International Professional Practices Framework

Supplemental Guidance
Practice Guide

Engagement Planning

Establishing Objectives and Scope

The Institute of Internal Auditors | Global

Table of Contents

Executive Summary

Planning is part of internal auditing's systematic, disciplined, and risk-based approach and is mandated by the *International Standards for the Professional Practice of Internal Auditing*. Planning internal audit engagements involves considering the strategies and objectives of the area or process under review, prioritizing the risks relevant to the engagement, determining the engagement objectives and scope, and documenting the approach. This practice guide contains the engagement planning steps necessary to fulfill Standard 2200 – Engagement Planning through Standard 2220 – Engagement Scope and related assurance (.A) and consulting (.C) implementation standards.

The exact order and details of planning an engagement, including establishing the objectives and scope, may vary according to the needs of the individual organization, internal audit activity, and engagement. However, the following planning steps are generally included:

- Understand the context and purpose of the engagement.
- Gather information to understand the area or process under review.
- Conduct a preliminary assessment of relevant risks.
- Form engagement objectives.
- Establish engagement scope.
- Allocate appropriate and sufficient resources.
- Document the plan.

To plan the engagement effectively, internal auditors should start by understanding the context and purpose of the engagement, why it was included in the annual internal audit plan, and how the organization's mission, vision, strategic objectives, and other elements align with those of the area or process under review. Internal auditors also consider whether the engagement is a request for assurance or consulting services, as stakeholder expectations and *Standards* requirements differ depending on the type of engagement.

Next, internal auditors gather information about the area or process under review to determine the engagement objectives, scope, and plan. Internal auditors may examine documentation from prior assurance engagements, review applicable policies and procedures, and interview relevant stakeholders to understand and map the process flow and controls in the area or process under review.

Conducting a preliminary assessment of the identified risks helps internal auditors prioritize the risks to be evaluated further during the engagement. Utilizing process maps and brainstorming potential risk scenarios are two techniques that help internal auditors identify risks and controls relevant to the area or process under review. This practice guide explains how internal auditors

can use a risk and control matrix and heat map to prioritize the risks, then use the results to form the engagement objectives and scope, in conformance with the *Standards*. In addition, this guide explores how to allocate resources and document the process of planning and establishing the engagement objectives and scope.

Introduction

As part of the internal audit activity's systematic, disciplined, and risk-based approach, planning is mandated by the *Standards*. Standard 2200 – Engagement Planning requires internal auditors to develop and document a plan for each engagement. It is important for internal auditors to understand the engagement planning process used by their organization's internal audit activity, which is often described in the internal audit policies and procedures manual.

Engagement planning involves considering the strategies and objectives of the area or process under review and prioritizing the risks relevant to the engagement. The plan must contain the engagement objectives, scope, timeline, and resource allocations. Established engagement objectives and scope enable internal auditors to focus efforts on the significant risks in the area or process under review, develop the engagement work program, and communicate clearly with management and the board.

Engagement objectives are broad statements developed by internal auditors that define intended engagement accomplishments. The scope then establishes the focus and boundaries of the engagement by specifying the activities, processes, systems, time period, and other elements included in the review. The objectives and scope also provide a basis to help internal auditors determine the engagement timeline, budget, and resource requirements.

Failing to properly establish engagement objectives may introduce risks that compromise the internal audit activity's ability to:

- Prioritize risks at the engagement level and align them to those of the organization.
- Meet the expectations of the organization and/or stakeholders.
- Protect and enhance organizational value by providing assurance, advice, and insight.
- Improve the organization's governance, risk management, and control processes.

Likewise, if the engagement scope is not properly defined before the engagement starts, the internal audit activity risks inefficiencies or inadequacies, such as:

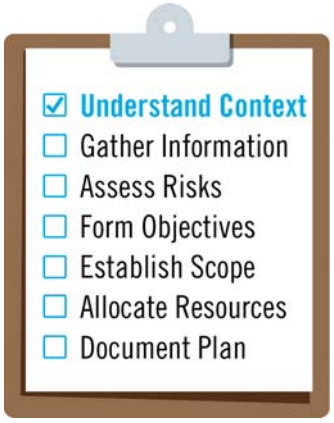
- Failing to address the significant risks to the area or process under review.
- Failing to ensure that management or personnel in the area under review understand the scope and purpose of the engagement.
- Duplicating efforts or performing work that does not add value.
- Allocating resources inadequately to complete the engagement.

Engagement Planning Steps

Several planning steps contribute to the development of the engagement objectives and scope. The specific details of the steps and the order in which they are performed may be adapted to suit the needs of the individual internal audit activity, organization, and engagement. For example, an internal audit activity might begin to formulate preliminary objectives before completing all of the steps necessary to finalize them. However, engagement planning generally includes the following steps:

- Understand the context and purpose of the engagement.
- Gather information to understand the area or process under review.
- Conduct a preliminary risk assessment of the area or process under review.
- Form engagement objectives.
- Establish engagement scope.
- Allocate resources.
- Document the plan.

Understanding Engagement Context and Purpose



Understanding the engagement context and purpose enables internal auditors to plan effectively and ensure that the goals and objectives set forth in the annual internal audit plan are accomplished. Internal auditors should begin by gaining an understanding of the annual internal audit plan, the planning and 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 activity's organizationwide risk assessment, conducted at least annually. 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 annual 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 area or process under review.

To obtain an understanding of the engagement context, internal auditors may also examine the alignment between the organization and the area or process under review, particularly with regard to the following elements:

- Mission, vision, and strategic objectives.
- Structure and processes related to governance, risk management, and control.
- Policies and procedures.
- Risk priorities.

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

Standards Requirements for Assurance and Consulting Engagements

Assurance

When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about the objectives, scope, and other expectations (Standard 2201.A1).

The objectives of assurance engagements must be aligned with the results of a preliminary assessment of the risks relevant to the area or process under review (Standard 2210.A1).

When developing engagement objectives, internal auditors must consider the probability (often referred to as likelihood) of significant errors, fraud, noncompliance, and other exposures (Standard 2210.A2).

Internal auditors must identify adequate and appropriate criteria by which to evaluate whether relevant objectives and goals have been accomplished (Standard 2210.A3).

Consulting

Internal auditors and consulting engagement clients must agree on engagement objectives, scope, expectations, and responsibilities and must document this if the engagement is significant (Standard 2201.C1).

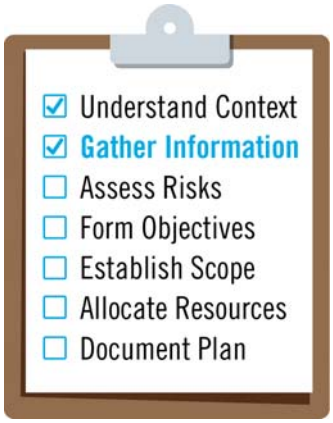
Objectives must address governance, risk management, and control processes to the extent agreed upon with the client (Standard 2210.C1).

Engagement objectives must be consistent with the organization's values, strategies, and objectives (Standard 2210.C2).

Throughout the engagement, internal auditors must address controls consistent with the engagement objectives and be alert to significant control issues (Standard 2220.C2).

auditors, whereas these are typically determined by the client for consulting engagements. Several implementation standards relevant to planning assurance and consulting engagements are listed in the chart on page 6.

Gathering Information



As part of engagement planning, internal auditors gather information about the area or process under review, such as its business objectives, the processes in place to achieve those objectives, the risks that could affect the achievement of those objectives, and the controls in place to mitigate those risks. Understanding the business objectives provides a basis for internal auditors to identify risks that should be included in the preliminary engagement-level risk assessment (as required by Standard 2210.A1).

To gather information, internal auditors typically perform the following actions:

- Review prior assessments of the area or process under review.
- Understand and map the process flow and controls in the area or process under review.
- Interview relevant stakeholders.
- Brainstorm potential risk scenarios.

Internal auditors must document the information they gather while developing the plan, in accordance with Standard 2200 – Engagement Planning. It is helpful to note that the aforementioned actions are not always performed as discrete, sequential steps. Rather, several of the actions, such as mapping processes and documenting information, are ongoing throughout engagement planning.

Reviewing Prior Assessments

Some information about the area or process under review may be gathered from organizational documents. Recently completed relevant engagement assessments and reports may contain information that internal auditors can incorporate into the plan.

Workpapers From Previous Audit Engagements – Internal auditors review workpapers from recent internal audit engagements of the area or process under review to gather information about the processes and controls that were in place during the last review. Reviewing previous workpapers also enables internal auditors to inquire about any corrective actions taken by management to address previous internal audit observations.

Organizationwide Risk Assessments – Internal auditors review the risk priorities that the organization has identified to determine whether any of those risks should be included in the current engagement.

Fraud Risk Assessments and Documents Related to Fraud Allegations and Investigations – Internal auditors should communicate with those in the organization responsible for managing fraud risks, allegations, and occurrences (e.g., legal, human resources, fraud risk management). In addition to discussing fraud occurrences or investigated allegations in the area or process under review, internal auditors should review relevant documentation to understand the facts from the allegation or investigation and the outcomes. Internal auditors may limit research to a reasonable timeframe for confirmed occurrences of fraud and for allegations that were investigated but not substantiated.

Reports by Other Assurance and Consulting Service Providers – Internal auditors may be able to rely on work performed by other internal or external assurance and consulting service providers, rather than duplicating efforts. Internal auditors' ability to rely on others' work is dependent on whether the internal auditors are satisfied that the service provider is sufficiently independent and competent and the work performed is relevant and reliable.

Providers of assurance and consulting services may include personnel responsible for risk management, compliance, environmental health and safety, IT, ethics, legal, security, quality, and more. Service providers may also include external entities such as external auditors or other contracted third parties. Internal auditors may meet with other assurance and consulting service providers to review and discuss reports and/or similar documentation of work performed in the area or process under review. Standard 2050 – Coordination and Reliance provides additional information about collaborating with other assurance and consulting service providers.

Understanding and Mapping the Process Flow and Controls

To identify the risks that could affect the achievement of business objectives, internal auditors must obtain an understanding of the area or process under review. A high-level process map, which depicts the broad inputs and outputs (e.g., activities, workflow, and processing of critical information), may be helpful. Internal auditors may create a process map or refer to one that has already been documented, if they can verify that it is accurate and current.

Process maps enable internal auditors to identify and better understand:

- The systems and information that should be considered when determining the engagement objectives and scope, interdependencies, and where critical information resides (e.g., one system or multiple systems).

- How critical information is used in the area or process under review, which information is relevant to the engagement, and how it will be evaluated during the assessment (e.g., standard testing, data analytics, and key performance metrics).
- Who has the ability to access critical information.
- Points in the process where effective controls may be missing or designed inadequately, or where there may be opportunities for process improvements.

Some of the information needed to populate the process map may be gathered from organizational documents, such as employee handbooks, manuals, and/or intranet websites that include policies and procedures. For example, the vision, mission, business objectives, and strategies relevant to the area under review are often documented. However, these may also be gathered during interviews with management.

Interviewing Relevant Stakeholders

Interviewing relevant stakeholders is a critical step that helps internal auditors better understand the objectives, design, operations, and control environment of the area or process under review. Often, organizational charts can assist internal auditors in identifying relevant stakeholders.

Open-ended questions encourage valuable dialogue between internal auditors and stakeholders, as they require stakeholders to elaborate, prompting additional inquiry opportunities. Internal auditors commonly interview stakeholders such as personnel who perform the steps in a process, management, IT personnel, legal counsel, compliance officers, contracted third parties, and others.

Personnel Who Perform the Steps in a Process – Insights may be gained through interviews with personnel at all levels of the process because they are likely to provide unique information about how the process actually works, not just the way it was designed to operate. Such information can be especially valuable for identifying fraud risk because the personnel responsible for performing the tasks in a process often have the best understanding of the controls and how those controls could be circumvented or overridden.

Management – Managers responsible for the area or process under review may provide the best overview of the way the process was designed to operate. Process information may be documented in the form of policies, procedures, and self-assessments. Additionally, existing documentation may describe the area's business objectives and key performance indicators (i.e., metrics that define whether objectives are being achieved), including how they support organizational objectives. Interviews with management may help internal auditors identify whether management's understanding of the steps in each process differs from that of the personnel who perform the steps. These interviews may also help internal auditors identify the

criteria to be applied when evaluating the governance, risk management, and controls of the area or process under review, as required for assurance engagements (Standard 2210.A3).

IT Personnel – Because IT and information security risks are critical, internal auditors should learn as much as possible about potential risks involving IT. Interviewing relevant stakeholders in IT processes that affect the area or process under review will ensure all applicable systems are considered and may reveal points where controls might be missing, inadequate, or circumvented.

Legal Counsel and Compliance Officers – Many areas and processes are subject to legal and regulatory compliance. Therefore, internal auditors may choose to meet with legal counsel and risk managers to solicit information received through whistleblower programs as well as information regarding unusual events and litigation (past and current) relevant to the engagement. Interviewing compliance officers, or others responsible for operating the systems of control, may provide insight on how effectively compliance with existing policies and procedures satisfies laws and regulations. Relevant laws and regulations may comprise part of the criteria that will be used to evaluate whether the area is accomplishing its business objectives (Standard 2210.A3).

Other Stakeholders – Internal auditors may interview or survey customers or other business areas that deal with the area or process under review to understand past and/or current issues that could indicate potential risks.

Brainstorming Potential Risk Scenarios

Internal auditors may brainstorm with individual personnel or in selected groups or task forces. During brainstorming sessions, to identify relevant risks, auditors may ask, “What would keep the business objectives from being met?” Additionally, to identify inherent risks, internal auditors may ask, “What could go wrong if no controls were in place?”

Due to the significance of fraud risks, Standard 2210.A2 specifically requires that fraud be taken into account when assurance engagement objectives are developed. Brainstorming fraud risk scenarios is especially useful because it gives internal auditors a variety of perspectives from which to consider incentives or pressures that could lead to fraud, opportunities to commit fraud (i.e., control weaknesses), and ways that management and others could override and/or circumvent controls.

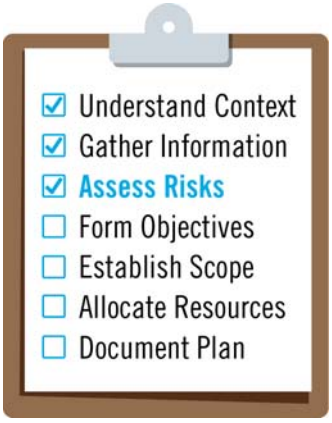
Documenting Gathered Information

By diligently documenting the information gathered during engagement planning, internal auditors can evaluate the data collected to gain perspective on the following:

- Objectives of the area under review.
- Strategies used to achieve those objectives.
- Risks to achieving those objectives.
- Processes and key controls.
- IT and other systems relevant to the area or process under review.
- Sources and reliability of data into and out of the area or process under review.

Obtaining a thorough understanding of the organization and the area or process under review enables internal auditors to conduct a preliminary assessment of the relevant risks, as required by Standard 2210.A1.

Conducting a Preliminary Risk Assessment



Due to time and resource constraints, not all risks can be reviewed during an engagement. Therefore, internal auditors must conduct a preliminary risk assessment and prioritize risks according to significance, which is measured as a combination of risk factors.

One effective way to perform and document a preliminary engagement-level risk assessment is to create a chart showing the relevant risks and controls, such as a risk and control matrix. A risk and control matrix is a tool commonly used by internal auditors to identify, organize, and assess the risks that may impact the business objectives of the area under review, as well as any mitigating controls. A risk and control matrix can be created in a spreadsheet, word processing document, or via an audit software program. The significance of each risk can then be represented on a basic graph, such as a heat map.

To create a heat map, internal auditors plot each risk based on two variables of significance, typically impact and likelihood. This approach creates clear documentation that can be retained as part of the engagement workpapers, which become part of the engagement work program (Standard 2240 – Engagement Work Program). The documents can also serve as part of the "sufficient, reliable, relevant, and useful information" required to support the engagement results and conclusions, according to Standard 2330 – Documenting Information.

Identifying Risks and Controls: Risk and Control Matrix

The risk and control matrix is populated with information gathered throughout the engagement planning process. **Figure 1**, on page 12, depicts an example of how a risk and control matrix could be completed for an accounts payable assurance engagement. The format of a risk and control matrix may vary.

Figure 1: Risk and Control Matrix for Accounts Payable

Business Objective	Inherent Risk	Impact (L,M,H)	Likelihood (L,M,H)	Control
A. Personnel expenses are appropriate and authorized.	A.1 Corporate cards are issued inappropriately, resulting in fraudulent expenses.	M	M	Duties are segregated.
	A.2 Personnel are not provided guidance on corporate card usage and expense policies, resulting in inappropriate expenses.	L	M	Expense policy is communicated to personnel authorized to incur organizational expenses.
	A.3 Expense reports are not submitted/reviewed timely, resulting in inappropriate expenses.	H	H	No control is in place.
	A.4 Expense reports with receipts are not reviewed and approved by appropriate personnel, resulting in inappropriate expenses.	H	M	Approvals are based on management hierarchy. Expense reports cannot be submitted until a manager approves them. Expense team conducts monthly reviews.
B. Operating expenses are appropriate and authorized.	B.1 Fictitious vendors are set up in the system, resulting in fraudulent expenses.	H	L	Duties are segregated.
	B.2 Vendors submit inaccurate, duplicate, or fictitious invoices that are not reviewed and approved by appropriate personnel.	H	M	Invoice approval is based on expense authorization limits.
	B.3 Expenses are not approved before committed to, resulting in inappropriate expenses.	M	L	No control is in place.
C. Payments are accurate and timely.	C.1 Payments are made after the due date, resulting in interest and penalties.	L	M	No control is in place.
	C.2 Discounts are not realized due to payments made after the discount date.	L	H	No control is in place.

The example on page 12 includes five columns with the following information:

- *Business Objective* – Each objective of the area under review (as determined during the information-gathering step).
- *Inherent Risk* – Individual inherent risks to achieving the business objectives. Inherent risks are the risks that could occur if no controls were implemented to mitigate the risk. Creating a simple system to identify each risk, such as the alphanumeric system used in Figure 1, will simplify the process of constructing a heat map later.
- *Impact* – The degree to which each identified inherent risk could affect achievement of the business objective (i.e., What level of impact, or consequence, to the organization or area would this risk have if it were to occur?). Impact is commonly described as high, medium, or low and should consider financial and nonfinancial factors.
- *Likelihood* – The probability and frequency of the occurrence of each identified inherent risk, commonly in terms of high, medium, or low (i.e., How likely is it that the risk would occur if no controls were in place to mitigate the risk?).
- *Control* – The controls intended to mitigate each risk, which were identified during the information-gathering step. Internal auditors may add columns to the risk and control matrix to categorize the controls in terms of:
  - *Criticality* – Key or nonkey.
  - *Type* – Preventative or detective.
  - *Automation* – Manual, systemic, or semi-automated. (Semi-automated controls are manual controls that rely on application functionality, such as an exception report.)
  - *Frequency* – Annually, quarterly, monthly, weekly, daily, or per transaction.

As noted above, internal auditors may rate the significance of each inherent risk by considering the impact and likelihood of the risk. Other measures of significance that could be noted in the matrix include velocity (i.e., speed of reaction and speed of recovery), vulnerability, volatility, interdependency, and correlation. In addition, internal auditors may use other methods or frameworks to identify, organize, and assess the objectives, risks, and controls of the area or process under review.

Determining the significance of risks requires internal auditors to employ their knowledge, experience, and logical thinking to make judgments about the organization, the area or process under review, and the engagement purpose and context. The time invested to gather information during the previous steps yields substantial benefits in this step. While internal auditors ultimately determine the final details of the engagement-level risk assessment, discussions with management of the area or process under review often provide additional perspectives and insights on the business objectives, inherent risks, controls, and ratings of relevant risks.

Prioritizing Risks: Heat Map

A heat map is a basic graph that internal auditors can create to visually represent the combined significance of the risk ratings from the risk and control matrix. The combined significance may be shown by plotting the risk's impact along one axis and likelihood along the other axis.

The alphanumeric character representing each risk is placed on the heat map where the plotted impact and likelihood intersect. For example, a risk with a high impact and high likelihood (H, H) would have its corresponding alphanumeric character placed in the upper right corner of the heat map (see A.3 in **Figure 2**). Conversely, a risk with a low impact and low likelihood (L, L) would be placed in the bottom left corner of the heat map. Typically, the combined significance of impact and likelihood is indicated using a color system: red denotes the highest priorities, orange denotes risks that are significant enough to warrant consideration, and yellow denotes risks that are not a significant threat to the achievement of business objectives.

One limitation with a heat map is that impact and likelihood appear to be equally important. While such equivalence could be true at times, impact usually

Figure 2: Heat Map

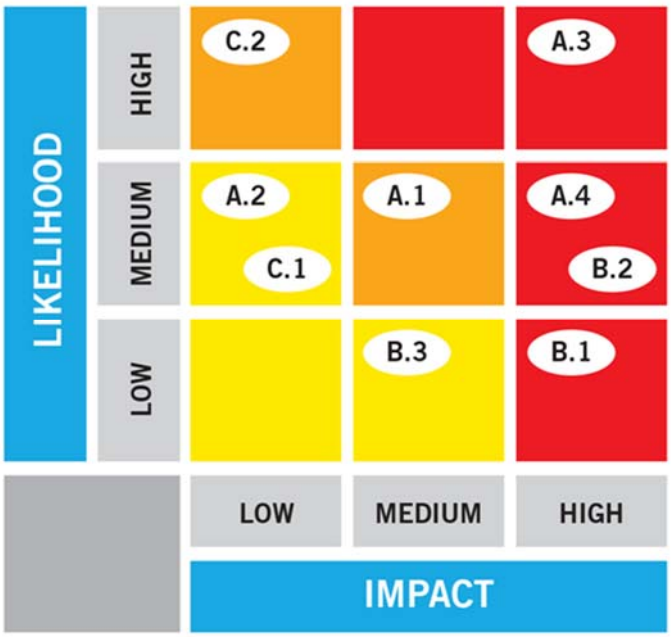


Figure 3: Significant Risks

Inherent Risk	Impact (L,M,H)	Likelihood (L,M,H)
A.3 Expense reports are not submitted/reviewed timely, resulting in inappropriate expenses.	H	H
A.4 Expense reports with receipts are not reviewed and approved by appropriate personnel, resulting in inappropriate expenses.	H	M
B.2 Vendors submit inaccurate, duplicate, or fictitious invoices that are not reviewed and approved by appropriate personnel.	H	M
B.1 Fictitious vendors are set up in the system, resulting in fraudulent expenses.	H	L
A.1 Corporate cards are issued inappropriately, resulting in fraudulent expenses.	M	M
C.2 Discounts are not realized due to payments made after the discount date.	L	H

takes priority over likelihood. For example, in most cases, a risk that is determined to have a high impact and low likelihood (H, L) should be prioritized over a risk that is considered to have a low impact, even if the likelihood is high (L, H). An additional limitation of a heat map is that it only shows two variables at a time (in this case, impact and likelihood).

Once the heat map has been created, internal auditors can easily identify the significant risks that need to be included when forming the engagement objectives (i.e, the risks that fall into the red and orange areas of the heat map). **Figure 3**, on page 14, illustrates the most significant accounts payable risks from the example on page 12, based on their impact and likelihood.

Forming Engagement Objectives

Once internal auditors have completed the preliminary risk assessment and identified the significant risks to evaluate during the engagement, they can form the engagement objectives. The engagement objectives articulate what the engagement is specifically attempting to accomplish; therefore, the objectives should have a clear purpose, be concise, and be linked to the risk assessment (Standard 2210.A1).

Assurance Engagement Objectives

Internal auditors should ensure that the objectives of the assurance engagement align with the business objectives of the area or process under review. The assurance engagement should focus on ensuring controls are in place to effectively mitigate the risks that could prevent the area or process from accomplishing its business objectives.

Internal auditors must also identify adequate criteria to evaluate the governance, risk management, and controls of the area or process under review and determine whether the business objectives and goals have been accomplished. Identifying such criteria ensures that assurance engagement objectives are measurable, practical, and aligned with the objectives of both the organization and the area or process under review.

Assurance engagement objectives must:

- Reflect risks to the business objectives of the area or process that were assessed as significant during the preliminary risk assessment (Standard 2210.A1).
- Consider the probability of significant errors, fraud, noncompliance, and other exposures (Standard 2210.A2).
- Be based on evaluative criteria (Standard 2210.A3).

According to Standard 2210.A3, internal auditors must use the criteria already established by management and/or the board, if such criteria exist. If no criteria are in place, internal auditors must identify appropriate criteria through discussion with management and the board. Internal auditors should also consider seeking input from subject matter experts to help develop relevant criteria.

Examples of criteria include:

- Existing key performance indicators.
- Targets set during strategic planning.
- The degree of compliance with area or process policies and procedures, external laws and regulations, and/or contracts.
- Industry standards or benchmarks.

To avoid misinterpretation or challenge by any personnel responsible for the area or process under review, the evaluation criteria should be relevant, reliable, and documented. Adequate, appropriate criteria will provide a reference for internal auditors to evaluate evidence, understand findings, and assess the adequacy of the controls in the area or process under review. The criteria, or lack thereof, should be compared to industry benchmarks, trends, and forecasts, as well as the organization's policies and procedures.

The following is an example of how assurance engagement objectives could be formulated for the aforementioned accounts payable engagement.

The internal audit activity will provide assurance that:

- Expenses incurred are appropriate according to the organization's expense policy.
- The expense report submission, approval, and payment process controls are effective and efficient.
- Personnel and operating expenses are appropriate and authorized.
- Expense payments are made accurately and timely.

Consulting Engagement Objectives

Due to consulting services being advisory in nature, the expectations and objectives are determined either by, or in conjunction with, the engagement client. Thus, consulting engagement planning typically occurs after the engagement objectives and scope have already been determined. Therefore, internal auditors may not need to complete a preliminary risk assessment, as they would when planning an assurance engagement. However, Standard

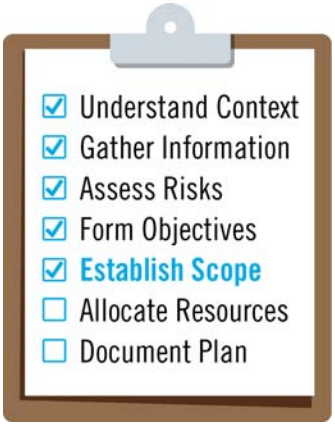
2201.C1 requires internal auditors to establish an understanding with the consulting engagement client about the objectives, scope, responsibilities, and other expectations. For significant engagements, this understanding must be documented.

Additionally, internal auditors must address governance, risk management, and control processes to the extent agreed upon with the consulting engagement client (Standard 2210.C1). Although the consulting engagement purpose and expectations are directed by the engagement client, internal auditors must ensure the engagement objectives are consistent with the organization's values, strategies, and business objectives (Standard 2210.C2).

An objective for an accounts payable consulting engagement could be:

> The internal audit activity will advise on the risks of outsourcing the accounts payable process to a third party.

Establishing Engagement Scope



Once the risk-based objectives have been formed, the scope of the audit engagement can be determined. Because an engagement generally cannot cover everything, internal auditors must determine what will and will not be included. The engagement scope sets the boundaries of the engagement and outlines what will be included in the review. Internal auditors must carefully consider the boundaries of the engagement to ensure that the scope will be sufficient to achieve the objectives of the engagement (Standard 2220 – Engagement Scope).

The scope may define such elements as the specific processes and/or areas, geographic locations, and time period (e.g., point in time, fiscal quarter, or calendar year) that will be covered by the engagement, given the available resources. Internal auditors must carefully consider the breadth of the scope to ensure it enables timely identification of reliable, relevant, and useful information to accomplish the identified engagement objectives (Standard 2210 – Engagement Objectives and Standard 2310 – Identifying Information).

Assurance Engagement Scope

When determining the scope of an assurance engagement, it is helpful for internal auditors to review the engagement objectives to ensure that each objective can be accomplished under the established parameters. To ensure the scope is sufficient to meet the engagement objectives and it aligns with the organization's annual internal audit plan, internal auditors must use sound professional judgment based upon relevant experience and/or supervisory

assistance. They must also consider relevant systems, records, personnel, and all physical properties (Standard 2220.A1).

Internal auditors should consider how legal factors may affect the engagement scope and approach as well. For example, if the organization or area under review has nondisclosure agreements with third parties, the organization may be required to notify regulatory authorities before starting the engagement. Pending or imminent litigation and cases of noncompliance should also be considered.

The following is a list of possible inclusions and exclusions for the scope of an accounts payable assurance engagement:

- Expenses (operational, travel, supplies, personnel, and/or corporate, etc.).
- Personnel (executive, management, all, etc.).
- Locations (corporate office, operational locations, countries, etc.).
- Timeframe (current, previous, month, quarter, year, etc.).
- Materiality (any amount or only amounts over certain authorized limits, etc.).
- Systems (only systems that process expenses or also human resources systems, all systems, etc.).

The following is an example of an engagement scope for the aforementioned accounts payable assurance engagement.

> The assurance engagement will cover personnel and operating expenses submitted for the 12-month period ending August 20XX and the processes for submitting, approving, and paying expense reports (including a third-party software used to submit expense reports). The engagement scope includes all personnel that utilize the third-party software to submit personnel and operational expenses. The engagement will also include a compliance review with the organization's expense policy.

If the assurance engagement scope is limited in any manner or if access to necessary sources of information is restricted, internal auditors must disclose these situations to senior management and/or the board. Such situations would be considered impairments to internal audit independence (Standard 1130 – Impairment to Independence or Objectivity).

While performing the engagement, internal auditors may gain new information that requires the engagement scope to be modified. For example, if a subsidiary is being closed and liquidated, the scope of the engagement may change to exclude the affected location and include a

different subsidiary instead. Similarly, if a process has changed recently, internal auditors should consider whether the process remains in scope (i.e., should still be included in the current engagement) or whether the change warrants a separate review. In such cases, internal auditors may choose to shift the engagement focus to provide assurance over the new process, incorporate the new process into the annual internal audit plan, or perform a separate consulting engagement.

Once an assurance engagement has begun, any modifications to the work program — including any changes to the scope — must be approved (Standard 2240.A1). Additionally, if significant consulting opportunities arise during the assurance engagement, internal auditors should consider whether a separate consulting engagement is warranted. If so, a specific written understanding as to the objectives, scope, respective responsibilities, and expectations should be reached, and the results of the consulting engagement should be communicated in accordance with consulting standards (Standard 2220.A2).

Consulting Engagement Scope

The scope of a consulting engagement is designed to satisfy the expectations of the engagement client. As Standard 2220.C1 states, the scope of consulting engagements must be sufficient to address the objectives that were agreed upon with the engagement client. If internal auditors develop reservations about the scope during the consulting engagement, these reservations must be discussed with the engagement client so that a decision can be made regarding whether to continue with the engagement. For example, internal auditors may develop reservations in situations where there is insufficient information to perform the consulting engagement, or if they recognize that the results of such an engagement are not likely to add value to the organization.

Additionally, Standard 2220.C2 requires internal auditors to address controls consistent with the engagement objectives and to remain alert to significant control issues. Furthermore, Standard 2130.C1 requires internal auditors to incorporate knowledge of controls gained from consulting engagements into the evaluation of the organization’s control processes.

Allocating Resources

After establishing the engagement objectives and scope, internal auditors must determine appropriate and sufficient resources to achieve the engagement objectives, as required by Standard 2230 – Engagement Resource Allocation. The interpretation of Standard 2230 clarifies that *appropriate* refers to the mix of knowledge, skills, and other competencies needed to perform the engagement, and *sufficient* refers to the quantity of resources needed to accomplish the engagement with due professional care.

Resources are allocated to the engagement based on the following:

- The knowledge internal auditors acquire during engagement planning.
- The nature and complexity of the engagement.
- Time constraints and/or the number of hours budgeted for the engagement.
- The knowledge, skills, and experience of available resources.

Internal auditors should consider whether external resources (e.g., specialists or supplemental resources) or technology will be necessary when the internal audit activity does not have appropriate or sufficient resources.

Documenting the Plan

During planning, internal auditors document information in engagement workpapers. This information becomes part of the engagement work program that must be established to achieve the engagement objectives, as required by Standard 2240 – Engagement Work Program.

The process of establishing the engagement objectives and scope may produce any or all of the following workpapers:

- Process map.
- Summary of interviews and brainstorming sessions.
- Preliminary risk assessment (e.g., risk and control matrix and heat map).
- Rationale for decisions regarding which risks to include in the engagement.
- Criteria that will be used to evaluate the area or process under review (required for assurance engagements, according to Standard 2210.A3).

The CAE and/or designated engagement supervisor should review all workpapers to confirm the information is complete and accurate. A supervisory review of the documents should verify that the engagement objectives and scope reflect the results of the preliminary risk assessment and that evaluation criteria have been identified or developed. For an assurance engagement, the work program must be approved before it is implemented (Standard 2240.A1). In contrast, the requirements for consulting engagement work programs depend upon the nature of the engagement.

In addition, the results of the preliminary risk assessment, the engagement objectives, and the engagement scope should be discussed with management of the area or process under review and key stakeholders across the organization (e.g., risk and compliance managers, the chief risk officer, and senior management). Such discussions provide an opportunity for all parties to mutually understand the results of the engagement-level risk assessment, to confirm the risks and controls relevant to the engagement, and to understand their place in the organizationwide risk assessment, if appropriate. Discussions should include assurance that key personnel and resources will be available during the engagement. Such information may also be communicated to the board.

Internal auditors may create an engagement planning memorandum (planning memo), to communicate the objectives, scope, and timing of the engagement. The planning memo provides an opportunity for internal auditors to ensure that management of the area or process under review understands and supports the engagement plan. If management disagrees with any elements of the plan, internal auditors can either make adjustments or document the rationale for why the engagement will not be modified despite management's disagreement. A planning memo may also help internal auditors communicate the engagement to other internal auditors and the board. Documentation of the plan and management's feedback is often incorporated into the engagement workpapers.

Thorough planning and documentation are not only necessary for conformance with the *Standards*, but are also crucial steps that enable internal auditors to prepare for and perform successful engagements. Because not every risk can — or should — be included in a single engagement, proper planning helps internal auditors focus their efforts on the most significant risks in the area or process under review.

Appendix A. Relevant IIA Standards

Selections from The IIA's *International Standards for the Professional Practice of Internal Auditing* relevant to this guide are listed below. To assist with implementation of the *Standards*, The IIA recommends that internal auditors refer to each standard's respective Implementation Guide.

Standard 2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.

Standard 2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

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

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

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

Standard 2210 – Engagement Objectives

Objectives must be established for each engagement.

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

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

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

Interpretation:

Types of criteria may include:

- *Internal (e.g., policies and procedures of the organization).*
- *External (e.g., laws and regulations imposed by statutory bodies).*
- *Leading practices (e.g., industry and professional guidance).*

Standard 2220 – Engagement Scope

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

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

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

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

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

Standard 2230 – Engagement Resource Allocation

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

Interpretation:

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the engagement. Sufficient refers to the quantity of resources needed to accomplish the engagement with due professional care.

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from The IIA's International Professional Practices Framework Glossary.

Assurance services* – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Consulting services* – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

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. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Engagement* – A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

Engagement objectives* – Broad statements developed by internal auditors that define intended engagement accomplishments.

Engagement scope – The focus and boundaries of the engagement established by internal auditors that specify the activities, processes, systems, time period, and other elements that are included.

Risk* – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

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 judgement assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

Acknowledgements

Guidance Development Team

Glenn Ho, CIA, CRMA, South Africa (Chairman)
Caroline Glynn, CIA, United States (Project Lead)
Doug Hileman, CRMA, CPEA, United States
Thomas Sanglier, CIA, CRMA, United States

Global Guidance Contributors

Farah Araj, CIA, QIAL, Canada
Özge Ascioglu, CIA, CFSA, CRMA, Turkey
Cheryl Dove, United Kingdom
Stephen Germain, CIA, United States
Lee Wyckoff, CIA, United States

IIA Global Standards and Guidance

Christine Hovious, CIA, CRMA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Lauressa Nelson, Technical Writer
Christina Brune, Technical Writer

The IIA would like to thank the following oversight bodies for their support: Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

About Supplemental Guidance

Supplemental Guidance is part of The IIA's International Professional Practices Framework (IPPF) and provides additional recommended (nonmandatory) guidance for conducting internal audit activities. While supporting the *International Standards for the Professional Practice of Internal Auditing*, Supplemental Guidance is not intended to directly link to achievement of conformance with the *Standards*. It is intended instead to address topical areas, as well as sector-specific issues, and it includes detailed processes and procedures. This guidance is endorsed by The IIA through formal review and approval processes.

About Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. As part of the IPPF Guidance, compliance with Practice Guides is recommended (nonmandatory). Practice Guides are endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

Copyright

August 17