CHAPTER 10

Risk Assessment and Audit Planning

Risk assessment is the starting point for internal audit service and product development and delivery. Like all business units in an organization, the internal audit function has limited resources and must decide what work to prioritize in a given period of time. Three considerations go into making this important decision:

- Expectations of key stakeholders (senior management and the board)
- Risks to the achievement of strategic and business objectives
- Professional requirements in delivering assurance and advisory services

Providing assurance that the major risks to the achievement of the organization's objectives are identified, accurately assessed, and effectively managed is the internal audit function's most valuable activity. It is a specific contribution that internal audit is uniquely positioned to make. However, organizations operate in vastly different environments and stakeholders have different requirements, expectations, and priorities. Chapter 1, "Developing an Internal Audit Strategy," and chapter 2, "Defining Internal Audit Products and Services," address how these variables impact the internal audit function's vision, mission, strategies, value propositions, and products and services. The choice of products and services delivered by internal audit defines the risk assessment effort. The products and services, based on the maturity level of the internal audit function as discussed in chapter 2, are detailed in **exhibit 10-1**.

A risk assessment is simply an assessment of a collection of risks. The output of a risk assessment enables the internal audit function to direct its work to areas where the most value can be provided, but it may also be a product by itself. Based on the complexity and collaboration involved in the risk assessment, it could contribute in other ways to management or the second line of defense efforts. Typically, the first step in a risk assessment is to create a universe or the population to be covered. This may be defined by the scope of anticipated assurance or advisory engagements or by a wider risk assessment purpose, for example, in collaboration with other functions. This chapter discusses how the universe or population covered in the risk assessment is different based on the products and services that are part of the internal audit strategy.

Many factors must be considered in the risk assessment and audit planning process. Internal auditors first need to understand the objectives of risk assessment and the related components, such as principles, types of audit engagements, and the resulting audit plans. Similarly, there are several factors that go into defining the risk assessment process, such as services and products stakeholders expect from the internal audit function and risk models and coordination expectations with other

Exhibit 10-1
Maturity of Internal Audit Value, Services, and Products

Level	Type of Services	Types of Products	Value of Internal Audit
Level 5	• Places risk management-based efforts in the context of the specific business objectives at risk by building on the prior levels below. • Internal audit is recognized as a key agent of change.	• Risk assessments are integrated with risk management efforts. • Assurance and advisory engagements are focused on helping management achieve objectives through improvement of risk management in both the first and second lines of defense.	• Internal audit takes ownership for communicating risk in terms management understands as it strives to achieve business objectives. • Business objective achievement is considered in all risk assessment and assurance and advisory engagements. • Internal audit recommendations and advice improve the organization's governance, risk management, and control (GRC).
Level 4	• Evaluation of risk management expectations first in risk assessment and audit program development, focused on strengthening controls from the top down. • Internal audit provides overall assurance on GRC.	• Risk assessments are focused on top strategic and operational risks. • Assurance and advisory services are focused on expected risk management and control activities from the top down.	• Internal audit places risks and findings in terms of risk management structures and tools that management should be developing and using as part of daily operations. • Internal audit efforts are more in line with management efforts on objective achievement.
Level 3	• Advisory services are provided. • Risk assessments are performed at least annually. • Audits are planned and findings are identified by risk likelihood and impact. • Assurance services expand on Levels 1 and 2.	• Risk assessments that include important operational areas • Risk-based audit reports with findings ranked • Advisory engagement results	• Internal audit uses risks to define priorities for management and the board. • Risk assessments and assurance and advisory engagement reports focus on risk priorities.
Level 2	• Evaluation of financial and important operational process controls	• Audit reports that include findings related to financial and operational process control weaknesses and analyses on their root causes	• Internal audit contributes to understanding and mitigation of financial and compliance risks and findings. • Internal audit contributes to understanding and improvement of operational process controls and mitigation of operational process risks and findings.
Level 1	Internal/external auditor services are provided and focus on: • Financial statement assurance and reviews of documents and transactions for accuracy and compliance • Compliance with external regulations, standards, and requirements • Compliance with internal policies and standards	• Audit reports are focused on financial reporting and noncompliance findings.	• Internal audit provides financial reporting assurance. • Internal audit provides compliance assurance.

internal groups in the Three Lines of Defense model. Ultimately, these factors and other decisions discussed later in the chapter drive the development of the audit plan and allocation of resources. The audit plan must then be approved with the expectation that there will be updates and ongoing stakeholder communication.

The products expected by stakeholders, the maturity of the internal audit function's services and products, the second line of defense functions, and enterprise risk management (ERM) efforts in general all directly impact the population and the risk assessment methods. In-depth knowledge of the organization is critical to adding value with these risk assessment efforts. Exhibit 10-1 illustrates where an internal audit function is related to the maturity of the value, services, and products it seeks to deliver. This understanding should inform the methods and processes employed to produce expected deliverables from risk assessment efforts.

Risk Assessment Objectives

Three general objectives for risk assessment activities apply to most of the maturity levels noted in exhibit 10-1. The scope and complexity of these objectives increases at the higher levels of 4 and 5.

1. Keep a current profile of the risks that impact the most critical objectives to enable management to implement effective risk mitigation practices. Behind this risk profile is an understanding of controls in place to manage these risks.
2. Allocate scarce internal audit resources to assurance and advisory engagements to help the organization protect and enhance organizational value by improving the effectiveness of risk management, control, and governance processes.
3. Contribute the internal audit perspective of organizational risk to complement existing risk assessing and managing practices within management and second line of defense functions. (This may not be an objective in every internal audit function.)

Risk Assessment Components

Based on the unique role of the internal audit function and its professional standards, internal audit is in the best position to help management and governance functions gain a holistic perspective of organizational risks and the state of internal controls. This insight is not only useful for developing the internal audit plans; it should be leveraged as practical for risk management purposes.

Risk Assessment Principles

- The internal audit function should focus its effort on areas with important organizational objectives and their risks.
- IT and third-party service providers are integral parts of business processes and operations and should be integrated into risk assessment efforts.
- The internal audit function should get inputs from key stakeholders to ensure their perspectives and risk appetite are considered and expectations are met.

- The internal audit function should validate risk assessment results with key stakeholders to ensure all perspectives are considered. Actual validation of mitigating controls does not usually happen as part of the risk assessment.
- Risk assessment benefits from having diversified perspectives. The internal audit function should collaborate with first line management, objective and risk owners, subject matter experts (SMEs), cross-functional teams, and second line risk professionals and compliance specialists to improve the effectiveness of risk assessment and management, coordinate audit work, and support development of risk management practices.
- The internal audit function should have a seat at the table at relevant committees and task-forces to offer timely perspectives and get timely information on risks.
- Risk intelligence requires ongoing analyses and environment scanning to identify emerging risks and early warning signs. Risk assessment should be updated when there are changes and new information is identified that would impact assessment results.
- The internal audit function should leverage the risk management function's risk assessment results for audit plan development.
- In organizations with mature ERM, internal audit should be an active contributor of risk data and provide risk management capability assessments of functions contributing to ERM efforts (specifically, second line of defense and management), as well as the effectiveness of ERM risk mitigation.
- Organizations should consider investments in technology, such as analytical and brand monitoring tools, to help leverage and analyze data to strengthen their risk-sensing capabilities. Governance, risk management, and control (GRC) technology may also help to organize various management and second line of defense function risk perspectives.
- Risk assessment documents should use plain language that speaks to a general business audience.

Assurance and Advisory Engagements

The internal audit function's primary purpose for performing a risk assessment is to meet professional expectations that its projects and plans are risk-based. Internal audit conducts two types of risk-based engagements:

- Assurance engagements are objective examinations of evidence for the purpose of providing an independent assessment on GRC processes to help the organization achieve its strategic, operational, financial, and compliance objectives. Examples may include technology project implementation, financial processes, operational performance, compliance, system security, and due diligence engagements.
- Advisory engagements, the nature and scope of which are agreed with business area management, are intended to add value and improve an organization's GRC processes. Examples include collaborating on incorporating control development considerations in project management standards for strategic projects, evaluating policy-writing processes to determine a method of valuing expected outcomes, and providing counsel, advice, insight, facilitation, and training.

Audit Plan Development - General Approach

Chief audit executives (CAEs) are responsible for leveraging information about stakeholder expectations and organizational risks to create a periodic (no less than annual) plan. This plan is reviewed and approved by the audit committee. In general, creating a risk-based audit plan is a professional expectation of CAEs. This is typically handled by treating the risk assessment as data and input to a separate audit planning effort. Such an effort includes:

- Selecting the audit plan development team
- Establishing accountability, budgets, and available resources (auditor time, external resources needed for technical projects)
- Defining the required assurance and advisory engagements
- Defining the budget, priorities, and schedules for risk-based assurance and advisory engagements

Performing Risk Assessment Activities

Preparation

Performing risk assessment activities is one of the most important responsibilities of the internal audit function. The decisions regarding where to audit, what to audit, and when to audit have a direct impact on internal audit's ability to meet professional expectations and the preservation and creation of organizational value to meet stakeholders' expectations. Performing risk assessment activities provides internal audit ample opportunities to interact with senior management, demonstrate understanding of the business, and display business acumen. In order to use time effectively and ask the right questions, internal auditors need to make good use of the information prepared by management for internal and external audiences. When internal auditors ask senior management basic questions on information that is widely available, it wastes time and undermines management's confidence in internal auditors' business acumen. In the limited time senior management is giving them their attention, internal auditors should ask for their insights, perspectives, and concerns.

The following materials provide a good understanding of the business and its risks from the perspectives of various parties. Internal auditors can get a multifaceted view of the organization through these diversified viewpoints and an in-depth understanding by making connections. They should review:

- Documentation of the last risk assessment performed and update for any changes. Ensure that the following points are well covered and current.
- The organization's structure, organizational chart, and general accountabilities for strategic and business objectives. Review its significant alliance partners, joint ventures, and service providers. Obtain, in writing, the organization's key objectives, strategic and operational priorities, and significant IT infrastructure and applications. Understand the mission of the organization, how it creates and preserves value, and the role of technology in this effort.

- Current and prior years' financial, performance, and operational reports to understand performance against objectives, external and internal risk factors that positively and negatively impact performance, challenges ahead, and management responses.
- Financial and nonfinancial reports filed with regulators. In many countries, organizations are required to submit reports that provide a comprehensive overview of the company's business and financial conditions and include audited annual financial statements and unaudited quarterly financial statements, major events that shareholders should know about, and material changes in a publicly traded company's operations. These reports provide a lot of information and insight about the company's operational and financial performance, as well as key risks and challenges from management's perspective.
- Other internal reports that help identify risks and top-of-mind issues and inform appropriate internal audit coverage as discussed in chapter 7, "Cultivating Business Acumen," such as:
  - Customer feedback
  - New customer segments, products, and services
  - Risk profile reports and results of risk assessments conducted by the business units or by second line of defense functions
  - Operational loss data and associated control breakdowns
  - Compliance breaches and associated control breakdowns
  - Lessons learned from scandals at other organizations
  - Regulatory issues and actions
  - Organizational culture assessments
  - Employee engagement survey results
  - Fraud risk assessments and indicators
  - Information on the organization's intranet and internet sites
- External sources that provide relevant insights on risks external to the organization (for example, competitive, political, or economic):
  - Regulatory and legal developments, queries, and requests that could affect the conduct of the organization's business, such as monetary, fiscal and foreign exchange policies and tariffs, import/export duties, or trade restrictions policies. The organization must adjust their business processes and platforms to meet these requirements.
  - Stock rating agency reports; understanding the ratings from agencies such as Fitch, Moody's, and Standard and Poor's that directly or indirectly affect the environment in which the organization operates. For example, when reviewing "Natural Catastrophe Risk," a good starting point is to review the company's presentation to the rating agencies and regulators and the insurance agencies to see what risks are of interest to them.
  - Ranking reports comparing organizations in the same or different industries. Understanding the factors that contribute to the organization's ranking or how it fares with its competitors helps the internal audit function identify relevant risks and engage with management on business issues that matter.
  - Industry outlooks and global trends that "predict" the future of the industry. Business strategies need to consider and respond to these predictions.
  - Technology trends that impact the business, strategies, and decision making.

- Thought leadership materials on what progressive organizations are doing to respond to challenges and opportunities ahead.

Risk Assessment Process Considerations

As previously discussed, risk assessment processes are highly dependent on the level of services and products the internal audit function seeks to deliver. Each level of service, product, and value were identified in exhibit 10-1. Level 1 is the least mature or ambitious and Level 5 is the most mature or ambitious. These levels serve as examples or a framework from which a process can be developed to meet any organization's specific expectations.

Level 1 – Initial (Low Level of Maturity)

Population Covered

Exhibit 10-2 notes Level 1 internal audit service and product expectations. At this level, stakeholders expect internal audit to provide financial and regulatory assurance. In this traditional environment, it is relatively straightforward to define the universe or population that the risk assessment will cover. It typically focuses on the finance, public reporting, and compliance programs within the organization.

Exhibit 10-2
Level 1 Internal Audit Services, Products, and Value

Type of Services	Types of Products	Value of Internal Audit
Internal/external auditor services are provided and focus on: • Financial statement assurance and reviews of documents and transactions for accuracy and compliance • Compliance with external regulations, standards, and requirements • Compliance with internal policies and standards	• Audit reports focused on financial reporting and noncompliance findings	• Internal audit provides financial reporting assurance. • Internal audit provides compliance assurance.

Audit Plan - Expected Products and Services

At Level 1 maturity, the internal audit function may be informal and may not have a CAE. Internal audit positions are generally established to address some specific, immediate needs, such as:

- Providing support to external auditors
- Providing Sarbanes-Oxley support to the corporate controller

- Performing compliance engagements required by law or regulation. Even if the risks of non-compliance are small, these engagements must be part of internal audit's audit universe.
- Evaluating compliance with corporate policies (for example, travel policies, expense policies, purchasing policies, conflicts of interest, warranty policies, and sales incentive policies)

At Level 1, internal audit most likely does not have a strong sponsor and advocate in the organization. This means that internal auditors have to take the initiative to promote and advocate its value. This can be done by getting a good understanding of the drivers for the current population of engagements to determine if they are still relevant. Some of the engagements may have outlived their purposes. Some may be duplicating work being performed by second line of defense functions or should be performed by other functions. Internal audit can conduct a risk assessment of the engagements assigned to determine if these are the best use of internal audit resources and where internal audit can add more value by fully applying its core competencies. For example, internal auditors can demonstrate leadership and competency by assisting other second line of defense functions to implement or improve risk management and compliance management or to help the organization move up the capabilities maturity curve by facilitating change management. Helping second line of defense conduct a risk assessment for the compliance program would pave the way for advancing to Level 2 maturity and beyond.

Procedures and Methods

At this level, there may not be a formal risk assessment process. Management may work directly with the public accountants to agree on resources committed to support the financial statement audit. When this is the case, management often identifies a list of engagements for the internal audit function to perform and allocates hours. Most engagements are repetitive and performed on a cycle basis, with some one-time engagements when warranted. Hours and approaches are refined over time. As procedures improve, internal auditors may define specific risk assessment procedures to identify financial and regulatory areas where internal audit services will be of value. When management adds or deletes engagements from the plan, the budgeted hours, the audit plan, and the financial budgets are adjusted accordingly. Without a sponsor with professional experience, Level 1 internal audit functions could stay this way for an extended period of time until internal and external factors require or create opportunities to move internal audit to the second level of maturity and beyond.

Value

Internal audit can offer assurance services related to its core competencies in compliance and financial reporting. Since many of the engagements are repetitive, internal auditors have opportunities to improve the efficiencies and effectiveness of conducting them and identify systemic issues. If management has not created a compliance function, internal audit can work with management to compile expectations, develop a process to assess compliance risks, and validate the completeness of a compliance universe.

Level 2 – Repeatable

Population Covered

Exhibit 10-3 notes Level 2 internal audit service and products. The internal audit function improves on Level 1 financial and regulatory assurance by focusing more on processes and compliance with process-level controls. In this environment, internal audit is still coming from a standard financial and regulatory assurance perspective, largely focused on the finance, public reporting, and compliance programs within the organization. When the internal audit function is at Level 2 maturity, it continues to provide services, products, and value offered at Level 1 but with more operational awareness. Internal audit functions at this level typically have four population areas to cover:

- Financial statement account and reporting process
  - Sarbanes-Oxley support to corporate controller
  - External audit support
  - Financial assurance work
- Operational processes
- Regulatory compliance
- Corporate policy compliance

Exhibit 10-3
Level 2 Internal Audit Services, Products, and Value

Type of Services	Types of Products	Value of Internal Audit
• Evaluation of financial and important operational process controls	• Audit reports that include findings related to financial and operational process control weaknesses and analyses on their root causes	• Internal audit contributes to understanding and mitigation of financial and compliance risks and findings. • Internal audit contributes to understanding and improvement of operational process controls and mitigation of operational process risks and findings.

Audit Plan - Expected Products and Services

At Level 2 maturity, the internal audit function is likely an established function with its own CAE, budget, and business plan. Internal audit adopts The IIA's International Professional Practices Framework (IPPF) and has access to information, assets, and people to conduct audit work. The internal audit function may not have the resources to achieve full compliance with the IPPF at this level. Compliance with the IPPF expands internal audit's scope of work and improves the quality of services. Internal audit begins to identify financial and operational process control weaknesses, analyze their root causes, and recommend that management take appropriate actions to address the root causes and prevent recurrence. Internal audit is helping the organization understand and mitigate financial, compliance, and operational risks related to findings in these areas.

Procedures and Methods

The CAE and internal audit function typically begin their risk assessment process development efforts at this level of maturity. When considering financial statement risks, the risk assessment processes are often borrowed from external auditors as a starting point. These risk assessment processes include concepts such as financial materiality, inherent risk, and residual risk. Each of these concepts is created to draw independent lines around what is being assessed. Although management input is sought to understand processes, these risk assessment methods and procedures are self-defined and self-operated. Other sources of information that drive this risk assessment are regulations, policies, and flowcharts. Risk is typically defined as "not meeting financial, regulatory, policy, or process expectations." However, risks are assessed for operational process root causes where breakdowns account for inefficient or ineffective effort and/or noncompliance. In setting up the scope of the risk assessment activity, the internal auditor typically considers various populations (universes) of risk information.

- **Financial Statement Account and Financial Reporting Process Universe**
  If the organization must comply with Sarbanes-Oxley-like requirements, the internal audit function should leverage the risk assessment of accounts and financial reporting processes or systems performed by the first and second lines of defense. If such an assessment has not been performed, internal audit should work jointly with management to develop the risk factors and the risk assessment process.

- **Operational Process Universe**
  When considering risks within operational processes, there is consideration of the compliance, efficiency, and effectiveness of those processes. If processes are ineffective and operations are impacted, the outcomes may include incomplete, fraudulent, or erroneous transactions or poor-quality products. With regard to financial, policy, and compliance risks, their supporting processes are reviewed to ensure transactional and procedural level controls are working.

  The procurement process is a common example. Financial data come from this process and must comply with policies and regulatory expectations. Is accountability for this process clear and is it operated in a way that supports robust transactional controls, efficiency, and effectiveness? In the risk assessment, management inquiry will provide an indication of process effectiveness.

  Process audits should include supporting IT systems and third-party service providers. Today, many controls have been automated to improve efficiency, control, and consistencies. It is important to assess the manual controls and automated controls together to get a complete view of the control system. However, internal audit functions operating at Level 2 maturity may not have the IT expertise and the management support to include system and external parties in the scope.

- **Regulatory Compliance Universe**
  At this stage, internal audit typically includes high-level compliance questions in the discussion with management. The internal audit function will look for new regulations not yet identified by management and determine where management may not have integration, training, or other response plans. Or internal audit may evaluate regulatory agency efforts anticipated for the coming year and ask management how they would respond if an external agency were to audit compliance with a set of regulations. Much public information is available on regulatory expectation, and many organizations may have a separate function responsible for identifying and managing these expectations. If that is the case, many internal auditors at Level 2 maturity may choose to assume that that function of the organization will cover regulatory risks. However, deciding not to assess such risks is likely to cause the internal audit function to not meet professional standards. At a minimum, internal auditors should understand how the organization identifies, manages, and monitors regulatory expectations and determine a level of risk as a result of their efforts.

- **Corporate Policy Compliance Universe**
  At this stage, internal audit may not have developed a complete understanding of the policies and expectations internal to the organization. They are likely aware of the financial, compliance, and some general business policies, but they may not venture outside these in their risk assessment. However, it would be typical at this level to consider internal policy on par with regulatory expectations.

  Detailed examples, templates, and tools for performing risk assessments at this level can be found at https://www.anao.gov.au/sites/g/files/net616/f/BPG-PSFS-toolkit-item-05.pdf.

Value

At Level 2, the internal audit function begins to add advisory services to assurance efforts related to its core competencies in compliance and financial reporting. This includes the beginning of root cause analysis related to why financial, regulatory, policy, and process noncompliance findings exist. Internal audit starts to strengthen not only the expectations but also the operational components that meet these expectations. Internal audit may also get involved in helping the organization move the compliance and internal policy efforts up the capabilities maturity curve.

Level 3 – Defined

Population Covered

Exhibit 10-4 documents how Level 3 internal audit services and products improve on those that are present at Level 2. Much of this improvement is based on a maturing professional function with support from management. Internal audit complies with the IPPF standards by conducting risk assessments at least annually, strives to be fully "risk-based" in all efforts, and continues to build on its range of audit services. Risk gains new definition at this level. It becomes more associated with what management anticipates could go wrong. This means that internal auditors' perceptions of financial

materiality or regulatory compliance that likely defined inherent risk are no longer broad enough to align with management's view of what could go wrong. Reputation risks, environmental risks, operational risks, and a host of other management concerns enter the population of what internal audit should consider. Consequently, the population of areas covered by the risk assessment process must be redefined more formally and broadly, beyond compliance and efficient and effective procedures.

Two common ways to organize the risk assessment population is by creating an inventory of business processes or organizational entities, business lines, and/or functions. This organization is typically aligned with the process and accountability structure of the organization. However, some of the major challenges that management and internal audit have to deal with are inadequate horizontal integration of various processors and lack of integration of IT in business processes, lines, units, and/or functions. In other words, lack of coordination among the spaces between the units on the organizational charts, at various levels deep from the top, can pose great risks to the achievement of objectives.

Often, when internal audit identifies a finding, management will indicate that it is not their responsibility and it should not be included in their report. While the conditions noted in the finding impact their operations and objectives, management may not even know who is responsible for addressing the finding. Likewise, business and operations management often view gaps involving technology as issues that should be addressed by IT management instead of as business or customer issues they should manage. Ultimately, internal audit has to navigate behind the organizational structure to conduct root cause analyses to identify all the parties who are accountable for resolving the finding. It is not unusual for management to learn about the lack of accountabilities through internal audit's root cause analyses of findings identified. Due to these experiences and the growing importance of IT in improving competitiveness in business and effectiveness and efficiencies in operations, internal audit starts to conduct integrated IT and business risk assessments and integrated audit engagements of IT and business strategies, processes, and operations.

Exhibit 10-4
Level 3 Internal Audit Services, Products, and Value

Type of Services	Types of Products	Value of Internal Audit
• Advisory services are provided. • Risk assessments are performed at least annually. • Audits are planned and findings are identified by risk likelihood and impact.	• Risk assessments that include important operational areas • Risk-based audit reports with findings ranked • Advisory engagement results	• Internal audit uses risks to define priorities for management and the board. • Risk assessments and assurance and advisory engagement reports focus on risk priorities.

Audit Plan - Expected Products and Services

At Level 3, risk is the driver for prioritizing assurance and advisory engagements, audit findings, and any resource allocation decisions. Required and cyclical engagements that do not pose high risk

to the organization are minimized or eliminated to free up resources for topics with high risks. The risk assessment results are summarized in a risk assessment report that management validates and the CAE presents to the audit committee. Heat maps illustrating the most important risks and the alignment of audit plans with these important risks are commonly used. Additionally, reporting of assurance and advisory engagements may become delineated between those that are risk-based and those that are not. Finally, within engagements that are risk-based, planning steps may be expanded to conduct further risk assessment at the beginning to hone in on the most critical risks in the area to be assessed.

Procedures and Methods

At Level 3, the internal audit function uses a more formal approach to define the procedures and methods of conducting a risk assessment. When internal audit is focused on what management anticipates could go wrong, the internal audit function must account for many potentially unfamiliar parts of the organization. This requires a specific methodology for organizing risk information at the beginning. A few common ways to organize the risk assessment are by business processes or by organizational entity, business line, or function. The idea of risk populations (universes) to be assessed begins to be replaced by a more complex idea that risk can come from anywhere. This leads to a need for tagging risks by metadata that can organize similar risks into categories. This may be based on operational processes or the natural organizational chart categories.

- **Organizing Risks by Operational Process**
  The organizational chart and its important processes structured by management provide a natural starting point for risk assessment procedures. However, this may not provide sufficient detail. Organizations that do not have an adequate process classification framework can leverage the American Productivity & Quality Center's (APQC's) Process Classification Framework (PCF)®. This is the most widely used process framework worldwide. It creates a common language for organizations to communicate and define work processes. Organizations use it to support benchmarking, manage content, and to perform other important performance management activities.[1]

- **Organizational Entity/Business Line/Function Audit Universe**
  In addition to the traditional financial statement and reporting process universe and operational process universe noted above, another common way of organizing the risk universe is by location, business lines, business units, functions as identified on the organization chart, cost center report, or other similar document. Each unit (also known as an auditable entity in some literature) is then a potential area for risk assessment.

  The advantage of this approach is its completeness. Every unit in the organization will be considered during the risk assessment.

  There are, however, several disadvantages to this approach. For example:
  - The same risk factors are usually assessed for every business unit. There might be unique risks in a particular unit that are not included in these risk factors.

- Completeness of organizational units does not always equal completeness of risk consideration.
- The level of risk depends largely on the size of the business unit. For example, if human resources is defined as a business unit, the risk rating will be much higher than if its component parts (hiring, training, payroll, benefits) are defined as business units.
- Some risk events do not occur within a business unit but in the interface between two units.
- Some risks do not exist within the organization at all, but they can be found in the external environment or in related organizations like suppliers on which the organization depends.

- **Common Risk Assessment Methods Used by Internal Auditors**
  At Level 3 maturity, because the risk assessment universe or population of areas that should be covered has expanded to nearly the whole organization, it is important that the risk assessment methodology and processes are documented, communicated, and understood by all involved. Common components involved are discussed below.

The Methodology – Risk Factors

The internal audit function defines a set of risk factors that are applied to each area reviewed. Because some risk factors are more significant than others, they are weighted using a numerical scale like 1 - 5, and higher numbers indicate greater importance. Internal audit rates each risk factor for each area using a similar numerical scale. They multiply the two numbers to arrive at a risk rating.

For example, using a 5-point scale, internal audit gives a weighting of 4 to the risk factor "complexity of operations" and a weighting of 3 to the risk factor "volume of transactions." For a business unit, internal audit rates the complexity of operations 4 and the volume of transactions 2. The complexity of operations for this unit would then be risk rated 4 x 4 = 16 and the volume of transactions 3 x 2 = 6. If only these two factors were considered, the risk rating for this unit would be 16 + 6 = 22. In reality, there are typically many more risk factors, adding up to a total risk number for the organizational unit. Internal audit then ranks all of the entities from the highest to the lowest risk.

The risk factors are different for every organization, depending on the industry, regulatory environment, and so forth. For each risk factor, internal audit should develop the process, indicators, circumstances, or objective facts that guide how they are rated. Some commonly used factors are:

- Value of assets
- Changes in systems
- New products or services
- Control consciousness within the area

Once all the information has been assessed, the ratings assigned, and the area ranked, the results of the risk assessment should begin to show which areas have the most risk. This should always be discussed with management to validate that significant risks unique to their areas, risks of particular interest to key stakeholders, and risk mitigation practices are not overlooked.

Other, less formal, less quantitative techniques and discussions are better for identifying and assessing qualitative and emerging risks and are more likely to generate strategically focused risks that affect the entire organization, not just a single business unit, process, or program. Business units and business processes intersect and overlap. It is common to assess business processes that cross the entity first and then assess business units for remaining business unit risks.

Management Interviews and Surveys

Gathering risk information in this process becomes much more dependent on management's operating philosophy, perception, and awareness of mitigating controls. No longer can internal audit depend on identifying inherent risk and estimating residual risks. Management's insight is needed. They largely assume that risk assessment efforts equate to residual risk after taking into account their controls and mitigation efforts. Also, many risks are easily missed in a risk assessment based on data accumulation, but they are very much on the minds of senior management. Qualitative risks or "soft controls," for example, include concerns about the ethics or competence of a key middle manager or uncertainty about the prudence of a new strategic decision. Emerging risks come from changes like new products, services, or IT applications, new regulations or competitors, new people, including new management, or penetration of a new market.

The best way to identify and assess qualitative and emerging risks and understand existing control is by meeting with senior management who oversees the areas of the organization reviewed. It is typical to begin and end with executives who validate overall risk assessment assumptions.

Senior management interviews can be informal or structured, depending on what works best with each manager. To give such interviews structure, internal auditors typically have an agenda of topics to be covered, such as:

- Key issues in strategy, objectives, reporting, compliance, operations, and systems
- Emerging risks

The internal audit function can also use a risk assessment survey to get input from middle management. This can be brief and open ended (for example, "What are the major risks facing your area in the coming year"), or it might be a structured survey asking managers to assess a number of risk categories or risk-related statements. In a structured survey, managers might be asked to rate risk categories like environmental or financial reporting risks for their own areas on a 5-point scale from low to high risk. Or they might be asked to rate risk statements like "Senior management of my business unit demonstrates high ethical standards" or "The performance targets in my work unit are realistic and obtainable" on a 4-point scale from "strongly agree" to "strongly disagree."

If human resources or an outside vendor administers an entitywide survey asking employees to evaluate elements of the work environment (sometimes called a cultural or engagement survey), this can also be a valuable source of risk assessment information. If the work environment in an area is negative, there is an increased risk of errors, inefficiency, turnover, and many other problems.

Risk Assessment Workshops

Another way of engaging managers in the risk assessment is with facilitated workshops. A simple way to conduct a risk assessment workshop is to use the same content as that of a structured survey. Responses on the chosen scales can be gathered, tabulated, and presented in graph form using confidential voting technology and a data projector.

The more managers that are involved in the risk assessment, and the more fully they are involved, the better the results. Also, managers who have been involved in the development of the audit plan are more likely to understand how and why assurance projects are selected and be more supportive, especially when their own area is selected.

On the other hand, involving more managers takes more time—theirs and internal auditors'. Internal audit must decide on the best and most cost-effective level and method for engaging management in the risk assessment.

IT Risk Considerations

The organization's chief information officer (CIO) or security officer may perform an assessment of the risks within the IT environment. IT environments are prone to operational processes that naturally evaluate risks. Internal auditors should be aware of this practice within their organization and leverage known risk and issue information. There may also be more abundant evidence of existing risk mitigating (control) efforts to leverage. Once understood, internal auditors with IT competence should evaluate IT infrastructure and applications identified as high risk and any associated infrastructure. Keep in mind that some of these technologies may reside in a service provider's data centers, overseas, or in a virtualized environment. It is common for internal audit to outsource its IT risk assessment when the CAE feels no one in the internal audit function has the skill to conduct it with competence, or if there is a specific technical expectation from the board or audit committee.

Example Process

Step 1: Based on a review of background information, performance, and other available reports, determine the priority for reviewing processes. Define the number of processes to be reviewed based on expectations of the risk assessment product.

Step 2: Determine if the priority processes likely to be included are global or local. For global common processes and systems that have been implemented at all the locations, plan to conduct one process risk assessment. If the process is local, plan to conduct an individual assessment.

Step 3: Determine at what level to conduct the risk assessment. For example, risk assessments can drill down into more defined objectives:

Exhibit 10-5
Example for Objective 1.0: Develop Vision and Strategy

Significance to the Organization	How significant is "Developing vision and strategy" to the: • Organization? • Key stakeholders? • Shareholders and investors? • Regulators? • Stock analysts?	**H**	It is critical to get this right. Vision and strategies drive the organization. These are the core responsibilities of senior management of which the board has oversight responsibilities. Significant interest will impact investment decisions of shareholders and investors. Regulators focus on corporate governance, compliance structure, and performance. High level of interest; buy/sell opinions are highly dependent on the organization's vision and strategies.
Complexity of Business Environment	Does the organization operate in one or multiple industries? Does the organization operate in highly regulated industries? Does the organization have many alliances, partners, and joint ventures? Are these new relationships? Does the organization use outsourced services?	**H**	The organization operates in multiple industries. The organization operates in multiple highly regulated industries. The organization has many alliances, partners, and joint ventures. Some are in countries with a high corruption index. Many relationships have been in place for a long time. However, there are plans to acquire new technology partners. These new partners are critical to its strategic objectives. The organization uses many outsourced service providers; some are located in countries with a high corruption index. Some technology outsourced services are located in countries with immature technology infrastructure and regulations.
Complexity of Regulatory Environment	Have there been a lot of changes in rules and regulations?	M	There have been few changes to the regulatory environment; only a few new regulations on the horizon. However, regulators are focusing attention on compliance with data privacy and money laundering regulations.
Complexity of Strategic Planning Process	Are there a lot of data points to consolidate? Is the process logical, documented, and easy to follow? Do participants attend the planning session onsite or via remote access?	**M**	There are many data points from various business lines, locations, and functions. The process is logical, documented, and easy to follow. Participants receive materials to prepare for the meeting. The discussion session is facilitated by an experienced facilitating team. All participants attend the strategic planning and team-building sessions on site.
Level of Judgment Involved	Does developing the vision and strategy require: • Considerable judgment, estimates, and projections? • Specific experience, knowledge, skills, and expertise?	**H**	It requires significant judgment in making projections about the economy, the market, customer needs and wants, and technological advancement. It requires extensive business knowledge, experience, and functional expertise.

- The highest level – 1.0 Develop vision and strategy
- The next level – 1.1 Define the business concept and long-term vision, or
- The next level – 1.1.1 Assess the external environment

Step 4: Determine who should be interviewed or participate at the assessment workshop.

- Business leaders responsible for the process objectives
- SMEs
- IT leaders
- Second line of defense function

Step 5 (a.): Assess the process against key process risk factors in the interview or workshop with management. Consider the example in **exhibit 10-5**. Be open to management's insight into the factors most important to the area.

Step 5 (b.): Determine a score for each risk factor from Low to High and an overall assessment of the likelihood and impact of risks within the area reviewed.

Step 6: Consider the information received in creating the risk factors and interviewing management; develop a list of risks or things that could go wrong with the process or area.

Step 7: Evaluate this list of risks for the area and define the impact and likelihood of each risk. Consider the controls and risk mitigation practices management noted and implied in information gathered to this point. A quality risk assessment requires critical thinking, professional judgment, effective interviews with management, and analyses of operational effectiveness of control/risk mitigation practices.

Impact can be gathered from the risk factors discussed with management. What if the process can no longer operate? How severe is its impact to the organization?

Likelihood requires professional judgment to note the hazards inherent in the environment and controls in place to prevent the process from disruption. It is also a vote of confidence by the internal auditor in the skill of management and the overall strength of their process and operation. For example, if the manager has been in his or her role for 10 years and the process has evolved over that time into a well-aligned process with skilled employees and enabling technology, the capacity to withstand many risks may be high and should be accounted for by a low likelihood score.

Criteria should be established for scoring impact and likelihood of risks.

Risk Scoring Matrix

Once risk likelihood and risk impact have been defined, choosing a risk score is mostly based on math. Follow the guidance below:

- High Likelihood & High Impact = Critical Risk
- High Likelihood & Moderate Impact = High Risk
- Moderate Likelihood & High Impact = High Risk
- Low Likelihood & High Impact = Moderate Risk
- High Likelihood & Low Impact = Moderate Risk
- Moderate Likelihood & Moderate Impact = Moderate Risk
- Moderate Likelihood & Low Impact = Low Risk
- Low Likelihood & Moderate Impact = Low Risk
- Low Likelihood & Low Impact = Low Risk

Exhibit 10-6 depicts the risk scoring matrix.

Exhibit 10-6
Risk Scoring Matrix

Risk Scoring Matrix		Likelihood		
		Low	Moderate	High
Impact	High	M	H	C
	Moderate	L	M	H
	Low	L	L	M

Step 8: Take the list of risks and their residual ratings and determine which risks are the most important to the organization, given the importance of the process/area and the residual risk likelihood and impact. From this list, determine what additional efforts from the second line of defense or through external consulting may address the risk. Remaining risks are the basis for developing audit plans.

Value

At Level 3 maturity, the internal audit function begins to define risk from management's perspective of what could go wrong. This creates a much wider universe from which internal audit can seek to add value. However, it also requires a much more formal methodology for risk assessment that anticipates organizing risks within process or entity categories that can reflect the wider universe. The value in this effort is creating discussion with management about their important processes and areas. Through interviews, surveys, and workshops, the internal audit function can obtain details on management's priorities and concerns as well as the quality of internal controls. This risk and control knowledge and the new, wider universe both place internal audit in a position to better understand and respond to where within the organization it can add the most value. This gives rise to more advisory opportunities to be identified by the internal audit function and management.

Level 4 – Managed

Population Covered

Level 4 takes a dramatic shift in risk assessment perspective. In the prior maturity levels, internal audit largely relies on its own risk definitions and external guidance or standards to define risks within the organization. This is an outside-in or bottom-up perspective. At Level 4, the perspective changes with the realization that risk management is a management practice and responsibility. It comes from the top down. Consequently, internal audit's assessment of risk benefits from also starting at the top of the organization and cascading down. Internal audit's risk assessment mirrors the direction of strategic and operational planning to help it transform from a provider of assurance, advisory, and insight services into a trusted advisor. The organization at this level has defined risk management processes that internal audit can leverage. Level 4 is difficult to achieve if management is not ready to own the responsibilities and practices of risk management. At Level 4, the CAE has support from key stakeholders who actively steer the internal audit function on a growth path.

Within this environment, there is typically an ERM program or GRC technology leveraged by the second line of defense. The role of ERM and second line functions for risk is relatively clear. This allows CAEs to recognize that the whole population of risk is not theirs to assess independently. Others have responsibility, too. At Level 4, risk assessment has two unique characteristics:

- It implies the incorporation of risk assessment efforts by the second line of defense functions, including any ERM group, into their risk assessment process.
- It begins at the top of the organization and is focused on the most important risks. This includes risks that are part of ERM, risks to strategic priorities, and important operational programs, functions, systems, and procedures.

All parties are more comfortable applying a coordinated, top-down approach for risk management, governance, and controls using a common language. Internal audit efforts align with management efforts on achievement of objectives.

Audit Plan - Expected Products and Services

At Level 4, the internal audit risk assessment efforts are either considered a stand-alone product or part of a larger product for risk management purposes. The focus is primarily on creating an accurate picture of the most important risks to the organization. This focus, if executed well, can make the assessment a valuable product to risk management and second line of defense functions, in addition to providing context for assurance and advisory engagement planning. See **exhibit 10-7**.

It is likely that an assessment of the capabilities of the ERM program and second line of defense functions in mitigating risks is part of the risk assessment. This enables the CAE to assess the effectiveness of the compliance program rather than evaluating every compliance risk for its likelihood and

Exhibit 10-7
Level 4 Internal Audit Services, Products, and Value

Type of Services	Types of Products	Value of Internal Audit
• Evaluation of risk management expectations first in risk assessment and audit program development, focused on strengthening controls from the top down. • Internal audit provides overall assurance on GRC.	• Risk assessments are focused on top strategic and operational risks. • Assurance and advisory services are focused on expected risk management and control activities from the top down.	• Internal audit places risks and findings in terms of risk management structures and tools that management should be developing and using as part of daily operations. • Internal audit efforts are more in line with management efforts on objective achievement.

impact. With a little more effort, specific program assessments of ERM and second line of defense functions, noting their capacity to achieve their risk-related goals, could be part of the product that the risk assessment offers.

Procedures and Methods

Conducting a risk assessment at Level 4 typically reflects the Level 3 process with these notable differences:

- The starting point is defined more by the ERM, strategic, and important operational areas of the organization. It is top down. The risk assessment may not cover the whole organization. It may be limited to assessing the most important areas.
- The interview and workshop processes are typically focused more on management-defined risk factors in these important areas. More weight is placed on identifying priorities from management's perspective and their mitigation efforts for important risks.
- The definition of likelihood may change based on more detail from management on what is in place to mitigate important risks. For example, management typically understands their objectives very well. They typically respond to their responsibilities for objectives by setting up metrics and measures and oversight reporting. To them, this is their first indicator of something going wrong and the first layer of internal control. If their oversight is maturing and trends have proven positive over time, they may dismiss inherent risks that concern auditors because they have no warnings that concern them in their oversight system of controls.
- Time is spent evaluating the efforts and overall capability of ERM and second line of defense efforts. If their efforts are inadequate, it may increase a risk in an important area. It may also lead to an advisory engagement to help these functions better manage risks for which they are responsible. At this level, internal auditors would rarely identify a new regulation as a risk; instead, they would comment on the compliance function's capacity to ensure new regulations are accommodated by the overall organization.

Organizations practicing ERM usually develop a set of risk categories and subcategories. The risk management function and/or business managers then identify and assess risk events that might occur within these categories. If an organization has developed such categories, the internal audit function may use them as its risk universe. However, the operational perspectives of business units and parent business processes defined in Level 3 may continue to serve well.

A disadvantage to this approach is that risks managed by second line of defense functions with potential high impact may not make the list as they are not directly connected to the top-down approach. Therefore, CAEs need to understand how capable risk management practices and second line of defense efforts are at mitigating all of these types of risks. An internal audit function transitioning to Level 4 may put assessments of second line of defense functions in their audit plans.

Relevant Definitions

The simple world of auditor-defined risk assessment definitions (in Level 3) begins to become more complicated at Levels 4 and 5. There is more to consider when approaching the risk assessment from the top down and relying on management to help define the current control structure. The definition of risk remains "the effect of uncertainty on objectives." However, the use of inherent and residual risk is impacted. For example, management may see a particular department as critical to the achievement of specific objectives. As such, management may have invested a lot of time and attention setting up oversight for that department and alignment of its people's skills with efficient processes and enabling technology.

From management's internal operational perspective, they have responded effectively to the vast majority of potential risks that may impact the area by creating robust oversight and resilient operations. An internal auditor trying to define an inherent internal risk that may impact department success may be perceived as wasting time, or a challenge to management's complex system of management controls in place. Rather, management at Level 4 is looking for internal audit to contribute its perspective of risk to the existing system of management controls. In short, the definitions of inherent and residual risk are less valuable as internal audit becomes a partner in risk assessment with management, leveraging their expertise in setting up resilient operations capable of achieving their objectives.

Value

The internal audit function has opportunities to create tremendous value at Level 4. However, the risk to the CAE and the internal audit function also increases. Whenever there is reliance on external factors (ERM and second line of defense functions), there is the possibility that expectations will not be met. Similarly, if internal auditors conduct a top-down risk assessment, they will not be able to go everywhere or get into great detail. This means they must rely on existing risk management and other second line of defense efforts and focus primarily on where the most value can be added. In a true Level 4 environment, the CAE is likely sharing risk data with risk management and second line

functions for the benefit of shared objectives in addressing risks. This creates options for internal audit to create a variety of risk reports and risk management assessment products in addition to an audit plan focused highly on areas where internal audit can add the most value. In this collaborative environment, internal audit is the only function with an organizationwide charter to help overall risk management efforts develop efficiency and effectiveness in their respective roles.

Level 5 – Optimizing

Population Covered

As ERM matures within the organization, two things become apparent:

- Risk management is a subset or sub-effort of objective management, meaning that risk is only a risk if it prevents the achievement of the objective at risk. ERM becomes a formal effort for managing the organization's most important objectives for success, implying integration of risk management with day-to-day management practices.
- If internal auditors continue to parallel risk management efforts within the organization, they must acknowledge that all risks must be placed in context of the business objectives at risk.

This conclusion leads to the realization that the natural context for the population covered by the internal audit function's risk assessment is the strategic and business objectives at risk. This perspective puts the CAE in lockstep with management's efforts, but it also requires an expanded look at what is viewed as risk mitigation. However, there remains a need to ensure that reputation, hazard, and other second line of defense risks are effectively evaluated and addressed. See **exhibit 10-8**.

Exhibit 10-8
Level 5 Internal Audit Services, Products, and Value

Type of Services	Types of Products	Value of Internal Audit
• Places risk management-based efforts in the context of the specific business objectives at risk by building on the prior levels below. • Internal audit is recognized as a key agent of change.	• Risk assessments are integrated with risk management efforts. • Assurance and advisory engagements are focused on helping management achieve objectives through improvement of risk management in both the first and second lines of defense.	• Internal audit takes ownership for communicating risk in terms management understands as it strives to achieve business objectives. • Business objective achievement is considered in all risk assessment and assurance and advisory engagements. • Internal audit recommendations and advice improve the organization's GRC.

Audit Plan - Expected Products and Services

Deliverables at Level 5 are similar to those at Level 4 with one important difference—they are cast in the context of the business or strategic initiatives at risk and include value preservation as well as value creation objectives. This is important for two reasons. It shows that CAEs have the capacity to

correctly value and understand the importance of the business objectives and also the capacity to credit management for activities that increase the likelihood of achievement. This expands the definition of internal control to parallel the practice of management to include things such as:

- Oversight processes for objectives = Management Controls
- Alignment of people, process, and technology to strengthen operations = Operational Controls, which can mature over time and generally reduce a variety of risks as they become stronger

It also includes consideration of a full range of risk mitigation practices such as transferring, avoiding, accepting, insuring, sharing, and even pursuing risks, which are part of everyday management decision making.

With more direct connection between risk and objectives, the opportunities identified in Level 4 to collaborate, share, create value, and improve results continue to expand. Conceptually at this level, GRC technology is enabling risk assessment performed by the second line of defense and internal audit for the benefit of management.

Procedures and Methods

Traditional Level 3 and 4 methods are continued with the added expectation that the starting point is the strategic and business objectives.

What are strategic and business objectives?

- Strategic objectives are periodic initiatives and projects that are the result of strategic planning. They are nearly always documented in writing.
- Business objectives are perpetual operational expectations typically closely aligned to the purpose statement of why a function or process exists. They are frequently implied rather than documented in writing.

Strategic objectives are typically transformational efforts to change something to achieve a desired outcome, destination, or mission. They are typically broken into initiatives assigned to relevant parts of the organization. They are different from operational or business objectives. Strategic objectives have a start and stop. Operational objectives resemble the purpose statement of why one component of the operation exists. Operational objectives clearly cascade down the chain of command to smaller, more detailed objectives until they reach transactions that have to be completed. Alignment of detailed objectives with overall business unit or departmental purposes is a natural expectation. However, human intervention and communication can be enablers and can also create breakdowns.

Aligning Management Effort and Risk Mitigation

Because Level 5 is focused on achievement of objectives, the risk conversation with management is about expected controls and risk mitigation practices around strategic and business objectives. These expectations include governance of the objectives, maturing alignment of operations (people, process, and technology), controls, and a full range of risk mitigation practices to accomplish them. Management should be part of assessing the existing state of residual risks in objective governance, operational alignment, controls, and other risk mitigation practices. Level 5 is where CAEs show strength and ability in understanding strategic and business objectives, interpreting the current state of objective GRC, identifying the actions needed to close any gaps, and communicating with management in this context.

It is also important to incorporate additional risks that become meaningful as risk assessment aligns with strategic and operational objectives. For example, there are a variety of risks associated with breakdowns in objective accountability and communication. More specifically, if a vice president breaks an objective into three sub-objectives and assigns them to multiple staff members, but one staff member does not understand the assignment, then the chance that the objective fails overall increases. This implies a cascading objective structure to strategic and operational objectives that a CAE must also understand.

What Is the Upside of Risk?

Effective risk management is about managing the downside risks and also the upside opportunities. Traditionally, internal audit functions are primarily involved in providing assurance for value preservation objectives (such as compliance with regulations, reliable financial statements), which if not achieved would erode shareholder value. At Level 5, internal audit starts to provide assurance for value creation objectives (such as increase market share by X percent, develop a new market for artificial intelligence products), which will create shareholder value and are key to the long-term success of the organization. For these engagements, in addition to applying expertise in governance, risk management, risk mitigation, and controls, internal audit will expand its expertise to provide assurance on the effectiveness of the decision-making process. The scope will focus on what must go right in the decision-making process to enable success: setting sound criteria, identifying the right findings, determining specifications for an effective decision, minimizing decision bias, turning decision into action, evaluating outcomes, and sharing and implementing lessons learned. As CAEs operate in the context of strategic and operational objectives and appropriately value risk likelihoods, they become true partners in organizational success.

Value

Level 5 provides a clear link to how the CAE becomes an effective business partner with management while maintaining independence, objectivity, and professionalism.

- Internal audit takes initiative to communicate risk in terms management understands as it strives to achieve business objectives.
- Achievement of value preservation and creation relative to business objectives is considered in all risk assessment and assurance and advisory engagements.
- Internal audit recommendations and advice improve the organization's GRC.

This level is theoretical for most internal audit functions, because it requires extensive collaboration and readiness on the part of management, risk management, and other invested stakeholders. However, this is an important ideal that, if achieved, allows the internal audit function to add substantial value.

Level 5 is the optimized state where the organization's management, risk management, governance and controls, and internal audit function's capabilities are at the top of the capabilities maturity curve. Reaching the top requires ambition, willpower, initiative, collaboration, and drive by all parties. An appropriately resourced, competent, professional internal audit function is uniquely qualified to lead this charge. Internal audit will earn the trust and confidence of management by advocating its own value, delivering on what matters to the board and management, and continuously improving its capabilities to add value and raise the performance bar for the organization. Advocacy is essential to let the board and management know what internal audit is capable of delivering at the optimized level, how those capabilities can help the organization succeed, and the support they need.

Annual Audit Plan Development - General Approach

As previously discussed, CAEs are responsible for leveraging information about stakeholder expectations and organizational risks into a periodic (no less than annual) plan. This plan is reviewed and approved by the audit committee.

The output from risk assessment activities can serve many purposes, one of which is as an input to a separate audit planning effort to allocate scarce resources. CAEs typically designate an experienced manager to lead audit plan development and provide the template, instructions, timeline, and reporting format.

Audit Plan Development Process

1. **Recap of Risk Assessment Activities**
   During risk assessment, based on the iterative process of obtaining input, analyzing information, identifying topics, and confirming information and assessment results, the internal audit leadership ranks the audit topics within the universe in terms of critical, high, medium, and low risk. CAEs are responsible for coordinating activities with other assurance providers to ensure appropriate coverage and minimize duplication of efforts. A good way to coordinate risk coverage is to document assurance work that will be performed by internal audit and second line of defense functions and risk mitigation work that will be performed by management for critical risk/high-

risk audit topics. Depending on the maturity levels of internal audit and the organization, these audit topics can be accounts, policies, regulations, units, processes, systems, objectives, or something else.

2. **Develop the Audit Plan**

The audit plan development team includes a list of projects in the audit plan that will be conducted over the four quarters, including critical risk/high-risk audit topics identified during risk assessment, regulatory expectations, governance directives, and significant requests from key stakeholders and management. In general, assurance engagements take priority over advisory engagements. The team allocates audit hours based on experience and professional judgment.

Most internal audit functions have a standard process and template for developing the audit plan. **Exhibit 10-9** shows an example of typical categories in an audit plan. Each category is supported by details from the risk assessment report.

The categories and recaps in exhibit 10-9 answer or prompt questions that might be of interest to CAEs, the board, and senior management. For example:

- Does internal audit have sufficient resources to address all of the critical risks and high-risk topics on the plan? If not, what is the plan to address the shortfall?
- Is the percentage of audit resources allocated to assurance and advisory engagements balanced? Advisory engagement objectives and scopes are set by management instead of by the internal audit function. While many internal/external groups can conduct advisory engagements, no other group within the organization has the mandate to provide independent, objective assurance services. Should some advisory engagements be handled by the first and second lines of defense or external parties instead?
- What is the percentage of hours devoted to audit and non-audit activities? This could be a measure of efficiency and productivity.
- What is the percentage of hours allocated to risk-based engagements compared to requested engagements? A high percentage of hours allocated to requested topics could be an indication of an ineffective risk assessment process. Why are topics important to management and key stakeholders not reflected in the risk assessment results?
- Is the reserve sufficient to address unplanned activities? Most internal audit functions allocate 15 to 20 percent of planned audit hours for unplanned engagements that may arise during the year. This percentage may increase as internal audit moves toward Level 5 and becomes a trusted advisor.
- Are the available audit hours realistic considering turnover and lead time for recruiting?
- Have arrangements been made to facilitate selecting, hiring, and on-boarding co-sourced resources?
- Have arrangements been made to facilitate selecting and on-boarding guest auditors?

Exhibit 10-9 illustrates audit engagement categories and allows for budgeting hours to each engagement.

Exhibit 10-9
Audit Plan Recap – Audit Hours by Types of Engagements and Sources

Priorities may vary subject to the organization's and internal audit's operating philosophy.	**Sources**	**Budgeted Number of Hours**	**% of Total Hours**
Recap by Types of Engagements – Detailed			
a. Regulatory requirements (regulators specify assurance requirements and internal audit as the assurance provider)	Regulators		
b. Financial statement assistance(based on agreed-upon procedures)	External Auditor		
c. Policy compliance audits (specified by key stakeholders)	Governance Requirement		
d. Critical investigation	Risk Assessment		
e. Assurance engagements – high-risk audit topics (for example, critical risks/objectives/units/functions/processes/systems/operations, critical risks that impact multiple objectives/units/functions/processes/systems/operations)	Risk Assessment		
f. Assurance engagement – board request	Board		
g. Assurance engagement – senior management request	Senior Management		
h. Assurance engagement – management request	Management		
i. Advisory engagement - high-risk audit topics (see e.)	Risk Assessment		
j. Advisory engagement – board request	Board		
k. Advisory engagement – senior management request	Senior Management		
l. Advisory engagement – management request	Management		
m. Follow-up on status of action plans	Risk Assessment		
n. Participation on committees/taskforces	Management Request		
o. Reserve for investigation	Unplanned		
p. Reserve for assurance engagements	Unplanned		
q. Reserve for advisory engagements	Unplanned		
r. Professional development	Internal Audit		
s. Operation and administration	Internal Audit		
Total Hours Needed		XX	
Less: Total Hours Available		YY	
Excess Hours/Shortfall		ZZ	
Recap by Types of Engagements			
Regulatory requirements (a)			
Financial statement assistance (b)			
Policy compliance audits (c)			
Critical investigation (d, o)			
Assurance engagements (e, f, g, h, p)			
Advisory engagements (i, j, k, l, q)			
Follow-up on status of action plans (m)			
Participation on committees/taskforces (n)			
Professional development (r)			
Operation and administration (s)			
Total Hours Needed			100%

Exhibit 10-9 (continued)

Recap by Sources			
Regulators (a)			
External auditor (b)			
Governance (c)			
Risk assessment (d, e, i, m)			
Board (f, j)			
Senior management (g, k)			
Management (h, l, n)			
Unplanned (o, p, q)			
Internal audit (r, s)			
Total			100%

3. Reconcile Hours Available to Critical Risk/High-Risk Audit Topics

Internal auditors perform various non-audit (support, administrative, and developmental) activities. Internal audit typically allocates 1,500 - 1,800 hours per auditor to audit activities (2,080 available hours minus holidays, vacations, sick days, training, administration, and meetings). Internal audit support staff will allocate most of their time to non-audit activities.

If available hours exceed hours needed, the extra hours can be added to the reserve for unplanned engagements. If hours needed exceed available hours, internal audit can close the gap in a variety of ways:

- Consider moving some audits to the following year.
- Change the audit approach.
- Request assistance from first or second line of defense functions.
- Rely on work performed by other assurance service providers.
- Use co-sourcing if budget permits.

If the internal audit function plans to rely on the work of other assurance or consulting service providers, the CAE remains accountable for the resulting assurance and advisory services. A consistent process should be established to monitor the work performed to ensure that the internal audit function can continue to place reliance on the function performing the services. The internal audit function also must determine whether that function has the independence, objectivity, and competence needed to provide assurance. If any of these factors are unknown, a review of that function may be required. The CAE should also have a clear understanding of the scope, objectives, and results of the work performed by other service providers.

Some internal audit functions share the risk coverage with the board that is available at various staffing levels so that key stakeholders can make prudent funding decisions. If the approved

staff size/budget could prevent internal audit from providing what the CAE considers adequate assurance, the CAE has an obligation to inform senior management and the board. If the audit committee approves the limitation, the decision should be documented in the audit plan.

4. **Critical Risk/High-Risk Topics and Requests Not Included in the Audit Plan**
   Key stakeholders are particularly interested in knowing if there are any critical risk/high-risk topics or requests that are not included in the audit plan, the reasons they are excluded, and internal audit's risk mitigation strategies. While there may be good reasons for the decision, this will likely be a discussion topic at the audit committee meeting.

5. **Five-Year Rolling Audit Plan**
   Most internal audit functions develop an annual audit plan. However, given the dynamic business environment, many internal audit functions are moving to an ongoing risk assessment process and prepare a quarterly rolling audit plan. As stakeholders are increasingly more interested in looking to the future, internal audit should consider presenting a more forward-looking plan covering a broader horizon, such as one that focuses on:

   Y-2 Y-1 Current Year Y+1 Y+2

   The plan should provide a highlight of areas covered in the past, key issues identified, corrective actions implemented, and the effectiveness of the corrective actions.

6. **Review and Approval**
   The results of the risk assessment effort, including the resulting audit plan, should be reviewed and agreed upon by the entire internal audit leadership team.

   After the audit plan is finalized, management may ask the CAE not to perform certain engagements or limit the scope of some audits. Such requests may come during planning, during the year, or even during an engagement. These requests may be for good reasons. For example, in an area that has known problems that are being addressed, an audit engagement would hinder progress. In such cases, the CAE should obtain sufficient information to concur either that an engagement should not be performed at this time or that the scope should be limited. The canceled and postponed engagements or scope limitations should be approved by the audit committee.

7. **Audit Committee Approves the Audit Plan**
   The CAE presents the annual audit plan to the audit committee for review and approval.

8. **Quarterly Audit Plan Update**
   The business environment is dynamic. The internal audit function needs to monitor changes and update its audit plan. Audit plan status, additions, deletions, and deferrals and reasons for these changes, including periodic risk assessment updates, should be reported quarterly to the CAE and audit committee for approval. Projects arising during the year may be approved retro-

actively if they are small or need to be started immediately. As the year progresses and specific engagements become known, these hours should be reallocated from reserve hours to the applicable categories.

The products and services that are part of the internal audit function strategic plans will drive the type of risk assessment activities that are undertaken by the internal audit function. The specific process of the risk assessment requires an early determination of the scope or choice of what populations (universes) of risk will be assessed. Exhibit 10-1 illustrates how the assessment of risk is impacted by the value that the internal audit function seeks to deliver. If the desired value is a Level 1 or 2, then the process focuses on narrow universes of risk. If the intent is that the process integrates with risk management efforts and adds a higher level of value, then it must come from the top down and the process becomes much more dependent on the natural structure of the business objectives at risk. This has cascading implications in how widely the products of the risk assessment will be used and how they will approach audit engagement planning and internal control assessing efforts.

Additional IIA Resources

Urton L. Anderson et al., *Internal Auditing: Assurance & Advisory Services*, Fourth Edition (Lake Mary, FL: Internal Audit Foundation, 2017). See in particular chapter 4, "Risk Management," and chapter 15, "The Consulting Engagement."

IIA Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000 (Lake Mary, FL: The Institute of Internal Auditors, 2010).

IIA Practice Guide, Coordinating Risk Management and Assurance (Lake Mary, FL: The Institute of Internal Auditors, 2012).