "a functional reporting relationship with the board"), rather than directly accountable to management of the activities over which it provides assurance and advice. A direct reporting relationship between the board and the chief audit executive enables the board to ensure that the internal audit function can perform internal audit services and communicate engagement findings, conclusions, and other results without interference or undue limitations. Examples of interference include management failing to provide requested information timely and restricting access to information, personnel, or physical properties. Limiting budgets or resources in a way that prohibits the internal audit function's ability to operate effectively is an example of undue limitation. (See also Standard 7.3 Safeguarding Independence and Standard 11.3 Communicating Results.)

Organizational independence of the internal audit function also depends upon the chief audit executive reporting directly to the board. By reporting directly to the board, the chief audit executive is able to avoid conditions that impair the ability of the internal audit function to carry out its responsibilities in an unbiased manner, such as receiving excessive pressure from the management of an activity under review to change findings or conclusions.

The board may demonstrate its understanding of the importance of the direct reporting relationship with the chief audit executive by confirming the relationship is documented in the board's charter, in addition to its required documentation in the internal audit charter.

The board should ensure the chief audit executive reports to a level within the organization that enables access to senior management and the authority to challenge management's judgments (often referred to as the chief audit executive's "administrative reporting relationship"). To achieve this authority, it is usually ideal for the chief audit executive to report administratively to the chief executive officer or equivalent, although reporting to another senior officer may achieve the same objective as long as appropriate safeguards are implemented. Subsidiary, branch, and divisional heads of the internal audit function also should report to a level commensurate to the senior management responsible for those areas.

Chief Audit Executive Practices

The chief audit executive should provide the board with information necessary for the board to evaluate whether the reporting relationships and organizational placement of the internal audit function support the function's ability to carry out its responsibilities in an unbiased manner. The chief audit executive establishes criteria and processes for discussing matters with senior management and the board. (See Standard 7.3 Safeguarding Independence and Principle 11 Communicates Effectively and relevant standards for additional requirements and considerations.)

Public Sector

In public sector organizations, the board may not have authority over the decisions to appoint, remove, or set remuneration for the chief audit executive. Additionally, members of the board who are external to the organization, such as elected members or nonexecutive directors, may not have authority to be involved with the appointment of the chief audit executive. Still, the board should advise management regarding performance evaluations and decisions to appoint and remove the chief audit executive.

Additionally, some chief audit executive positions in the public sector are elected positions, determined by public voting. Others may be appointed by governing bodies other than the board. In some cases, the reporting relationships for the chief audit executive and positioning of the internal audit function in the public sector are established by law or regulation.

Evidence of Conformance

- The internal audit charter, which documents the internal audit function's reporting relationships.
- Meeting minutes or other evidence of the chief audit executive's direct communication with senior management and the board.
- Board meeting minutes or other documentation showing that the chief audit executive confirmed with the board the ongoing independence of the internal audit function or discussed impairments affecting the internal audit function's ability to fulfill its mandate and the safeguards to manage the impairments.
- Board meeting minutes or other documentation showing the board was involved in decisions regarding the chief audit executive's appointment, removal, performance evaluation, and remuneration.

Standard 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications

Requirements

Board Responsibilities

The board must approve the chief audit executive's roles and responsibilities and identify the necessary qualifications and competencies to carry out these roles and responsibilities.

The board must ensure the chief audit executive has the qualifications and competencies to manage the internal audit function effectively and ensure quality performance of internal audit services.

The chief audit executive's primary role is to manage the internal audit function, including its performance of internal audit services, as described in Domain IV. Managing the Internal Audit Function. The board must understand the actual or potential impairments to the internal audit function's independence before assigning the CAE additional roles or responsibilities beyond the scope of internal auditing.

If nonaudit roles and responsibilities impair or appear to impair the internal audit function's independence, the board must ensure appropriate safeguards are implemented. (See also Standard 7.3 Safeguarding Independence.)

Chief Audit Executive Responsibilities

The chief audit executive must provide the board with the information it needs to understand the qualifications, competencies, and requirements necessary to manage the internal audit function.

Before taking on any nonaudit roles and responsibilities, the chief audit executive must communicate the implications of such and propose safeguards to manage actual, potential, and perceived impairments to the board.

After taking on any approved nonaudit roles and responsibilities, the chief audit executive must confirm to the board that appropriate safeguards to the internal audit function's independence have been implemented and are effective.

The chief audit executive must take responsibility for maintaining and enhancing the qualifications and competencies necessary to fulfill the roles and responsibilities expected by the board. (See also Principle 3 Demonstrate Competency and relevant standards.)

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The board should collaborate with senior management to determine which competencies and qualifications the organization expects in a chief audit executive. The competencies may vary according to the internal audit mandate, the complexity and specific needs of the organization, the organization's risk profile, and the industry and jurisdiction within which the organization operates, among other factors. The desired competencies and qualifications are typically documented in a job description and typically include:

- A comprehensive understanding of the Global Internal Audit Standards and leading internal audit practices.
- Industry or sector experience.
- Building an effective internal audit function by recruiting, hiring, and training internal auditors and helping them develop relevant competencies.
- Certified Internal Auditor designation or other relevant professional education, certifications, and credentials.

While this list includes ideal competencies and qualifications, the chief audit executive may be selected for other leadership qualities or areas of expertise that are supplemented by the competencies of other members of the internal audit function, especially when the chief audit executive has entered the position from a different role, industry, or sector. In such cases, the chief audit executive should work collaboratively with knowledgeable members of the internal audit function to gain relevant experience.

The board also should encourage the chief audit executive to pursue continuing professional education, membership in professional associations, professional certifications, and other opportunities for professional development. (See also Principle 3 Demonstrate Competency and relevant standards).

In addition to the responsibilities of managing the internal audit function, the chief audit executive is sometimes asked to take on nonaudit roles for which management is normally responsible, which may impair or appear to impair the internal audit function's independence. Examples include situations such as:

- A new regulatory requirement prompts an immediate need to develop policies, procedures, controls, and risk management activities to ensure compliance.
- The chief audit executive has the most appropriate expertise to adapt existing risk management activities to a new business segment or geographic market.
- The organization's resources are too constrained or the organization is too small to afford a separate compliance function.
- The organization's processes are immature, and the chief audit executive has the most appropriate expertise to initiate a risk management plan or program.
- The organization expects the internal audit function to be responsible for managing the effectiveness of the system of internal control and any specific control processes.
- The chief audit executive has been responsible for an activity under review within the last 12 months.

Board Practices

Before a chief audit executive is hired, the board should be involved in the recruitment and appointment process. For example, the board may discuss the qualifications and competencies necessary to manage the internal audit function and perform any additional roles and responsibilities expected by the organization. The board may review and approve the job description for the chief audit executive to ensure it reflects the expected qualifications and competencies. Additionally, the board should participate in the decision to appoint the chief audit executive by reviewing candidates' résumés or curricula vitae and participating in interviews before a candidate is selected.

The board should discuss any nonaudit roles and responsibilities with the chief audit executive and senior management to ensure a shared understanding of the rationale, risks, and plans to ensure impairments to independence are managed (See also Standard 7.3 Safeguarding Independence). Considerations should

include whether the roles and responsibilities are intended to be a long-term or permanent part of the chief audit executive's responsibilities or are temporary and intended to be transferred to a member of management.

Chief Audit Executive Practices

During discussions of nonaudit roles and responsibilities, the chief audit executive should emphasize the standards and considerations related to independence, how those support objectivity, and the risks of impairment presented by the proposed roles and responsibilities. The chief audit executive is likely to be well-informed about potential safeguards to manage the risks and should make suggestions aligned with Standard 7.3 Safeguarding Independence.

Evidence of Conformance

- Documented approval by the board of the chief audit executive's job description and/or appointment or other evidence that the board evaluated the qualifications and competencies required for the chief audit executive's role.
- Meeting minutes or other notes from discussions of nonaudit roles and responsibilities, potential impairments, and board approved plans for safeguards.
- Internal audit charter documenting board approval of long-term nonaudit roles and responsibilities and corresponding safeguards to independence, including the expected duration of the roles, responsibilities, and safeguards and how the effectiveness of the safeguards will be evaluated periodically.

Standard 7.3 Safeguarding Independence

Requirements

Safeguards must be in place to manage impairments to the internal audit function's independence.

Board Responsibilities

The board must protect the independence of the internal audit function by ensuring safeguards to manage the risk of impairment are designed adequately and operating effectively.

Chief Audit Executive Responsibilities

The chief audit executive must discuss with the board any current or proposed roles and responsibilities that have the potential to impair the internal audit function's independence, either in fact or appearance. The chief audit executive must advise the board on the different types of safeguards that may be appropriate to address each impairment.

The chief audit executive must discuss any impairment affecting the ability of the internal audit function to perform its duties independently with senior management and the board and seek their support to resolve the situation.

Additionally, the chief audit executive must disclose existing impairments to senior management and other appropriate parties. To determine the other parties to which disclosure should be made, the chief audit executive must take into account the nature of the impairment, the impairment's impact on the reliability of the results of internal audit services, and the expectations of relevant stakeholders. If an impairment is discovered after an

engagement has been completed and it affects the reliability or perceived reliability of the engagement findings, recommendations, and/or conclusions, the chief audit executive should discuss the concern with the management of the activity under review, senior management, the board, and/or other affected stakeholders and determine the appropriate actions to resolve the situation. (See also Standard 11.4 Errors and Omissions.)

Joint Responsibilities

When the chief audit executive has ongoing nonaudit responsibilities, the responsibilities, the nature of work, and established safeguards must be documented in the internal audit charter. If those areas of responsibility are subject to internal auditing, alternative processes to obtain assurance must be established, such as contracting with an objective, competent assurance provider from outside the organization that reports independently to the board.

When the chief audit executive's nonaudit responsibilities are temporary, assurance for those areas must be overseen by an independent third party both during the temporary assignment and for the subsequent 12 months. If the chief audit executive's nonaudit responsibilities are temporary, a plan must be established to transition the nonaudit responsibilities to management.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Situations that may introduce impairments to independence include:

- The chief audit executive lacking direct communication or interaction with the board.
- Management attempting to limit the scope of the internal audit services that were previously approved by the board and documented in the internal audit charter.
- Management attempting to restrict access to the data, records, and other information as well as personnel and physical properties required to perform the internal audit services.
- Management pressuring internal auditors to suppress or change internal audit findings.
- The budget for the internal audit function being reduced to a level whereby the function is unable to fulfill its responsibilities as outlined in the internal audit charter.
- An assurance engagement being performed by the internal audit function or supervised by the chief audit executive in a functional area for which the chief audit executive is responsible, has oversight, or is otherwise able to exert significant influence. (See also Standard 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications.)
- The internal audit function performing or chief audit executive supervising assurance services related to an activity that is managed by a senior executive to which the chief audit executive reports administratively. For example, the chief audit executive reporting to the chief financial officer and being responsible for auditing treasury, a function that also reports to the chief financial officer.

Board Practices

The board's oversight activities include monitoring impairments to the internal audit function's independence and ensuring safeguards are in place to manage any impairments. The board should discuss with senior management and the chief audit executive the nature and cause of potential, perceived, and actual impairments as well as proposed safeguards to independence. Safeguards include activities such as periodically evaluating reporting lines and responsibilities and developing alternative processes to obtain assurance in areas where independence may be impaired.

The board should be specific about how safeguards will be implemented, by whom, and when. An interim safeguard may be applied until a permanent one is implemented. At least annually and whenever responsibilities change, the board should verify that the safeguards are still operating effectively.

Chief Audit Executive Practices

Based on an understanding of the standards related to independence, the chief audit executive should evaluate conditions including reporting relationships, roles, and responsibilities to determine whether actual, potential or perceived impairments exist. The chief audit executive should proactively communicate with senior management and the board about independence and impairments to educate them and understand their expectations. Additionally, the chief audit executive may be able to resolve situations of perceived impairments that do not in fact affect the internal audit function's ability to perform its responsibilities in an unbiased manner through discussions with the concerned parties.

Joint Practices

Plans for the chief audit executive to accept nonaudit roles and responsibilities should:

- Include safeguards to independence.

- Identify potential impacts to the internal audit plan and resources.
- Specify a timeline for transitioning any temporary nonaudit responsibilities to management, if applicable.

Evidence of Conformance

- Meeting minutes and other documentation showing that impairments to independence were discussed with senior management, the board, and other relevant stakeholders.
- Meeting minutes and other documentation showing that safeguards to manage the risk of impairment were agreed upon by appropriate parties, were designed adequately, and are operating effectively.
- Documented policies and procedures to be followed when an impairment is suspected or identified.
- Formal action plans that outline specific safeguards to address independence concerns.
- Documentation of assurance services to be provided by other internal or external providers as a safeguard to independence.

Principle 8 Overseen by the Board

The board oversees the internal audit function to ensure the function's effectiveness.

Board oversight is essential to ensure the overall effectiveness of the internal audit function. Achieving this principle requires collaborative and interactive communication between the board and the chief audit executive as well as the board's support in ensuring the internal audit function obtains sufficient resources to fulfill the internal audit mandate. Additionally, the board receives assurance about the quality of the performance of the chief audit executive and the internal audit function through the quality assessment and improvement program, including the board's direct review of the results of the external quality assessment.

Standard 8.1 Board Interaction

Requirements

Board Responsibilities

The board must interact with the internal audit function to understand the effectiveness of the organization's governance, risk management, and control processes.

Board oversight must include ongoing communication with the chief audit executive to ensure the internal audit function is fulfilling the internal audit mandate. The board must communicate its perspective on the organization's strategies, objectives, and risks to assist the chief audit executive with determining internal audit priorities.

The board must set expectations for:

- The frequency of communications with the chief audit executive.

- The criteria for determining which issues should be escalated to the board, such as significant or material risks that exceed the board's risk tolerance.
- The process for escalating communications from management to the board.

Chief Audit Executive Responsibilities

The chief audit executive must provide the board with the information needed to conduct its oversight responsibilities. In addition to communications about the internal audit mandate and independence, the chief audit executive must communicate the results of internal audit services, including conclusions, assurance, advice, and insights to help the board fulfill its responsibilities. (See also Standard 11.3 Communicating Results.)

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Board Practices

The frequency of communications between the board and the chief audit executive should take into account the need for timely communication about significant issues. The board should communicate its perspectives and expectations related to understanding and oversight of not just financial risk management but also a broad range of nonfinancial governance and risk management concerns including strategic initiatives, cybersecurity, health and safety, sustainability, business resilience, and reputation. To identify the issues the board expects the chief audit executive to escalate beyond senior management, the board may set criteria for significance or materiality that exceed the board's risk tolerance. The criteria should be linked to a process that the chief audit executive will follow to escalate communications from management to the board.

Typically, formal board meetings may allow formal communication at least quarterly. Additionally, the chief audit executive and board members often communicate between meetings as needed, sometimes informally.

Through discussions with the chief audit executive and senior management, the board should gain reasonable confidence that information reported by the chief audit executive is not restricted or modified by senior management in a way that alters the meaning of the information or diminishes the impact of the reporting.

Chief Audit Executive Practices

To provide the board with timely communications, the chief audit executive may use a variety of methods such as written and oral reports and presentations, formal meetings, and informal discussions. The chief audit executive may document the board's expectations formally, in policies and procedures. Periodically, the chief audit executive should confirm with the board that the frequency, nature, and content of communications meet the board's expectations and help the board achieve its oversight responsibilities.

Evidence of Conformance

- Board agendas and meeting minutes documenting the nature and frequency of discussions with the chief audit executive.
- Presentations made by the chief audit executive to the board.
- Internal audit communications to board members.
- Criteria for identifying issues to be brought to the attention of the board and process for communicating such issues, sometimes known as an "escalation matrix."
- Document showing how communications from the chief audit executive support the board's expectations as noted in its charter.

Standard 8.2 Resources

Requirements

Board Responsibilities

The board must ensure the internal audit function has sufficient resources to fulfill the internal audit mandate and achieve the internal audit plan.

At least annually, the board must ask the chief audit executive about the sufficiency of internal audit resources to fulfill the internal audit mandate and achieve the internal audit plan. The board must consider the impact of insufficient resources on the mandate and plan. If the resources are determined to be insufficient, the board must inform senior management of the issue, its potential impact on the internal audit plan, and advocate for the necessary resources.

Chief Audit Executive Responsibilities

The chief audit executive must propose a strategy to obtain sufficient resources and must inform the board when internal audit resources are insufficient to fulfill the internal audit mandate and achieve the internal audit plan.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Board Practices

In addition to including a discussion of the sufficiency of internal audit resources on its agenda annually, the board should request to review documents related to the chief audit executive's resourcing strategy and should analyze the relationship between the internal audit function's resources and its ability to fulfill the mandate and achieve the plan. The board should implement a process for advising or giving input to senior management that helps support the chief audit executive in obtaining sufficient resources.

Chief Audit Executive Practices

The chief audit executive should periodically evaluate whether resources are sufficient to fulfill the internal audit mandate and achieve the internal audit plan and should inform the board of any resourcing concerns in a timely manner. To analyze the sufficiency of the financial, human, and technological resources necessary to fulfill the mandate and achieve the plan, the chief audit executive should perform a gap analysis between an inventory of the resources within the internal audit function and those needed to perform internal audit services. (See also Principle 10 Manages Resources.) The chief audit executive's strategy should include providing a resource plan, which may include a budget request, and should take into account options for staffing the internal audit function as well as using technology to perform services. The chief audit executive should perform a cost-benefit analysis of the various approaches to present to the board.

Joint Practices

Although a discussion of resources between the board and the chief audit executive is required at least annually, having a quarterly discussion is a leading practice. The discussion should include considering the options to achieve the desired internal audit coverage, including outsourcing or using guest auditors, as well as implementing technology to improve the internal audit function's efficiency and effectiveness.

Public Sector

In the public sector, the board may not have the authority to allocate resources to the internal audit function due to law, statute, or governance structure. Also, budgets may be approved at another tier or branch of government, such as the parliament or legislature, particularly in provincial or state governments, where the legislature approves the budget for each agency. Still, the chief audit executive must inform the board of any resource limitations so the board can provide input to senior management or the appropriate budgeting authority on the need for sufficient resources to fulfill the internal audit mandate and achieve the internal audit plan.

Evidence of Conformance

- Agendas, meeting minutes, and communications between the chief audit executive and the board and/or senior management, documenting discussions of the sufficiency of internal audit resources.
- Internal audit resource plans indicating the sufficiency of resources needed to achieve the internal audit plan.
- Budget requests pertaining to internal audit resources.
- Documentation of gap analyses between the internal audit plan and known resources.
- Documentation of the chief audit executive's resourcing strategy.

Standard 8.3 Quality

Requirements

Board Responsibilities

The board must ensure that the chief audit executive develops, implements, and maintains a quality assurance and improvement program.

A quality assurance and improvement program is designed to evaluate whether the internal audit function conforms with the Standards and achieves its performance objectives. Additionally, the program is intended to ensure the internal audit function pursues continuous improvement.

The program must include two types of assessments:

- External assessments. (See Standard 8.4 External Quality Assessment.)
- Internal assessments. (See Standard 12.1 Internal Quality Assessment.)

At least annually, the board must approve the internal audit function's performance objectives. (See Standard 12.2 Performance Measurement.)

The board must conduct or participate with senior management in an annual assessment of the chief audit executive's performance. Such an assessment includes:

- Reviewing the internal audit function's performance objectives, including its conformance with the Standards and any additional regulations, ability to meet the internal audit mandate, and progress toward completion of the internal audit plan.
- Considering the results of the internal audit function's quality assurance and improvement program.
- Determining the extent to which the internal audit function's performance objectives are being met.
- Reviewing and contributing to the organization's assessment of the chief audit executive's performance.

Chief Audit Executive Responsibilities

The chief audit executive must develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the internal audit function. At least annually, the chief audit executive must communicate the results of the internal quality assessment to the board. Such communications include:

- The internal audit function's conformance with the Standards and achievement of performance objectives.
- Plans to address the internal audit function's deficiencies and opportunities for improvement.

Considerations for Implementation and Evidence of Conformance

Implementation

Board Practices

The board's annual assessment of the chief audit executive should include:

- The level of contribution to the improvement of governance, risk management, and control processes.
- Increased internal audit staff productivity.
- Increased cost efficiency of the internal audit process.
- Adequate engagement planning and supervision.
- Effectiveness in building relationships and meeting the needs of stakeholders.

The board's assessment should contain qualitative and quantitative measures. Performance measures should be specific to the organization and meaningful to the internal audit function.

Chief Audit Executive Practices

The chief audit executive should ensure the board obtains the necessary information to provide oversight of the internal audit function's quality assurance and improvement program, including:

- The scope, frequency, and results of internal and external quality assessments conducted under the direction of or assisted by the chief audit executive.
- Action plans that address opportunities for improvement. Any such actions should be agreed upon with the board.
- Progress toward completing the agreed-upon actions.

Public Sector

The quality assurance and improvement program should include compliance with any laws or regulations governing the internal audit function in the jurisdiction within which the organization operates.

Evidence of Conformance

- Agendas and minutes from board meetings documenting discussions with the chief audit executive about the internal audit function's quality assurance and improvement program.
- Chief audit executive presentations and other communications covering the results of the quality assessments and status of action plans to address any opportunities for improvement.
- Minutes from board meetings or other documentation showing that the board reviewed and contributed to the chief audit executive's performance assessment.

Standard 8.4 External Quality Assessment

Requirements

The board must ensure an external quality assessment of the internal audit function is conducted at least every five years.

The external quality assessment must be conducted by an independent assessor or assessment team that is qualified in the professional practice of internal auditing as well as the quality assessment process. To be independent, the assessor or assessment team must be from outside the organization, not an employee or otherwise a part of or under the control of the organization in which the internal audit function operates. Independent assessors, assessment teams, and their organizations must be free from actual, potential, or perceived conflicts of interest that could impair their objectivity.

The external quality assessment requires a comprehensive review of the adequacy of the internal audit function's:

- Mandate, charter, strategy, methodologies, processes, risk assessment, and internal audit plan.
- Conformance with the Global Internal Audit Standards.
- Performance criteria and measures as well as assessments results.
- Competencies, including the sufficient use of tools and techniques and focus on process improvement.
- Integration into the organization's governance process, including the relationships between and among those involved in that process.
- Contribution to the organization's governance, risk management, and control processes.
- Contribution to the improvement of the organization's operations and ability to attain its objectives.
- Effectiveness and efficiency in meeting expectations codified by the board, senior management, and stakeholders.

External quality assessments are conducted in two ways: an external assessment performed by an independent third party or a self-assessment with independent validation.

Board Responsibilities

The board must determine the scope and frequency of the external quality assessment. When defining the scope, the board must consider the responsibilities of the internal audit function and the chief audit executive, as contained in the internal audit charter, and regulatory requirements that may affect the internal audit function.

The chief audit executive's plan for the performance of an external quality assessment must be reviewed and approved by the board. Such approval must cover, at a minimum:

- The scope and frequency of assessments.
- The competencies and independence of the external assessor, assessment team, or individual selected to validate a self-assessment.
- The rationale for conducting a self-assessment with independent validation rather than an external quality assessment performed by an independent third party.

The board must receive the complete results of the external quality assessment or self-assessment with independent validation directly from the assessor. The board must review and approve the chief audit executive's

action plans to address identified deficiencies and opportunities for improvement. Additionally, the board must approve a timeline for completion of the action plans and monitor the chief audit executive's progress.

Chief Audit Executive Responsibilities

The chief audit executive must develop a plan for the performance of an external quality assessment and obtain the board's approval. The external assessment must be conducted by a qualified, independent assessor or assessment team from outside the organization. When selecting the independent assessor, assessment team, or individual to validate a self-assessment, the chief audit executive must ensure the following criteria are met. To be qualified, the independent assessor or assessment team must evidence:

- Experience with and knowledge of the Standards and leading internal audit practices.
- Experience as a chief audit executive or comparable senior level of internal audit management.
- Previous experience performing external quality assessments.
- Completion of external quality assessment training recognized by The IIA.
- At least one person on the team with an active Certified Internal Auditor designation.
- Attestation to the absence of conflicts of interest, in fact or appearance.

Self-assessment with Independent Validation

The requirement for an external quality assessment may be met periodically through a self-assessment with independent validation. However, a self-assessment with independent validation does not fully replace the requirement for the internal audit function to conduct external quality assessments. The self-assessment may be alternated with the external quality assessment once every ten years.

The self-assessment typically is conducted by the internal audit function, then validated by a qualified, independent external assessor. A self-assessment with independent validation is more limited in scope and consists of:

- A comprehensive and fully documented self-assessment process that emulates the external quality assessment process in terms of evaluating the internal audit function's conformance with the Standards.
- Onsite validation by a qualified, independent external quality assessor. The independent validation must determine that the self-assessment was conducted completely and accurately.
- Consideration of benchmarking, leading practices, and interviews with key stakeholders, such as board members, senior management, and operational management.

Considerations for Implementation and Evidence of Conformance

Implementation

Chief audit executive

The chief audit executive should be aware of potential impairments of independence of assessors. Examples of potential impairments include past, present, or future relationships with the organization, its personnel, or its internal audit function (for example, external audit of financial statements, assistance to the internal audit function, personal relationships, previous or future participation in internal quality assessments, or advisory services in governance, risk management, financial reporting, internal control, or other related areas).

If a potential assessor is a former employee of the organization, the length of time the assessor has been independent should be considered.

Individuals from another department of the organization, although organizationally separate from the internal audit activity, are not considered independent for the purpose of conducting an external assessment. In the public sector, internal audit functions in separate entities within the same tier of government are not considered independent if they report to the same chief audit executive. Likewise, individuals from a related organization (for example, 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) are not considered independent.

Reciprocal peer assessments between two organizations are not considered independent. However, reciprocal assessments among three or more peer organizations — organizations within the same industry, regional association, or other affinity group — may be considered independent. Care must be exercised to ensure that independence and objectivity are not impaired and all team members are able to exercise their responsibilities fully.

Joint Practices

The board should gain an understanding of the internal audit function's processes for ensuring quality and conformance with the Standards, including the process related to external quality assessments.

The Standards require the internal audit function to undergo an external quality assessment at least once every five years. However, the board and chief audit executive may determine that it is appropriate to conduct an external assessment more frequently. There are several reasons to consider a more frequent review, including changes in leadership (for example, senior management or the chief audit executive), significant changes in internal audit policies or procedures, the merger of two or more internal audit organizations into one internal audit function, or significant staff turnover. Additionally, some organizations, such as those in highly regulated industries or those directly serving the public, may prefer or be required to increase the frequency or scope of the external quality assessments.

The board and chief audit executive typically collaborate to determine whether such adjustments are necessary.

Rather than contracting a service provider to perform an external quality assessment, an organization may reduce costs by working with two or more organizations in the same industry or geographic area to conduct a series of assessments. To achieve the requisite independence, two organizations cannot directly assess one another. However, a group of three or more organizations may enter an agreement whereby A assesses B, B assesses C, and C assesses A, for example.

Qualifications and Competencies of External Assessors

In addition to the required qualifications and independence criteria outlined in the Standards, it is preferred practice that the leader of the external quality assessment team holds an active Certified Internal Auditor designation.

Public Sector

The external quality assessment of an internal audit function in the public sector should include team members knowledgeable of public sector activities and governance structures.

Evidence of Conformance

- Formal external quality assessment report prepared by a qualified, independent assessor.
- Presentations to the board by external assessors covering the results of the external quality assessment.
- Chief audit executive presentations to the board covering external assessment results and action plans, as appropriate.
- Board meeting minutes where the chief audit executive's external quality assessment plan is discussed and approved by the board.
- Board meeting minutes where the external quality assessor's qualifications and independence is discussed and confirmed.
- The chief audit executive's documented rationale for performing a self-assessment with independent validation.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

IV. Managing the Internal Audit Function

The chief audit executive is responsible for managing the internal audit function in accordance with the internal audit charter and Global Internal Audit Standards. This responsibility includes strategic planning, obtaining and deploying resources, building relationships and communicating with stakeholders to provide objective assurance and advice, and ensuring and enhancing the performance of the function.

The individual responsible for managing the internal audit function is expected to conform with the Standards including performing the responsibilities described in this domain whether the individual is directly employed by the organization or contracted through an external service provider.

The specific job title and responsibilities may vary across organizations. For example, the chief audit executive may have a title such as “auditor general,” “head of internal audit,” “chief internal auditor,” “internal audit director,” or “inspector general.” The chief audit executive may delegate responsibilities to other qualified professionals in the internal audit function but retains ultimate accountability.

The direct reporting relationship between the board and the chief audit executive enables the internal audit function to fulfill its mandate. (See also Standard 7.1 Organizational Independence.) In addition, the chief audit executive typically has an administrative reporting line to the highest-ranking person in senior management, such as the chief executive officer, to support day-to-day activities and establish the status and authority necessary to ensure the results of the internal audit services are given due consideration.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Principle 9 Plans Strategically

The chief audit executive plans strategically to ensure the internal audit function fulfills its mandate and is positioned for long-term success.

Planning strategically requires the chief audit executive to understand the internal audit mandate and the organization's governance, risk management, and control processes. The internal audit strategy ensures the function is sufficiently resourced and positioned to support the organization's success. The internal audit charter documents the internal audit mandate, the scope and priorities of internal audit services, and the conditions that support the function's ability to fulfill the mandate. In addition, the chief audit executive creates and implements methodologies to guide the internal audit function and an internal audit plan to deliver the strategy.

Standard 9.1 Understanding Governance, Risk Management, and Control Processes

Requirements

To develop an effective internal audit strategy, charter, and plan, the chief audit executive must understand the organization's governance, risk management, and control processes.

To understand governance processes, the chief audit executive must consider how the organization:

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

To understand risk management and control processes, the chief audit executive must consider how the organization identifies and assesses significant risks and selects appropriate control processes. This includes understanding how the organization identifies and manages the following key risk areas:

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

Considerations for Implementation and Evidence of Conformance

Implementation

The chief audit executive's understanding is developed by gathering information broadly and viewing it comprehensively. Sources of information include discussions with senior management and the board, communications and workpapers from internal audit engagements, and assessments and reports completed by other providers of assurance and advisory services.

Understanding Governance Processes

The chief audit executive should be well informed about leading governance principles, globally accepted governance frameworks and models, and professional guidance specific to the industry and sector within which the organization operates. Based on the knowledge, the chief audit executive should identify whether any of these have been implemented in the organization and should gauge the maturity of the organization's governance processes. The organization's governance structure, processes, and practices may be affected by unique organizational characteristics such as the type, size, complexity, structure, and process maturity as well as the legal and regulatory requirements to which the organization is subject.

The chief audit executive may review board and committee charters and agendas and minutes from their meetings to gain additional insight into the role the board plays in the organization's governance, especially regarding strategic and operational decision-making.

The chief audit executive may speak with individuals in key governance roles (for example, the board chair, top elected or appointed official in a governmental entity, chief ethics officer, human resources officer, chief compliance officer, and chief risk officer) to gain a clearer understanding of the organization's processes and assurance activities. The chief audit executive may review the reports and/or results of previously completed governance reviews, paying particular attention to any identified concerns.

Understanding Risk Management Processes

The chief audit executive should understand globally accepted risk management principles, frameworks, and models as well as professional guidance specific to the industry and sector within which the organization operates. The chief audit executive should gather information to assess the maturity of the organization's risk management processes, including identifying whether the organization has defined its risk appetite and implemented a risk management strategy and/or framework. Discussions with senior management and the board help the chief audit executive understand their perspectives and priorities related to the organization's risk management.

To gather risk information, the chief audit executive should review recently completed risk assessments and related communications issued by senior and operational management, those charged with risk management, external auditors, regulators, and other internal and external providers of assurance services.

Understanding Control Processes

The chief audit executive should become familiar with globally accepted control frameworks and consider those used by the organization. For each identified organizational objective, the chief audit executive should develop and maintain a broad understanding of the organization's control processes and their effectiveness. The chief audit executive may develop an organizationwide risk and control matrix to:

- Document identified risks that may affect the ability to achieve organizational objectives.
- Indicate the relative significance of risks.
- Understand key controls in organizational processes.
- Understand which controls have been reviewed for design adequacy and deemed to be operating as intended.

A thorough understanding of the organization's governance, risk management, and control processes enables the chief audit executive to identify and prioritize opportunities to provide internal audit services that can enhance the organization's success. The identified opportunities form the basis of internal audit strategy and plan.

Evidence of Conformance

- Documented frameworks and processes used by the organization for governance, risk management, and/or controls.
- Risk appetite statement.
- Agendas and minutes from board meetings indicating discussion of the organization's governance, risk management, and control processes, including the strategies, approaches, and oversight of each.
- Board and committee charters.
- Meeting minutes or notes from discussions with those in the organization with roles in governance and risk management.
- Laws, regulations, and other requirements for governance, risk management, and controls.
- Communications received from regulators.
- Business strategies and business plans.
- Organizationwide risk and control matrix.

Standard 9.2 Internal Audit Strategy

Requirements

The chief audit executive must develop and implement a strategy for the internal audit function that supports the strategic objectives and success of the organization and aligns with the expectations of senior management, the board, and other key stakeholders.

The internal audit strategy must include a vision, strategic objectives, and supporting initiatives for the internal audit function.

The chief audit executive must review the internal audit strategy with senior management and the board at least annually.

Considerations for Implementation and Evidence of Conformance

Implementation

An internal audit strategy helps guide the internal audit function toward the fulfillment of the internal audit mandate. To develop the vision and strategic objectives of the internal audit strategy, the chief audit executive should start by considering the organization's strategy and objectives and the expectations of senior management and the board. The chief audit executive may also consider the types of services to be performed and the expectations of other stakeholders served by the internal audit function, as agreed in the internal audit mandate. In addition to fulfilling the requirement to review the internal audit strategy with senior management and the board at least annually, the chief audit executive may seek approval from the board.

The vision describes the desired future state – in the next three to five years, for example – of the internal audit function and provides direction to help the function fulfill its mandate. The vision is also designed to inspire and motivate internal auditors and the function to continuously improve. The strategic objectives define actionable targets to attain the vision. The supporting initiatives outline more specific tactics and steps for achieving each strategic objective.

One approach to developing a strategy is to identify and analyze the internal audit function's strengths, weaknesses, opportunities, and threats – an exercise designed to determine ways to improve the function. Another approach is to perform a gap analysis between the current and the desired states of the internal audit function.

The initiatives supporting the strategy should include:

- Opportunities to help internal auditors develop their competencies.
- The introduction and application of technology when it improves the internal audit function's efficiency and effectiveness.
- Opportunities to improve the internal audit function as a whole.

When the chief audit executive determines the strategic objectives and supporting initiatives, the actions to be taken should be prioritized and assigned target dates.

The internal audit strategy should be adjusted whenever there are changes in the organization's strategic objectives or stakeholders' expectations. Factors that may prompt a more frequent review of the internal audit strategy include:

- Changes in the organization's strategy or the maturity of its governance, risk management, and control processes.
- Changes in the organization's policies and procedures or the laws and regulations to which the organization is subject.
- Changes in senior management, members of the board, or the chief audit executive.
- Results of internal and external assessments of the internal audit function.

The chief audit executive may delegate specific responsibilities related to the strategic objectives and initiatives among members of the internal audit function. Additionally, the chief audit executive may design a timeline for implementation as well as key performance indicators and a self-assessment process to measure whether the strategy is achieved. The annual review of the internal audit strategy should include a discussion of the internal audit function's progress on initiatives.

Evidence of Conformance

- Documented internal audit strategy, including vision, strategic objectives, and supporting initiatives.

- Minutes or correspondence from meetings with senior management, the board, and/or other stakeholders where expectations were discussed.
- Notes showing the information and analyses that informed the strategy.
- Internal audit policies and procedures for producing and reviewing the internal audit strategy and monitoring its implementation.
- Results of self-assessments or other reviews of the progress on initiatives.

Standard 9.3 Internal Audit Charter

Requirements

The chief audit executive must develop and maintain an internal audit charter that specifies at a minimum the internal audit function's:

- Purpose of Internal Auditing.
- Commitment to adhere to the Global Internal Audit Standards.
- Mandate and board's responsibilities to support the internal audit function.
- Organizational position and reporting relationships.
- Responsibilities of the internal audit function, including scope and types of services to be provided.
- Commitment to quality assurance and improvement.

If assurances are to be provided to parties outside the organization, the nature of these assurances also must be defined in the internal audit charter.

The chief audit executive must discuss the charter with senior management and the board and obtain board approval. The chief audit executive and the board must review the charter periodically. If changes are needed, the chief audit executive must seek the board's approval of the revised charter. (See also Standard 6.1 Internal Audit Mandate.)

Considerations for Implementation and Evidence of Conformance

Implementation

Although internal audit charters may vary by organization, the charter typically includes the following topics:

- Introduction – indicates the Purpose of Internal Auditing and the internal audit function’s commitment to ethics and professionalism, conformance with the Standards, and compliance with relevant laws and regulations (specified as needed). (See Domains I and II.)
- Mandate – specifies the authority, roles, and responsibilities of the internal audit function and the chief audit executive as approved by the board. (See Standard 6.1 Internal Audit Mandate.)
- Organizational position and reporting relationships – documents the chief audit executive’s reporting relationship and the internal audit function’s organizational position, which together enable organizational independence. (See Standards 7.1 Organizational Independence and 7.2 Chief Audit Executive Roles, Responsibilities, and Qualifications.) This section should define the terms “board” and “senior management” for the purposes of clarifying the internal audit function’s reporting relationships and should specify the board responsibilities to support and oversee the internal audit function. (See also Principle 6 Authorized by the Board and Principle 8 Overseen by the Board and relevant standards.) It may also describe administrative responsibilities, such as supporting information flow within the organization and approving the internal audit function’s human resource administration and budgets.
- Safeguards to objectivity and independence – describes the safeguards to be implemented if impairments exist. (See Standard 2.2 Safeguarding Objectivity and Standard 7.3 Safeguarding Independence.)
- Responsibilities – describes the scope and types of internal audit services to be provided and specifications for communicating with senior management and the board. Any responsibilities for providing assurance and advice on governance, risk management, and control processes should be identified (for example, delivering training, monitoring reports of ethics violations, performing fraud investigations, and others).
- Quality assurance and improvement – describes the expectations for developing and maintaining internal and external assessments of the internal audit function and communicating the results of the assessments. (See Standard 8.3 Quality, Standard 8.4 External Quality Assessment, and Principle 12 Enhances Quality and its related standards.)
- Signatures – indicates agreement among the chief audit executive, a designated board representative, and the individual to whom the chief audit executive administratively reports. This section includes the date, names, and titles of signatories.

Once drafted, the proposed charter should be discussed with senior management and the board to confirm that it accurately reflects their understanding and expectations of the internal audit function. The chief audit executive should present a final draft during a board meeting to be discussed and approved.

The chief audit executive and the board should also agree on the frequency with which to review and reaffirm whether the charter’s provisions continue to enable the internal audit function to accomplish its objectives. A leading practice is to review the charter annually, reference it as needed when questions about the internal audit mandate arise, and update it as needed.

Public Sector

If the mandate is specified in another governing document, such as in law or regulation, such a document may serve as the charter.

The administrative reporting relationship may be established by law and may be to the board only, not to management.

Evidence of Conformance

- Minutes of the board meetings during which the internal audit charter was discussed and approved.
- The approved charter, dated and with names and titles of signatories.
- Minutes of board meetings that include evidence that the chief audit executive periodically reviews the internal audit charter with senior management and the board.

Standard 9.4 Methodologies

Requirements

The chief audit executive must establish methodologies (policies, processes, and procedures) to guide the internal audit function to achieve its mandate and conform with the Standards.

The methodologies must guide internal audit processes and services, including:

- Assessing risks for the organization as a whole and for each engagement.
- Developing the internal audit plan.
- Determining the balance between assurance and advisory engagements.
- Coordinating with internal and external assurance providers.
- Managing external service providers, when used.
- Safeguarding data and information to which auditors have access.
- Performing internal audit engagements:
 - Identifying authoritative frameworks and guidance to support the governance, risk management, and control considerations for the activity under review.
 - Analyzing business processes and prioritizing risks for testing.
 - Testing the design and operation of control processes.
 - Determining root cause.
 - Obtaining required documentation and approvals.
 - Supervising the internal audit engagement performance and documentation.
 - Determining the significance of engagement findings and conclusions.
- Communicating the results of internal audit services.
- Retaining and releasing engagement records and other information, consistent with the organization's guidelines and any pertinent regulatory or other requirements.
- Monitoring the completion of management's action plans.
- Assuring the quality and improvement of the internal audit function.
- Performing additional services identified in the internal audit mandate.

The chief audit executive must ensure the internal audit function receives training on the methodologies.

The chief audit executive must evaluate the effectiveness of the methodologies and update them as necessary to improve the internal audit function and in response to significant changes that affect the function.

(See also Standards under Principle 13 Plan Engagements Effectively, Principle 14 Conduct Engagement Work, and Principle 15 Communicate Engagement Conclusions and Monitor Action Plans.)

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The form, content, level of detail, and degree of documentation of methodologies may differ based on the size, structure, and maturity of the internal audit function and the complexity of its work. Methodologies may exist as individual documents (such as standard operating procedures) or may be collected into an internal audit manual or integrated into internal audit management software.

To help ensure the internal audit function's success, the chief audit executive establishes methodologies that align with and support the Standards and guide internal auditors with a systematic approach to performing internal audit processes and conducting services. Internal audit methodologies supplement the Standards by providing specific instructions and criteria that help internal auditors implement the Standards and perform services with quality. For example, to support internal auditors in evaluating engagement findings and conclusions, the chief audit executive should develop a methodology and scale for rating, ranking, or otherwise indicating the significance of individual engagement findings and the significance of the engagement conclusion, based on consideration of the engagement findings in aggregate. (See also Standard 14.3 Evaluation of Findings and 14.5 Developing Engagement Conclusions.)

Some methodologies require developing a process or system. For example, the chief audit executive is required to establish a process to monitor whether management has implemented actions to address engagement findings. Internal auditors use the methodology and process established by the chief audit executive. (See also Standard 15.2 Confirming the Implementation of Action Plans.)

Additionally, internal audit methodologies describe processes and procedures for communicating, handling operational matters, and performing services in addition to assurance engagements, which the chief audit executive determines in agreement with senior management and the board. Examples of such services include delivering training, monitoring reports of ethics violations, performing fraud investigations, and performing environmental, health, and safety assessments. When the internal audit function is expected to provide such services, the chief audit executive is required to establish methodologies and train internal auditors appropriately.

The effectiveness of the internal audit methodologies should be reviewed during assessments of the internal audit function's quality. Changes that could require the chief audit executive to update the methodologies include significant changes in professional internal audit standards and guidance, legal and regulatory requirements, and technological innovations.

Evidence of Conformance

- Documentation of or software program incorporating methodologies.
- Meeting agendas and minutes, emails, signed acknowledgments, training schedules, or similar documentation evidencing communications to internal audit personnel about internal audit methodologies.
- Documentation of audit work demonstrating methodologies followed.

Standard 9.5 Internal Audit Plan

Requirements

The chief audit executive must develop an internal audit plan that supports the achievement of the organization's objectives.

The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from senior management and the board as well as an understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually.

The internal audit plan must:

- Consider the internal audit strategy and the full range of internal audit services.
- Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
- Consider coverage of information technology governance, fraud risk, and the effectiveness of the organization's compliance and ethics programs.
- Identify the necessary financial, human, and technological resources.
- Be dynamic and updated timely in response to changes in the organization's business, risks, operations, programs, systems, controls, and organizational culture.

The chief audit executive must review and revise the internal audit plan as necessary and communicate timely to senior management and the board:

- The impact of any resource limitations on internal audit coverage.
- The rationale for not including in the plan an assurance engagement in an area or activity with high risk.
- Conflicting demands for services between major stakeholders, such as high-priority requests based on emerging risks and requests to replace planned assurance engagements with advisory engagements.
- Limitations on scope or restrictions on access to information.

The chief audit executive must discuss the internal audit plan, including significant interim changes, with senior management and the board. The plan and significant changes to the plan must be approved by the board.

Considerations for Implementation and Evidence of Conformance

Implementation

The frequency for creating and revising an internal audit plan should be determined based on factors including the degree and frequency of change in the organization and risk environment. This standard requires an organizationwide risk assessment to be completed at least annually as the basis for the plan. However, the chief audit executive should keep apprised of risk information continuously, updating the risk assessment and internal audit plan accordingly. If the organization's environment is dynamic, the internal audit plan may need to be updated as frequently as every six months, quarterly, or even monthly.

One approach to preparing the internal audit plan initially is to design an audit universe (also called "risk universe") to organize potentially auditable units within the organization and facilitate the identification and assessment of risks. An audit universe is most useful when it is based on an understanding of the organization's objectives and strategic initiatives and aligned with the organization's structure or risk framework. Auditable units may include business units, processes, programs, and systems. The chief audit executive can link those organizational units to key risks in preparation for a comprehensive risk assessment and the identification of assurance coverage throughout the organization. This process enables the chief audit executive to prioritize the risks to be evaluated further during internal audit engagements.

To ensure that the audit universe and risk assessment cover the organization's key risks, the internal audit function typically independently reviews and validates the key risks that were identified within the organization's risk management system. The internal audit function should only rely on management's information about risks and controls if it has concluded that the organization's risk management processes are effective.

To complete the organizationwide, or comprehensive, risk assessment, the chief audit executive should consider objectives and strategies not just at the broad organizational level but also at the level of specific auditable units. Additionally, the chief audit executive should give due consideration to risks – such as those related to ethics, fraud, information technology, third-party relationships, and noncompliance with regulatory requirements – that may be tied to more than one business unit or process and may require more complex evaluation.

To support this risk assessment, the chief audit executive may gather information from recently completed internal audit engagements as well as discussions with the board and senior management. (See also Standard 9.1 Understanding Governance, Risk Management, and Control Processes and Standard 11.3 Communicating Results.) The chief audit executive may implement a methodology for continuously assessing risks. Risks should be considered not only in terms of negative effects and barriers to achieving objectives but also in terms of opportunities that enhance the organization's ability to achieve its objectives.

The chief audit executive should develop a strategy to ensure all significant and new or emerging risks can be identified and considered adequately for the audit plan. For example, resource limitations, especially in small internal audit functions, may make it impossible for the internal audit function to assess every risk in the audit universe annually. In such cases, the chief audit executive may need to increase reliance on sources of risk information such as management's risk assessments, meetings with senior management and the board, and the results of previous engagements and other audit work. The chief audit executive should plan to reevaluate reliance periodically.

To develop the internal audit plan, the chief audit executive considers the results of the levels of residual risk identified in the organizationwide risk assessment, along with the other requirements of this standard, including the input and requests made by senior management and the board, the assurance coverage throughout the organization, and the internal audit function's ability to rely on the work of other assurance providers. Internal audit planning may incorporate the concepts of continuous auditing or agile auditing, allowing the internal audit function to respond nimbly and dynamically to changes throughout the year, with audit plans considered to be "rolling," "fluid," or "dynamic."

To ensure the internal audit plan covers all mandatory and risk-based engagements, internal auditors should consider:

- Engagements required by law or regulation.
- Engagements critical to the organization's mission or strategy.
- Areas and activities with significant levels of residual risk.
- Whether all significant risks have sufficient coverage by assurance providers.
- Advisory and ad hoc requests.
- The time and resources required for each potential engagement.
- Each engagement's potential benefits to the organization, such as the engagement's potential to contribute to the improvement of the organizations' governance, risk management, and control processes.

To schedule internal audit engagements, the chief audit executive should take into account:

- The organization's operational priorities.
- Schedule of external audit engagements and regulatory reviews.
- Competencies and availability of internal auditors.
- Ability to access the activity under review.

For example, if an engagement needs to occur during a specific time of year, the resources needed to complete that engagement should also be available at that time. Likewise, if the activity to be reviewed is unavailable or constrained during a certain period of the year, the engagement should be scheduled to avoid that period.

The proposed internal audit plan typically includes:

- The list of proposed engagements, specifying whether the engagements are assurance or advisory.
- Rationale for selecting each proposed engagement; for example, significance of risk, organizational theme or trend (root cause), regulatory requirement, or time since last engagement.
- General purpose and preliminary scope of each proposed engagement.
- A list of nonaudit activities or projects to improve the internal audit function.
- A percentage of hours to be reserved for contingencies and ad hoc requests.

The chief audit executive, senior management, and the board should agree upon the criteria that defines the significant changes that require a revision of the audit plan. The agreed-upon criteria and protocol should be incorporated into the internal audit function's methodologies. Examples of significant changes include canceling or postponing engagements related to significant risks or critical strategic objectives. If risks arise that make it necessary to implement revisions to the plan before a formal discussion with the board can be scheduled, the board should be informed of the changes immediately and a formal approval should occur as soon as possible.

Evidence of Conformance

- Approved internal audit plan.
- Documented risk assessment/prioritization, including the inputs upon which the plan is based.
- Minutes of meetings in which the chief audit executive discussed with senior management and the board the audit universe, organizationwide risk assessment, internal audit plan, and the criteria and protocol for handling significant changes to the plan.
- Notes documenting discussions to gather information to inform the organizationwide risk assessment and internal audit plan.
- Documented list of those to whom the internal audit plan was distributed.
- Documented methodologies for organizationwide risk assessment and protocol for handling significant changes.

Standard 9.6 Coordination and Reliance

Requirements

The chief audit executive must coordinate with internal and external providers of assurance services and consider relying upon their work.

Coordination of services minimizes duplication of efforts, highlights gaps in coverage of key risks, and enhances the overall value added by all providers.

The chief audit executive must develop a methodology for evaluating other providers of assurance and advisory services that includes a basis for relying upon their work. The evaluation must take into account the providers' roles, responsibilities, organizational independence, competency, and objectivity, as well as the due professional care applied to the work. The chief audit executive must understand the scope, objectives, and results of the work performed.

When the internal audit function relies on the work of other assurance service providers, the chief audit executive is still responsible for the conclusions reached by the internal audit function and accountable for ensuring the conclusions are supported by adequate information.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The chief audit executive should identify the organization's assurance and advisory service providers by communicating with senior management and reviewing the organizational reporting structure and board meeting agendas or minutes. Internal providers of assurance and advice include functions that may report to or be part of senior management, such as compliance, environmental, financial control, health and safety, information security, legal, risk management, and quality assurance. External assurance providers may report to senior management, external stakeholders, or the chief audit executive.

Examples of coordination include:

- Synchronizing the nature, extent, and timing of planned work.
- Ensuring a common understanding of assurance techniques, methods, and terminology.
- Providing access to one another's work programs, workpapers, and reports.
- Using management's risk management information to provide joint risk assessments.
- Coordinating the scheduling of engagements.
- Creating a shared risk universe.
- Combining results for joint reporting.

The process of coordinating assurance activities varies by organization, from informal in small organizations to formal and complex in large or heavily regulated organizations. The chief audit executive considers the organization's confidentiality requirements before meeting with the various providers to gather the information necessary to coordinate services. Frequently, the providers share the objectives, scope, and timing of upcoming engagements and the results of prior engagements. They also discuss the potential for relying on one another's work.

One method to coordinate assurance coverage is to create an assurance map by linking identified significant risk categories with relevant sources of assurance and rating the level of assurance provided for each risk category. Because the map is comprehensive, it exposes gaps and duplications in assurance coverage, enabling the chief audit executive to evaluate the sufficiency of assurance services in each risk area. The results can be discussed with the other assurance providers so that the parties may reach an agreement about how to coordinate activities. In a combined assurance approach, the chief audit executive coordinates the internal audit function's assurance engagements with those other assurance providers to reduce the nature, frequency, and redundancy of engagements, maximizing the efficiency of assurance coverage.

The chief audit executive may choose to rely on the work of other providers for various reasons, such as to assess specialty areas outside of the internal audit function's expertise, to decrease the amount of testing needed to complete an engagement, and to enhance risk coverage beyond the internal audit plan.

To determine whether the internal audit function may rely on the work of another provider, the methodology should take into account the provider's:

- Potential or actual conflicts of interest and whether disclosures were made.
- Reporting relationships and the potential impacts of this arrangement.
- Relevance and validity of professional experience, qualifications, certifications, and affiliations.
- Methodology and the care applied in planning, supervising, documenting, and reviewing the work.
- Findings and whether they are based on sufficient, reliable, and relevant evidence and appear reasonable.

After evaluating the work of another assurance provider, the chief audit executive may determine that the internal audit function cannot rely upon the work. Internal auditors may either retest the work and gather additional information or independently perform assurance services.

If the internal audit function intends to rely upon the work of another assurance provider on an ongoing or long-term basis, the parties should document the agreed-upon relationship and specifications for the assurance to be provided and the testing and evidence required to support the assurance.

Evidence of Conformance

- Communications regarding distinct assurance and advisory roles and responsibilities, which may be documented in the notes from meetings with individual providers of assurance and advisory services or in minutes of meetings with senior management and the board.
- Assurance maps and/or combined assurance plans that identify which provider is responsible for assurance services in each area.
- Documentation of the methodology established by the chief audit executive to determine whether the internal audit function may rely on a provider's work.
- Agreements with other assurance providers, such as a charter, confirming the specifications of the assurance work they will perform.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Principle 10 Manages Resources

The chief audit executive manages resources to implement the internal audit function's strategy, complete its plan, and achieve its mandate.

Managing resources requires obtaining and deploying financial, human, and technological resources effectively.

The chief audit executive follows the organization's processes to obtain the resources required to perform internal audit responsibilities and deploys the resources according to the methodologies established for the internal audit function.

Standard 10.1 Financial Resource Management

Requirements

The chief audit executive must manage the internal audit function's financial resources.

The chief audit executive must develop a budget that enables the successful achievement of the internal audit mandate and plan. The budget includes the resources necessary for the operation of the function, including training and acquisition of technology and tools. The chief audit executive must manage the day-to-day activities of the internal audit function effectively and efficiently, in alignment with the budget.

The chief audit executive must present the budget to the board for approval. The chief audit executive must communicate timely the impact of insufficient financial resources to senior management and the board.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

At least monthly, the chief audit executive should review the planned versus actual budget and analyze significant variances to determine whether adjustments are needed. The budget may include reserves for unexpected but necessary changes to the internal audit plan.

If significant additional resources are needed due to unforeseen circumstances, the chief audit executive should discuss the circumstances with senior management and the board.

Public Sector

When the budget is set by law or regulation, the chief audit executive still must determine how to allocate internal audit function resources within the given budget and must notify the board and management when the budgeted financial resources are inadequate.

Small Internal Audit Functions

If a small internal audit function's budget is established within a larger budget managed by another department, business unit, or authority, the chief audit executive still should understand the funds allocated to the internal audit function, track spending, monitor the sufficiency of the financial resources deployed in the internal audit function, and keep the board informed.

Outsourced

For organizations that outsource the internal audit function, a comprehensive, holistic budget for the internal audit function still must be established (rather than individual project budgets) and reviewed periodically to confirm that it is sufficient, and the board should advocate for sufficient resources when necessary.

Evidence of Conformance

- Documentation of the internal audit plan against the budget, forecast, and actual expenses.
- Minutes of meetings in which the chief audit executive discussed the internal audit budget with senior management and the board.
- Board meeting minutes discussing the internal audit function's budget and approval.

Standard 10.2 Human Resource Management

Requirements

The chief audit executive must establish a program to recruit, develop, and retain qualified internal auditors required to successfully fulfill the internal audit charter and achieve the internal audit plan.

The chief audit executive must ensure that human resources are appropriate, sufficient, and effectively deployed to achieve the approved internal audit plan. *Appropriate* refers to the mix of knowledge, skills, and abilities; *sufficient* refers to the quantity of resources; and *effective deployment* refers to assigning resources in a way that optimizes the achievement of the internal audit plan.

The chief audit executive must communicate with senior management and the board regarding the appropriateness and sufficiency of the internal audit function's human resources. The board must approve the resource plan. If the function lacks appropriate and sufficient human resources to achieve the internal audit plan, the chief audit executive must determine how to obtain the resources or communicate the impact of the limitations to senior management and the board timely.

The chief audit executive must evaluate the competencies of individual internal auditors within the internal audit function and encourage professional development. The chief audit executive must collaborate with internal auditors to help them develop their individual competencies through training, receiving supervisory feedback, and/or mentoring.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The structure and approach to resourcing the internal audit function should align with the internal audit charter and support the achievement of the internal audit plan and strategic objectives.

In formulating a program for managing the internal audit function's human resources, the chief audit executive should:

- Consider organizational characteristics, such as structure and complexity, geographic regions of operations, diversity of cultures and languages, and volatility of the risk environment in which the organization operates.
- Consider the internal audit budget and the cost effectiveness and flexibility of various staffing approaches (for example, hiring an employee versus contracting with an external service provider).
- Understand the options for obtaining the human resources needed to fulfill the internal audit charter and achieve the internal audit plan.
- Communicate with senior management and the board to agree upon an approach.

To support a program for recruiting qualified internal auditors, the chief audit executive should:

- Collaborate with the human resources function to develop job specifications or descriptions that align with the requirements of Standard 3.1 Competency and professional competency frameworks.
- Consider the benefits of recruiting internal auditors with diverse backgrounds, experiences, and perspectives and creating an inclusive work environment that allows for effective collaboration and sharing of diverse views.
- Participate in recruitment activities, such as job fairs, student events, professional networking opportunities, and interviews with prospective candidates for hire.

To develop and retain internal auditors, the chief audit executive should:

- Implement compensation, promotion, and recognition activities that support the achievement of the internal audit function's strategic objectives.
- Implement methodologies for training, evaluating performance, and promoting the professional development of internal auditors.
- Consider the human resource objectives of the internal audit function and the organization, such as cross-functional sharing of knowledge and succession planning.
- Cultivate an ethical, professional environment and ensure internal auditors are adequately trained and collaborating effectively. (See also Domain II. Ethics and Professionalism.)

To evaluate whether the human resources are appropriate and sufficient to achieve the plan, the chief audit executive should take into account:

- The competencies of the internal auditors and the competencies needed to perform internal audit services.
- The time required to complete the services.
- The nature and complexity of the services.
- The number of internal auditors and productive work hours available.
- Scheduling constraints, including the availability of internal auditors and the organization's information, people, and properties.
- The ability to rely on the work of other assurance providers. (See also Standard 9.6 Coordination and Reliance.)

The chief audit executive may use a competency framework to identify, assess, and create an inventory of the internal audit function's competencies and experience. The chief audit executive reviews the competencies needed to achieve the internal audit plan. (See also Standard 3.1 Competency).

In addition to competencies, the chief audit executive considers the timing or schedule of internal audit engagements, based on the schedules of individual internal auditors and the availability of staff responsible for

the activity under review. Certain engagements may need to occur during a specific time of year, and the resources needed to complete that engagement must also be available at that time.

If the resources are insufficient to cover the planned engagements, the chief audit executive may provide training for existing staff, request an expert from within the organization to serve as a guest auditor, hire additional staff, rely on other assurance providers, develop a rotational auditing program, or contract with an external service provider. External service providers may provide specialized skills, complete special projects, or perform a limited number of engagements.

When the internal audit function is sourced internally, internal audit staffing may be supplemented by a rotational staffing model, whereby employees from other business units join the internal audit function temporarily and later return to the business unit. Employees transferring into the internal audit function may provide specialized skills and knowledge as well as unique perspectives and insights. Additionally, when employees transfer back into business units, their internal audit experiences contribute to a deeper understanding of the organization's governance, risk management, and control processes. When a rotational model is used, the chief audit executive should be aware of potential impairments to objectivity and the required safeguards. (See also Standard 2.2 Safeguarding Objectivity.)

While internal auditors are responsible for ensuring their individual professional development and may use a competency framework to assess their own skills and opportunities for development, the chief audit executive also should support the professional development of internal auditors. The chief audit executive may establish minimum expectations for professional development and should encourage the pursuit of professional qualifications. The chief audit executive should include funding for training and professional development in the internal audit budget and provide opportunities internally as well as externally, through continuing professional education, training, and conferences. (See also Standard 3.1 Competency and Standard 10.1 Financial Resource Management.)

The internal audit methodology for supervising engagements should include sufficient opportunities for internal auditors to receive constructive feedback from more experienced internal auditors in supervisory roles; such feedback may be provided through written or oral comments in the supervisory reviews of workpapers and other communications. Mentorship programs offer on-the-job experiences through which less experienced internal auditors to follow and directly observe knowledgeable staff performing engagements. The ongoing monitoring and periodic self-evaluations that comprise the internal audit function's internal assessments provide additional opportunities for internal auditors to receive feedback and suggestions to increase their effectiveness. (See also Standard 12.1 Internal Assessments.) Individual performance evaluations carried out at regular intervals, such as annually, are another source of input that can contribute to internal auditor's professional development.

Public Sector

In the public sector, the chief audit executive may not have the authority to make remuneration decisions but should still collaborate with the human resources function to ensure that job classifications specify the appropriate competencies and qualifications for internal auditors and that recruitment and retention efforts include assessments of those competencies.

Evidence of Conformance

- Documented analysis of gaps between competencies of internal auditors on staff and those required.
- Job descriptions.
- Résumés of internal auditors employed by the organization.
- Documented training plans.
- Documented evidence of completed training.
- Internal auditors' performance evaluations.
- External service provider contracts and résumés of internal auditors assigned by the provider.
- Meeting minutes documenting discussions regarding the internal audit budget.

- The internal audit plan, with the estimated schedule of engagements and resources allocated.
- Post-engagement comparison of budgeted work hours to actual hours.
- Assessments of the performance of the internal audit function and individual internal auditors.

Standard 10.3 Technological Resources

Requirements

The chief audit executive must ensure that the internal audit function has appropriate technology to support the internal audit process.

The chief audit executive must regularly evaluate the technology used by the internal audit function and pursue opportunities to improve effectiveness and efficiency.

When implementing new technology, the chief audit executive must ensure that internal auditors receive appropriate training to use the technological resources effectively. The chief audit executive must collaborate with the organization's information technology and information security functions to ensure technological resources are implemented properly and appropriate controls are operating effectively.

The chief audit executive must communicate the impact of technology limitations on the effectiveness or efficiency of the internal audit function to senior management and the board.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The internal audit function should use technology to improve its effectiveness and efficiency. Examples of such technology include:

- Audit management systems.
- Process mapping applications.
- Tools that assist with data science and analytics.
- Tools that assist with communication and collaboration.

To ensure the internal audit function has appropriate technological resources to perform its responsibilities, the chief audit executive should:

- Assess the feasibility of acquiring and implementing technology-enabled enhancements across the internal audit function's processes.
- Present sufficiently supported technology funding requests to senior management and the board for approval.
- Develop and implement plans to introduce approved technologies. Plans should include training internal auditors and demonstrating the realized benefits to senior management and the board.
- Identify and respond to the risks that arise from technology use, including those related to information security and privacy of individual data.

Evidence of Conformance

- Documented discussions or plans related to requests for and implementation of technologies.
- List of technology applications in use by the internal audit function.
- Records of technology implementation, training, and use, including workpapers evidencing use of technology during engagements.
- The names of internal auditors and their technology-related certifications and qualifications.
- Information security, records management, and other policies and procedures relevant to the internal audit function's use of technological resources.

Principle 11 Communicates Effectively

The chief audit executive ensures the internal audit function communicates effectively with its stakeholders.

Effective communication requires building relationships, establishing trust, and ensuring that stakeholders benefit from the results of internal audit services. The chief audit executive is responsible for helping the internal audit

function establish ongoing communication with stakeholders to build trust and foster relationships. Additionally, the chief audit executive oversees the internal audit function's formal communications with senior management and the board to ensure quality and provide insights based on the results of internal audit services.

Standard 11.1 Building Relationships and Communicating with Stakeholders

Requirements

The chief audit executive must develop an approach for the internal audit function to build relationships and trust with key stakeholders, including the board, senior management, operational management, regulators, and internal and external service providers.

The chief audit executive must promote formal and informal communication between the internal audit function and stakeholders, contributing to the mutual understanding of:

- Organizational interests and concerns.
- Approaches for identifying and managing risks and providing assurance.
- Roles and responsibilities of all parties and opportunities for collaboration.
- Relevant regulatory requirements.
- Significant organizational processes, including financial reporting.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Regular, ongoing communication contributes to a common understanding among senior management, the board, and the internal audit function of the organization's risks and assurance priorities and promotes adaptability to changes. The chief audit executive should be included in the organization's communication channels to keep current with major developments and planned activities that could affect the objectives and risks of the organization. The chief audit executive also should attend meetings with the board and key governance committees, as well as senior management and groups that report directly to senior management, such as compliance, risk management, and quality control.

In addition, the chief audit executive should discuss a methodology for communication with senior management and the board to determine the criteria defining significant issues requiring formal communication, the format and content of formal communication, and the frequency with which such communication should occur.

Meeting independently with individual senior executives and members of the board allows the chief audit executive to build relationships with them and learn about their concerns and perspectives. To better understand business objectives and processes, internal auditors may meet with key members of operational management, such as the head of a business unit and employees who perform operational tasks. In certain highly regulated industries or sectors, meetings between the chief audit executive and external auditors and regulators may be appropriate.

The chief audit executive and internal auditors may initiate discussions with management and the board about strategies, objectives, and risks as well as industry news, trends, and regulatory changes. Such discussions, along with surveys, interviews, and group workshops, are useful tools for obtaining input, especially on emerging risks and fraud risks. Websites, newsletters, presentations, and other forms of communication can be effective methods for sharing the internal audit function's role and benefits with employees and other stakeholders.

In large internal audit functions, the chief audit executive may delegate individual internal auditors to be responsible for maintaining ongoing communication with the management of key functions such as global operations, information technology, compliance, and human resources. (See also Standard 9.6 Coordination and Reliance.)

Communication should include opportunities for ongoing, informal interaction between internal auditors and the organization's employees. When informal interactions occur consistently, employees gain trust in internal auditors, increasing the likelihood of candid discussions that might not occur in formal meetings. As a part of relationship building, informal interaction may enhance internal auditors' comprehensive understanding of the organization and its control environment. Rotating internal auditors into and out of assignments in specific business units or locations balances the benefits of informal communication against the need to protect internal auditors' objectivity.

Public Sector

Internal auditors should consider the public at large to be a direct stakeholder of the organization. To serve the public, the internal audit function may consider input from the public, such as users of services including utilities, public transit systems, and parks and recreation facilities. Additional stakeholders may include elected officials; however, internal auditors should involve management and the board before taking direction from officials who do not provide direct governance over the organization.

Evidence of Conformance

- The internal audit function's documented relationship management plan.
- Agendas or minutes from meetings among members of the internal audit function and stakeholders.
- Surveys, interviews, and group workshops through which internal auditors solicit input from internal stakeholders.
- Websites or web pages, newsletters, presentations, and other outlets through which the internal audit function communicates with stakeholders in the organization.

Standard 11.2 Effective Communication

Requirements

The chief audit executive must ensure that internal audit communications are accurate, objective, clear, concise, constructive, complete, and timely.

Communication must be:

- **Accurate:** free from errors and distortions and faithful to the underlying facts.
- **Objective:** impartial, unbiased, and the result of a fair and balanced assessment of all relevant facts and circumstances.
- **Clear:** logical and easily understood by relevant stakeholders, avoiding unnecessary technical language.
- **Concise:** succinct and free from unnecessary detail and wordiness.
- **Constructive:** helpful to stakeholders and the organization and enabling improvement where needed.
- **Complete:** relevant, reliable, and sufficient information and evidence to support the results of internal audit services.
- **Timely:** appropriately timed, according to the significance of the issue, allowing management to take appropriate corrective action.

Considerations for Implementation and Evidence of Conformance

Implementation

To ensure that internal audit communications are accurate, objective, clear, concise, constructive, complete, and timely, the chief audit executive establishes methodologies that may include policies, criteria, and procedures to guide the internal audit function's communications and achieve consistency. The communication methodology should take into account the expectations of senior management, the board, and other relevant stakeholders. (See also Standard 9.4 Methodologies.) The chief audit executive may provide communications training to internal auditors, such as training on writing engagement reports or preparing presentations of final communications.

Supervisory reviews ensure that engagement communications are checked for the following characteristics and considerations:

- Accurate – When communicating, internal auditors should use precise terms and descriptions, supported by information gathered. Internal auditors should also consider other standards related to accuracy, including Standard 11.4 Errors and Omissions.
- Objective – Findings, recommendations, conclusions, and other results of internal audit services must be based on balanced assessments of all relevant circumstances. Communications should focus on identifying factual information and linking the information to objectives. Internal auditors should avoid terms that may be perceived as biased. (See also Principle 2 Maintain Objectivity and Standard 2.1 Individual Objectivity.)
- Clear – Clarity is increased when internal auditors use language that is consistent with terminology used in the organization and easily understood by the intended audience. Internal auditors should avoid unnecessary technical language and define important terms that are uncommon or used in a way that is specific or unique to the report or presentation. Internal auditors improve the clarity of their communications by including significant details that support findings, recommendations, and conclusions.
- Concise – Internal auditors should avoid redundancies and exclude information that is unnecessary, insignificant, or unrelated to the engagement or service.
- Constructive – Internal auditors should express information with a cooperative and helpful tone that facilitates collaboration with the activity under review to determine opportunities for improvement and action plans.
- Complete – Completeness enables the reader to reach the same conclusions as those reached by internal auditors. Internal auditors prepare communications for various recipients and the nature of the communications should be adapted for each recipient group. For example, communications to senior management and the board may differ from those delivered to the management of an activity under review. To ensure completeness, internal auditors consider the information necessary for the recipient to take the actions for which they are responsible.
- Timely – Timeliness may be different for each organization and depend upon the nature of the engagement.

In addition to engagement supervision, the chief audit executive may establish key performance indicators to measure and monitor the effectiveness of internal audit communication, which can be used as part of the function's quality assurance and improvement program. (See also Standard 8.3 Quality, Principle 12 Enhances Quality, and relevant standards.)

Evidence of Conformance

- Records of participation in training or meetings on effective communication skills.
- Final communications and other documents approved by the chief audit executive, as well as supporting documents that demonstrate the characteristics of effective communications.

- Presentation slides or meeting minutes that demonstrate the characteristics of effective communications.
- Record demonstrating the timeliness of communications.
- Workpapers that demonstrate the characteristics of effective communications.
- Workpapers with supervisory review notes on improving communication effectiveness.
- Results of stakeholder surveys regarding the quality of internal audit communications.
- Results of quality assurance and improvement program.

Standard 11.3 Communicating Results

Requirements

The chief audit executive must communicate the results of internal audit services periodically. The chief audit executive must understand the expectations of senior management and the board regarding the nature and timing of communications.

The results of internal audit services include:

- Engagement conclusions.
- Themes such as effective practices or root causes.
- Conclusions such as at the level of the business unit or organization.

Engagement Conclusions

The chief audit executive must review and approve the final engagement communication and decide to whom and how it will be disseminated before it is issued. If these duties are delegated to other internal auditors, the chief audit executive retains overall responsibility. The chief audit executive must seek the advice of legal counsel and/or senior management before releasing final communications to parties outside the organization, unless otherwise mandated or restricted by law or regulation. (See also Standard 11.4 Errors and Omissions and Standard 11.5 Communicating the Acceptance of Risk.)

Themes

The findings and conclusions of multiple engagements, when viewed holistically, may reveal patterns or trends, such as root causes. When the chief audit executive identifies themes related to the organization's governance, risk management, and control processes, the theme must be communicated timely, along with insights, advice, and/or conclusions, to senior management and the board.

Conclusions at the Level of the Business Unit or Organization

The chief audit executive may be required to make a conclusion at the level of the business unit or organization about the effectiveness of governance, risk management, and/or control processes, due to industry requirements, laws or regulations, or the expectations of senior management, the board, and/or other stakeholders. Such a conclusion reflects the professional judgment of the chief audit executive based on multiple engagements and must be supported by relevant, reliable, and sufficient information.

When communicating such a conclusion to senior management or the board, the chief audit executive must include:

- Summary of the request for the conclusion.
- The conclusion, which may be expressed as a rating, opinion, or other description.
- The criteria used as a basis for the conclusion, for example a governance framework or risk and control framework.
- The scope, including limitations and the time period to which the conclusion pertains.
- A summary of the information that supports the conclusion.
- A disclosure of reliance on the work of other assurance providers, if any.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The results of internal audit services may be based on the individual engagements, multiple engagements, and interactions with senior management and the board over time.

Engagement Communications

While Standard 13.1 Engagement Communication requires internal auditors to communicate throughout an engagement with those responsible for the activity under review, the chief audit executive is responsible for ensuring the final engagement communication is disseminated to the appropriate parties. Appropriate parties may include senior management, the board, and/or those responsible for developing and implementing management's action plans. (See Standard 13.1 Engagement Communication and Standard 15.1 Final Engagement Communication.)

The chief audit executive should encourage internal auditors to acknowledge satisfactory and positive performance in engagement communications. Examples of good practices identified across engagements may be transferable to other parts of the organization or serve as a benchmark throughout the organization.

Themes

Tracking the findings, recommendations, and conclusions of multiple engagements may enable the identification of trends, such as the improvement or worsening of conditions compared to criteria, a root cause underlying the conditions, or an opportunity to share a practice that increases effectiveness or efficiency.

Communications to senior management and the board should include:

- Significant control weaknesses and a robust root cause analysis.
- Thematic or systemic issues, actions, or progress across multiple engagements or business units.

Insights obtained from other assurance providers may be considered when identifying themes. (See also Standard 9.6 Coordination and Reliance.)

Conclusions at the Level of the Business Unit or Organization

When communicating conclusions at the levels of the business unit or organization overall, the chief audit executive should consider how a conclusion relates to the strategies, objectives, and risks of the organization. The chief audit executive also should consider whether the conclusion will solve a problem, add value, and/or provide management or other stakeholders with confidence regarding an overall theme or condition.

The chief audit executive also considers the time period to which the conclusion relates and any scope limitations to determine which engagements would be relevant to the overall conclusion. All related engagements or projects are considered, including those completed by other internal and external assurance providers. (See also Standard 9.6 Coordination and Reliance.)

For example, an overall conclusion may be based on aggregate engagement conclusions at the organization's local, regional, and national levels, along with results reported from outside entities such as independent third

parties or regulators. The scope statement provides context for the overall conclusion by specifying the time period, activities, limitations, and other variables that describe the conclusion's boundaries.

The chief audit executive should summarize the information on which the overall conclusion is based and identify the relevant risk or control frameworks or other criteria used as a basis for the overall conclusion. The chief audit executive should articulate how the overall conclusion relates to the strategies, objectives, and risks of the organization. Overall conclusions are typically communicated in writing, although there is no requirement in the Standards to do so.

Public Sector

When communication to the public or key stakeholders outside the organization is a part of the internal audit function's mandate, final engagement communications should be available on a timely basis as specified by relevant laws, regulations, or policies.

Often, internal audit functions in the public sector are required to present internal audit results at public meetings. If the internal audit function reports to a board or elected body, they may be permitted to release the results without seeking the advice of senior management and legal counsel, although they must still communicate the results to management during closing communications, as required in Standard 13.1 Engagement Communication.

Evidence of Conformance

- Final engagement communications, including engagement findings, recommendations, and conclusions.
- The chief audit executive's outline, meeting minutes, speaking notes, slides, or documents indicating communication with senior management and the board.
- Analyses including data reports, diagrams, and graphs showing trends.
- Relevant risk or control frameworks or other criteria used as a basis for the overall conclusion.

Standard 11.4 Errors and Omissions

Requirements

If a final engagement communication contains a significant error or omission, the chief audit executive must communicate timely corrected information to all parties who received the original communication.

Significance is determined according to criteria agreed upon with the board.

Considerations for Implementation and Evidence of Conformance

Implementation

The chief audit executive and the board should agree upon criteria indicating that an error or omission is significant and a protocol for communicating the correction. To determine the significance, the chief audit executive should evaluate whether the mistaken or omitted information could have legal or regulatory consequences or change the findings, conclusions, recommendations, or action plans.

The chief audit executive determines the most appropriate method of communication to ensure the corrected information is received by all parties who received the original communication. In addition to communicating the corrected information, the chief audit executive should identify the cause of the error or omission and take corrective action to prevent a similar situation from occurring in the future.

Evidence of Conformance

- Internal audit policies and procedures for handling errors and omissions.
- Criteria agreed upon with the board and used by the chief audit executive to determine the level of significance.
- Correspondence and other records showing how the chief audit executive determined the significance and cause of the error or omission.
- The chief audit executive's calendar, board or other meeting minutes, internal memos, and email correspondence where an error or omission was discussed.
- The original and corrected final communication documents.
- Documentation from all parties involved of any corrected communications received.

Standard 11.5 Communicating the Acceptance of Risks

Requirements

The chief audit executive must communicate unacceptable levels of risk.

When the chief audit executive concludes that management has accepted a level of risk that exceeds the organization's risk tolerance, the matter must be discussed with senior management. If the chief audit executive determines that the matter has not been resolved by senior management, the matter must be escalated to the board. It is not the responsibility of the chief audit executive to resolve the risk.

Considerations for Implementation and Evidence of Conformance

Implementation

The chief audit executive gains an understanding of the organization's risks and risk tolerance through discussions with senior management and the board, relationships and ongoing communication with stakeholders, and the results of internal audit services. (See also Standard 8.1 Board Interactions; Standard 9.1 Understanding Governance, Risk Management, and Control Processes; and Standard 11.1 Building Relationships and Communicating with Stakeholders.) This understanding provides the chief audit executive with perspective about the level of risk the organization considers acceptable. If the organization has a formal risk management process, it may include a risk acceptance policy, which the chief audit executive should understand.

The chief audit executive may discuss and seek the board's agreement on methodologies for documenting and communicating the acceptance of risks that exceed the organization's stated risk tolerance. Methodologies should take into account the requirements of the Standards and the organization's risk management process, policies, and procedures. The risk management process may include a preferred approach to communicating significant risk issues. Specifications may include the timeliness of communicating, the hierarchy of reporting, and requirements for consultation with the organization's legal counsel or head of compliance. The internal audit methodology also should include procedures for documenting the discussions and actions taken, including a description of risk, the reason for concern, management's reason for not implementing internal audit recommendations or other actions, the name of the individual responsible for accepting the risk, and the date of discussion.

The chief audit executive may become aware that management has accepted a risk by reviewing management's response to engagement findings and monitoring management's progress to implement agreed-upon action plans. Building relationships and maintaining communication with stakeholders are additional means of remaining apprised about risk management activities including management's acceptance of risk.

Examples of risks that may exceed the organization's risk tolerance include those that may result in:

- Harm to the organization's reputation.
- Harm to the organization's employees or other stakeholders.
- Significant regulatory fines, limitations on business conduct, or other financial or contractual penalties.
- Material misstatements.
- Conflicts of interest, fraud, or other illegal acts.
- Significant impediments to achieving strategic objectives.

The chief audit executive's professional judgment contributes to the determination of whether management has accepted a level of risk that exceeds the organization's risk tolerance. If management has made insufficient progress on previously agreed-upon action plans, for example, the chief audit executive may conclude that management has accepted a level of risk that exceeds the organization's risk tolerance. Before escalating a concern to senior management and/or the board, the chief audit executive should address the issue directly with management responsible for the risk area to share concerns, understand management's perspective, and agree on a resolution, which could include an action plan.

The requirements of this standard are only implemented when the chief audit executive cannot reach agreement with the management responsible for managing the risk. If the risk identified as unacceptable remains unresolved after a discussion with senior management, the chief audit executive escalates the concern to the board. The board is responsible for deciding about how to address the concern with management.

Public Sector

When the internal audit function is funded by an authority or oversight body outside the organization, regulations may require the chief audit executive to notify the funding authority or body in addition to the board.

Evidence of Conformance

- Documentation of discussions and agreement with the board on methodologies for communicating risk concerns.
- Documentation of discussions about the risk and actions recommended to operational management and senior management, including minutes of meetings.
- Documentation explaining the risk concern and internal audit actions taken to address the concern, including the process of escalating the discussion from operational management to senior management.
- Documentation from meetings with the board, including private or closed sessions during which the concern was escalated to the board.

Principle 12 Enhances Quality

The chief audit executive ensures conformance with the Global Internal Audit Standards and continuously improves the internal audit function's performance.

Quality is a combined measure of conformance with the Global Internal Audit Standards and the achievement of the internal audit function's performance objectives. A quality assurance and improvement program is designed to evaluate and ensure the internal audit function conforms with the Standards, achieves performance objectives, and pursues continuous improvement. The program includes internal and external assessments. (See also Standard 8.3 Quality and Standard 8.4 External Quality Assessment.)

The chief audit executive is responsible for ensuring that the internal audit function continuously improves. This requires the development of criteria and measures to assess the performance of internal audit engagements, the internal auditors, and the internal audit function. These measures form the basis for evaluating the progress toward performance objectives.

Standard 12.1 Internal Quality Assessment

Requirements

The chief audit executive must develop and conduct internal assessments of the internal audit function's progress toward performance objectives and conformance with the Global Internal Audit Standards.

The chief audit executive must establish a methodology for internal assessments that includes:

- Ongoing monitoring of the internal audit function's progress toward performance objectives and its conformance with the Standards.

- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices to evaluate conformance with all elements of the Standards.
- Communication with the board at least annually about the results of internal assessments.

Based on the results of a periodic self-assessment, the chief audit executive must develop an action plan to address instances of nonconformance with the Standards and opportunities for improvement, including a proposed timeline for actions. The chief audit executive must communicate the results of periodic self-assessments and action plans to the board. (See also Standard 8.1 Board Interaction and Standard 9.4 Methodologies.)

Internal assessments must be documented and included in the evaluation conducted by an independent third party as part of the organization's external quality assessment. (See also Standard 8.4 External Quality Assessment.)

If nonconformance with the Standards impacts the overall scope or operation of the internal audit function, the chief audit executive must disclose to senior management and the board the nonconformance and its impact.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Ongoing Monitoring

Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit function. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit function and includes processes, tools, and information considered necessary to evaluate conformance with the Standards.

The internal audit function's progress toward performance objectives and conformance with the Standards is monitored primarily through continuous activities such as engagement planning and supervision, established internal audit methodologies, workpaper procedures and sign-offs, and supervisory reviews of engagement workpapers and final communications. These activities include identification of any weaknesses or areas in need of improvement and action plans to address them. The chief audit executive may develop templates or automated workpapers for internal auditors to use throughout engagements, ensuring standardization and consistency in the application of the work practices.

Adequate supervision is a fundamental element of any quality assurance and improvement program. Supervision begins with planning and continues throughout the engagement. Supervision may include setting expectations, encouraging communications among team members throughout the engagement, and reviewing and signing off on workpapers timely. (See also Standard 12.3 Ensuring and Improving Engagement Performance.)

Additional mechanisms commonly used for ongoing monitoring include:

- Checklists or automation tools to provide assurance on internal auditors' compliance with established practices and procedures and to ensure consistency in the application of performance standards.
- Feedback from internal audit stakeholders regarding the efficiency and effectiveness of the internal audit team. Feedback may be solicited immediately following the engagement or on a periodic basis (for example, semi-annually or annually) through survey tools or discussions between the chief audit executive and management.
- Other measurements that may be valuable in determining the efficiency and effectiveness of the internal audit function include metrics indicating the adequacy of resource allocation (such as budget-to-actual variance), the timeliness of engagement completion, the achievement of the internal audit plan, and surveys of stakeholder satisfaction.

In addition to validating conformance with the Standards, ongoing monitoring may identify opportunities to improve the internal audit function. In such cases, the chief audit executive may address these opportunities and develop an action plan, including key performance indicators. Once changes are implemented, the indicators can be used to monitor success.

Periodic Self-assessments

Periodic self-assessments provide a more holistic, comprehensive review of the Standards and the internal audit function. Periodic self-assessments address conformance with every standard, whereas ongoing

monitoring focuses on the standards relevant to performing engagements. Periodic self-assessments may be conducted by senior members of the internal audit function, a dedicated quality assurance team, individuals within the internal audit function who have extensive experience with the Standards, Certified Internal Auditors, or other competent internal audit professionals from elsewhere in the organization. The chief audit executive should consider including internal auditors in the self-assessment process, which may improve their understanding of the Standards.

Periodic self-assessments enable the internal audit function to validate its conformance with the Standards. When a self-assessment is performed shortly before an external assessment, the time and effort required to complete the external assessment is typically reduced.

Periodic self-assessments evaluate:

- The adequacy and appropriateness of the internal audit function's methodologies.
- How well the internal audit function enhances the organization's success.
- The quality of internal audit services performed and supervision provided.
- The degree to which stakeholder expectations are met and performance objectives are achieved.

The individual or team conducting the self-assessment typically evaluates the internal audit function's conformance against each standard and may interview and survey the internal audit function's stakeholders. Through this process, the chief audit executive is typically able to assess the quality of the internal audit function's methodologies and the function's degree of adherence to policies and procedures for conducting engagements.

As part of the periodic-self assessment, the internal audit function may conduct:

- Post-engagement review – The internal audit function may select a sample of engagements from a particular timeframe and conduct a review to assess compliance with internal audit function's methodologies and conformance with the Standards. These reviews are typically conducted by internal audit staff who were not involved in the respective engagement. In a larger or more mature organization, this process may be handled by a quality assurance specialist or team.
- Performance measure analysis – The internal audit function may also monitor and analyze performance measures related to the efficiency of internal audit practices. Examples of performance measures include:
 - Budget-to-actual engagement hours.
 - Percentage of the internal audit plan completed.
 - Number of days between fieldwork completion and issuance of final engagement communication.
 - Percentage of management action plans implemented following engagements.
- The number of internal auditors on staff who hold a professional certification, their years of experience in internal auditing, and the number of continuing professional education hours they earned during the year.

Public Sector

The system of internal assessment also must include ongoing monitoring of the conformance with applicable regulations.

Small Internal Audit Functions

Small internal audit functions may face challenges in conducting internal quality assessments due to financial and staff constraints. Therefore, the chief audit executive of a small internal audit function may need to consider requesting assistance from others within the organization to conduct periodic assessments, such as former internal auditors or others with suitable knowledge of internal auditing. The chief audit executive should oversee such assessments.

To perform ongoing monitoring, the chief audit executive may need to increase the use of checklists or other automated tools to monitor conformance with the Standards during each engagement.

Evidence of Conformance

- Completed checklists that support workpaper reviews, survey results, and performance measures related to the efficiency and effectiveness of the internal audit function.
- Documentation of completed periodic assessments, which include the scope of the review and plan, workpapers, and communications.
- Presentations to the board and management and meeting minutes covering the results of internal assessments.
- Documented results of both ongoing monitoring and periodic self-assessments, including corrective action plans.
- Actions taken to improve the internal audit function's conformance, efficiency, and effectiveness.

Standard 12.2 Performance Measurement

Requirements

The chief audit executive must develop objectives to evaluate the internal audit function's performance. The chief audit executive must consider the input and expectations of senior management and the board when developing the performance objectives. The chief audit executive is responsible for ensuring that the internal audit function achieves its performance objectives.

The chief audit executive must develop a performance measurement methodology that includes performance criteria and measures to assess progress toward achieving the function's performance objectives. When assessing the internal audit function's performance, the chief audit executive must solicit feedback from senior management and the board.

The chief audit executive must develop an action plan to address any issues and opportunities for improvement.

Considerations for Implementation and Evidence of Conformance

Implementation

The establishment of performance measures is critical to determining whether an internal audit function achieves its performance objectives in accordance with the Standards and its charter. The first step is for the chief audit executive to identify key performance measures for internal audit services that stakeholders believe add value, help address risks, improve the organization's operations, and strengthen controls.

Sources to consider when identifying key performance measures of the internal audit function's effectiveness and efficiency include the Global Internal Audit Standards, the internal audit function's mandate and charter, applicable laws and regulations, and the internal audit function's strategies and performance objectives. Measures of effectiveness and efficiency may be quantitative or qualitative.

The internal audit function's performance measures should include operational and strategic outcomes. Achievement of the internal audit plan should not be the sole measure of success. Performance measures may include:

- Level of contribution to improving risk management, control, and governance processes.
- Achievement of key goals and objectives.
- Evaluation of progress against the internal audit plan.
- Coverage of risks identified as critical.
- Improvement in staff productivity.
- Increase in efficiency of the audit process.
- Increase in the number of action plans for process improvements.
- Adequacy of engagement planning and supervision.
- Evaluation of whether stakeholders' needs are met.
- Results of quality assessments and the internal audit function's quality improvement program.
- Clarity of communications with stakeholders.
- Average time lapsed between completion of audit testing and issuance of the final engagement communication.
- Percentage of recommendations accepted by management.
- Return on investment.
- Level of consideration of equity when conducting engagements.

Once key effectiveness and efficiency measurements and targets have been identified, the chief audit executive should establish a monitoring process and a method of communicating to stakeholders (for example,

format, timing, and metrics). The internal audit function should obtain feedback from key stakeholders on audit effectiveness and make adjustments where needed.

Evidence of Conformance

- Internal communications of the performance measurements used to monitor progress.
- Summary communications presented to senior management and the board.

Standard 12.3 Ensuring and Improving Engagement Performance

Requirements

The chief audit executive must ensure that engagements are properly supervised, quality is assured, and competencies are developed.

- To ensure proper supervision, the chief audit executive must provide internal auditors with guidance throughout the engagement, verify work programs are complete, and confirm engagement workpapers adequately support findings, conclusions, and recommendations.
- To assure quality, the chief audit executive must ensure engagements are performed in conformance with the Standards and the internal audit function's methodologies.
- To develop competencies, the chief audit executive must provide internal auditors with feedback about their performance and opportunities for improvement.

The extent of supervision required depends on the maturity of the internal audit function, the proficiency and experience of internal auditors, and the complexity of engagements.

The chief audit executive is responsible for supervising engagements, whether the engagement work is performed by the internal audit staff or by other service providers. Supervisory responsibilities may be delegated to appropriate and qualified individuals, but the chief audit executive retains ultimate responsibility.

The chief audit executive must ensure that appropriate evidence of supervision is documented and retained, according to the internal audit function's established methodology.

Considerations for Implementation and Evidence of Conformance

Implementation

When planning engagement supervision, the chief audit executive or a designated engagement supervisor should review the engagement objectives. Supervision may include opportunities for staff development, such as post-engagement meetings between the internal auditors who performed the engagement and the chief audit executive or designee.

Assessing the skills of the internal audit staff is an ongoing process extending beyond reviewing engagement workpapers. Based on the results of skill assessments, the chief audit executive may identify which internal auditors are qualified to supervise engagements and assign tasks accordingly.

Engagement supervision begins with engagement planning and continues throughout the engagement. During the planning phase, the engagement supervisor approves the engagement work program and may assume responsibility for other aspects of the engagement. (See also Principle 13 Plan Engagements Effectively and relevant standards).

The primary criterion for approval of the work program is whether it achieves the engagement objectives efficiently. The work program includes procedures for identifying, analyzing, evaluating, and documenting engagement information. Engagement supervision also involves ensuring that the work program is completed and approving changes to the work program.

The engagement supervisor should maintain ongoing communication with the internal auditors assigned to perform the engagement and with management of the area or process under review. The engagement supervisor reviews the engagement workpapers that describe the audit procedures performed, the information identified, and the findings and preliminary conclusions made during the engagement. The supervisor evaluates whether the information, testing, and resulting evidence are relevant, reliable, and sufficient to achieve the engagement objectives and support the engagement conclusions.

Standard 11.2 Effective Communication requires that engagement communications should be accurate, objective, clear, concise, constructive, complete, and timely. Engagement supervisors review engagement communications and workpapers for these elements because workpapers provide the primary support for engagement communications.

Throughout the engagement, the engagement supervisor and/or chief audit executive meet with the internal auditors assigned to perform the engagement and discuss the engagement process, which provides opportunities for training, development, and evaluation of the internal auditors. Supervisors may ask for additional evidence or clarification when reviewing the engagement communications and workpapers, which document all aspects of the engagement process. Internal auditors may be able to improve their work by answering questions posed by the engagement supervisor.

Usually, the supervisor's review notes are cleared from the final documentation once adequate evidence has been provided or workpapers have been amended with additional information that addresses the supervisor's concerns and/or questions. Alternatively, the internal audit function may retain a separate record of the engagement supervisor's concerns and questions, the steps taken to resolve them, and the results of those steps.

The chief audit executive is responsible for all internal audit engagements and significant professional judgments made throughout the engagements, regardless of whether the work was performed by the internal audit function or other assurance providers. The chief audit executive develops policies and procedures designed to minimize the risk that internal auditors will make judgments or take actions that are inconsistent with the chief audit executive's professional judgment and may adversely affect the engagement. The chief audit executive establishes a means to resolve any professional judgment differences. This may include discussing pertinent facts, pursuing additional inquiry or research, and documenting differing viewpoints in engagement workpapers as well as any conclusions. If there is a difference in professional judgment over an ethical issue, the issue may be referred to individuals in the organization who are responsible for ethical matters.

Small Internal Audit Functions

Ensuring engagement performance is a challenge for small audit functions where there may not be individual auditors for supervision and ongoing internal assessment. The chief audit executive may consider the use of tools such as checklists or other automated tools to assist in ensuring basic conformance to the Standards in each engagement.

Evidence of Conformance

- Engagement workpapers, either signed or initialed, and dated by the engagement supervisor (if documented manually) or electronically approved (if documented within a workpaper program).
- Completed checklists that support workpaper reviews.
- Interview and survey results that include feedback about the engagement experience from internal auditors and other individuals directly involved with the engagement.
- Documentation of communication between engagement supervisor and staff internal auditors regarding the engagement work.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

V. Performing Internal Audit Services

Performing internal audit services requires internal auditors to effectively plan engagements; conduct the engagement work to develop findings, recommendations, and conclusions; and collaboratively communicate with the management and employees responsible for the activity under review throughout the engagement and after it closes.

Although the standards for performing engagements are presented in a sequence, the steps in performing engagements are not always distinct, linear, and sequential. In practice, the order in which steps are performed may vary by engagement, with overlapping and iterative aspects. For example, engagement planning includes gathering information and assessing risks, which may continue throughout the engagement. Each step may affect another or the engagement as a whole. Therefore, internal auditors should review and understand all standards in this domain before beginning the engagement process.

Internal audit services are often viewed as providing assurance, advice, or both. Internal auditors are expected to apply and conform with the Standards when performing engagements, whether they are providing assurance or advice, except when otherwise specified in individual standards.

Through assurance services, internal auditors provide objective assessments of the differences between the existing conditions of an activity under review and a set of evaluation criteria. Internal auditors evaluate the differences to determine whether there are significant findings and to provide an engagement conclusion about the findings when viewed collectively. Assurance services are intended to provide confidence about governance, risk management, and control processes to the organization's stakeholders, especially the board, senior management, and the management of the activity under review.

Internal auditors perform advisory engagements and other advisory activities at the request of the board, senior management, or the management of an activity. The nature and scope of advisory services are subject to agreement with the party requesting the services. Examples of advisory engagements include internal auditors providing advice on the design of processes or systems or the development and implementation of new policies. Other advisory activities include internal auditors providing facilitation and training. When performing advisory services, internal auditors maintain objectivity by not taking on management responsibility.

Principle 13 Plan Engagements Effectively

Internal auditors plan each engagement using a systematic, disciplined approach.

The Global Internal Audit Standards along with the methodologies established by the chief audit executive form the foundation of internal auditors' systematic, disciplined approach to planning engagements. Internal auditors are responsible for effectively communicating at all stages of the engagement.

Engagement planning starts with understanding the initial expectations for the engagement and the reason the engagement was included in the internal audit plan. When planning engagements, internal auditors gather the information that will enable them to understand the organization and the activity under review and to assess the risks relevant to the activity. The engagement risk assessment allows internal auditors to identify and prioritize the risks to determine the engagement objectives and scope. Internal auditors also identify the criteria and resources

needed to perform the engagement and develop an engagement work program, which describes the specific engagement steps to be performed.

Standard 13.1 Engagement Communication

Requirements

Internal auditors must communicate effectively throughout the engagement.

Effective engagement communication must be accurate, objective, clear, concise, constructive, complete, and timely, as defined in Standard 11.2 Effective Communication.

Engagement communication must include initial, ongoing, closing, and final communications with the management of the activity under review.

Initial engagement communications comprise:

- Announcing the engagement.
- Discussing the engagement risk assessment, objectives, scope, and timing.
- Requesting the information and resources necessary to perform the engagement.
- Setting expectations for additional engagement communication.

Ongoing communication requires providing updates about the engagement progress. The extent of ongoing communication depends upon the nature and length of the engagement. If applicable, internal auditors must communicate:

- Governance, risk management, or control issues that require immediate attention.
- Changes to the scope, objectives, timing, or length of the engagement.

Internal auditors must have a closing communication, usually a meeting, with the management of the activity under review when engagement work has been completed and before issuing a final communication. The closing communication gives internal auditors and management an opportunity to resolve differences related to the engagement findings, recommendations, and conclusions before a final communication is issued.

The closing communication must include discussion of:

- The engagement findings, recommendations, and conclusions.
- Management's action plans to address the findings.
- The feasibility of recommendations and/or action plans.
- The timing to address each finding.
- The owner responsible for the action.

If internal auditors and management do not agree on a finding, recommendation, or conclusion, internal auditors must discuss and try to reach a common understanding about the issue with the management of the activity under review during the closing communication. If a common understanding still cannot be reached, internal auditors must not feel obligated to change any portion of the engagement results unless there is a valid reason to do so. Internal auditors must state both positions and the reasons for the differences in the final engagement communication. (See also Standard 15.1 Final Engagement Communication.)

Considerations for Implementation and Evidence of Conformance

Implementation

To ensure communication is effective, a variety of methods should be used: formal and informal, written and oral. Engagement communications may occur through scheduled meetings, presentations, emails and other documents, and informal discussions. Requirements for the quality and content of engagement communications are typically established by the chief audit executive in alignment with the expectations of senior management and the board and documented in internal audit methodologies. (See also Standard 11.2 Effective Communication.)

With the announcement communication, internal auditors give advance notice of the engagement to the appropriate stakeholders, typically the management and/or relevant staff of the activity under review, to set the foundation for cooperation and open dialogue. Internal auditors should follow the policy established by the chief audit executive to determine the amount of notice to give. The announcement should inform management about the reason for the review, the proposed starting time, and the approximate duration of the engagement.

Announcements take various forms but are typically written communications, such as a message, notification, memo, or letter. The announcement includes the timing of the engagement to ensure that the planned work does not conflict with other significant events occurring in the activity under review. Additionally, internal auditors request the information and documentation that will be needed to assess risks and begin developing the work program.

Another common initial communication is an opening or entrance meeting, which generally occurs after the risk assessment has been completed and internal auditors have established the initial engagement objectives and scope. This discussion provides an opportunity for internal auditors to ensure that the management of the activity under review understands and supports the objectives, scope, and timing of the engagement. The meeting also allows the parties to make adjustments and establish the expectations for additional communication, including the frequency of communications and who will receive the final communication.

After the opening meeting, internal auditors should create an engagement planning memorandum to document the discussion. Such documentation should be incorporated into the engagement workpapers.

Ongoing communication between internal auditors and the management of the activity under review throughout the engagement is essential for transmitting information that requires immediate attention and updating relevant parties about engagement progress or changes in scope. Ongoing communication helps internal auditors and the management of the activity under review gain clarity and avoid or resolve misunderstandings and differences.

The required closing communication (also called an “exit conference”) is a planned, structured opportunity for internal auditors, the management of the activity under review, and other relevant staff to validate and finalize the engagement findings, recommendations, and conclusions before a final communication is issued. The closing communication also provides an opportunity for management and internal auditors to discuss and potentially resolve any differences or disagreements about findings, recommendations, and/or conclusions. While the goal is to reach agreement, when that is not the case, this standard requires the inclusion of the viewpoints of both management and internal auditors in the final engagement communication.

Discussing the feasibility of internal auditors' recommendations may include weighing the costs, such as the severity of the risk versus the benefits of implementing the recommendations. Management action plans may not be fully developed before the closing communication, but management may have ideas about the actions it will take to address the findings. Even if management has not completely developed action plans, ideas can be discussed and evaluated. After the discussion, management can confirm its action plans, the expected timing of implementation, and the personnel who will be responsible for implementing the actions.

Evidence of Conformance

Initial Communication

- Emails, meeting minutes, or pre-engagement planning documentation (such as notes or a memo) indicating that the engagement was announced in advance.
- Minutes from the opening engagement meeting, including evidence of discussing the risk assessment, objectives, scope, and timing.
- Engagement planning memorandum documenting the opening meeting.
- Feedback (such as through surveys) from the management of the activity under review.

Ongoing Communication

- Documentation (emails, meeting minutes, workpapers, or notes) showing communication throughout the engagement, including progress updates, required notifications about urgent issues and changes, and input from the management of the activity under review.

Closing Communication

- Meeting minutes or notes showing structured two-way communication about internal audit findings, recommendations and conclusions, and management action plans.
- Draft of internal audit findings, recommendations, and conclusions and management action plans with management's responses.
- Documentation of feedback solicited and received from the management of the activity under review (such as through surveys).

Standard 13.2 Engagement Risk Assessment

Requirements

Internal auditors must develop an understanding of the activity under review and assess relevant risks.

To develop the understanding, internal auditors must identify and gather sufficient information and conduct an engagement risk assessment.

Internal auditors must understand:

- The strategies, objectives, and risks of the organization that are relevant to the activity under review.
- The organization's risk tolerance.
- The risk assessment supporting the internal audit plan.
- The objectives of the activity under review.
- The governance, risk management, and control processes of the activity under review.

- Authoritative frameworks, guidance, and criteria that may be used to evaluate the effectiveness of those processes.

To conduct the engagement risk assessment, internal auditors must:

- Identify the significant risks to the objectives of the activity under review.
- Identify the means by which the activity controls its risks to a level within the organization's risk tolerance.
- Evaluate the significance (impact and likelihood) of the risks.
- Assess the design adequacy of the activity's control processes.
- Consider specific risks including those related to fraud and information technology and systems.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

To develop an understanding of the activity under review and assess relevant risks, internal auditors should start by understanding the internal audit plan, the discussions that led to its development, and the reason the engagement was included. Engagements included in the internal audit plan arise from the internal audit function's organizationwide risk assessment. When internal auditors begin an engagement, they should consider the risks applicable to that particular engagement and inquire whether any changes have occurred since the internal audit plan was developed. Reviewing the organizationwide risk assessment and any other risk assessments recently conducted (such as those completed by management) may help internal auditors identify risks relevant to the activity under review.

Internal auditors should examine the alignment between the organization and the activity under review. Internal auditors gather and consider the information about the organization's strategies and processes for governance, risk management, and control as well as the organization's objectives, policies, and procedures. Then, internal auditors consider how these aspects of the organization relate to the activity under review and to the engagement as they begin to develop the engagement risk assessment.

Useful information may be found in:

- Risk assessments recently conducted by the internal audit function or management.
- Results of engagements previously performed by the internal audit function and other assurance and advisory service providers.
- Reports by other assurance and advisory service providers, such as financial, environmental, social responsibility, and governance.
- Organizationwide risk assessments and internal audit plans.
- Workpapers from previous engagements.

To gather information, internal auditors may:

- Review reference materials including the authoritative guidance of The IIA and other standards, guidance, laws, and regulations relevant to the organization's sector, industry, and jurisdiction.
- Use organizational charts and job descriptions to determine who is responsible for relevant information, processes, and other aspects of the activity under review.
- Inspect physical property of the activity under review.
- Examine documentation from the information owner or outside sources, including management's policies, procedures, flowcharts, and reports.
- Examine websites, databases, and systems.
- Inquire through interviews, discussions, or surveys.
- Observe a process in action.
- Meet with other assurance and consulting service providers.

Internal auditors review the gathered information to understand how processes are intended to operate and identify the criteria that management uses to measure whether the activity is achieving its objectives. Surveys, interviews, physical inspections, and process walk-throughs allow internal auditors to observe the current conditions in the activity under review. Internal auditors should document and summarize relevant information in a single planning document that is retained as an engagement workpaper. (See also Standard 14.6 Documenting Engagements.)

To perform the engagement risk assessment, internal auditors use the gathered information to understand and document the objectives of the activity under review, the risks that could affect the achievement of each objective, and the controls intended to manage each risk.

Internal auditors may create a chart, spreadsheet, or similar tool to document the risks and the controls designed to manage these risks. Such documentation, often called a risk and control matrix, enables internal auditors to apply professional judgment, experience, and reason to consider the information gathered in the context of the activity under review and to roughly estimate the significance of the risks in terms of a combination of impact, likelihood, and possibly other risk factors.

As part of due professional care, internal auditors should consider input from the management of the activity under review. Discussions with the management of the area or process under review often provide additional perspectives and insights on the business objectives, inherent risks, controls, and significance of relevant risks. Establishing a mutual understanding of the risks of the activity under review increases the usefulness of the risk assessment. Internal auditors also should consult with the engagement supervisor while planning.

A risk and control matrix is typically developed throughout the course of the engagement. As the engagement progresses through the testing phase, the matrix may be used to document the cause, risk event, effect (consequence), assessment of inherent risk, and the control with description of type (that is, preventive, detective, or corrective). The risks to be addressed during the engagement can then be prioritized according to significance. This is often illustrated by plotting the variables on a basic graph, such as a heat map. Such documentation should be retained as part of the engagement workpapers.

For the most significant risks, assessing the adequacy of the design of the controls helps internal auditors determine which controls to continue testing. The risks rated highest priority form the basis of the engagement objectives and scope, described in Standard 13.3 Engagement Objectives and Scope. When performing the engagement analyses, internal auditors seek to determine the residual risk and note any risks that exceed the acceptable tolerance range of the activity. (See also Standard 14.2 Analyses and Potential Engagement Findings.)

Evidence of Conformance

Workpapers documenting:

- Relevant organizational strategies, objectives, and risks of the organization.
- Objectives of the activity being reviewed.
- Governance, risk management, and control processes of the activity under review.
- Organizational charts and job descriptions.
- Notes and/or photographs from direct observation or inspection.
- Policies and procedures for the activity.
- Relevant laws and regulations and documented compliance assessments.
- Relevant information gathered from websites, databases, and systems.
- Notes from interviews, discussions, or surveys.
- Relevant information from the work of other assurance providers and previously completed risk assessments and engagements.
- Risk and control matrix or other documentation indicating each risk's significance and the adequacy of the control design.

Standard 13.3 Engagement Objectives and Scope

Requirements

Internal auditors must establish and document the objectives and scope for the engagement.

The engagement objectives must articulate the purpose of the engagement and take into account the results of the engagement risk assessment.

The scope establishes the engagement focus and boundaries by specifying the activities, locations, processes, systems, components, and other elements to be reviewed and the period of time to be covered in the engagement. The scope must be sufficient to achieve the engagement objectives. Scope limitations must be disclosed in the opening and final engagement communications.

The chief audit executive or a designee must approve the engagement objectives and scope.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Engagement objectives and scope enable internal auditors to focus efforts on the significant risks in the activity under review, develop the engagement work program, and communicate clearly with management and the board. The objectives and scope also provide a basis to help internal auditors determine the engagement timeline, budget, and resource requirements.

Determining the engagement objectives and scope requires internal auditors to gather the necessary information to:

- Understand the purpose of the engagement and the reason it is included in the internal audit plan.
- Consider the strategies and objectives of the activity under review.
- Prioritize the risks relevant to the engagement through the engagement risk assessment. (See also Standard 13.2 Engagement Risk Assessment.)

Internal auditors should consider whether the engagement is a request for assurance or advisory services, because stakeholder expectations and the requirements of the Standards differ depending on the type of engagement. The objectives and scope of assurance engagements may also differ significantly from those of advisory engagements. For assurance engagements, the objectives and scope are determined primarily by the internal auditors, whereas for advisory engagements the objectives are typically determined by the party requesting the advisory engagements.

When engagement objectives and scope are properly defined before the engagement starts, internal auditors are able to:

- Address the significant risks to the activity under review.
- Avoid duplicating efforts or performing work that does not add value.
- Allocate appropriate and sufficient resources to complete the engagement.

Engagement objectives are broad statements developed by internal auditors that define intended engagement accomplishments. Objectives specify what the engagement is intended to accomplish and help internal auditors determine which procedures to perform. Internal auditors should ensure that the objectives of the engagement align with the business objectives of the area or process under review as well as those of the organization.

Assurance engagements focus on providing assurance that the controls in place are adequately designed and operating to manage the risks that could prevent the area of the organization from achieving its business objectives. The objectives of these engagements direct the priorities for testing the controls of processes and systems during the engagement. These include controls designed to manage risks related to:

- Assignment of authority and responsibility.
- Compliance with policies, plans, procedures, laws, and regulations.
- Reporting accurate, reliable information.
- Effectively and efficiently using resources.
- Safeguarding assets.

Once the engagement objectives have been established, internal auditors should use professional judgment and consult with the engagement supervisor as necessary to determine the scope of engagement work. The

scope must be broad enough to achieve the engagement objectives. When determining the scope, internal auditors should consider each engagement objective independently to ensure that it can be accomplished within the scope.

Internal auditors generally consider and document any scope limitations and requests from the engagement stakeholders for items to be included in or excluded from the scope. Examples of scope limitations include:

- Length of the engagement.
- Resource limitations (financial, human, and technological).
- Access to data, records, and other information as well as the personnel and physical properties.

Internal auditors communicate the objectives, scope, and timing of the engagement during the opening or entrance meeting. The information should be documented in an engagement planning memorandum and incorporated into the engagement workpapers. (See also Standard 13.1 Engagement Communication.)

Evidence of Conformance

- Engagement planning memorandum.
- Final engagement communication.
- Engagement workpapers documenting:
 - Alignment of objectives and the risk assessment.
 - Scope that achieves engagement objectives.
 - Approved engagement work program containing the objectives and scope.
 - Minutes from meetings with stakeholders about objectives and scope.
 - Scope limitations and requests from engagement stakeholders for items to be included or excluded.

Standard 13.4 Evaluation Criteria

Requirements

Internal auditors must identify measurable criteria to be used to evaluate the aspects of the activity under review defined in the engagement objectives and scope.

Internal auditors must ascertain the extent to which management or the board has established adequate criteria to determine whether the activity under review has accomplished its objectives and goals. If adequate, internal auditors must use such criteria in their evaluation.

If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.

Examples of criteria are:

- Internal (policies, procedures, key performance indicators, or targets for the activity).
- External (laws, regulations, and contractual obligations).
- Authoritative practices (frameworks, standards, guidance, and benchmarks specific to an industry, activity, or profession).

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

As part of gathering information and planning the engagement, internal auditors identify the criteria used by the organization to evaluate the effectiveness and efficiency of the governance, risk management, and control processes of the activity under review. Auditors then focus on the evaluation criteria most relevant to the engagement. Such criteria should represent the desired state of the activity and provide practical, measurable specifications against which to compare the existing state (condition). For example, if an engagement objective is to assess the effectiveness of the control processes in the activity under review, the criteria, or desired state, could be the expected results or outcomes of the activity's control processes, while the condition is revealed by the actual outcomes.

Adequate criteria are essential for identifying a difference between the desired state and the condition, which represents potential findings; determining the significance of the findings; and reaching meaningful conclusions. Internal auditors use professional judgment to determine whether the organization's criteria are adequate. Adequate criteria are relevant, aligned with the objectives of the organization and the activity under review, and produce reliable comparisons. In addition to the examples of criteria listed in this standard, criteria may include established organizational practices, expectations based on the design of a control, and procedures that may not be formally documented.

When evaluating the adequacy of the criteria, internal auditors should determine whether the organization has established basic principles about what constitutes appropriate governance, risk management, and control practices. Internal auditors should consider whether management has clearly articulated its risk tolerance, including materiality thresholds for various business units, functions, or processes. Internal auditors also should ascertain whether the organization has adopted or clearly articulated a definition of control and should identify management's understanding of what constitutes a satisfactory level of control. For example, satisfactory could mean that a certain percentage of transactions within one control objective are conducted in accordance with established control procedures or that a certain percentage of controls overall are working as intended.

Additionally, internal auditors should research recommended practices and compare management's criteria to that used by other organizations. Determining the criteria that is best for achieving the engagement objectives also requires internal auditors to apply professional judgment. Internal auditors may determine that the documented policies, procedures, and/or other criteria lack detail or are otherwise inadequate. Internal auditors may assist management in determining adequate criteria or may seek input from experts to help identify or develop relevant criteria. Management's criteria may appear adequate generally, but internal auditors may suggest better criteria for the engagement.

When the criteria used by the activity under review is inadequate or nonexistent, internal auditors may recommend that management implement the criteria identified by the internal auditors. The discussion about the lack of adequate criteria may lead to a decision to provide advisory services.

Internal auditors should ensure that the management of the activity under review understands the criteria that will be used during the engagement. To avoid misinterpretation or challenge by any personnel responsible for the activity under review, the agreed-upon criteria should be documented.

Evidence of Conformance

- Workpapers documenting the sources of criteria considered and the process used to determine the adequacy of the criteria.

- Documentation, such as meeting minutes, a planning memo, or an email, indicating internal auditors' discussion of criteria with the management of the activity under review and/or the board.

Standard 13.5 Engagement Resources

Requirements

When planning an engagement, internal auditors must identify the resources necessary to achieve the engagement objectives.

Internal auditors must determine the types and quantity of resources that will be needed to perform the engagement. The determination requires considering:

- The nature and complexity of the engagement.
- The time frame within which the engagement must be completed.
- Whether the available financial, human, and technological resources are appropriate and sufficient to achieve the engagement objectives.

If the available resources are inappropriate or insufficient, internal auditors must discuss the concerns with the chief audit executive or a designee responsible for obtaining the resources.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Identifying and assigning resources is a step in planning an engagement that is typically handled by an internal auditor who has been designated to lead and supervise the engagement. To determine the type and quantity of resources needed for an engagement, the engagement supervisor should understand the information gathered and developed throughout engagement planning, paying special attention to the nature and complexity of work to be performed. The supervisor then applies professional judgment to identify the steps that should be taken to achieve the engagement objectives and the time that each step is expected to take. It is also important to consider fixed specifications and constraints that may affect the performance of the engagement, such as the number of hours budgeted for the engagement as well as the timing, language, and logistics.

When planning engagements, internal auditors should consider the most efficient and effective application of available financial, human, and technological resources. The engagement supervisor may have access to the chief audit executive's information about the specialized competencies held by members of the internal audit function. Planning the engagement resources requires determining whether the available resources are appropriate and sufficient or if it is necessary to obtain additional resources to complete the engagement.

When resource limitations interfere with the internal audit function's ability to achieve the engagement objectives, the engagement supervisor is responsible for escalating the concern to the chief audit executive. The chief audit executive is responsible for discussing with senior management and the board the implications of the resource limitations and determining the course of action to take. For example, when the chief audit executive is unable to obtain the necessary resources, the engagement scope may need to be reduced. (See also Standard 10.1 Financial Resource Management, Standard 10.2 Human Resource Management, and Standard 10.3 Technological Resources.)

To improve the effective implementation of resources, internal auditors may document the actual time spent performing the engagement against the budgeted time. The documentation can be reviewed to improve future resource planning.

Evidence of Conformance

- Chief audit executive's inventory of competencies of the internal audit function.
- Internal audit function's policies and procedures for resourcing engagements.
- Approved engagement work program showing utilization of appropriate and sufficient resources.
- Planning documentation (workpapers) analyzing the engagement's resourcing needs and noting assignment of resources.
- Post-engagement survey of the management of the activity under review inquiring about timeliness and resource adequacy.
- Contracts and/or relationships with external service providers.

Standard 13.6 Work Program

Requirements

Internal auditors must develop and document an engagement work program that will achieve the engagement objectives.

The engagement work program is based on the information obtained during engagement planning, including the results of the engagement risk assessment.

The engagement work program must identify:

- Tasks to achieve the engagement objectives.
- Methodologies and tools to perform the tasks.
- Internal auditors assigned to perform the tasks.

The chief audit executive or a designee must review and approve the engagement work program before it is implemented. Subsequent changes to the work program must be discussed and approved by the chief audit executive or a designee.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Work programs document the tasks to be completed in an engagement and the roles and responsibilities assigned to each member of the engagement team. Work programs are reviewed by the chief audit executive or a designated engagement supervisor and typically include a method for indicating review and approval of the various tasks completed, along with the names of the internal auditors who completed the work, and the date the work was completed.

The engagement work program builds on the information gathered and developed during engagement planning and details the procedures that will be used to analyze and evaluate information as internal auditors develop engagement findings, recommendations, and conclusions. Work performed during the planning phase is typically documented in workpapers and referenced in the work program.

To develop the work program, internal auditors can expand the risk and control matrix by linking the risks and controls with a testing approach to be implemented. As analyses and evaluations are conducted, the matrix can be expanded to link the risks and controls to the findings, recommendations, and conclusions. Work programs should specify the testing objectives, criteria, and methodologies such as the analytical procedures to be used for testing the effectiveness of key controls, in addition to the specifications described in the standard. Work programs should also include the sampling methodology, population, and size.

The level of analysis and detail applied during the planning phase varies by internal audit function and engagement. Evaluating the adequacy of control design is often completed as part of engagement planning, because it helps internal auditors clearly identify key controls to be further tested for effectiveness. The work program may include a documented evaluation of the adequacy of control design.

However, the most appropriate time to perform this evaluation depends on the nature of the engagement. If it is not completed during planning, the control design evaluation may occur as a specific stage of engagement performance, or internal auditors may evaluate the control design while performing tests of the controls' effectiveness.

Evidence of Conformance

- Workpapers supporting the development of the work program.
 - Risk and control matrix with testing approach.
 - Maps or descriptions of control processes.
 - Notes on evaluation of the adequacy of the control design.
 - Plan for additional testing.
- Minutes, notes, or documentation from planning meetings during which tasks and procedures were determined.
- Complete engagement work program with documented approval.
- Documentation of approval of changes to the work program.

Principle 14 Conduct Engagement Work

Internal auditors implement the engagement work program to achieve the engagement objectives.

When planning an engagement, internal auditors collect and organize information to create a work program. The work program describes the tasks and methodologies to be used to achieve the engagement objectives.

To implement the work program, internal auditors gather information and perform analyses and evaluations. These steps enable internal auditors to identify potential findings; determine the causes, effects, and significance of the findings; and develop recommendations and conclusions.

Standard 14.1 Gathering Information for Analyses and Evaluation

Requirements

Internal auditors must gather relevant, reliable, and sufficient information to perform analyses and evaluations.

Internal auditors must gather and analyze information to produce and support engagement findings.

Internal auditors must evaluate whether the information is relevant and reliable and whether it is sufficient such that analyses provide a reasonable basis upon which to formulate potential engagement findings. The results of the analyses and the supporting information are collectively referred to as “evidence.” (See also Standard 14.2 Analyses and Potential Engagement Findings.)

Information is relevant when it is consistent with engagement objectives, is within the scope of the engagement, and contributes to the development of engagement findings, recommendations, and conclusions.

Information is reliable when it is factual and current. Internal auditors use professional skepticism to evaluate whether information is reliable. Reliability is strengthened when the information is:

- Obtained directly by an internal auditor or from an independent source.
- Corroborated.
- Gathered from a system with effective governance, risk management, and control processes.

Information is sufficient when it enables internal auditors to perform analyses and complete evaluations. Evidence is sufficient when it can enable a prudent, informed, and competent person to repeat the engagement work program and reach the same conclusions as the internal auditor. When evidence is not sufficient to produce or support engagement findings, internal auditors must gather additional information for analyses and evaluation.

Considerations for Implementation and Evidence of Conformance

Implementation

When gathering information to complete each step in the engagement work program, internal auditors focus on the information that is relevant to the engagement objectives and within the engagement scope. In applying professional skepticism, internal auditors should critically assess whether the information is factual, current, and obtained directly (such as by observation) or from a source independent of those responsible for an activity under review. Corroborating the information by comparing it against more than a single source is another way to increase reliability.

Procedures to gather information for analyses may include:

- Interviewing or surveying individuals involved in the activity.
- Directly observing a process, also known as performing a walk-through.
- Obtaining confirmation or verification of information from an individual who is independent of the activity under review.
- Inspecting or examining physical evidence such as documentation, inventory, or equipment.
- Directly accessing organizational systems to observe or extract data.
- Working with system users and administrators to obtain data.

When gathering information, internal auditors consider whether they will test a complete data population or a representative sample. If they choose to select a sample, they should apply methods to ensure that the sample is as representative of the whole population as possible.

Evidence of Conformance

- Engagement work program, which includes procedures for gathering data relevant to the engagement objectives.
- Description of information gathered, including its source, the date it was gathered, and the period to which it pertains.
- Documented explanation of how the internal auditor determined that the information gathered was sufficient to perform an analysis.

Standard 14.2 Analyses and Potential Engagement Findings

Requirements

Internal auditors must analyze relevant, reliable, and sufficient information to develop potential engagement findings.

Internal auditors must analyze information to determine whether there is a difference between the evaluation criteria and the existing state of the activity under review, known as the “condition.” (See also Standard 13.4 Evaluation Criteria.) Internal auditors determine the condition by using information and evidence gathered during the engagement. A difference between the criteria and the condition indicates a potential engagement finding that must be noted and further evaluated. Common examples of potential engagement findings include errors, irregularities, illegal acts, and opportunities for improving efficiency or effectiveness.

If initial analyses do not provide sufficient evidence to support a potential engagement finding, internal auditors must exercise due professional care when determining whether additional analyses are required. If so, the work program must be adjusted accordingly and approved by the chief audit executive or a designee.

Considerations for Implementation and Evidence of Conformance

Implementation

The engagement work program may include a list of specific analyses to be conducted, such as:

- Tests of the accuracy or effectiveness of a process or activity.
- Reasonableness tests.
- Ratio, trend, and regression analyses.
- Comparisons between current period information with budgets and forecasts or similar information from prior periods.
- Analyses of relationships among sets of information (for example, financial information, such as recorded payroll expenses, and nonfinancial information, such as changes in the average number of employees).
- Internal benchmarking, or comparisons of information from different areas within the organization.
- External benchmarking, or comparisons using information from other organizations.

Internal auditors should understand and use technologies that improve the efficiency and effectiveness of analyses, such as software applications that enable testing of an entire population rather than just a sample.

The analyses should yield a meaningful comparison between the evaluation criteria and the condition. When the analyses indicate a difference between the criteria and the condition, subsequent engagement procedures should be employed to determine the cause and effect of the difference and significance of the potential findings. Findings may also be called “observations,” particularly in advisory engagements.

Internal auditors exercise due professional care to determine the extent and type of additional procedures that should be used to evaluate the potential findings and determine their cause, effect, and significance. The chief audit executive and the internal audit methodologies may provide guidance for determining whether to perform additional analyses. Considerations include:

- Results of the engagement risk assessment, including the adequacy of control processes.
- Significance of the activity under review and the potential findings.
- Extent to which the analyses support potential engagement findings.
- Availability and reliability of information for further evaluation.
- Costs versus the benefits of performing additional analyses.

Evidence of Conformance

- Workpapers that document the analyses performed (including data analytics programs or software used, test populations, sampling processes, and sampling methods).
- Workpapers cross-referenced in the work program and/or final communication.
- Documentation related to the final communication.
- Supervisory reviews of the engagement.
- External and internal assessment results. (See Standard 8.4 External Quality Assessment and Standard 12.1 Internal Quality Assessment.)

Standard 14.3 Evaluation of Findings

Requirements

Internal auditors must evaluate each potential engagement finding to determine its significance.

When evaluating potential engagement findings, internal auditors must identify the root cause, determine the potential effects, and evaluate the significance of the issue. To determine the significance of the risk, internal auditors consider the likelihood of the risk occurring and the impact the risk may have on the organization or its governance, risk management, or control processes.

If internal auditors determine that the organization is exposed to a significant risk, the issue must be documented and communicated as a finding.

Internal auditors must provide a rating, ranking, or other indication of priority for each engagement finding, based on the significance of the finding, using methodologies established by the chief audit executive.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

To develop engagement findings, internal auditors start by comparing the established criteria to the existing condition in the activity under review. (See also Standard 14.2 Analyses and Potential Engagement Findings.) If there is a difference between the two, internal auditors investigate the potential finding further and explore:

- The root cause of the difference, which typically relates to a control deficiency. At its simplest, determining the root cause often involves asking a series of questions about why the difference exists.
- The effect or impact of the difference, which explains why the condition may be a cause for concern. In some cases, the effect may be objectively quantifiable, but in many cases the extent of the exposure will be an estimate informed by internal auditors' due professional care with input from management of the activity under review. (See also Principle 4 Exercise Due Professional Care.)

To determine the significance of a finding, internal auditors use methodologies developed by the chief audit executive. They identify and evaluate existing controls for design adequacy and effectiveness, then determine the level of residual risk, or the risk that remains despite having controls in place.

Internal auditors assign a rating based on the methodology established by the chief audit executive, which ensures consistency across all internal audit engagements. When determining the rating, internal auditors should consider:

- The impact and likelihood of the risk.
- The organization's risk tolerance.
- Methodologies developed by the chief audit executive.
- Any additional factors important to the organization.

A rating can be an effective communication tool for describing the significance of each finding and may assist management with prioritizing their action plans. Examples of ratings are low, medium, high, and critical.

The chief audit executive may provide templates for internal auditors to use to document engagement findings, ensuring proper documentation of various elements such as the:

- Criteria.
- Condition.
- Cause.
- Effect.
- Significance rating.
- Recommendations to resolve the findings. (See also Standard 14.4 Recommendations and Action Plans.)

Findings should be written succinctly, in simple language, such that the management of the activity under review understands internal auditors' evaluation. Findings should explain the difference between the conditions and the criteria and should link to documented evidence that supports internal auditors' evaluation and judgment about their significance.

Evidence of Conformance

- Workpapers explaining the criteria used to evaluate the findings.
- Workpaper that lists the criteria, condition, root cause, effect (risk or potential exposure), and a rating of significance for each finding.
- Workpaper or other documentation explaining the materiality, risk tolerance, and elements of any cost-benefit analysis used as the basis of the finding(s) analysis.
- Relevant internal audit policies, templates, and guidance.

- Documentation related to the final engagement communication.

Standard 14.4 Recommendations and Action Plans

Requirements

Internal auditors must formulate recommendations and if applicable obtain management's action plans.

Recommendations are suggested actions to:

- Resolve the differences between the established criteria and the existing condition.
- Mitigate identified risks.
- Enhance or improve the activity under review.

Internal auditors must discuss recommendations with the management of the activity under review.

For assurance engagements, internal auditors must obtain management's action plans to address the root cause of each finding.

If internal auditors and management disagree about the recommendations and/or action plans and a resolution cannot be reached, the final communication must state both positions and the reasons for the disagreement. (See also Standard 13.1 Engagement Communications.)

Although internal auditors must make recommendations for corrective actions, it is management's responsibility to determine the appropriate course of action and implement action plans to address the findings. (See also Standard 15.1 Final Engagement Communication.) Advisory engagements do not require action plans.

Considerations for Implementation and Evidence of Conformance

Implementation

Internal auditors are required to have ongoing communications with management throughout the engagement. (See also Standard 13.1 Engagement Communication.) Internal auditors should discuss the findings and recommendations with the management of the activity under review throughout the course of the engagement. The required closing communication, which must occur before a final communication is issued, is typically a formal or structured opportunity, such as an exit conference. (See also Standard 13.1 Engagement Communication.) Internal auditors should use the methodology established by the chief audit executive to determine which findings warrant escalation.

Recommendations should be addressed to the parties who have sufficient authority to make and oversee changes to the activity under review. The chief audit executive may create a policy or guidance to help internal auditors identify the appropriate parties. For example, an internal audit policy may mandate that only a given role or level (such as a manager, director, or vice president) should respond to internal audit recommendations and develop action plans.

If a specific corrective action is identified that addresses a finding, internal auditors should communicate it as a recommendation. Alternatively, internal auditors may present several options for management to consider. In some cases, internal auditors may recommend for management to research options and determine the appropriate course of action. A single finding may have multiple recommended corrective actions.

If the internal auditor and the management of the activity under review disagree about the engagement findings or recommendations, the chief audit executive should work with higher levels of management to facilitate a resolution. Per the requirements of Standard 13.1 Engagement Communication, when such a resolution cannot be reached, internal auditors must deliver a final communication that documents the positions of both parties. Additionally, a formal statement from each party may be attached as an appendix to the communication. If not attached as an appendix, each party's complete comments should otherwise be made available upon request.

Internal auditors should evaluate and discuss with management the feasibility and reasonableness of the recommendations and action plans. The evaluation and discussion typically include a cost-benefit analysis and determination of whether the action plans will address the risk satisfactorily in accordance with the organization's risk tolerance.

Public Sector

Laws and regulations often require internal auditors working in the public sector to disclose all management comments in the final communication.

Evidence of Conformance

- Workpapers for each finding, with the criteria, condition, effect, root cause, and recommendation(s) included.
- Relevant internal audit policies, procedures, templates, and guidance.
- Notes, workpapers, or other documentation evidencing discussions with management regarding the findings and feasibility of recommendations and action plans.
- Documentation related to the final communication.

Standard 14.5 Developing Engagement Conclusions

Requirements

Internal auditors must develop an engagement conclusion.

An engagement conclusion is the internal auditor's judgment about the overall significance of the engagement findings when viewed collectively. It must include a summary of the findings and the outcomes of the engagement relative to the engagement objectives and scope.

The conclusion must be developed in accordance with the internal audit function's established methodologies.

Based on the engagement conclusion, internal auditors must issue a rating, ranking, or other indicator of the significance of the aggregated findings.

For an assurance engagement, the engagement conclusion must include the internal auditors' judgment regarding the effectiveness of the governance, risk management, and/or control processes of the activity under review.

Considerations for Implementation and Evidence of Conformance

Implementation

The individual ratings of engagement findings should be aggregated to determine an overall engagement conclusion or summary about the activity under review. The chief audit executive's methodologies for the internal audit function, determined in advance, provide a scale indicating whether reasonable assurance exists regarding the effectiveness of controls. For example, the scale may indicate satisfactory, partially satisfactory, needs improvement, or unsatisfactory depending on the internal auditors' assessments.

Typically, internal auditors use the criteria and methodology, including a rating system, that has been developed by the chief audit executive and reviewed with senior management and the board before the engagement occurs. The rating system should be based on the organization's overall risk appetite and the risk tolerance of the activity under review and should provide the basis for developing engagement conclusions and ratings across all internal audit engagements. Having an agreed-upon understanding for the conclusions and ratings provides consistency across engagements.

The conclusion may add context regarding the impacts of the findings within the activity under review and the organization. For example, some findings may have a material impact on the achievement of goals or the management of risks at a micro level, but not at a macro level (for example, the failure to manage potential duplicate payments may be material to a subsidiary but not to the organization as a whole). Internal auditors should consider how well the controls in place manage the risk to the achievement of management's objectives.

Evidence of Conformance

- A workpaper showing the basis for the overall engagement conclusion and alignment to the chief audit executive's rating system for engagements.
- A policy or meeting notes showing alignment between the chief audit executive, management, and the board on the rating system to be used by the internal audit function.

Standard 14.6 Documenting Engagements

Requirements

Internal auditors must document information and evidence to support the engagement findings, recommendations, and conclusions.

The analyses, evaluations, and supporting information relevant to an engagement must be documented such that an informed, prudent internal auditor, or similarly informed and competent person, could repeat the work and derive the same findings, recommendations, and conclusions.

Engagement documentation must include:

- Date or period of the engagement.
- Work program.
- Engagement risk assessment.
- Engagement objectives and scope.
- Description of analyses, including details of procedures and source(s) of data.
- Findings, recommendations, and conclusions.
- Evidence of communication to appropriate parties.
- Names or initials of the individuals who performed and supervised the work.

Internal auditors must ensure that the engagement documentation is reviewed for accuracy, relevance, and completeness. The chief audit executive or a designee must review and approve the engagement documentation.

Internal auditors must retain all engagement documentation according to relevant laws and regulations as well as policies and procedures of the internal audit function and the organization.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

Documentation of the internal audit engagement through workpapers is an important part of a systematic and disciplined engagement process because it organizes engagement information in a way that enables reperformance of the work and supports engagement conclusions and results. Documentation provides the basis for supervising individual internal auditors and allows the chief audit executive and others to evaluate the quality of the internal audit function's work. Appropriate documentation also serves to demonstrate the internal audit function's conformance with the Standards.

Internal auditors should use the methodology established by the chief audit executive to document the engagement, including the steps and format to be used. This may include templates or software for developing workpapers and a system for retaining the documentation. The workpapers show the information used to determine engagement findings, recommendations, and conclusions.

Generally, workpapers are organized according to the structure developed in the work program and cross-referenced to relevant pieces of information. The end result is a complete collection of documentation of the procedures completed, information obtained, conclusions reached, recommendations derived, and the logical basis for each of the steps. This documentation constitutes the primary source of support for internal auditors' communication with stakeholders, including senior management, the board, and the management of the activity under review. Perhaps most importantly, workpapers contain sufficient and relevant information that would enable a prudent, informed, and competent person, such as another internal auditor or an external auditor, to reach the same conclusions as those reached by the internal auditors who conducted the engagement.

A basic format for workpapers:

- Index or reference number.
- Title or heading that identifies the activity under review.
- Date or period of the engagement.
- Scope of work performed.
- Statement of purpose for obtaining and analyzing the data.
- Planning documentation.
- Process map, flowchart, or narrative descriptions of key processes.
- Summaries of interviews conducted or surveys issued.
- Risk and control matrix.
- Source(s) of data covered in the workpaper.
- Description of population evaluated, including sample size and method of selection used to analyze data (testing approach).
- Details of tests conducted and analyses performed.
- Conclusions including cross-referencing to the workpaper on audit observations.
- Proposed follow-up engagement work to be performed.
- Internal audit final communication with management responses.
- Name of the internal auditor(s) who performed the engagement work.
- Review notation and name of the internal auditor(s) who reviewed the work.

The chief audit executive should develop a methodology for the review of workpapers. The chief audit executive should establish a reliable process to ensure internal auditors achieve engagement objectives and receive training, feedback, and coaching to ensure that the internal audit function continually develops and improves the quality of its performance.

Public Sector

Internal auditors working in the public sector must understand how the laws and regulations relevant to the jurisdictions within which the organization operates may affect or dictate requirements for the release of workpapers. In some jurisdictions, internal auditors are forbidden from releasing workpapers

publicly, while in other jurisdictions, some or all workpapers may be subject to public disclosure as soon as management receives a draft report or upon release of the final communication.

Evidence of Conformance

- Internal audit methodology and templates or software in place for the preparation, content, review, and retention of workpapers and engagement information.
- Workpapers following the methodology.
- Results of internal quality assessment reviews validating conformance with workpaper and supervision policies.

Principle 15 Communicate Engagement Conclusions and Monitor Action Plans

Internal auditors communicate the engagement findings and conclusions to the appropriate parties and monitor management's progress toward the completion of action plans.

Internal auditors are responsible for issuing a final communication after completing the engagement and communicating with management about the findings, recommendations, conclusions, and action plans. Internal auditors continue to communicate with the management of the activity under review to confirm that agreed-upon actions are implemented.

Standard 15.1 Final Engagement Communication

Requirements

For each engagement, internal auditors must develop a final communication that includes the engagement's objectives, scope, and conclusions. Recommendations and/or agreed-upon action plans also must be included.

For assurance engagements, the final communication also must include:

- The findings and the ratings, rankings, or other indication of the significance of the findings.
- An explanation of scope limitations, if any.

The final communication must specify the individuals responsible for taking action on the findings, as well as the planned date by which the actions should be completed. When internal auditors become aware that management has initiated or completed actions to address a finding before the final communication, the actions must be acknowledged in the communication.

The final communication must be accurate, objective, clear, concise, constructive, complete, and timely, as described in Standard 11.2 Effective Communication. Internal auditors must ensure the final communication is reviewed and approved by the chief audit executive or the appropriate designee before it is issued.

Internal auditors must follow the policies and procedures established by the chief audit executive regarding releasing or communicating the final communication. The workpapers supporting the final communication must be retained and accessible to the organization and the internal audit function, including when the engagement is performed by a contracted service provider.

A statement that the engagement is conducted in conformance with the Global Internal Audit Standards must be included in the final engagement communication if the internal auditors followed the Standards and the results of the most recent quality assurance and improvement program support this statement.

If the engagement is not conducted in conformance with the Standards, internal auditors must disclose the following details about the nonconformance:

- Standard(s) with which conformance was not achieved.
- Reason(s) for nonconformance.
- Impact of nonconformance on the engagement findings and conclusions.

PUBLIC EXPOSURE DRAFT
DO NOT REPRODUCE

Considerations for Implementation and Evidence of Conformance

Implementation

The style and format of final engagement communication varies across organizations but typically are established by the chief audit executive. The chief audit executive may provide templates and procedures.

Multiple versions of a final communication may be issued, with formats, content, and level of detail customized to address specific audiences. The final engagement communication should be customized for specific audiences based upon how much they know about the activity under review, how the findings and conclusions impact them, and how they plan to use the information.

When issued as a report, the final communication often includes the following components:

- Title.
- Objectives (purpose of engagement).
- Scope (activities, nature and extent of work, scope limitations).
- Background (brief synopsis of the activity being reviewed or an explanation of the process).
- Recognition (positive aspects of area being reviewed and/or appreciation of cooperation).
- Individual findings grouped by area or process, if applicable, and listed in order of significance:
 - A title and reference.
 - Statement of facts (condition, criteria, cause, effect/risk), which can be substantiated with relevant examples, data, analytics, tables, or charts.
 - Significance of the finding (rating, ranking, or other indicator of the significance of the finding).
 - Recommendations (corrective action to mitigate the risk identified in the finding).
 - Management's action plans (corrective action, activity owner, and target date for completion).
- Engagement conclusion (summary assessment of the engagement, often highlighting critical findings).
- Rating for the engagement as a whole (based on the conclusion, for example, satisfactory, marginal, unsatisfactory, pass, or fail).
- Distribution list.
- The statement regarding conformance with the Global Internal Audit Standards.

The review of the final communication typically includes ensuring:

- The work performed and documented was consistent with the engagement objectives and scope and Standards (when claiming conformance). (See also Standard 8.3 Quality and Standard 12.1 Internal Quality Assessment.)
- The findings, recommendations, conclusions, and action plans are clearly stated and supported by relevant, reliable, and sufficient information. (See also Standard 14.1 Gathering Information for Analyses and Evaluation.)
- Areas needing additional clarification or documentation are addressed.
- The requirements for communicating with the activity under review were met.
- All necessary information is included and superfluous details have been omitted.

The chief audit executive or a designee determines the means by which final engagement communication is disseminated. Oral presentations are usually supported with a digital or printed copy of the presentation and/or a written report.

Internal auditors should comply with any additional laws and regulations relevant to a specific sector, such as the public sector, or industry, such as financial services, for disseminating the final engagement communication.

Evidence of Conformance

- Written final communications.
- Slides and/or meeting notes of presentations when final communication is oral.
- Documentation indicating final communication was reviewed and approved.
- Documentation that requirements for communicating with the activity under review were met.

Standard 15.2 Confirming the Implementation of Action Plans

Requirements

Internal auditors must confirm that management has implemented the agreed-upon action plans.

Internal auditors must follow an established methodology to confirm that management has implemented actions to address engagement findings.

The methodology includes:

- Inquiring about progress on action plans.
- Performing follow-up assessments and analyses.
- Updating the status of action plans in a tracking system.

Internal auditors must request to be notified by management of any changes to the activity under review that cause the engagement findings and action plans to be no longer applicable. Internal auditors must verify the changes reported by management and determine when the changes were made. If internal auditors believe findings remain and action plans are still needed, they must document the information and inform the chief audit executive.

If management has not implemented the agreed-upon action plans according to the established completion dates, internal auditors must obtain and document an explanation from management. Internal auditors must discuss the issue with the chief audit executive, who is responsible for determining whether senior management has accepted the risk of delaying or not taking action. (See Standard 11.5 Communicating the Acceptance of Risks).

Considerations for Implementation and Evidence of Conformance

Implementation

The methodology established by the chief audit executive states how internal auditors are to monitor progress and ensure the effective implementation of management's action plans.

Internal auditors typically use a software program, spreadsheet, or system to track whether action plans are implemented according to the established timelines. The tracking system also indicates whether actions remain open or are past due and provides a useful tool for internal auditors to communicate with senior management and the board. In addition, a program or system may automate the workflow from risk assessment to action plan completion. For example, the workflow could include automated emails that notify the appropriate parties regarding actions that are nearing their target completion dates.

Internal auditors track the status of management's action plans and communicate with the management of the activity under review, the board, and chief audit executive as described in the internal audit methodology. The methodology specifies how and when to follow up on open actions and includes criteria for determining when to perform follow-up assessments and analyses to confirm that action plans have effectively addressed findings and mitigated significant risks. Follow-up assessment and analyses may be performed for all completed action plans on a selective basis, depending on the significance of the risk. Under certain circumstances, regulators may require reporting on management's action plans.

When inquiring about progress, if actions have not been implemented, internal auditors should request that management provide an explanation. If management decides on an alternative action plan and internal auditors agree that the alternative plan is satisfactory or better than the original action plan, then progress on the alternative plan should be tracked until completion.

Public Sector

In some jurisdictions, internal auditors may be required to produce a public report on the implementation status of recommendations.

Evidence of Conformance

- A routinely updated exception tracking system (for example, a spreadsheet, database, or other tool) that contains the prior audit observations, associated corrective action plan, status, and internal audit's confirmation.
- Corrective action status reports prepared for senior management and the board.
- Evidence of periodic reporting to the board on the status of implementation.
- Public records of status implementation reports.