THE IIA's CIA LEARNING SYSTEM®

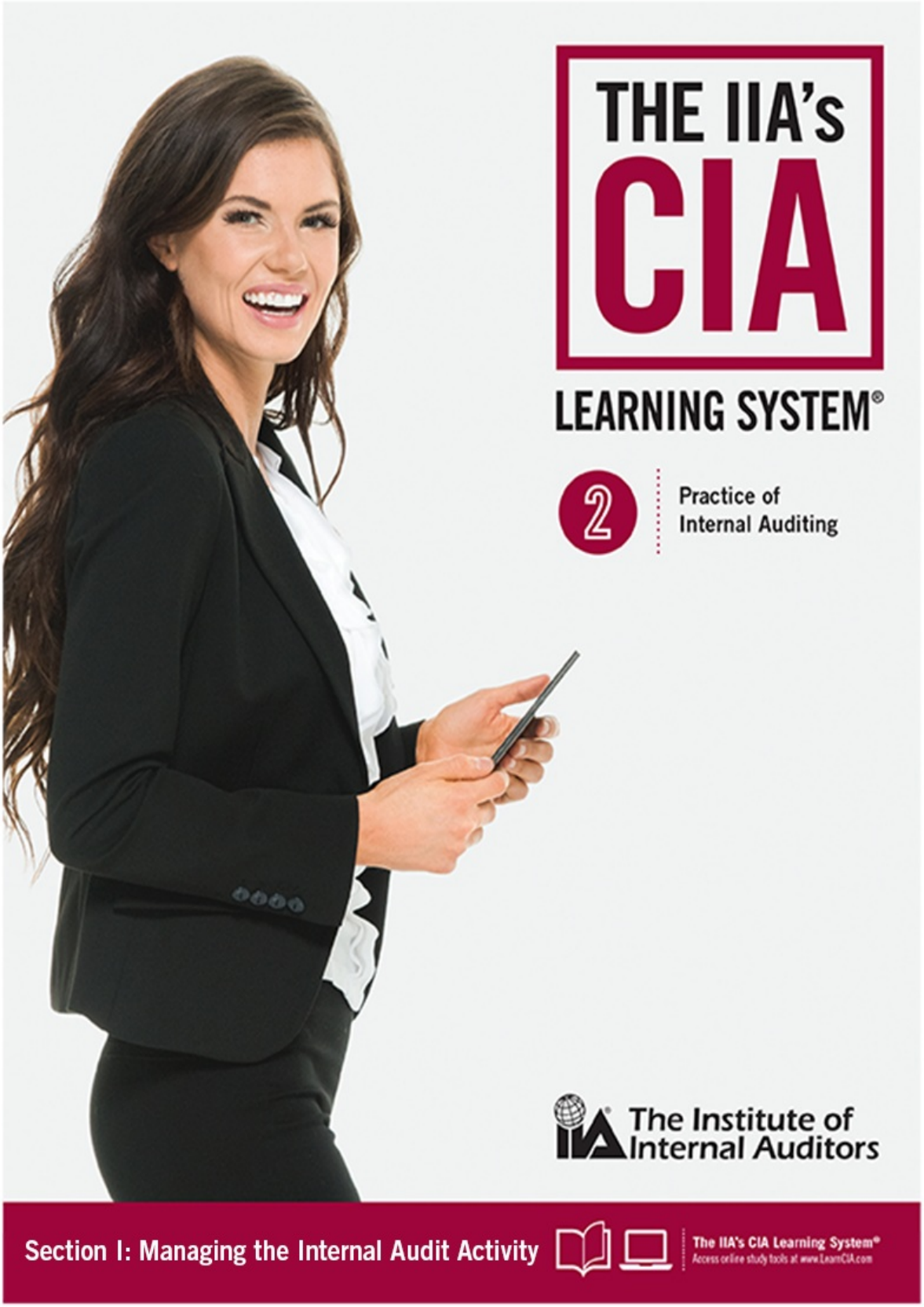
2

Practice of Internal Auditing

The Institute of Internal Auditors

Section I: Managing the Internal Audit Activity

The IIA's CIA Learning System®
Access online study tools at www.LearnCIA.com


THE IIA's
CIA
LEARNING SYSTEM®
2
Practice of
Internal Auditing
The Institute of
Internal Auditors
Section I: Managing the Internal Audit Activity
The IIA's CIA Learning System®
Access online study tools at www.LearnCIA.com

Part 2: Practice of Internal Auditing

Welcome to Part 2 of The IIA's CIA Learning System®.

The self-study text for the learning system includes the content addressed in The IIA's CIA syllabus. (You can download the syllabus from the online Resource Center or from The IIA's website.) However, in some cases, the content has been reorganized to facilitate instruction and understanding. Refer to the Table of Contents for an outline of the content.

To get the most out of the course materials, complete the course in this order:

1. Begin by accessing the course at www.learncia.com.
2. Read the overview and return to the menu. Select Part 2 from the menu.
3. Complete the pre-test and view the report to help focus your study efforts.
4. Read each section and follow the Next Steps directions included at the end of the section.
5. Complete Part 2 as outlined in the online overview.

Note that Part 2 of the CIA exam will consist of 100 multiple-choice questions and test takers are given 120 minutes to complete this portion of the exam. You can go to https://na.theiia.org/certification/CIA-Certification/Pages/CIA-Certification.aspx to register for the exam separately.

Study Support

The IIA's CIA Learning System includes online tools to support your study. These tools may be accessed from the menu at any time.

- Glossary—Refer to the glossary for definitions of terms used in all three parts of The IIA's CIA syllabus.
- Reports—Refer to the reports to review your most recent test scores and progress through the learning system.
- Resource Center—Refer to the Resource Center to access information

about The IIA's International Professional Practices Framework, updates, test-taking tips, printable flashcards, related links, and reference material and to provide feedback to The IIA regarding the learning system.

The IIA's CIA Learning System®

The IIA's CIA Learning System® is based on the Certified Internal Auditor® (CIA®) syllabus developed by The IIA. However, program developers do not have access to the exam questions. Therefore, while the learning system is a good tool for study, reading the text does not guarantee a passing score on the CIA exam.

Every effort has been made to ensure that all information is current and correct. However, laws and regulations change, and these materials are not intended to offer legal or professional services or advice. This material is consistent with the revised *Standards* of the International Professional Practices Framework (IPPF) introduced in July 2015, effective in 2017.

Copyright

Acknowledgments

The IIA would like to thank the following dedicated subject matter experts who shared their time, experience, and insights during the development and subsequent updates of The IIA's CIA Learning System.

Pat Adams, CIA
Terry Bingham, CIA, CISA, CCSA
Raven Catlin, CIA, CPA, CFSA
Patrick Copeland, CIA, CRMA, CISA, CPA
Don Espersen, CIA
Michael J. Fucilli, CIA, QIAL, CRMA, CGAP, CFE
Al Marcella, PhD, CISA, CCSA
Markus Mayer, CIA
Vicki A. McIntyre, CIA, CFSA, CRMA, CPA
Gary Mitten, CIA, CCSA
Lynn Morley, CIA, CGA
Lyndon Remias, CIA

James D. Hallinan, CIA, CPA, CFSA, CBA

Larry Hubbard, CIA, CCSA, CPA, CISA

Jim Key, CIA

David Mancina, CIA, CPA

James Roth, PhD, CIA, CCSA

Brad Schwieger, CPA, DBA

Doug Ziegenfuss, PhD, CIA, CCSA, CPA, CMA, CFE, CISA, CGFM, CR.FA., CITP

Part 2 Overview

Part 2 of The IIA's CIA Learning System focuses on the auditor's abilities related to the Performance Standards (series 2000, 2200, 2300, 2400, 2500, and 2600). Performance Standards describe the nature of internal auditing and provide quality criteria against which the performance of internal auditing services can be measured. Note that Standard 2100 ("Nature of Work") is addressed in Part 1, Section V, "Governance, Risk Management, and Control."

Part 2 is made up of four sections:

I. **Managing the Internal Audit Activity.** The chief audit executive (CAE) must effectively manage the internal audit activity to ensure that it adds value to the organization (Standard 2000).

II. **Planning the Engagement.** 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 2200).

III. **Performing the Engagement.** Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives (Standard 2300).

IV. **Communicating Engagement Results and Monitoring Progress.** Internal auditors must communicate the results of engagements (Standard 2400). The CAE must establish and maintain a system to monitor the disposition of results communicated to management (Standard 2500), discuss any remaining unacceptable risk levels with senior management, and communicate any unresolved issues related to unacceptable risk levels to the board (Standard 2600).

Those managing engagements must ensure that engagements are conducted in a professional manner—from planning through supervision and communication to monitoring engagement outcomes—and with a continuous

awareness of risk.

Section I: Managing the Internal Audit Activity

This section is designed to help you:

- Describe policies and procedures of internal auditing operations.
- Interpret administrative activities of internal audit.
- Identify sources of potential engagements.
- Identify a risk management framework to assess risks.
- Prioritize audit engagements based on the results of a risk assessment.
- Interpret the types of assurance engagements.
- Interpret the types of consulting engagements.
- Describe coordination of internal audit efforts with external auditors, regulatory oversight bodies, and other internal assurance functions.
- Describe potential reliance on other assurance providers.
- Describe how the chief audit executive (CAE) communicates the annual audit plan and its results to senior management and the board.
- Identify how the CAE seeks board approval of the annual audit plan.
- Identify significant risk exposures and control and governance issues for the CAE to report to the board.
- Recognize that the CAE reports on the overall effectiveness of the organization's internal control and risk management processes to senior management and the board.
- Identify internal audit key performance indicators that the CAE communicates to senior management and the board periodically.

The Certified Internal Auditor (CIA) exam questions based on content from this section make up approximately 20% of the total number of questions for Part 2. Most of the topics are covered at the "B—Basic" level, meaning that you are responsible for comprehension and recall of information. (Note that this refers to the difficulty level of questions you may see on the exam; the content in these areas may still be complex.) A few topics are covered at the "P—Proficient" level, meaning that you are responsible not only for comprehension and recall but also for higher-level mastery, including application, analysis, synthesis, and evaluation.

Section Introduction

Performance Standard 2000, "Managing the Internal Audit Activity," states that the chief audit executive must effectively manage the internal audit

activity to ensure that it adds value to the organization. Interpretation tells us that *"the internal audit activity adds value to the organization and its stakeholders when it considers strategies, objectives, and risks; strives to offer ways to enhance governance, risk management and control processes; and objectively provides relevant assurance."*

This section focuses on the criteria for effectively managing the internal audit function at both strategic and operational levels.

From a strategic perspective, the CAE must ensure the establishment of a risk-based plan for managing the function's activity. This will require that internal audit leaders:

- Manage changes needed to implement and support the organization's strategy.
- Establish relationships throughout the organization to foster communication and cooperation.
- Assess and promote an ethical climate and good governance.
- Develop an appropriate system to measure the efficiency and effectiveness of the internal audit function and report performance to senior management and the board.
- Manage interactions with external auditors, regulatory bodies, and other internal assurance functions.

From an operational perspective, the CAE must ensure that the function is managed in a professional manner and that:

- Policies and procedures are in place to plan, organize, direct, and monitor internal audit operations.
- The function is administered to make the best use of internal audit resources.
- The function is staffed appropriately for its tasks.
- A risk-based audit plan is used to identify potential engagements and

prioritize engagements.

- Management is informed about the effectiveness of the organization’s internal control and risk management frameworks.
- The quality of internal audit work is monitored, assessed, and reported to management, and a quality assurance and improvement program is in place.

Chapter 1: Internal Audit Operations

Chapter Introduction

Strategically managed organizations recognize the need to operate not just as organizationally connected functions but as fully integrated, often interdependent parts of a whole. Functional and operational strategies must be aligned with the organizational strategy. The organization's risk management approach must be enterprise-wide.

The internal audit activity plays a critical role in ensuring that the organization's resources are being used efficiently and effectively toward accomplishing organizational objectives and that the organization's internal control framework is adequate for controlling the variety of internal and external risks to which the organization is vulnerable.

The topics in this chapter focus on the role of internal audit at an operational level, including how the CAE ensures that the activity can fulfill its role and responsibilities. This includes:

- Formulating policies and procedures that support the activity's independence, objectivity, proficiency, and due professional care.
- Directing administrative functions that allow the activity to operate efficiently and effectively.

Topic A: Policies and Procedures for Internal Audit Operations (Level B)

Policies and Procedures

Engagement management is the process of planning, organizing, directing, and monitoring an internal audit activity's resources (people, equipment and technology, time, and money) so that objectives can be met within the defined scope, time, and cost constraints of assurance and consulting engagements.

- **Planning,** which is at a strategic level, includes activities such as developing a risk-based audit plan and reviewing staff competency needs and planning for hiring and development. The audit plan is discussed in the next chapter.
- **Organizing,** which is at an operational level, involves designing structures and processes aimed at achieving activity objectives and overall goals of efficiency and effectiveness. This may include assigning auditors to specific engagements on the basis of their experience with similar engagements and their business experience. It may also involve allocating time for engagement activities like planning, developing and implementing the audit program, conducting fieldwork, and writing reports.
- **Directing** includes the many tasks in leading internal audit. Communication and coordination must be maintained within the organization, with the board, and with external bodies, as applicable. New staff members must be interviewed and hired or contracted with. Performance management systems should be implemented.
- **Monitoring** involves activities such as ensuring that budgets are monitored and assessed; that the audit committee, senior management, and engagement clients are receiving value-added services; and that the activity is meeting its strategic objectives, including the requirements of the audit plan.

Audit policies and procedures help the chief audit executive in carrying out these management activities. Establishing policies and procedures might entail developing processes to support engagement work, such as engagement initiation/transition meetings and report review processes, processes for qualifying and contracting with external service providers, structures for communicating different types of activity information, monitoring processes aimed at maintaining quality and budget adherence (e.g., dashboards), and channels for gathering this data.

Internal audit policies typically include guidance on:

- The overall purpose and responsibilities of the internal audit activity.
- Adherence to the mandatory guidance of the International Professional Practices Framework (IPPF).
- Independence and objectivity.
- Ethics.
- Protecting confidential information.
- Record retention.
- Staff training.
- Establishing a quality assurance and improvement program.

Internal audit procedures typically include guidance on:

- Preparing a risk-based audit plan.
- Planning an audit and preparing the engagement work program.
- Performing audit engagements.
- Documenting audit engagements.
- Communicating results/reporting.
- Monitoring and follow-up processes.

Interpretation of Standard 2040 stipulates that *"the form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work."*

Audit Manuals

The audit manual provides a guide to existing and new members of the internal auditing activity about the activity's objectives, the way these objectives will be accomplished (the policies and procedures), and the use of internal audit standards. The documents may include methods and tools for training and may require internal auditors to provide acknowledgment by signature that they have read and understood the policies and procedures.

The CAE is responsible for ensuring that an audit manual is created and maintained, that it is distributed throughout the internal auditing activity, and that the policies and procedures contained in the audit manual are consistently and continually enforced.

The purpose of the audit manual is, in general, to:

- Provide guidance to activity members that will support adherence to the profession's code of ethics and professional standards.
- Define a high level of performance expectations for staff that will enable the activity to fulfill its role in supporting the organization's governance, risk management, and control objectives and to fulfill the activity's own strategic objectives.
- Focus activity members on key objectives and values. For example, an activity may focus on assuring controls or adding value to the organization by identifying opportunities for greater efficiency and quality—or it may balance both roles.
- Coordinate roles and responsibilities within the activity and in relation to other internal and external bodies.
- Codify critical processes, such as the steps involved in performing different types of engagements, and policies, such as protection of

confidential information and communication and monitoring of engagement results.

- Provide the basis on which to evaluate the internal auditing activity's performance.

As suggested in Implementation Guide 2040, audit manuals can vary in content and format. Exhibit I-1 lists possible topic headings for audit manuals.

Exhibit I-1: Sample Audit Manual Content

Topic	Description
Internal audit charter	Establishes the purpose, scope of authority, and responsibilities of the CAE and the internal audit activity, including professional standards, responsibilities, and ethics/code of conduct
Internal audit organization	Reporting structures, services provided by internal audit
Internal audit strategic plan	Process and schedule for developing strategic goals and objectives
Annual audit plan	Process for developing and modifying the annual audit plan, from identifying audit universe through risk analysis and allocation of resources, including risk management tools to be used
Personnel	Roles and responsibilities, training and career development, certification opportunities, continuing education requirements, and performance management system
Communication	Guidelines for communicating with internal clients and external bodies; handling of confidential information
Audit engagement procedures	Procedures to be followed, from planning through reporting; requirements regarding workpapers; report template
Quality assurance and improvement program (QAIP)	Description of QAIP requirements; evaluation processes
Administration	Policies regarding tracking of time, documentation, and document retention

Implementation Guide 2040 explains that in small internal audit activities, close and daily supervision may take the place of formal internal audit operations manuals. However, in large audit activities, more formal and comprehensive policies and procedures may be essential to guide the internal audit staff in the execution of the internal audit plan.

Audit Activity Organizational Charts

It is important that internal auditors understand the roles and responsibilities of each layer of the internal audit organization's reporting structures (the second item listed in Exhibit I-1). Exhibit I-2 shows an example of an organizational chart for an internal audit activity. Note that CAEs have significant flexibility in determining job titles and the organizational structure of the internal audit activity. Also, the number of persons on staff in the internal audit activity may influence the type of structure. Therefore, treat this as one example of how the activity might be organized.

Exhibit I-2: Sample Internal Audit Activity Organizational Chart

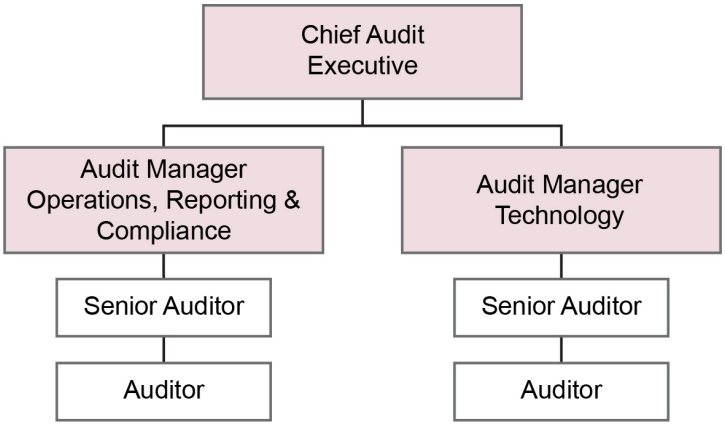


Exhibit I-3 explores these internal auditor authority levels.

Exhibit I-3: Internal Audit Activity Authority Levels

Title	Description
Chief audit executive	The CAE is a corporate executive in charge of internal auditing. This individual typically has a dual reporting structure: first, reporting functionally to the audit committee of the board of directors to ensure independence from management and, second, reporting administratively to the chief executive officer (CEO). The

	CAE ensures that a risk assessment is performed periodically and uses this, plus knowledge of corporate objectives, to establish risk-based audit plans and internal audit priorities. The CAE coordinates with other internal and external assurance providers to minimize duplicate work and ensure proper and efficient audit coverage in accord with the approved annual audit plan. He or she monitors engagements for timely completion and provides an annual holistic opinion on the adequacy and effectiveness of governance, risk management, and control processes.
Audit manager (for a specific area)	An audit manager directs the performance of assurance and consulting engagements and interacts with functional area managers in areas being audited to fully understand the activities being performed and any relevant issues while remaining independent from these areas. For example, an audit manager for operations, compliance, and reporting (this mirrors the three control objectives in the COSO internal control framework) needs to have a good understanding of the organization's operations. An audit manager for information technology (IT) would need competencies in understanding IT risk and control and the impact of technology on organizational objectives. Audit managers for any area will also coach, counsel, and direct auditors in their area in accordance with the IPPF to ensure that these professionals get the development they need to meet changing needs.
Senior auditor	A senior auditor conducts assurance and consulting engagements of up to moderate complexity and exercises good business judgment and skills to develop appropriate audit recommendations in accordance with the IPPF. Senior auditors are expected to understand client business operations, develop and maintain professional working relationships with clients, and work in a professional manner. A senior auditor may also be charged with providing staff auditors with day-to-day direction and guidance under the overall supervision of the audit manager.
Auditor (staff member)	An internal auditor staff member works under supervision to conduct assurance audits and develop recommendations in accordance with the IPPF. Auditors are expected to work alongside senior auditors to learn professional practices on audits, gain exposure to various types of projects, learn about operations in various functional areas, build a knowledge base of organizational operations, perform general research, and provide support.

Topic B: Administrative Activities of Internal Audit (Level B)

As the leader of internal audit, the CAE is tasked with many aspects of functional management, including budgeting and staffing. (Staffing includes things like workforce planning or resourcing, creating or revising position descriptions or organizational charts, recruiting, recruit selection, and contractor management.) These administrative activities are key components of successful internal auditing.

Budgeting

Effective budgeting depends on a sound organizational structure, meaning a budget in which authority and responsibility for each operational phase are clearly defined. Budgets built on a solid foundation of research and analysis are better equipped to produce realistic goals that aid in achieving the organization's desired growth and profitability. Here are some of the main benefits of budgeting:

- **Planning ahead.** A solid budget plan requires all levels of management to be involved and to formalize goals on an annual or more frequent basis.
- **Definite objectives.** Identifying definite objectives provides for performance evaluation at each responsibility level.
- **Early warning system.** Working from an established budget allows for early identification of potential sources of conflict or issues so that these situations can be addressed by management in a timely manner.
- **Coordination of activities.** A budget links segmented goals within the company's overall list of objectives so that the organization as a whole can incorporate multiple facets of its various departments.
- **Management awareness.** Budgeting results in a greater awareness of the organization's overall operations at the management level, including the impact that external factors might have on the operation as a whole.

- **Personnel motivation.** Meeting budget objectives can motivate personnel through use of various incentive or reward mechanisms that are also tied to maintaining high quality work rather than being based solely on meeting the budget.

A well-developed budget is the key component of planning that enables the internal audit activity to perform its mission on time and within established financial parameters. The CAE will also create a schedule budget, aligning the number of available audit personnel against available work hours to determine the amount of coverage that can be provided during a fiscal year as well as within each audit project.

Staffing

Staffing begins with workforce planning, followed by creating or revising position descriptions. It then proceeds to recruiting and screening applicants or contractors with the desired skills, knowledge, and characteristics; interviewing applicants or contractors to confirm that they possess the necessary qualifications; and selecting and hiring those applicants who can succeed in the job and the organization. In large organizations, the CAE or designee may work with the human resources department, who can provide invaluable assistance and reduce staffing risks by ensuring that the process conforms to employment laws and regulations (and, in the case of contractors, tax laws) and organizational hiring and contracting policies. HR can also offer experience in the selection process to reduce the risk of a bad hire or an ineffective contractor. In smaller organizations, the CAE or designee may do the interviewing and hiring themselves or use external service providers.

Workforce Planning (Resourcing)

Workforce planning involves determining the number of employees and/or contractors that are required in each position for the internal audit activity. HR may already have performed workforce planning for the entire organization, and, if so, the CAE will need to conform to the limits established in the workforce plan as well as in the budget. If the CAE feels that the workforce plans are unbalanced or insufficient, he or she can raise

the issue with HR and the appropriate executives.

Position Descriptions and Organizational Charts

Before recruiting applicants, the CAE or designee should establish and update existing job descriptions for the position(s) being filled. If it is a new position or if the position has changed (for example, has a different authority level or a different location in the chain of command), the organizational chart may also need revising. A good position description should accurately and specifically reflect the requirements for the position but should also be in alignment with the organization's and the internal audit activity's strategic objectives. For example, an IT auditor may be expected to know specific platforms and applications, but, as an organization begins to expand its online presence, the auditor may also need an understanding of distributed or web-based computing and associated security controls.

Recruiting and Contractor Sourcing

Recruiting starts with advertising the open position and spreading the word through various formal and informal networks. HR functional areas often have considerable resources available to devote to this endeavor as well as multiple methods at their disposal, from memberships on recruiting websites to associations with external recruiters, campus recruitment services, and so on. If such resources do not exist, internal auditors should weigh the cost of a given method against its benefits to ensure that the best value is gained from each investment. HR (or internal audit) will also need to keep detailed records of applications received in order to fulfill diversity or other compliance requirements and may also need to submit such records to government bodies as required.

Recruit and Contractor Selection

Recruit selection involves narrowing the choice down to those applicants who have the requisite qualifications and then conducting one or more rounds of interviews with those applicants. Background checks and other procedures may also be needed.

It is critical that anyone conducting interviews be trained or receive training from HR to reduce the risk of interviewers asking illegal questions, requesting that applicants take illegal or invalid tests, or being inconsistent in the use of allowed questions or tests. Managers will also need training in valid reasons for selection or nonselection so they do not use (or record) reasons that are illegal. Failure to follow such practices creates serious noncompliance risk, including the risk of losses from lawsuits and reputation risk.

Contractor selection will involve many of the same steps as recruit selection, but a key factor here is ensuring compliance with national tax laws related to use of contractors. Since some organizations have overused contractors to avoid paying benefits and taxes, many nations have created tax and employment regulations related to contractor duties and how they are managed.

Applicants may be interviewed with the intent of confirming what has been said on the application and what the applicant understands about the job's requirements and conditions. Screening calls may be held with HR initially and later with the CAE or designee.

Applicants are then selected for more in-depth interviews, which are usually conducted on site. Interviewers must prepare for the meeting by carefully reviewing the application against the job description and identifying critical areas that must be confirmed or explained. If multiple interviewers will be involved, their questions should be coordinated.

There are different approaches for interviewing applicants, which can be combined in a single interview:

- Structured interviews follow an interview guide that has been developed to focus on necessary skills, knowledge, experience, and attitudes. The guide helps ensure consistency and completeness in the interviewing process and also supports legal compliance. Applicants are asked the same questions, with follow-up questions as needed.
- Behavioral interviews focus on obtaining feedback and indicators of past behavior, considered a predictor of future job performance. Applicants may

be asked how they handled a specific situation in a previous position, such as coordinating with an engagement client to ensure access and efficient practices.

- Situational interviews are similar to behavioral interviews in that they try to obtain more concrete information about possible job performance, but in this case the applicants are asked about hypothetical situations rather than real experiences. For example, applicants might be asked how they would handle a client who would not accept audit findings and recommendations.

The interview should be a conversation that allows both the CAE or designee and the applicant to get to know one another and to determine if this working relationship will meet the needs of both the internal audit activity and the applicant. There are social dimensions to these needs as well as work dimensions. For example, those involved in interviewing applicants should consider whether an individual will thrive in the organization's culture. An applicant that tends toward abrupt, abrasive behavior may not work well in an organization that values positive relationships among employees.

For this reason, effective interviewing includes skills beyond asking the right questions. Effective interviewing skills include:

- Establishing a relaxed and open atmosphere that is more likely to produce honest and complete answers.
- Listening actively—asking open-ended and/or follow-up questions that encourage the applicant to talk openly or that confirm the interviewer's understanding.
- Observing nonverbal behaviors and identifying red flags (signs that indicate that an applicant may not be telling the truth or the whole story) as one would in an engagement interview.
- Taking notes. Note taking should not interfere with the discussion, but notes will be invaluable later in remembering key points and supporting hiring decisions.

When ready to make a selection, it is important to check with HR regarding updates to regulations or laws and to ensure that any discriminatory hiring decisions are avoided.

Employee and Contractor On-Boarding, Training, and Management

Once new internal auditors are hired or contracted with, they need to be led and managed, and the CAE may need to work with HR to ensure that new employee orientation is conducted as appropriate. The CAE will also need to ensure that specific technical training or other ongoing training is provided as necessary and appropriate. See Section I, Chapter 1, of Part 3 of this learning system for more information on leadership and management.

Chapter 2: Establishing a Risk-Based Internal Audit Plan

Chapter Introduction

Management is responsible for establishing and maintaining a system of internal controls in an organization. The *Standards* Glossary defines **control** as follows:

> 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.

Structures, activities, processes, and systems that help management effectively mitigate risk are all examples of internal controls. Internal controls are an integral component in risk management.

Because internal auditors are experts in understanding organizational risks and internal controls available to mitigate these risks, they are in a unique position to help management protect their organizations from risk exposures —present and future—ranging from minor disruptions to major catastrophes. The internal audit activity assists both management and the oversight body (the board or its audit committee) in enterprise risk management (ERM) by:

- Helping management to understand governance, internal controls, and risk management processes.
- Developing and implementing a risk assessment framework for internal audit planning.
- Bringing a systematic, disciplined auditing approach to assessing the effectiveness of internal controls and risk management processes.
- Providing objective and independent assurance that the organization’s risks have been appropriately mitigated.
- Making recommendations for improvements as warranted.

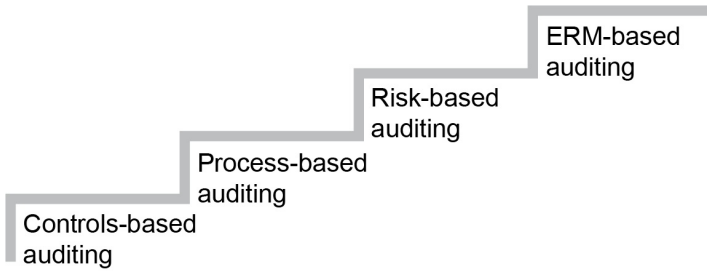
Risk is a part of conducting business. Companies must take risks to pursue their strategies and objectives. The key is how to do this while also mitigating or reducing risk. Ideally, ERM is a robust process that identifies and mitigates threats and/or occurrences that can thwart organizational success. The internal auditing function's risk assessment role plays an important part in confirming management successes and identifying exceptions for management actions.

While helping an organization to embrace a framework of internal control and an ERM framework are critical for organizational governance and are integral to most controls, internal auditing itself needs to incorporate the same ERM techniques into its audit planning procedures. To be truly value-added to the organization, the annual audit plan and specific engagements must focus on significant risks. What is considered significant can be defined as those risks that are considered likely (highly probable) and/or would have a real impact (highly damaging even if less probable) on the achievement of the organization's objectives or goals for that area.

Standard 2010, "Considerations," notes that risk is central to planning prioritization, stating that the CAE "must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals." For assurance engagements, planning "must be based on a documented risk assessment, undertaken at least annually," according to Standard 2010.A1. For consulting engagements, "improving management of risk" is also a consideration in what consulting engagements to accept, per Standard 2010.C1.

Auditing Maturity Level

When developing a risk-based internal audit plan, it is important for auditors to assess the internal audit activity's maturity level. Consider the following maturity levels of annual audit planning and audit engagement objective setting:



- **Controls-based auditing.** Prior to the 1980s, controls-based internal auditing was the standard. This method is basically an extension of external audit procedures, consisting primarily of providing assurance of the validity of various account balances and other financial details; audits of compliance with laws, regulations, policies, and procedures; and audits of specific transaction controls from initiation to reporting. The focus was to understand the laws, regulations, policies, and procedures in the area and then to identify and correct exceptions and errors.

- **Process-based auditing.** Process-based audits were developed in the 1980s to address some flaws with controls-based auditing such as its low value to decision makers. Process-based audits look at processes as a whole and evaluate their design, efficiency, and effectiveness. These audits began to stress measuring gaps between prescribed and actual processes and how they relate to achievement of business objectives, but the primary focus of the audits was often still controls-based.

- **Risk-based auditing.** Risk-based auditing was developed in the 1990s to demonstrate further added value, especially as more consulting firms entered into co-sourcing arrangements for internal auditing and had to justify their fees. The intent was to limit the audit engagement to significant risks, starting by developing a thorough understanding of the organization and its risks. Relatively low-risk controls could be omitted from engagements (or included in scope infrequently as part of a regular rotation) to ensure a greater return on the investment in auditing. This auditing maturity level satisfies the mandates of the *Standards* to be risk-based in selecting engagements, audit objectives, and specific audit tests. It is a method that is intuitive for management to understand and endorse. However, organizations that have relatively mature risk-based processes can move to an even higher auditing maturity level—ERM-based auditing.

- **ERM-based auditing.** ERM-based auditing was developed in the late 1990s as a counterpart to the organization-wide use of ERM for holistic risk-based assessment and decision making. In addition to setting project priorities based on perceived risk to key business objectives, it focuses strongly on measuring risk based on relevant key performance indicators (KPIs), considering risk appetite and risk tolerance levels, and planning responses based on what ERM capabilities already exist. Rather than focusing just on mitigating risks to an acceptable level, ERM-based auditing assesses how well ERM activities are supporting organizational objectives by managing risks to an acceptable level within a risk appetite/tolerance. Thus, the focus is on the gaps in ERM effectiveness, based not only on the auditor's objective assessment of what risks are significant but also on management's assessment of those risks.

  Advantages of maturing to an ERM-based auditing methodology include:
  - Creating a foundation for audit judgments based on organizational strategy and objectives, risk appetite, and governance maturity.
  - Developing an assurance framework for assessing the adequacy of ERM and governance activities.
  - Synchronizing the auditor's tolerance for risk with management's tolerance for risk, rather than focusing solely on the auditor's, as in prior audit methods.
  - Emphasizing the critical need to base performance measurements on what will provide real incentives to accomplish organizational objectives.
  - Focusing on the organization's future capability to assess and manage risk rather than on just its historical risk response track record.

The remainder of this chapter refers to risk-based auditing, which should be taken as a generalization that could refer to either risk- or ERM-based audits, with the goal of achieving the maturity level of an ERM-based audit.

The chapter starts by identifying sources of potential engagements, highlighting the importance of understanding the organization and its industry and market when considering audit priorities. The second topic discusses the need to establish a framework for assessing risk and how to

rank and validate risks by priority. The third and fourth topics provide detailed descriptions of various types of assurance and consulting engagements. Although all audit engagements have common elements and factors, such as developing an audit plan or putting together an audit team, each type of engagement also has individual and specialized components. It is critical that internal auditors can identify these differences and apply the correct methods of performing the engagements. The last topic describes coordinating internal audit efforts with the work of other internal and external assurance and consulting service providers.

Topic A: Sources of Potential Engagements (Level B)

The Audit Universe

In most organizations, the potential audit universe is vast. Identifying the audit universe is vital in laying the foundation for internal audit's annual risk assessment and planning process. The internal audit plan is derived from the annual risk assessment process. This plan outlines the priority of audit cycle requirements for the internal audit activity, including the objectives, scope, and frequency of audit engagements to be performed in the coming year. It also contains any annual portions of engagements that are cycled out over a period longer than 12 months (e.g., 24 months, 36 months).

The audit universe includes the major functions, operations, operating units, subsidiaries, and business, service, and product lines of the organization, each of which is considered an "auditable unit." It also includes any applicable areas (e.g., financial reporting or compliance) that have a pervasive, organization-wide impact and fall under the internal audit "umbrella" from an assurance coverage perspective.

In highly regulated industries, such as financial services, health care, insurance, oil and gas, or brokers/dealers, the audit universe will include audits of the relevant regulatory mandates. In addition to this, government agency examiners often set expectations around independent compliance assessments of high-risk areas, even in the absence of specific laws and regulations requiring independent audits. An example is internal auditors for insured depository institutions conducting reviews related to the U.S. Bank Secrecy Act and related anti-money-laundering laws. Another example might be internal auditors for a federal government defense contractor performing independent assessments of organizational compliance with contract provisions.

A major area of financial reporting and legal compliance impact for U.S. organizations (or foreign organizations traded on U.S.–based exchanges) involves the U.S. Sarbanes-Oxley Act (SOX) and the internal control over