CIA Review Reference Book

SURGENT
CIAreview

Part 2

Practice of Internal Auditing

2023

CIA Part 2
Practice of Internal Auditing

Part 2, Domain I
Managing the Internal Audit Activity

Section A: Internal Audit Operations

Learning Outcomes:

1. Describe policies and procedures for the planning, organizing, directing, and monitoring of internal audit operations. Basic Level.
2. Interpret administrative activities (budgeting, resourcing, recruiting, staffing, etc.) of the internal audit activity. Basic Level.

Managing the Internal Audit Function

A. According to the Standards, the chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization. The internal audit activity is effectively managed when:
   1. It achieves the purpose and responsibility included in the internal audit charter.
   2. It conforms to the Standards.
   3. Its individual members conform to the Code of Ethics and the Standards.
   4. It considers trends and emerging issues that could impact the organization.

B. Managing the internal audit activity involves overseeing its day-to-day operations, including the following administrative activities:
   1. Formulating policies and procedures for the planning, organizing, directing, and monitoring of internal audit operations.
   2. Budgeting and human resource administration, including recruiting, staffing, personnel evaluations and compensation.

C. **Internal Audit Policies and Procedures** – The Standards state that the CAE must establish policies and procedures to guide the internal audit activity. Therefore, the CAE or head of internal audit is responsible to formulate policies and procedures for the planning, organizing, directing, and monitoring of internal audit operations. Guidance on internal audit policies and procedures is provided in implementation guide 2040 – Policies and Procedures, which is summarized below.

1. The form and content of the policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work. While a large, mature internal audit activity may have a formal internal audit operations' manual that includes the policies and procedures, a smaller or less mature internal audit activity may not. Instead, policies and procedures may be published as separate documents.
2. It is essential to ensure that internal audit policies and procedures are aligned with:
    a. The Mandatory Guidance of the International Professional Practices Framework (IPPF).
    b. The internal audit charter.
    c. The organization's strategies, policies, and processes.
3. The following topics are generally included in an internal audit manual or otherwise documented to help guide the internal audit activity:
    a. Internal audit policies:
        i. The overall purpose and responsibilities of the internal audit activity.
        ii. Adherence to the Mandatory Guidance of the IPPF.
        iii. Independence and objectivity.
        iv. Ethics.
        v. Protecting confidential information.
        vi. Record retention.
    b. Internal audit procedures:
        i. Preparing a risk-based audit plan.
        ii. Planning an audit and preparing the engagement work program.
        iii. Performing audit engagements.
        iv. Documenting audit engagements.
        v. Communicating results/reporting.
        vi. Monitoring and follow-up processes.
    c. Quality assurance and improvement program.
    d. Administrative matters.
        i. Training and certification opportunities.
        ii. Continuing education requirements.
        iii. Performance evaluations.
4. To ensure internal audit personnel are properly informed about internal audit policies and procedures, the CAE may issue individual documents, training materials, or a comprehensive manual; and training sessions may be conducted to review the information.
5. Internal audit policies and procedures should be reviewed periodically. Such reviews may be included in the internal audit activity's internal assessments and the external assessment.

D. **Budgeting and Resources Management**

1. According to the Standards, the CAE must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.
    a. **Appropriate** refers to the mix of knowledge, skills, and other competencies needed to perform the plan.
    b. **Sufficient** refers to the quantity of resources needed to accomplish the plan.
    c. **Effectively deploying resources** means that the resources are used in a way that optimizes the achievement of the approved plan.
2. Ensuring the adequacy of internal audit resources is ultimately a responsibility of the organization's senior management and the board; the CAE should assist them in discharging this responsibility. The CAE is primarily responsible for the **sufficiency and management** of internal audit resources in a manner that ensures the fulfillment of internal audit's responsibilities, as detailed in the charter. This includes determining:
    a. Financial budgets.
    b. Number of auditors required and staffing plans.
    c. Knowledge, skills, and other competencies required from auditors to complete their work.
3. The CAE communicates to senior management and the board the internal audit activity's resource requirements including resources for employees, external service providers, financial support, and technology-based audit techniques.
4. From an overall resource management standpoint, the CAE:
    a. Develops the operating and financial budget for internal audit operations. The budget should be developed annually and then submitted to management and the board for their review and approval.
    b. Conducts a periodic skills' assessment or inventory to determine the specific skills required to perform the internal audit activities.
    c. Ensures that resources are deployed effectively.
    d. Considers succession planning, staff evaluation and development programs, and other human resource disciplines.
    e. Develops appropriate metrics, goals, and objectives to monitor the overall adequacy of resources.

Passing Tip:	Internal audit activity resources must be adequate and sufficient to meet the audit plan requirements.

5. When faced with limited resources (both financial and/or human resources), the least desirable option for completing future engagements would be to eliminate certain engagements from the work-schedule. The following options may be attempted:
    a. Using self-assessment questionnaires to address audit objectives.
    b. Employing information technology whenever possible.
    c. Filling any human resource vacancies with personnel from operating departments that are not being audited (considering potential impairments to independence and objectivity).
6. Any resource limitations or other related factors that might affect the scope of engagements or the engagement work schedule must be promptly reported to senior management and the board.

Talent Management

(Adapted from the *IIA's Practice Guide "Talent Management"*)

A. The CAE should assess whether the internal audit activity collectively has the competencies needed to fulfill its mission and meet stakeholders' expectations. This competency assessment should be based on a systematic process, including the following steps:
    1. Assess stakeholders' needs and expectations.
    2. Develop an audit plan to meet stakeholders' needs and expectations, with consideration for organizational objectives, strategies, and risks.
    3. Leverage the Internal Audit Competency Framework to identify competencies required to execute the audit plan.
    4. Perform a competency gap analysis.
    5. Develop a talent management strategy.
    6. Periodically reassess the internal audit's collective competencies and address key gaps.

B. After the competency assessment, the CAE and internal audit managers are involved in four key activities of talent management: recruiting, developing, motivating, and retaining talent.

C. **Recruiting** – Recruitment may be internal or external.
    1. **Internal Recruitment** includes:
        a. **Full-time Permanent Recruitment** – Internal recruitment may result in acquiring talent with high-level organizational awareness and strong business knowledge. However, internal recruits may need additional training to develop core audit skills. In addition, impaired objectivity may be a potential concern. Effective training programs, supervision, and thoughtful assignment planning can help to mitigate such concerns.

b. **Rotational Recruitment** – Rotational programs provide a training ground for internal candidates from other departments while filling talent gaps in internal audit. Rotational programs can be outbound or inbound:

   i. **Outbound** rotational programs rotate internal auditors out of internal audit and into other business units. Rotating out gives internal auditors the opportunity to enhance their business knowledge in other functional areas.

   ii. **Inbound** rotational programs rotate employees from other business units into internal audit for a limited time. Inbound programs provide an opportunity for high-performing staff members outside of internal audit to learn about governance, risk management, and internal control practices. The primary challenges associated with inbound rotational programs are potential impairments to individual objectivity, providing audit skills training to inbound employees, and scheduling.

c. **Guest Auditor Program** – A guest auditor program can be used to fill competency gaps for specific audit engagements. This provides an opportunity for personnel from other parts of the organization to make a short-term commitment to internal audit. A guest auditor typically serves as a subject matter expert on a unique internal audit engagement, enhancing knowledge sharing within the organization.

2. **External Recruitment**

   a. External recruitment finds talent from outside of the organization. External talent may be sourced from public accounting firms, internal audit activities at other organizations, colleges and universities, and areas outside of the traditional internal audit domain.

      i. Candidates from public accounting firms (external auditors) typically have high-level audit expertise and may have broad industry experience. However, conflicts of interest can arise if candidates are recruited from the organization's public accounting firm.

      ii. Candidates from internal audit activities at other organizations may have relevant internal audit competencies, but still require onboarding and training to become familiar with the new organization.

      iii. Undergraduate or Master of Business Administration candidates may require more focused training, supervision, and on-the-job experiences to reach satisfactory levels of performance.

b. **Candidate Selection**

i. Job descriptions should be clearly defined and a standard set of competency-based interview questions should be used consistently with all candidates. This standardization and consistency helps to establish baseline criteria from which to evaluate a pool of candidates.

ii. Tips for candidate selection include:

- Ensure that human resources has an understanding of internal audit's role and need for talent, and that desired competencies are reflected in the job description.
- Coordinate with human resources to leverage the organization's intranet and websites, general job boards, professional association job boards, and recruiting agencies to search for potential candidates.
- Screen candidates by assessing their relevant competencies and alignment with the organization's espoused values.
- Verify candidate experience and qualifications, and complete background checks, as applicable.
- Prepare competency-based interview questions, ensure that interviewers are knowledgeable of legal constraints (i.e., types of questions or answers to avoid), and trained in conducting behavioral or competency-based interviews, as appropriate.

c. **Interview Candidates**– The CAE is ultimately responsible to interview candidates for internal audit positions. While this task may be delegated in larger internal audit functions, ultimate responsibility for recruitment rests with the CAE. When interviewing candidates for internal audit positions, several attributes are preferred in potential candidates:

i. **Education and background** – internal auditors are preferred to have as much background information as possible. Certification is a significant plus for potential candidates.

ii. **Experience** – the required experience for internal auditors depends on the position within the internal audit function, and the types of engagements that the internal audit function is expected to perform. Generally, the CAE ultimately matches the required experience to the position.

iii. **References and background checks** – it's crucial to obtain references and background checks of any potential candidates to be employed in sensitive positions. Internal auditing is considered a sensitive position since they will be in privity to a wide array of documents and information, and thus the CAE must obtain contact references and obtain background information to ensure the integrity of potential candidates.

iv. **No impairment to independence and objectivity** – internal auditors must be independent and must carry out their duties with objectivity, and thus, upon interviewing potential candidates, the CAE must ensure that no actual or potential conflicts of interest or impairments to independence exist.

v. **Technical skills** – some internal audit functions require specialized skills, and thus if this is the case, the CAE must ensure that applicants possess the required technical skills. For example, if the internal audit department conducts operational and compliance audits of a nuclear plant, it is essential that any auditor have the related technical skills.

vi. **Know when to seek help** – internal audit candidates may not necessarily possess the extensive technical skills, but they must be able to realize when they need help. They should be able to determine when they require help and how to seek it. It may be by researching technical literature or consulting with industry experts.

3. **Outsourcing and Co-sourcing** – Internal audit activities may engage outside parties to perform tasks that require specialized expertise. Outsourcing alternatives include many types that are discussed later in this section.

4. **Professional vs. Specialist Recruitment** – Internal or external recruitment may be for either professional or specialist individuals

   a. **Professional** – Internal auditors are recruited from inside or outside the organization to practice the profession of internal audit. Usually, this model yields the best results in an environment in which there is sufficient career progression within the internal audit department to allow professional progression.

   b. **Specialist** – Internal auditors with special expertise are recruited to be specialized in specific audit assignments. Examples include environmental, security, investment, or information technology specialists. The advantage of this type is that there are always well-trained personnel available to carry out complex audit assignments in their respective fields. The disadvantage is that these expert auditors do not always have the flexibility to perform audit assignments of general nature.

D. **Developing Talent** – The CAE should align internal audit's talent development approach with the organization's professional development practices. Efforts to develop talent typically include professional development plans, training and continuing education, and mentoring.

1. **Professional Development Plans** – Individual professional development plans require staff members to take ownership of their professional development. A professional development plan may support a particular career path identified by the organization or by the individual internal auditor. For example:

a. **Career internal auditor** – Career internal auditors pursue internal audit as a long-term profession. This career path might include rotating in and out of internal audit as a way to enhance the career internal auditor's organizational knowledge.

b. **Business operations** – Internal auditors may serve in audit to gain a broad and deep understanding of the organization's business operations, risk management, internal controls, and governance. They then leverage this experience to seek operational roles.

c. **Executive leadership** – A rotation through internal audit may be part of an organization's executive leadership development program.

2. **Training and Continuing Education** – Internal audit can meet its development plan goals through various training and continuing education activities. The best result generally can be achieved through a combination of activities. Internal audit should develop its training plan based on an assessment of staff competencies against the Competency Framework. The plan should meet the collective needs of the internal audit activity as well as the professional development needs of individual internal auditors.

   a. **On-the-job Training** – On-the-job training can be highly effective, especially for new staff members. It provides them with hands-on experience performing internal audit tasks. On-the-job training should include ongoing feedback and coaching from experienced team members.

   b. **Classroom Training** – Many organizations have in-house training programs to provide specific training based on job roles and responsibilities. For example, training may cover the organization and its processes, the regulatory framework governing the organization's business, and other governance structures. Training also could include specific technical skills for internal auditors such as data analytics and fraud control. IIA chapters and institutes often offer or provide technical training to their members.

      i. **Workshops** are a special form of classroom training that require a higher level of individual and group participation. Depending on participant interaction, this approach may work best when participants already have a certain degree of experience and knowledge.

   c. **E-learning** – E-learning may be delivered by internal as well as external providers. It provides greater flexibility for scheduling and does not require travel or absence from the office. The main disadvantage is minimal interaction with the facilitator and other participants.

   d. **Assessing Training Options** – Reading and writing articles for professional publications, attending professional conferences, and networking are other types of ways to gain internal audit knowledge and skills.

3. **Mentoring** – A mentoring program can be key to developing talent, not only for new hires but also for more experienced staff. Mentoring programs should be largely informal, with consideration given to the following:
    a. A mentor must be more experienced than the mentee.
    b. Each auditor may be assigned a mentor.
    c. It is best if the mentor is not the individual's supervisor.
    d. Meetings between the mentor and the mentee should be informal, without official documentation.
4. **Succession Plan**
    a. Succession planning should start in advance of any potential employment event. Succession plans should identify potential candidates for existing positions, taking into consideration the needs of the organization and the candidates' career goals, competencies, and potential for development.
    b. Potential candidates could be approached regarding their interest in possible succession opportunities. Interested persons then could be developed for future roles and responsibilities.

E. **Motivating and Retaining Talent**

1. Potential motivators can be mapped against Maslow's hierarchy of needs. Although it is important to find the best combination of motivators for each individual, challenging work, career opportunities, quality of work environment, and recognition rather than compensation, are leading drivers of staff retention. Rewards and recognition, flexible working practices, and work–life balance all can be potential motivators of retention.
2. **Rewards**
    a. Transparent processes for rewarding staff members should be established, such as:
        i. Establishing criteria that define which behaviors or actions will be rewarded/recognized.
        ii. Making recognition eligibility open to all employees.
        iii. Consistent application of rewards to all who qualify.
    b. Recognition should occur as close to the performance as possible, so that it reinforces behavior. A reward should always be preceded by recognition, but recognition can be given without the reward.

c. Rewards may be financial or nonfinancial. Nonfinancial rewards include:

i. Increasing responsibilities.

ii. Appointing the employee to be a team leader.

iii. Enrolling the employee in certification programs.

iv. Publicly recognizing employee performance in staff/office meetings.

3. **Flexible Work Practices –** Flexible work practices can help retain talent. In implementing flexible work practices, CAEs should pay special attention to balancing employee workload with engagement and business needs. They should still expect internal audit staff to comply with internal policies and confidentiality standards, especially when working remotely.

Outsourcing Internal Audit Activity

A. **Types of Outsourcing Alternatives** – Outsourcing alternatives include:

1. **Total Outsourcing** where 100% of the internal audit services are obtained from external sources, usually on an ongoing basis.

2. **Partial Outsourcing** where **less** than 100% of the internal audit services are obtained from external sources, usually on an ongoing basis or for specific terms.

3. **Co-sourcing** through which external resources participate on joint engagements with in-house internal audit staff.

4. **Co-sourcing or Subcontracting** for a specific engagement or portion of some engagement is performed by an external party, typically for a limited time period. Management and oversight of the engagement normally is provided by in-house internal audit staff.

B. Partial Outsourcing, Co-sourcing, and Subcontracting – In these cases, the organization has its own internal audit activity but obtains some internal audit services from external service providers.

1. **External service provider** is a person or firm, independent of the organization, who has special knowledge, skill, and experience in a particular discipline.

2. When an external service provider is used, the CAE needs to consider his/her competency, independence, and objectivity as they relate to the proposed assignment. (If the selection of the external service provider is made by someone other than the CAE, and the CAE determines that he or she should not use and rely on the work of the external service provider, the results of such assessment need to be communicated to senior management or the board.)

a. When assessing the proficiency (knowledge, skills, and other competencies) of the external service provider, The CAE considers the following:
    i. Professional certification, license, or other recognition of the external service provider's competency in the relevant discipline.
    ii. Membership of the external service provider in an appropriate professional organization and adherence to that organization's code of ethics.
    iii. The reputation of the external service provider. This may include contacting others familiar with the external service provider's work.
    iv. The external service provider's experience in the type of work being considered.
    v. The extent of education and training received by the external service provider in disciplines that pertain to the particular engagement.
    vi. The external service provider's knowledge and experience in the industry in which the organization operates.
b. When assessing the independence and objectivity of the external service provider the following needs to be considered:
    i. The financial interest the provider may have in the organization.
    ii. The personal or professional affiliation the provider may have to the board, senior management, or others within the organization.
    iii. The relationship the provider may have had with the organization or the activities being reviewed.
    iv. The extent of other ongoing services the provider may be performing for the organization.
    v. Compensation or other incentives that the provider may have.

3. The external service provider to perform extended audit services may be the organization’s external auditor. If this is the case, the CAE needs to ascertain that work performed does not impair the external auditor’s independence.
    a. Extended audit services are services performed beyond the requirements of the generally accepted auditing standards adhered to by external auditors.
    b. Independence needs to be assessed in relation to the full range of services provided to the organization.

4. If the CAE relies on an external service provider for internal auditing activities, the work of the provider is subject to the same compliance procedures as those that the internal audit activity and internal audit staff are subject to. The CAE evaluates the adequacy of work performed, which includes sufficiency of information obtained to afford a reasonable basis for the conclusions reached and the resolution of exceptions or other unusual matters.
5. If the CAE intends to refer to services performed by an external service provider, the CAE is required to obtain the approval of the provider prior to such reference.

C. **Total Outsourcing** – As mentioned above, total outsourcing refers to obtaining 100% of the internal audit services from external sources, usually on an ongoing basis.

1. **Board Approval** – Given the significance of internal auditing to the organization's governance process, any recommendation to totally outsource (or to outsource a significant portion of) the internal audit activity should require approval of the board.
2. **Oversight and Responsibility** – In cases where total outsourcing is selected, oversight and responsibility for the internal audit activity **cannot be outsourced**. An in-house liaison, preferably a designated chief audit executive or optionally an executive or senior management-level employee, should be assigned responsibility for management of the internal audit activity. The role of the board or equivalent governing body also is important in the oversight process.
3. **Quality Assurance and Improvement Program** – The responsibility for creating and maintaining a QAIP remains with the employee, as the standard applies to the function, not the provider.
4. **Independence** – Consideration of the independence of the assigned in-house liaison must be evaluated if this individual has other (non-internal audit) responsibilities.
3. **External Auditor** – Even if allowed by law or regulations, internal auditing should never be outsourced to the same external audit firm that audits the organization's financial statements as this would impair independence

Section B: Establish Risk-Based Internal Audit Plan

Learning Outcomes:

1. Identify sources of potential engagements (audit universe, audit cycle requirements, management requests, regulatory mandates, relevant market and industry trends, emerging issues, etc.). Basic Level.
2. Identify a risk management framework to assess risks and prioritize audit engagements based on the results of a risk assessment. Basic Level.
3. Interpret the types of assurance engagements (risk and control assessments, audits of third parties and contract compliance, security and privacy, performance and quality audits, key performance indicators, operational audits, financial and regulatory compliance audits). Proficiency Level.
4. Interpret the types of consulting engagements (training, system design, system development, due diligence, privacy, benchmarking, internal control assessment, process mapping, etc.) designed to provide advice and insight. Proficiency Level.
5. Describe coordination of internal audit efforts with the external auditor, regulatory oversight bodies, and other internal assurance functions, and potential reliance on other assurance providers. Basic Level.

Internal Audit Plan

A. **Three Levels of Planning** – Generally, planning is a continuous process throughout the internal audit activity's operations and over several time spans. The types of plans may be combined into less or more levels depending on the organization and nature of engagement, but generally, there are three basic levels of planning:

   1. **Internal audit plan** – for each period, an internal audit plan is developed that covers the planned audits of the internal audit activity during the period. This plan would be the result of the risk assessment of the entire organization. The plan would detail what engagements are planned to be performed during the period.
   2. **Engagement Plan** – for each engagement, the internal auditor develops an audit plan which is based on a detailed risk assessment of the engagement area and identifies the engagement objectives (Discussed in Domain-II of Part-2).
   3. **Engagement Work Program** – lists detailed procedures that should be conducted by the auditor to achieve specific audit objectives that will achieve the engagement objectives (Discussed in Domain-II of Part-2).

B. According to the Standards, the CAE must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

   1. To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

C. The internal audit plan usually includes:

   1. A list of proposed audit engagements (and specification regarding whether the engagements are assurance or consulting in nature).
   2. Rationale for selecting each proposed engagement (e.g., risk rating, time since last audit, change in management, etc.).
   3. Objectives and scope of each proposed engagement.
   4. A list of initiatives or projects that result from the internal audit strategy but may not be directly related to an audit engagement.

D. When developing the internal audit plan, the CAE should coordinate with other assurance providers.

   1. The CAE considers the internal audit activity's ability to rely on the work of other internal and external assurance providers to ensure proper coverage and minimize duplication of efforts.
   2. Coordination and discussions with other assurance providers may highlight new areas of significance that might require internal audit attention, resulting in new potential engagements.

E. Although audit plans typically are prepared annually, they may be developed according to another cycle. For example, the internal audit activity may maintain a rolling 12-month audit plan and reevaluate projects on a quarterly basis. Or, the internal audit activity may develop a multi-year audit plan and assess the plan annually.

F. Planning for the internal audit activity must be consistent with its charter and with the goals of the organization. The planning process involves establishing goals for the internal audit activity and developing engagement work schedules and budgets.

   1. **The goals of the internal audit activity** must be capable of being accomplished within specified operating plans and budgets and, to the extent possible, should be measurable. They should be accompanied by measurement criteria and targeted dates of accomplishment.
   2. **Engagement work schedules and budgets** normally include the following:
      a. What activities are to be performed,
      b. When they will be performed (the commencement date), and

c. The estimated time required, taking into account the scope of the engagement work planned and the nature and extent of related work performed by others.

d. Measurability criteria.

e. Staffing requirements and time allocation.

f. Detailed expense budget.

G. The internal audit plan is intended to ensure that internal audit coverage adequately examines areas with the greatest exposure to the key risks that could affect the organization's ability to achieve its objectives. Planning for the internal audit activity involves the following steps which will be discussed separately:

1. Determining all potential engagements.
2. Prioritizing engagements based on risk assessment.
3. Identifying resource requirements.
4. Communicating the plan for review and approval.

Determining Potential Engagements

The first step in internal audit planning is to determine all potential engagements within the scope of internal audit. The sources of potential engagements include:

A. **Audit Universe** – is a list of all possible audits that could be performed within an organization. Defining the audit universe requires reviewing the number of auditable entities in terms of both the business units or areas of operations within the organization and the number of auditable units or activities within and across those business units.

1. The audit universe includes audit projects and initiatives related to the organization's strategic plan, and it may be organized by business units, product or service lines, processes, programs, systems, or controls.
2. Some examples of auditable activities include:
   a. Policies, procedures, and practices both on an organization level and those specific to areas or locations.
   b. Information system security.
   c. Information system infrastructure.
   d. Major contracts or product lines.
   e. Functions such as manufacturing, distribution, purchasing, accounting, finance, marketing and other functions.
3. It is advisable to assess the audit universe (and related audit plan) on at least an annual basis to reflect changes in the organization's strategy, management direction, objectives, emphasis and focus. In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the organization's business, operations, programs, systems, and controls.

B. **Market, Product, and Industry Knowledge** – Internal auditors use market, product, and industry knowledge to identify new internal audit engagement opportunities. Any information available to internal auditors may be utilized to identify new engagement opportunities. Examples include:

   1. During a period of intense and/or fierce competition, internal auditors may wish to conduct an operational audit to ensure both the effectiveness and efficiency of operations. Such an audit may focus on potential cost reductions, and/or seek to eliminate inefficiencies in the process.

   2. New trends in an industry may reflect directly on operations, and create a potential for new internal audit engagements, such as the fragmentation of an industry, competition from other industries, regulation over the industry by the government or other authority, introduction of new laws impacting the industry . . . etc.

   3. An internal auditor learns of product features that may not be in compliance with existing laws and regulations, and/or industry standards, and thus a compliance audit may be required.

   4. New environmental standards are to be implemented that may affect the product or the production process, and thus, a potential environmental audit and/or product audit may be required.

C. **Management Requests** – When developing the plan, the CAE considers requests by senior management, the audit committee, or the governing body as they may require the internal audit activity to conduct specific engagements.

D. **Regulatory Mandates** – regulatory agencies may impose new regulations on the organization that may require the organization to conduct certain audits or demonstrate compliance with certain regulations. The CAE considers these mandates when determining potential engagements and developing the plan.

E. **Organization's Strategic Plan and Risk Exposures** – In identifying the potential engagements and preparing the internal audit plan, the CAE starts by consulting with senior management and the board to understand the organization's strategies, business objectives, risks, and risk management processes.

   1. The audit universe (potential engagements) can include components from the organization's strategic plan. By incorporating components of the organization's strategic plan, the audit universe will consider and reflect the overall business objectives. The organization's strategic plan considers the environment in which the organization operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

   2. The internal audit activity's plan is designed based on an assessment of risk and exposures that may affect the organization's ability to achieve its strategic objectives. Ultimately, the audit objective is to provide management with information to mitigate the negative consequences associated with accomplishing the organization's objectives.

3. The audit universe can be influenced by the results of the risk management process. When developing audit plans the outcomes of the risk management process should be considered. Thus, the audit universe and audit plan preparation usually involves reviewing the results of any risk assessments that management may have performed. In addition, the CAE considers the maturity of the organization's risk management processes, including whether the organization uses a formal risk management framework to assess, document, and manage risk.
4. To ensure that the audit universe covers all of the organization's key risks, the internal audit activity typically independently reviews and corroborates the key risks that were identified by senior management.
5. The Importance of Independent Risk Assessment
    a. Conducting an organization-wide risk assessment enables the CAE to focus on those risks that rate among the most significant and to identify manageable, timely, and value-adding engagements that reflect the organization's priorities.
    b. Organizations that have implemented ERM may have created a comprehensive risk register (also known as a risk inventory). Internal auditors use management's information as one input into internal audit's organization-wide risk assessment. However, internal auditors should do their own work to validate that all key risks have been documented and that the relative significance of risks is reflected accurately.

Prioritizing Engagements Based on Risk Assessment

A. The internal audit plan is intended to ensure that internal audit coverage adequately examines areas with the greatest exposure to the key risks that could affect the organization's ability to achieve its objectives. Therefore, the audit plan is based on, among other factors, an assessment of risk priority and exposure. Prioritizing is needed to make decisions for applying relative resources based on the significance of risk and exposure.

B. **Definitions**

1. **Risk** is the probability that an event or action may adversely affect the organization or activity under audit. Risk is usually measured by the potential dollar or materiality of adverse exposure to the organization.
2. **Risk Identification** is the process of identifying all risks that affect the organization objectives. All imaginable risks that may affect the success of the organization must be identified, ranging from the more significant business risks down to the less important risks related to individual projects or smaller business units
3. **Risk Assessment** is a systematic process for assessing and integrating professional judgments about probable adverse conditions and/or events. The risk assessment process should provide a means of organizing and integrating professional judgments for development of the audit plan.

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

D. The internal audit activity needs to establish a risk-assessment framework for identifying potential engagements, prioritizing them, and selecting the risk priorities to be included in the annual audit plan. The risk-assessment framework employs various quantitative and qualitative methods to determine risk weightings.

E. The best risk assessment technique is usually a comprehensive approach to risk management taking into consideration, the causes, the event, and the impact. This would be achieved by assessing risk levels of current and future events, their effect on achievement of the organizational objectives, and their underlying causes.

F. Linking critical risks to specific objectives and business processes helps the CAE organize the audit universe and prioritize the risks. The CAE uses a risk-factor approach to consider both internal and external risks.

   1. **Internal risks** may affect key products and services, personnel, and systems. Relevant risk factors related to internal risks include the degree of change in risk since the area was last audited, the quality of controls, and other factors.

   2. **External risks** may be related to competition, suppliers, or other industry issues. Relevant risk factors for external risks may include pending regulatory or legal changes and other political and economic factors.

G. The CAE should ensure that the schedule of audit priorities is revised and updated in accordance with the most recent risk assessment and prioritization of the risks. In addition, the CAE should maintain an ongoing dialogue with senior management and the board to stay abreast of changes that may affect risk assessments and affect current audit priorities.

H. A variety of risk models exist to assist the chief audit executive in prioritizing potential audit subject areas. Most risk models utilize risk factors to establish the priority of engagements such as:

   - Dollar materiality
   - Asset liquidity
   - Management competence
   - Quality of internal controls
   - Degree of change or stability
   - Time of last audit engagement
   - Complexity
   - Employee and government relations, etc.

   1. Other methods that may be used to prioritize risks may involve a matrix involving a risk reduction factor, a cost savings factor, and the extent of changes since last engagement. The auditor would typically have to assign weights to the aforementioned factors and give priority to the audits with the highest total weights.
   2. The expertise of available audit staff is considered least important when prioritizing engagements since audit needs rather than auditor skills should determine the priorities in the risk-based plans.

3. Changes in management direction, objectives, emphasis, and focus are normally reflected in updates to the audit universe and related audit plan.
4. In conducting audit engagements, methods and techniques for testing and validating exposures need to be reflective of the risk materiality and likelihood of occurrence.

Passing Tip:

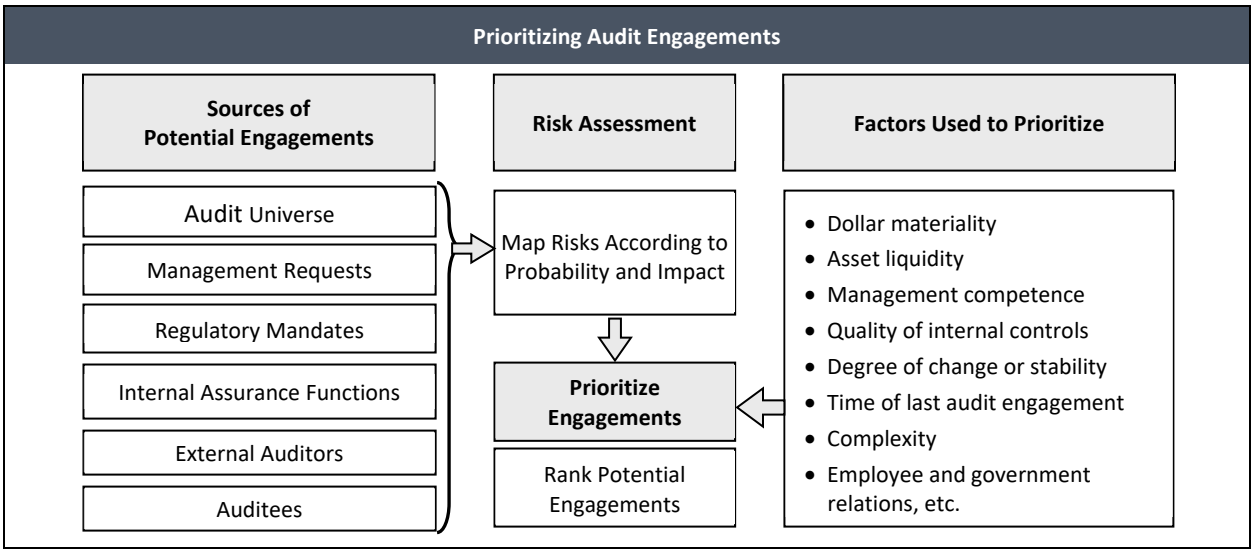
The following is the prioritizing of risks when internal audit resources are limited. Likely risks are given first priority before possible risks (regardless of criticality), and risks with remote likelihood have least priority.

		Likelihood		
		Likely	Possible	Remote
Impact	Critical	1	4	7
	Major	2	5	8
	Minor	3	6	9

Further, when there is a possibility of fraud, it would normally receive higher attention than an area that has not been previously audited or requests of external auditors.

I. Matters to be considered in establishing engagement priorities include:
   1. The dates and results of the last engagement.
   2. Updated assessments of risks and effectiveness of risk management and control processes.
   3. Requests by senior management, the audit committee, and the governing body.
   4. Current issues relating to organizational governance.
   5. Major changes in the enterprise's business, operations, programs, systems, and controls.
   6. Opportunities to achieve operating benefits.

J. The CAE should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Those engagements that have been accepted must be included in the plan.



Passing Tip: The rationale for using risk assessment for audit planning is because it provides a systematic process for assessing and integrating professional judgment about probable adverse conditions.

Illustration of Prioritizing Audit Engagements

For example, an auditor is evaluating 5 engagements based on the following three factors:

1. The engagement's potential to reduce risk to the organization.
2. The engagement's potential to save money to the organization.
3. The extent of change in the related area since the last engagement.

The auditor typically assesses the above three factors to each engagement and associates each factor with a High, Moderate, or Low assessment. Based on the auditor's judgment, the matrix would look like this:

Audit	Risk Reduction	Cost Savings	Changes
1	High	Moderate	Low
2	High	Low	Low
3	Low	High	Moderate
4	Moderate	Moderate	High
5	High	Moderate	High

Next, the auditor would typically assign a weight to each factor when assigning score points. The weight for all three factors may be equal or more emphasis is placed on one factor than the others.

The auditor may normally assign points as follows (or using any other objective criteria):

Assessment	Points
High	3
Moderate	2
Low	1

If all factors are weighted equally, the audit priorities become as follows:

Audit	Risk Reduction	Cost Savings	Changes	Total Score	Audit Priority
1	High (3)	Moderate (2)	Low (1)	6	3
2	High (3)	Low (1)	Low (1)	5	4
3	Low (1)	High (3)	Moderate (2)	6	3
4	Moderate (2)	Moderate (2)	High (3)	7	2
5	High (3)	Moderate (2)	High (3)	8	1

If the Risk Reduction factor and the Cost Savings factor are considered twice as important as the changes, the audit priorities become as follows:

Audit	Risk Reduction	Cost Savings	Changes	Total Score	Audit Priority
1	High (6)	Moderate (4)	Low (1)	11	2
2	High (6)	Low (2)	Low (1)	9	4
3	Low (2)	High (6)	Moderate (2)	10	3
4	Moderate (4)	Moderate (4)	High (3)	11	2
5	High (6)	Moderate (4)	High (3)	13	1

Identifying Resource Requirements

A. As indicated earlier, the CAE must ensure that internal audit resources are **appropriate**, **sufficient**, and **effectively deployed** to achieve the approved plan.

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

B. After developing the internal audit plan, the CAE determines the resources needed to accomplish the plan, based on the risk-based priorities identified during the planning process. Resources may include:

   1. People – work hours and skills.
   2. Technology – audit tools and techniques.
   3. Timing – availability of resources.
   4. Funding.

C. For determining the needed resources, the CAE usually begins by gaining a deeper understanding of the resources available to the internal audit activity.

   1. The CAE considers the number of internal audit staff and productive work hours available to implement the plan within the organization's schedule constraints.
   2. The CAE reviews a documented skills assessment or gather information from employees' performance appraisals and post-audit surveys to gain an overview of the internal audit activity's collective knowledge, skills, and other competencies
   3. The CAE reviews the approved budget and consider the funds available for training, technology, or additional staffing in order to achieve the plan.

D. The CAE then compares the resources needed to accomplish the plan's priorities with those available to the internal audit activity to determine whether any gaps exist. This comparison can be used as a basis for determining the impact of resource limitations.

E. To fill gaps related to the internal audit staff's knowledge, skills, and competencies, the CAE could provide training for existing staff, request an expert from within the organization to serve as a guest auditor, hire additional staff, or hire an external service provider.

F. Any resource limitations (both financial or human resources) that might affect the scope of the audit plan must be promptly reported to Senior Management and the Board.

Types of Engagement – Assurance Engagements

Assurance services involve the internal auditor's objective assessment of evidence to provide opinions or conclusions regarding an entity, operation, function, process, system, or other subject matters.

According to the IIA Glossary, assurance service is an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

The different types of assurance engagements are discussed in the following sections.

A. **Risk and Control Self-Assessment**

1. **Control Self-Assessment (CSA)**, or risk and control self-assessment, is the process of assessing the effectiveness of the organization's risk management and internal control system. All employees participate in the process that is mainly aimed at ensuring effective and efficient achievement of the organizational goals. Using the CSA method, everyone in the organization becomes the process owner.
2. CSA can be used by management or the internal audit activity as an audit technique. In a CSA, internal auditors work with local team members in an area of the organization, leading them in an effort to evaluate their current control procedures and then to use the review results to improve internal controls.
3. CSA enhances the system of internal control in a procedural manner as follows:
    a. Identifying potential risks and assessing related controls.
    b. Establishing satisfactory controls in terms of effectiveness and cost-effectiveness.
    c. Emphasizing management's responsibility for the internal control system.
    d. Communicating results.
4. The primary advantages of CSA include
    a. Indicates the degree of the functionality of control processes and the significance of the residual risks.
    b. Enhances employees' understanding of business risks and controls and encourages communication and cooperation among them.
    c. Early identification of risks and improvement of the general risk-control environment.
    d. Provides internal auditors with more on-hand information about the control processes, (thus enabling them to directly concentrate their efforts on weak areas).

5. **CSA Approaches –** There is a wide variety of approaches used for CSA processes. The approach used needs to be suitable for the unique characteristics of the organization and should be dynamic so as to respond to organizational change and development:
    a. **Facilitated team** where work teams of different levels in the function hold discussions leading to a rough report. The report is then reviewed by the group. Such workshops may take several forms, as follows:
        i. **Risk-based format:** A comprehensive method whereby members considering all possible risks that may hinder goal achievement, assess related controls for effectiveness, and highlight residual risks.
        ii. **Control-based format:** Having the risks and controls already identified for them, team members in this type of workshop assess the effectiveness of the controls against management's expectations.
        iii. **Process-based format:** Focuses on selected activities in processes. Members identify the objectives of, and aim at generally developing, the process and its component activities.
        iv. **Objective-based format:** Focuses on determining the best way to achieve business objectives. Members examine the effectiveness of controls in supporting the objectives and then check the level of the residual risks for reasonableness.
    b. **Questionnaire –** is another approach of CSA used in gathering information on risks and controls within the organization. Questionnaires typically include simple "yes-no" questions that are easy to understand. Questionnaires usually save time and money and ensure more honest feedback.
    c. **Self-certification approach –** in this approach the internal auditors use the information gathered from managers' assertions about the state of internal controls within their units or functions. The internal auditors may synthesize these certifications with other information to enhance the understanding about controls and to share the knowledge with managers in business or functional units as part of the organization's CSA program.
6. The internal audit activity's role in the CSA program could range from owning the process (designing, implementing, etc.) to playing the role of consultant and verifying the final evaluations.

B. **Audits of Third Parties and Contract Auditing**

1. **External Business Relationships** – The following guidance is obtained from the IIA's Practice Guide, Auditing External Business Relationships:

   a. Organizations often use external business relationships to satisfy a variety of business needs and accomplish their objectives. With these business relationships also come inherent and control risks associated with working with external business partners.

      i. It is management's responsibility to manage these risks and achieve the benefits.

      ii. Internal auditors can help management and the board identify, assess, and manage these risks.

   b. Examples of external business relationships include

      i. **Service provider** such as payroll processing, IT services, internal audit outsourcing, or call centers.

      ii. **Supply-side partners** such as production outsourcing, R&D outsourcing, suppliers, or vendors.

      iii. **Demand -side partners** such as distributor, franchisee, licensee.

      iv. **Strategic alliances and joint ventures**.

      v. **Intellectual property partners**.

   c. The following are examples of risks associated with external business relationships. The internal auditor needs to be alerted to these risks when auditing external business relationships:

      i. External business partner's actions may adversely affect the organization's reputation by violating laws or regulations, misrepresenting the organization's values, or not complying with contractual obligations.

      ii. The external business partner may not maintain adequate insurance coverage.

      iii. Disputes or disagreements may arise regarding the scope of services between the organization and its external business partner.

      iv. The external business partner may have conflicts of interest in providing services. For example, quality or timeliness of work may be adversely affected due to contractual obligations to others.

      v. Intellectual property licensed to others could be receiving inappropriate royalty streams due to theft, or misuse of ideas or technology.

      vi. The organization may be overcharged for inefficiencies or services not performed.

vii. The external business partner may become insolvent, go out of business, or become unable to fulfill contractual obligations.

viii. The organization's confidential information shared with the external business partner may be exposed, which may result in competitive, reputational or legal risks.

d. **Auditing External Business Relationships** – the general steps for auditing external business relationships are as follows:

i. **Understand the organization**, its environment, and the nature of each external business relationship.

ii. **Assess risks and controls** – The internal auditor assesses the risk to the organization associated with the external business relationship. This includes:

- Determine potential impacts on the organization in the absence of any controls of inherent risks that the organization has assessed, along with those that the internal auditor has identified and assessed.
- Understand the design of controls the organization has put in place to mitigate risks.
- Determine the key controls, which if not effective would mean the risks are not mitigated.
- Understand the external business partner's environment, processes, and controls.
- Determine whether the external business partner's internal auditor has performed work relating to the contract with the organization.

iii. **Perform Audit Procedures** – Based on the audit objectives, the internal auditor determines if audit procedures need to be performed at the external business partner. Some external business partners may not allow access by a business partner's internal audit activity unless the contract provides access.

- For example, if the organization has outsourced its information systems processing facilities to a third party (external business relationship), its continued processing would be dependent on the third party. The internal auditors may be assigned with the approval of the third party to audit the third party to ensure that all risks that may affect its ability to provide continuous service are mitigated through adequate and effective controls.

iv. **Report and monitor progress** – The internal auditors determines the frequency and content of reports to the board and senior management, and determine whether findings have been addressed appropriately.