2018 Edition

CIA

Preparatory Program

Part 2
Sample

Internal Audit Practice

Brian Hock, CIA, CMA
and
Carl Burch, CIA, CMA

Hock international

HOCK *international*, LLC
P.O. Box 6553
Columbus, Ohio 43206

(866) 807-HOCK or (866) 807-4625
(281) 652-5768

www.hockinternational.com
cia@hockinternational.com

Published January 2018

Acknowledgements

Acknowledgement is due to the Institute of Internal Auditors for permission to use copyrighted questions and problems from the Certified Internal Auditor Examinations by The Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, Florida 32701 USA. Reprinted with permission.

The authors would also like to thank the Institute of Certified Management Accountants for permission to use questions and problems from past CMA Exams. The questions and unofficial answers are copyrighted by the Certified Institute of Management Accountants and have been used here with their permission.

The authors also wish to thank the IT Governance Institute for permission to make use of concepts from the publication Control Objectives for Information and related Technology (COBIT) 3rd Edition, © 2000, IT Governance Institute, www.itgi.org. Reproduction without permission is not permitted.

Thanks

The authors would like to thank the following people for their assistance in the production of this material:

- Kekoa Kaluhiokalani for his assistance with copyediting the material,
- Lynn Roden, CMA for her assistance in the technical elements of the material,
- Kevin Hock for his work in the formatting and layout of the material,
- All of the staff of HOCK Training and HOCK *international* for their patience in the multiple revisions of the material,
- The students of HOCK Training in all of our classrooms and the students of HOCK *international* in our Distance Learning Program who have made suggestions, comments and recommendations for the material,
- Most importantly, to our families and spouses, for their patience in the long hours and travel that have gone into these materials.

Editorial Notes

Throughout these materials, we have chosen particular language, spellings, structures and grammar in order to be consistent and comprehensible for all readers. HOCK study materials are used by candidates from countries throughout the world, and for many, English is a second language. We are aware that our choices may not always adhere to "formal" standards, but our efforts are focused on making the study process easy for all of our candidates. Nonetheless, we continue to welcome your meaningful corrections and ideas for creating better materials.

This material is designed exclusively to assist people in their exam preparation. No information in the material should be construed as authoritative business, accounting or consulting advice. Appropriate professionals should be consulted for such advice and consulting.

Topic I B. Operational Role of Internal Audit

The operational role of internal auditing is to make sure that engagements have been properly planned for, that the IAA has the resources (human and financial) to carry out the engagements, and that the results of the engagements are communicated to those who can take action. The CAE must effectively manage the IAA so that management and the board will regard all of these functions as value-added activities.

The following section discusses the role of internal auditing within the organization's risk management framework.

B1. Developing Policies and Procedures

Standard 2040: Policies and Procedures

The chief audit executive must establish policies and procedures to guide the internal audit activity.

Interpretation:

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.

Another duty of the CAE is to establish the policies and procedures to guide the IAA and the individual internal auditors in their work. These policies and procedures are essential in helping the staff comply with the IAA's standards of performance. The extent, depth, and formalization of the policies and procedures will depend upon the size and structure of the IAA and the complexity of its work. In a small IAA with a simple business structure, policies and procedures will be less developed and less formal than those in a multinational business in a very complex business environment.

A small IAA is managed much more informally with personal and daily contact. Control may take place through meetings and internal memorandum. In a large IAA, where contact with the managers may not be frequent, there will need to be a more formal set of policies and procedures to guide staff in their work.

Practice Advisory 2040-1: Policies and Procedures

1. The chief audit executive develops policies and procedures. Formal administrative and technical audit manuals may not be needed by all internal audit activities. A small internal audit activity may be managed informally. Its audit staff may be directed and controlled through daily, close supervision and memoranda that state policies and procedures to be followed. In a large internal audit activity, more formal and comprehensive policies and procedures are essential to guide the internal audit staff in the execution of the internal audit plan.

The Audit Manual

In a large enough organization, the policies and procedures of the internal audit function and guidance for engagements will be formalized in what is generally called an **audit manual**. The audit manual covers everything from the Internal Audit Charter to performance reviews and evaluations. It provides guidance from planning the engagement to the final report.

Note: The guidance in the audit manual can make reference to the IIA Standards and Implementation Guides or other sources of guidance.

While every audit manual will be different, below is the Table of Contents for a sample internal audit manual.

Part 1 – Policies, Standards and Guidelines

1) Introduction
2) Policies and Standards of Internal Audit (including Internal Audit Charter)
3) Internal Control Framework
4) Organizing Internal Audit (including structure, services, types of audit and budget)
5) Performance Monitoring and Evaluation (including KPI)

Part 2 – Practices (Risk-based Approach and Methodologies)

1) Strategies and Annual Work Planning
2) Conducting Internal Audit Assignments
3) Preparing Internal Audit Report
4) Audit Tools and Techniques
5) Advisory Services and Approach
6) Quality Assurance and Improvement
7) Follow up on Audit Recommendations
8) Reporting to Audit Committee
9) Personnel and Training

Question 8: Policies and procedures relative to managing the internal audit activity should

a) Ensure compliance with its performance standards.

b) Give consideration to its structure and the complexity of the work performed.

c) Result in consistent job performance.

d) Prescribe the format and distribution of engagement communications and the classification of engagement observations.

(CIA Adapted)

Question 9: In most cases, an internal audit activity should document policies and procedures to ensure the consistency and quality of its work. The exception to this principle is directly related to:

a) Departmentation

b) Division of labor

c) Size of the internal audit activity

d) Authority

(CIA Adapted)

Planning

> **Standard 2010: Planning**
>
> The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity and to make certain that they are consistent with the organization’s goals.
>
> **Interpretation:**
>
> 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.

When prioritizing risk, the CAE takes into consideration the company’s risk-management framework, including the levels of risk appetite that management sets for different parts of the organization. If management has not yet developed a risk-management framework, the CAE will use his or her own judgment of risks after consulting with senior management and the board.

This much larger, overall planning process is broken down into four smaller categories that the CAE is responsible for:

- Goals
- Engagement work schedules
- Staffing plans and financial budgets
- Activity reports

Setting the Goals of the Internal Audit Activity

> **Note:** For memorization purposes, the five goals of the IAA form the acronym SMART.

The goals that the IAA sets should be:

- **Specific**. Goals should be specifically defined.
- **Measurable**. The method of measuring the goals should be defined. By making goals measurable, the CAE, the audit committee, and board of directors can progress toward achieving specific goals—and by extension they can quantify the value of the IAA.
- **Agreed To**. All interested parties (including senior management and the board) need to agree to the goals.
- **Realistic and Achievable**. Realistic and achievable goals keep expectations reasonable; conversely, unrealistic and unachievable goals create unnecessary tension in an organization.
- **Timely**. Goals should have specific completion dates, because open-ended timeframes reduce the sense of urgency about objectives.

Risk Assessment in Planning

One of the significant inputs into the planning process is the risk management process. The engagements of the internal audit activity should focus on and address the specific area of risk that the company has identified. PA 2010-2 addresses the use of risk assessment in the planning process.

Practice Advisory 2010-2 - "Using the Risk Management Process in Internal Audit Planning"

6. Internal audit planning needs to make use of the organizational risk management process, where one has been developed. In planning an engagement, the internal auditor considers the significant risks of the activity and the means by which management mitigates the risk to an acceptable level. The internal auditor uses risk assessment techniques in developing the internal audit activity's plan and in determining priorities for allocating internal audit resources. Risk assessment is used to examine auditable units and select areas for review to include in the internal audit activity's plan that have the greatest risk exposure.

7. Internal auditors may not be qualified to review every risk category and the ERM process in the organization (e.g., internal audits of workplace health and safety, environmental auditing, or complex financial instruments). The chief audit executive (CAE) ensures that internal auditors with specialized expertise or external service providers are used appropriately.

8. Risk management processes and systems are set up differently throughout the world. The maturity level of the organization related to risk management varies among organizations. Where organizations have a centralized risk management activity, the role of this activity includes coordinating with management regarding its continuous review of the internal control structure and updating the structure according to evolving risk appetites. The risk management processes in use in different parts of the world might have different logic, structures, and terminology. Internal auditors therefore make an assessment of the organization's risk management process and determine what parts can be used in developing the internal audit activity's plan and what parts can be used for planning individual internal audit assignments.

9. Factors the internal auditor considers when developing the internal audit plan include:

- Inherent risks—Are they identified and assessed?
- Residual risks—Are they identified and assessed?
- Mitigating controls, contingency plans, and monitoring activities—Are they linked to the individual events and/or risks?
- Risk registers—Are they systematic, completed, and accurate?
- Documentation—Are the risks and activities documented?

In addition, the internal auditor coordinates with other assurance providers and considers planned reliance on their work. Refer to The IIA's Practice Advisory 2050-2: Assurance Maps.

10. The internal audit charter normally requires the internal audit activity to focus on areas of high risk, including both inherent and residual risk. The internal audit activity needs to identify areas of high inherent risk, high residual risks, and the key control systems upon which the organization is most reliant. If the internal audit activity identifies areas of unacceptable residual risk, management needs to be notified so that the risk can be addressed. The internal auditor will, as a result of conducting a strategic audit planning process, be able to identify different kinds of activities to include in the internal audit activity's plan, including:

- Control reviews/assurance activities—where the internal auditor reviews the adequacy and efficiency of the control systems and provides assurance that the controls are working and the risks are effectively managed.

- Inquiry activities—where organizational management has an unacceptable level of uncertainty about the controls related to a business activity or identified risk area and the internal auditor performs procedures to gain a better understanding of the residual risk.
- Consulting activities—where the internal auditor advises organizational management in the development of the control systems to mitigate unacceptable current risks. Internal auditors also try to identify unnecessary, redundant, excessive, or complex controls that inefficiently reduce risk. In these cases, the cost of the control may be greater than the benefit realized and therefore there is an opportunity for efficiency gains in the design of the control.

14. A selection of lower risk level business unit or branch type audits need to periodically be included in the internal audit activity's plan to give them coverage and confirm that their risks have not changed. Also, the internal audit activity establishes a method for prioritizing outstanding risks not yet subject to an internal audit.

15. An internal audit activity's plan will normally focus on:

- Unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately.
- Control systems on which the organization is most reliant.
- Areas where the differential is great between inherent risk and residual risk.
- Areas where the inherent risk is very high.

B2. Review the Role of Internal Audit in the Risk Management Process

Note: This topic is presented immediately before B5 because one of the IAA's main roles in the risk management process is to provide assurance to management, which is included in Topic B5 and 6.

B3. Direct Administrative Activities

The administrative activities of the internal audit activity are wide and varied. It is not expected that the CAE will carry out these administrative duties personally, but there must be a mechanism of oversight in place. One of the most important administrative duties is connected to human resources within the internal audit activity. There must be plans and procedures in place to ensure that the proper, qualified, required staff are hired and that their work schedules are managed for maximum efficiency and effectiveness.

Developing the Engagement Work Schedules

The planning process and specific work schedules for engagements should include the following:

- **Which** engagements should be performed
- **When** engagements should be performed
- The **time required** for each engagement—taking into account the scope of the planned engagement work and the nature and extent of related work performed by others
- Which engagements should receive **priority** over other engagements

Once these questions are answered, the CAE can develop individual work programs for specific engagements.

Managing Resources

Standard 2030: Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Interpretation:

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

Standard 2030 states that internal audit resources must be “appropriate, sufficient, and effectively deployed.” As outlined in the interpretation of the standard, **appropriate** means having the right mix of staff who together have the appropriate competencies to perform the plan; **sufficient** means having the right number of staff to accomplish the plan; **effectively allocated** means that the staff is used in the way that optimizes achieving the approved plan.

The CAE needs to oversee the assignment of individual staff with a short-term and long-term view. In the short term, all of the jobs need to be staffed by qualified and capable internal auditors so that the job can be completed to the highest level. In the long term, however, the staff needs to be assigned to jobs that will allow them to grow and become senior auditors.

This long-term view requires occasionally assigning jobs to staff members who may not currently have all of the necessary skills and experience. Under such circumstances, the CAE needs to make sure that a skilled supervisor can provide the needed support and guidance to the junior member of the team. Also, training can be provided or additional resources can be made available to that auditor to assist in this process.

Some factors to consider when assigning staff to individual engagements are:

- The complexity of the engagement
- The resources that are available in the IAA
- The experience (skill level) of the staff
- The training and developmental needs of the audit staff

Practice Advisory 2030-1

1. The chief audit executive (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 internal audit charter. This includes effective communication of resource needs and reporting of status to senior management and the board. Internal audit resources may include employees, external service providers, financial support, and technology-based audit techniques. Ensuring the adequacy of internal audit resources is ultimately a responsibility of the organization’s senior management and board; the CAE should assist them in discharging this responsibility.
2. The skills, capabilities, and technical knowledge of the internal audit staff are to be appropriate for the planned activities. The CAE will conduct a periodic skills assessment or inventory to determine the specific skills required to perform the internal audit activities. The skills assessment is based on and considers the various needs identified in the risk assessment and audit plan. This includes assessments of technical knowledge, language skills, business acumen, fraud detection and prevention competency, and accounting and audit expertise.
3. Internal audit resources need to be sufficient to execute the audit activities in the breadth, depth, and timeliness expected by senior management and the board, as stated in the internal audit charter. Resource planning considerations include the audit universe, relevant risk levels, the internal audit plan, coverage expectations, and an estimate of unanticipated activities.

4. The CAE also ensures that resources are deployed effectively. This includes assigning auditors who are competent and qualified for specific assignments. It also includes developing a resourcing approach and organizational structure appropriate for the business structure, risk profile, and geographical dispersion of the organization.

5. From an overall resource management standpoint, the CAE considers succession planning, staff evaluation and development programs, and other human resource disciplines. The CAE also addresses the resourcing needs of the internal audit activity, whether those skills are present or not within the internal audit activity itself. Other approaches to addressing resource needs include external service providers, employees from other departments within the organization, or specialized consultants.

6. Because of the critical nature of resources, the CAE maintains ongoing communications and dialog with senior management and the board on the adequacy of resources for the internal audit activity. The CAE periodically presents a summary of status and adequacy of resources to senior management and the board. To that end, the CAE develops appropriate metrics, goals, and objectives to monitor the overall adequacy of resources. This can include comparisons of resources to the internal audit plan, the impact of temporary shortages or vacancies, educational and training activities, and changes to specific skill needs based on changes in the organization’s business, operations, programs, systems, and controls.

The Internal Audit Budget

The size of the budget for the internal audit function is determined by the internal audit plan, the organizational structure, and the staffing strategy. The CAE needs to carefully analyze the funds that are available and the needed budgeting to accomplish the objectives of the IAA. The budget must include all of the activities that are needed to accomplish the objectives of the IAA, including:

- Paying staff
- Training and staff development
- Hiring external specialists as needed
- Any other expenses that the department will incur in the performance of its duties

Recruiting and Promoting

The CAE needs to coordinate with human resources in recruiting and retaining qualified audit staff. The most important criteria in hiring is the education and experience of the candidate. The individual needs to have the technical skills or background for the job. This does not mean that everyone who is hired needs to be a CIA, but there should be some indication that candidates will be able to do the job based on their formal education or by experience in a previous position. Not everyone in the IAA needs to be a trained or qualified accountant because there are many engagements that are not related to accounting or financial statements.

The ability of the candidate to communicate, both in written and verbal forms, and the individual’s overall interpersonal skills should also be considered. These are critical elements of the IAA because a poor communicator is a much less effective internal auditor regardless of their technical skills.

Once the staff has been hired, the next HR issue relates to staff promotion and filling higher-level positions in the IAA. When a higher-level position becomes available, the CAE has two options: the CAE can fill the opening with someone from inside or outside the organization.

Hiring from **inside the organization** can be done quickly and with less “start-up” time for the person who gets the position because the employee is already familiar with company policies and procedures. Also, there is less risk because the CAE has already worked with the individual and is more aware of what the individual can and cannot do. Hiring from within the organization is also generally a good motivating factor for others in the IAA because they know that good work will be rewarded with promotion. If, however, the wrong people are promoted, or people are promoted because of reasons other than their work skills, then promotion may have a negative effect on the others in the department.

Hiring someone from **outside the organization** is riskier, but it also has its advantages. For example:

- The outside person could bring new ideas and new perspectives to the job and the organization.
- It is possible that the person may have skills or experiences that are not within the organization.
- It is also possible that that management training costs could be lowered because it is assumed that the person is already qualified and will not require additional training.

Job Descriptions

An important basis for the recruitment and promotion of staff is the job description. Job descriptions should be established for all positions, listing the **necessary skills and requirements for the position**. Accurate, concise job descriptions and a strict adherence to hiring guidelines make the recruitment process smooth and easy because all potential candidates know what is required to be promoted and that only qualified people will be hired.

With detailed and complete job descriptions, the CAE has an easy time determining if the IAA is properly staffed. If the people in all of the positions have the necessary skills as outlined in the job description, then the function is properly staffed. If, however, there are some people without the necessary skills in some positions, there is a missing element in the IAA, which will need to be addressed either through training or the addition of someone to the IAA who possesses those skills.

Training, Staff Development, and Performance Evaluations

The CAE is also responsible for the training, counseling, and performance evaluations of the staff. Training gives the staff the necessary skills to perform their jobs in the short term and also to develop and broaden their skills for their long-term development. Individuals often see training as a benefit, and a well-developed training program is an excellent recruiting tool for the company. Training should benefit the individual and also help the IAA meet its organizational goals. Therefore, some staff may be trained in areas where the IAA does not currently have all of the required skills, even if the staff does not have a personal interest in those areas.

Counseling, or **mentoring**, is an important element of staff development. The CAE has a responsibility for counseling and assisting staff members in their growth in the organization. In a large internal audit department, there may be a formal counseling and mentoring program and, in such a situation, the CAE most likely is responsible for the oversight and management of the process. Additionally, the CAE may be the counselor for some of the higher-level staff members in the department.

Performance evaluations should be made at least annually, or more often if needed. The performance evaluations need to focus on the skills that are necessary for the individual to perform his or her work and for IAA as a whole to perform its duties. These staff evaluations should be seen as a means of giving internal audit employees the opportunity to identify their weaknesses and give them an opportunity to improve their performance. The evaluation should not be based on personal likes or dislikes or other non-employment related factors, especially when the evaluation is an engagement evaluation of work on a specific assignment and not an annual evaluation.

There should be sufficient time to allow everyone to prepare for the annual evaluation. This usually involves the auditor and the manager both filling out the evaluation form and preparing for the meeting. The meeting should be scheduled when both parties are not pressed for time so that anything that arises during the evaluation can be discussed and addressed in a timely manner.

The performance evaluation form can be a standard worksheet focused on the most important areas. However, for the process to work as well as possible, the evaluation needs to be carefully constructed and should not include over-general comments that are applicable to everyone. Examples and specific references to events should be included in order to make the evaluation as detailed as possible.

Question 10: An important part of an internal audit activity's personnel development plan should be on-the-job training. Which of the following activities is the most important in broadening a staff internal auditor's knowledge?

a) Rotating staff internal auditors through a variety of assignments.

b) Developing expertise in a few particular areas by continuously assigning the same internal auditor to those areas.

c) Allowing staff internal auditors to participate in choosing the projects assigned.

d) Assigning staff internal auditors to particular supervisor-trainers for extended periods.

(CIA Adapted)

Question 11: The chief audit executive can best ensure that staff internal auditors are prepared to meet their existing responsibilities by

a) Enforcing established recruiting and selection criteria.

b) Counseling them on their performance and providing appropriate training opportunities.

c) Having experienced internal auditors supervise their work closely.

d) Conducting formal evaluations of their performance on each assignment.

(CIA Adapted)

B4. Interviewing Candidates for Internal Audit Positions

As part of the hiring process, members of the internal audit staff may be involved in interviewing candidates. The process may involve a number of different interviews. It is common for the first interview to be brief and conducted by the HR department (if one exists). There may also be some standardized tests.

Additional interviews with internal audit managers and staff might follow. If these are satisfactory, the CAE will usually conduct the final interview to make a final decision as well as follow up on any areas of concern.

Throughout the interview process, the interviewer needs to asses a number of areas about the candidate. Among them are:

- Does the candidate have the necessary skills for the position? (The necessary skills will depend on the level of the position and the expected duties, but they should be outlined in the job description.)
- Does the candidate have the required experience and education?
- How will the candidate fit in with the internal audit department and within the corporate culture?

As part of the interview process, the candidate may be presented with work-related situations and asked to respond or recommend an appropriate course of action. While it would be ideal to observe the candidate in an actual work situation, the interviewer can create work scenarios as best as possible in the interview setting.

Asking Good Questions

Asking thoughtful and thought-provoking questions helps the interviewer find get a sense of the candidate beyond the information written on a CV. The interviewer should ask:

- Open-ended questions that require more than a "yes" or "no" answer
- What they would do in different situations
- Details about their relevant experience

In some situations, the interviewer may not have the requisite knowledge or expertise to adequately question a given candidate. In that case, it may be necessary for a second interview, one who does have the appropriate expertise, to complete the interview process.

Listening Effectively

The interviewer must carefully listen to and properly understand the candidate's answers. The interviewer should not interrupt answers unless it is clear that a given response is not appropriate or adequate. The interviewer also needs to be able to use the information that they learn during the interview to change or add a line of questions. Furthermore, non-verbal cues are also important indicators, and a skillful interviewer will take note of any clues such as fidgeting, distracted behavior, or failure to maintain eye contact.

In summary, the interviewing process should identify any potential weaknesses that the candidate has or any issues that might arise. It is far better to identify any potential problems and reject a candidate rather than discover significant problems after they have been hired.

B2. Review the Role of Internal Audit in the Risk Management Process

> **Note:** This topic is presented immediately before B5 because one of the IAA's main roles in the risk management process is to provide assurance to management, which is included in Topic B5 and 6.

Risk management is a key responsibility of management, but the internal auditor also plays a role in this process. Internal auditors, acting in both assurance and consulting roles, can assist both management and the audit committee by examining, evaluating, reporting, and recommending improvements to the adequacy and effectiveness of management's risk processes. It is with the guidance of the internal auditor's findings that senior management and the board can then oversee the organization's risk management and control processes.

The assessment and reporting of an organization's risk management processes are normally a high audit priority, and the charter should clearly outline management and the board's expectations for the IAA. The IAA's role in risk management is likely to be determined by such factors as the culture of the organization, the skill-set of the internal audit staff, and local conditions and customs of the host country in which the audit takes place.

Internal auditors should address any risk exposures that they encounter in any engagement and evaluate them further as necessary, even if it is not part of the immediate engagement.

The IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management provides a very good overview of this issue.

Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management

Internal auditing is an independent, objective assurance and consulting activity. Its core role with regard to ERM is to provide objective assurance to the board on the effectiveness of risk management. Indeed, research has shown that board directors and internal auditors agree that the two most important ways that internal auditing provides value to the organization are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively.

Internal auditors will normally provide assurances on three areas:

- Risk management processes, both their design and how well they are working;
- Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them; and
- Reliable and appropriate assessment of risks and reporting of risk and control status.

It is important to remember that the IAA's role in the risk management process is not static and could possibly change over time. PA 2120-1 (*Assessing the Adequacy of Risk Management Processes)* provides a list of four different roles that the internal audit activity can be in the risk management process.

PA 2120-1: Assessing the Adequacy of Risk Management Processes

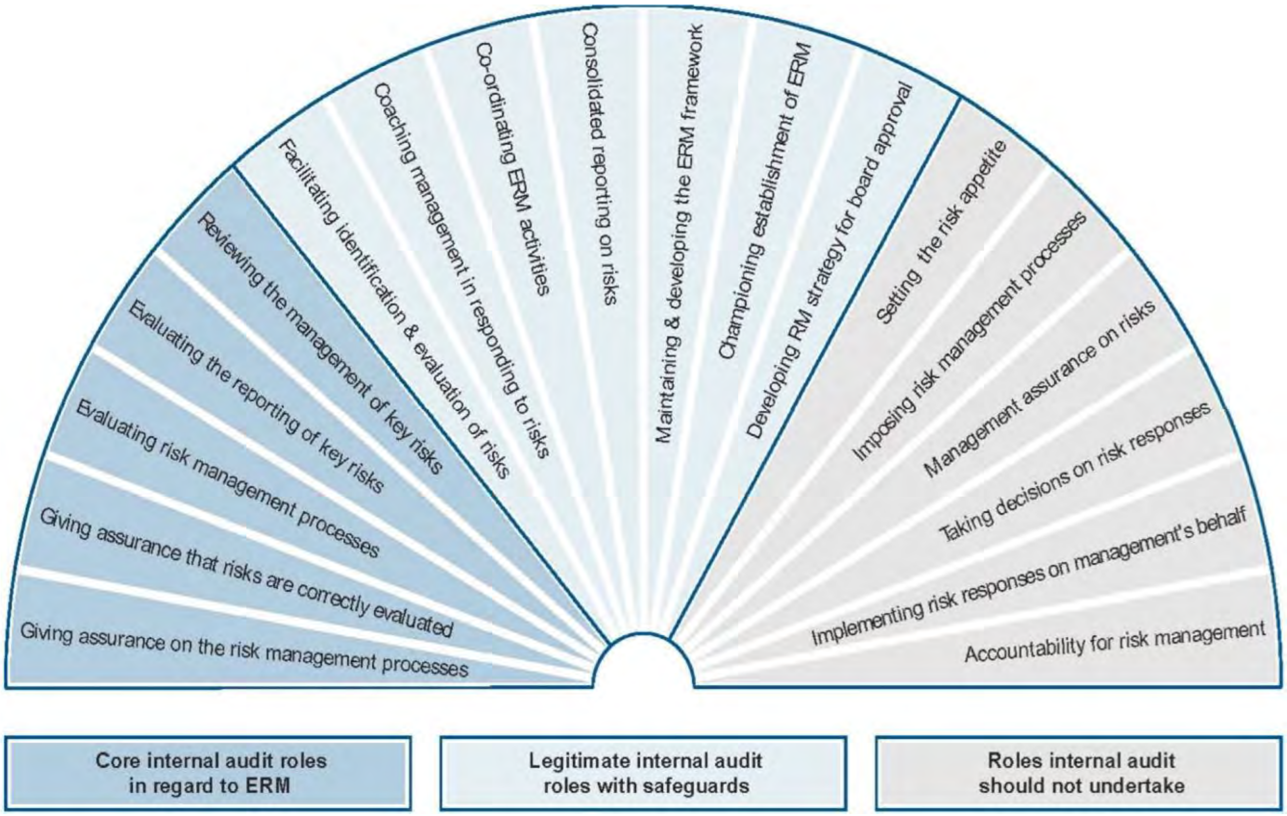
4. The CAE is to obtain an understanding of senior management's and the board's expectations of the internal audit activity in the organization's risk management process. This understanding is then codified in the charters of the internal audit activity and the board. Internal auditing's responsibilities are to be coordinated between all groups and individuals within the organization's risk management process. The internal audit activity's role in the risk management process of an organization can change over time and may encompass:

- No role.
- Auditing the risk management process as part of the internal audit plan.
- Active, continuous support and involvement in the risk management process such as participation on oversight committees, monitoring activities, and status reporting.
- Managing and coordinating the risk management process.

Possible Roles for Internal Audit

The IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management outlines three categories of possible roles for the IAA in respect the risk management process in the company. The first category is comprised of core roles that the IAA should fill. The second category, made of consulting roles, is comprised of roles that the IAA may legitimately have but does not need to have. When the IAA is filling roles in the second category, there must be sufficient safeguards in place to endure the objectivity and independence of the internal auditors. The third category of roles are roles that the IAA should not play.

In this diagram, the items on the left make up the first category of roles, the items in the middle the second, and the items to the right are the roles that internal audit should not play.


Giving assurance on the risk management processes
Giving assurance that risks are correctly evaluated
Evaluating risk management processes
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing RM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake

Core Internal Audit Roles in Regard to ERM

Note: These are assurance activities.

- Giving assurance on the risk management process
- Giving assurance that risks are correctly evaluated
- Evaluating risk management processes
- Evaluating the reporting of key risks
- Reviewing the management of key risks

Legitimate Internal Audit Roles in Regard to ERM

Note: These are consulting roles.

- Facilitating identification and evaluating risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Consolidated reporting on risks
- Maintaining and developing the ERM framework
- Championing the establishment of ERM
- Developing the RM strategy for board approval

Roles Internal Audit Should Not Undertake

- Setting the risk appetite
- Imposing risk management processes
- Management assurance on risks
- Taking decisions on risk responses
- Implementing risk responses on management's behalf
- Accountability for risk management

Determination of Role of IAA in Risk Management

5. Ultimately, it is the role of senior management and the board to determine the role of internal auditing in the risk management process. Their view on internal auditing's role is likely to be determined by factors such as the culture of the organization, ability of the internal audit staff, and local conditions and customs of the country. However, taking on management's responsibility regarding the risk management process and the potential threat to the internal audit activity's independence requires a full discussion and board approval.

B5. Report on the Effectiveness of Risk Management

While responsibility for risk management in a company rests with senior management and the board, the internal auditors can examine, evaluate, and report on the adequacy and effectiveness of the risk management process. In addition, they may also make recommendations to improve the risk management process.

Standard 2120 and PA 2120-1 address the role of internal audit in assessing the risk management process.

Standard 2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation: Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes

1. Risk management is a key responsibility of senior management and the board. To achieve its business objectives, management ensures that sound risk management processes are in place and functioning. Boards have an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective. In this role, they may direct the internal audit activity to assist them by examining, evaluating, reporting, and/or recommending improvements to the adequacy and effectiveness of management's risk processes.

Every organization will have its own particular methodology to implement the risk management process. PA 2120-1 includes information about the different processes that an organization may have.

PA 2120-1: Assessing the Adequacy of Risk Management Processes

6. The techniques used by various organizations for their risk management practices can vary significantly. Depending on the size and complexity of the organization's business activities, risk management processes can be:

- Formal or informal.
- Quantitative or subjective.
- Embedded in the business units or centralized at a corporate level.

7. The organization designs processes based on its culture, management style, and business objectives. For example, the use of derivatives or other sophisticated capital markets products by the organization could require the use of quantitative risk management tools. Smaller, less complex organizations could use an informal risk committee to discuss the organization's risk profile and to initiate periodic actions. The internal auditor determines that the methodology chosen is sufficiently comprehensive and appropriate for the nature of the organization's activities.

The internal auditor must determine whether or not the risk management process is effective and also if the methodology is clearly understood by the key groups in the company, including the board and audit committee. Therefore, the internal auditor must be satisfied that the organization's risk management processes address these five key objectives:

1) Risks that arise from business strategies and activities are identified and prioritized.
2) Management and the board set the level of risk acceptable to the organization (that is, an assessment of risk appetite).
3) Risk mitigation or reduction activities are designed and implemented to reduce or otherwise manage risk at acceptable levels.
4) Risk are periodically reassessed on an ongoing basis.
5) Reports are given periodically to the board and management on the results of the risk assessment process.

The IAA needs to assess these five objectives in order to ascertain the adequacy of the risk management processes, which is addressed in all engagements. The auditors need to look vigilantly for signs that might indicate a problem or a cause for concern related to risk management.

Question 12: Which of the following does not address a key objective of the risk management process?

a) Risks that arise from business strategies are identified and prioritized.

b) Risk mitigation (reduction) activities are designed and implemented to reduce, or manage, risk at levels that are acceptable.

c) Review of previous risk evaluation reports by management, external auditors, and other sources.

d) Risk is periodically reassessed on an ongoing basis.

(HOCK)

Gathering Evidence for Assessment

Paragraph 8 of PA 2120-1 provides a list of procedures that the internal auditor should consider during evidence-gathering procedures:

PA 2120-1: Assessing the Adequacy of Risk Management Processes

8. Internal auditors need to obtain sufficient and appropriate evidence to determine that the key objectives of the risk management processes are being met to form an opinion on the adequacy of risk management processes. In gathering such evidence, the internal auditor might consider the following audit procedures:

- Research and review current developments, trends, industry information related to the business conducted by the organization, and other appropriate sources of information to determine risks and exposures that may affect the organization and related control procedures used to address, monitor, and reassess those risks.
- Review corporate policies and board minutes to determine the organization's business strategies, risk management philosophy and methodology, appetite for risk, and acceptance of risks.
- Review previous risk evaluation reports issued by management, internal auditors, external auditors, and any other sources.
- Conduct interviews with line and senior management to determine business unit objectives, related risks, and management's risk mitigation and control monitoring activities.
- Assimilate information to independently evaluate the effectiveness of risk mitigation, monitoring, and communication of risks and associated control activities.
- Assess the appropriateness of reporting lines for risk monitoring activities.
- Review the adequacy and timeliness of reporting on risk management results.
- Review the completeness of management's risk analysis and actions taken to remedy issues raised by risk management processes, and suggest improvements.
- Determine the effectiveness of management's self-assessment processes through observations, direct tests of control and monitoring procedures, testing the accuracy of information used in monitoring activities, and other appropriate techniques.
- Review risk-related issues that may indicate weakness in risk management practices and, as appropriate, discuss with senior management and the board. If the auditor believes that management has accepted a level of risk that is inconsistent with the organization's risk management strategy and policies, or that is deemed unacceptable to the organization, refer to Standard 2600 and related guidance for additional direction.

The assessment of risk is, unfortunately, not always something that can be put into a formula and easily measured. The successful assessment of risk often rests with the professional judgment and experience of the internal auditors and the CAE.

The Standards state that the evidence to support the auditor's assessment of the risk management process is obtained from engagements throughout the year, as well as through other specific engagements. The conclusion is the result of all of the work that the internal auditor performs during this period.

When No Risk Management Process Exists

If an organization does not have a formal risk management process, the CAE must convince the board and senior management to establish one, even if it just an informal set of procedures.

PA 2120-1: Assessing the Adequacy of Risk Management Processes

5. In situations where the organization does not have formal risk management processes, the chief audit executive (CAE) formally discusses with management and the board their obligations to understand, manage, and monitor risks within the organization and the need to satisfy themselves that there are processes operating within the organization, even if informal, that provide the appropriate level of visibility into the key risks and how they are being managed and monitored.

Assessing the Adequacy of Risk Management Processes for Formal Consulting Services

By providing consulting services, the internal auditor adds value to the organization's operations. For example, internal auditing might be asked to assist, establish, or improve risk management processes. Internal auditors should be proactive, particularly when it comes to risk management, but consulting engagements must not impair the auditor's independence or objectivity.

Note: A **consulting service** is defined as advisory and related client-service activities, the nature and scope of which are agreed upon with the client. They are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples of consulting services include counseling, giving advice, facilitation of various activities, and training.

Concerning risk management, internal auditors must utilize knowledge gained from consulting engagements to identify and evaluate significant risk exposures. If auditors identify significant risk exposure or control weaknesses, management must be alerted. In some cases, particularly where there are significant risk exposures, it might be necessary for the internal auditor to communicate directly with the board or audit committee.

As with any assessment engagement, the internal auditor should use professional judgment to

- **Determine the significance of exposures or weaknesses** and the actions taken or contemplated to mitigate or otherwise correct these exposures or weaknesses.
- **Ascertain the expectations** of management, the audit committee, and board in having these matters reported.

Internal auditors need to avoid managing risks during a consulting engagement (Standard 2120.C3) because doing so might result in a negative outcome, which could be perceived as an internal audit failure and irreparably damage the reputation of the IAA.

Standard 2120 – Risk Management

2120.C1 – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

B6. Report on Effectiveness of Internal Control Framework

Responsibility for the internal control system rests with management and the board, and the internal auditor must assist the organization in maintaining effective controls.

Standard 2130 – Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

2130.C1 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

Practice Advisory 2130-1: Assessing the Adequacy of Control Processes

3. The chief audit executive (CAE) forms an overall opinion about the adequacy and effectiveness of the control processes. The expression of such an opinion by the CAE will be based on sufficient audit evidence obtained through the completion of audits and, where appropriate, reliance on the work of other assurance providers. The CAE communicates the opinion to senior management and the board.

Determining the Scope of Coverage and Gathering Evidence

Because internal controls should exist throughout an organization, the potential scope of engagements is extensive. The CAE will need determine which controls are the most critical to be assessed. Areas of the business that have undergone significant changes recently or any parts of the business that have been restructured or recently acquired would require specific attention.

In addition to specific engagements, the internal control system is a part of every engagement that is performed by the IAA. Therefore, the results and evidence from the ongoing engagements will be combined with the evidence from specific internal control assessment engagements to reach the conclusion. Additionally, relevant work may have been performed by other assurance providers during the period. As a result, any work done by other assurance providers will also be considered in the conclusion.

In the course of an engagement, the CAE should make adjustments based on new or unexpected evidence. For example, if an engagement indicates a weakness that had not been considered, additional work should be performed in that area.

Practice Advisory 2130-1: Assessing the Adequacy of Control Processes

4. The CAE develops a proposed internal audit plan to obtain sufficient evidence to evaluate the effectiveness of the control processes. The plan includes audit engagements and/or other procedures to obtain sufficient, appropriate audit evidence about all major operating units and business functions to be assessed, as well as a review of the major control processes operating across the organization. The plan should be flexible so that adjustments may be made during the year as a result of changes in management strategies, external conditions, major risk areas, or revised expectations about achieving the organization's objectives.

5. The audit plan gives special consideration to those operations most affected by recent or unexpected changes. Changes in circumstances can result, for example, from marketplace or investment conditions, acquisitions and divestitures, organizational restructuring, new systems, and new ventures.

6. In determining the expected audit coverage for the proposed audit plan, the CAE considers relevant work performed by others who provide assurances to senior management (e.g., reliance by the CAE on the work of corporate compliance officers). The CAE's audit plan also considers audit work completed by the external auditor and management's own assessments of its risk management process, controls, and quality improvement processes.

7. The CAE should evaluate the breadth of coverage of the proposed audit plan to determine whether the scope is sufficient to enable the expression of an opinion about the organization's risk management and control processes. The CAE should inform senior management and the board of any gaps in audit coverage that would prevent the expression of an opinion on all aspects of these processes.

Evaluating Effectiveness of Internal Control Processes

All the evidence that is collected from ongoing and special engagements, as well as from other assurance providers, needs to be assessed to reach the conclusion.

The key factors to assess are:

- Weaknesses or deficiencies
- Any corrections
- Any improvements
- Significant weaknesses or problems that indicate controls are not working at an acceptable level

Signs of weakness do not automatically mean that internal controls are ineffective. The nature and extent of the weakness, as well as its potential consequences, need to be taken into account when reaching the conclusion.

Practice Advisory 2130-1: Assessing the Adequacy of Control Processes

8. A key challenge for the internal audit activity is to evaluate the effectiveness of the organization's control processes based on the aggregation of many individual assessments. Those assessments are largely gained from internal audit engagements, reviews of management's self-assessments, and other assurance providers' work. As the engagements progress, internal auditors communicate, on a timely basis, the findings to the appropriate levels of management so prompt action can be taken to correct or mitigate the consequences of discovered control discrepancies or weaknesses.

9. In evaluating the overall effectiveness of the organization's control processes, the CAE considers whether:

- Significant discrepancies or weaknesses were discovered,
- Corrections or improvements were made after the discoveries, and
- The discoveries and their potential consequences lead to a conclusion that a pervasive condition exists resulting in an unacceptable level of risk.

10. The existence of a significant discrepancy or weakness does not necessarily lead to the judgment that it is pervasive and poses an unacceptable risk. The internal auditor considers the nature and extent of risk exposure, as well as the level of potential consequences in determining whether the effectiveness of the control processes are jeopardized and unacceptable risks exist.

Report on Internal Control Processes

The report should be provided annually. It should contain the internal auditor's professional judgment about the effectiveness of the control processes and it should also:

- Emphasize the importance of internal controls to the organization
- Describe the nature and extent of the work the internal auditor performed
- Note the work of other assurance providers that was used in formulating the conclusion

Practice Advisory 2130-1: Assessing the Adequacy of Control Processes

11. The CAE's report on the organization's control processes is normally presented once a year to senior management and the board. The report states the critical role played by the control processes in the achievement of the organization's objectives. The report also describes the nature and extent of the work performed by the internal audit activity and the nature and extent of reliance on other assurance providers in formulating the opinion.

B7. Maintain an Effective Quality Assurance and Improvement Program

Note: The topic of the Quality Assurance and Improvement Program (QAIP) is also tested on the Part 1 Exam. The materials presented here are the same as in the Part 1 Textbook. If you have already studied Part 1, we still recommend that you review this material, even though it is already familiar to you.

Note: Because of the very large Practice Advisories for this topic, the full text of these are presented in Appendix C. The full text of the *Standards* and excerpts of the Practice Advisories will be included here as needed.

Another important function of the CAE is to assure the quality of the work performed by the internal audit activity. This assurance is done by establishing a **quality assurance and improvement program (QAIP)**. The QAIP is designed to evaluate whether or not the work of the IAA is in conformance with the definition of internal auditing and the *Standards* and the Code of Ethics. The QAIP also enables the assessment of the efficiency and effectiveness of the IAA and can also identify areas for improvement.

The QAIP includes both **internal** and **external quality assessments** and also **periodic and ongoing assessments**. Each part of the program is designed to help the IAA add value to the organization, improve the organization's operations, and provide assurance that the internal audit activity conforms to the Definition of Internal Auditing and the *Standards*.

Standard 1300: Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Interpretation:

A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement. The chief audit executive should encourage board oversight in the quality assurance and improvement program.

QAIP assessments should include evaluations of:

1) Compliance with the Definition of Internal Auditing, the Code of Ethics, and the *Standards,* including timely corrective actions to remedy any significant instances of noncompliance

2) Adequacy of the IAA's charter, goals, objectives, policies, and procedures

3) Contribution to the organization's governance, risk management, and control processes

4) Compliance with applicable laws, regulations, and other governmental or industry standards

5) Effectiveness of continuous improvement activities and adoption of best practices

6) The extent to which the internal auditing activity adds value and improves the organization's operations

The results of these assessments are provided to the stakeholders of the activity (such as senior management, the board, and external auditors). At least once a year the CAE should report to senior management and the board the results of internal assessments on the efforts and results of the QAIP.

Defining Quality

A common issue that arises with quality program assessments is that "quality" can mean different things to different people. This potential discrepancy is particularly true of service operations such as the internal audit activity. For example, the internal audit department may be conforming to the *Standards*, but such adherence does not necessarily mean that an organization is operating in an effective or efficient manner. To resolve this potential problem, organizations develop **quality circles**.

A quality circle is a group of five to fifteen employees who are intimately familiar with a specific operation and who are brought together to improve quality and productivity. They achieve this objective by studying the operation or problem and then making specific recommendations. Depending on the operation, they may also have the authority to implement recommendations.

Quality circles frequently use benchmarking as a means to improve quality and productivity. **Benchmarking** is the process of a company using the standards set by other companies as a target or model for its own operations. (This is also called **best practices**.) In other words, benchmarking is the process of continuously trying to emulate the best companies in the world. By striving to meet the standards of the best companies, an organization may be able to create a **competitive advantage** by achieving a higher standard than its competitors. Benchmarking can use both financial (such as with profit margins) and nonfinancial (such as the percentage of units produced that are defective).

The benchmark company does not necessarily need to be in the same industry as the company that is striving to raise its standards. If the desired function is the same across multiple industries, then the best company should be used as the benchmark.

Requirements of the QAIP

Standard 1310 – Requirements of the Quality Assurance and Improvement Program

The quality assurance and improvement program **must include both internal and external assessments**.

The CAE is responsible for the implementation, monitoring, and assessment of a quality program. The quality program must include both **internal** and **external assessments**.

These internal and external assessments reassure the company stakeholders (that is, top management, audit committee, and external auditors) about the competency of the services the IAA is providing to the organization. In addition, these assessments can provide a way for the CAE to identify opportunities for improving the operational effectiveness and efficiency of the IAA.

1. Internal Assessments (Standard 1311)

Internal assessments are performed by the internal auditors in the IAA.

The internal audit assessment must include two types of assessments:

1) **Ongoing internal assessments** of performance of the internal audit activity

2) **Periodic internal assessments** of the program through self-assessment or from an independent person within the organization who is familiar with the internal auditing program

Note: The cost of an internal review will be lower than an external review, but the CAE must be cautious because the internal review may not be quite as rigorous as it could be because people inside the organization are involved. In Practice Advisory 1311-1 there is guidance about how the internal assessments should be performed.

Standard 1311 – Internal Assessments

Internal assessments must include:

- **Ongoing monitoring** of the performance of the internal audit activity.
- **Periodic self-assessments** or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

Interpretation:

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

Periodic assessments are **conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the *Standards***.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.

The information in the following two bullet lists come from PA 1311-1 (*Internal Assessments*).

Ongoing Internal Assessments are the conclusions and follow-up actions to assure that appropriate improvements are implemented. Ongoing reviews may be conducted through:

1) Supervision of the internal auditor's work during the course of the audit engagement
2) Checklists, and other means, to provide assurance that processes adopted by the audit activity are being followed
3) Peer review of workpapers by auditors not involved in the engagement
4) Feedback from audit customers and other stakeholders
5) Analyses of performance metrics (for example, cycle time and recommendations accepted)
6) Project budgets, timekeeping systems, audit plan completion, cost recoveries, and so forth

Periodic Reviews should be designed to assess compliance with the activity's charter, the Definition of Internal Auditing, the Code of Ethics, and the *Standards.* Periodic internal assessment may:

1) Include more in-depth interviews and surveys of stakeholder groups
2) Be performed by members of the IAA (that is, self-assessment)
3) Be performed by CIAs or other competent audit professionals currently assigned elsewhere in the organization
4) Include self-assessment and preparation of materials subsequently reviewed by CIAs or other competent audit professionals from elsewhere in the organization
5) Include benchmarking of the IAA practices and performance metrics against relevant best practices of the internal audit profession

A key item to remember in respect to internal assessments is that they are done internally. This provides a number of advantages (for example, internal assessments are less expensive than external ones), but also has a potentially significant disadvantage that the internal audit activity is reviewing itself. This disadvantage is overcome by having external assessments.

Note: An internal assessment that is performed soon before an external assessment can reduce the cost of the external assessment by allowing the IAA to identify and fix issues prior to the external assessment.

2. External Assessments (Standard 1312)

External reviews are opportunities to provide an independent opinion about the quality of the audit activity to the CAE and other various stakeholders of the activity (such as senior management, the board, and external auditors). It is recommended that a qualified, independent person or team outside the organization conduct these external reviews **at least once every five years**.

1312 - External Assessments

External assessments must be conducted at least once every five years **by a qualified, independent assessor or assessment team from outside the organization**. The chief audit executive must discuss with the board:

- The form and frequency of external assessment.
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

Interpretation:

External assessments may be accomplished through a full external assessment, or a self-assessment with independent external validation. The external assessor must conclude as to conformance with the Code of Ethics and the Standards; the external assessment may also include operational or strategic comments.

A qualified assessor or assessment team demonstrates competence in two areas: the professional practice of internal auditing and the external assessment process. Competence can be demonstrated through a mixture of experience and theoretical learning. Experience gained in organizations of similar size, complexity, sector or industry, and technical issues is more valuable than less relevant experience. In the case of an assessment team, not all members of the team need to have all the competencies; it is the team as a whole that is qualified. The chief audit executive uses professional judgment when assessing whether an assessor or assessment team demonstrates sufficient competence to be qualified.

An independent assessor or assessment team means not having either an actual or a perceived conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs. The chief audit executive should encourage board oversight in the external assessment to reduce perceived or potential conflicts of interest.

When the assessment is conducted from outside the organization, it is more independent and not as likely to be biased as an internally generated assessment. Of course, this advantage is offset by the higher cost of the assessment, and so the CAE must carefully decide on the merits of such a process.

Additionally, an external assessment will probably not be able to look at all of the cost/benefit analyses necessary to determine if the IAA is in fact "profitable" to the company. This limitation occurs because the financial information that would be necessary to make such a determination may not be as available to an external assessor as it would be to an internal assessor.

During the review, an external assessor will tend to focus on:

- The adequacy of the internal audit charter
- The goals, objectives, policies, and procedures of the IAA
- Whether or not the work done by the IAA is in accordance with the charter
- Whether or not the work done is in conformance with the Definition of Internal Auditing, the Code of Ethics, and the *Standards*
- The contribution of the IAA to the organization's risk management, governance, and controls
- The methods and work programs of the IAA
- The skills and work performed by the individuals in the IAA
- Whether or not the IAA adds value and improves the operations of the organization

Practice Advisory 1312-1 (*External Assessments*) lays out two approaches for conducting an external assessment:

1) Having a **full external assessment conducted by an external assessor** or **review team**.

2) Having an independent assessor or review team conduct an independent validation of the **internal self-assessment** and the corresponding report that was completed by the internal audit activity.

Ideally, a full external review is preferred, but there may be cases where this is simply not practical. Practice Advisory 1312-2 (*External Assessments: Self-assessment with Independent Validation*) gives some instances where a full external review might not be appropriate or necessary. For example:

- The IAA may be in a business or industry that is subjected to strict regulations and supervision.
- The IAA may be otherwise subject to extensive external oversight and direction relating to governance and internal controls.
- The IAA may have been recently subjected to an external review or consulting services in which there was extensive benchmarking with best practices.
- The CAE may determine that the benefits of self-assessment for staff development and the strength of the internal quality assurance and improvement program currently outweigh the benefits of a quality assessment by an external term.

1) External Assessments (PA 1312-1)

According to PA 1312-1 Paragraph 10, a full external assessment has a very broad scope of coverage of the areas of the IAA. It includes:

- Conformance with the Definition of Internal Auditing, the *Standards*, the Code of Ethics, the charter, plans, policies, procedures and practices.
- Board and senior management expectations of the IAA.
- The integration of the IAA into the organization's governance process, including relationships between key groups.
- The skills and experience of the staff.
- Determination if the IAA adds value and improves the organization's operation.

The preliminary results of the assessment are discussed with the CAE and final results are communicated to the CAE, and perhaps additional officials who authorized the review to take place.

The communication includes:

- An opinion on the IIA's conformance with the Definition of Internal Auditing, the Code of Ethics, and the *Standards*
- An assessment and evaluation of the use of best practices
- Recommendations for improvement
- Response from the CAE that includes an action plan and implementation dates

The CAE must communicate the results of external quality assessments, including details of the planned actions for significant actions, to senior management, the board, and the external auditor. As planned actions are accomplished, this should also be communicated.

2) Self-Assessment with Independent Validation (PA 1312-2)

After the self-assessment has been completed under the direction of the CAE, a draft report, similar to that for an external assessment, is prepared. This draft report should include the CAE's assessment of the IAA's conformance with the *Standards*.

The external assessor then performs sufficient tests of the self-assessment to validate the results and express an opinion on the level of the activity's conformance with the Definition of Internal Auditing, the Code of Ethics, and the *Standards.*

In essence, the independent validation is auditing the self-assessment to make certain that the conclusion reached in the self-assessment is correct.

As part of the independent validation, the external assessor will do the following:

- Review the draft report and attempt to reconcile unresolved issues, if any.
- If the external assessor agrees with the evaluation, he or she might include additional wording to the report as needed, concurring with the self-assessment process and opinion as well as the report's findings, conclusions, and recommendations.
- If the external assessor disagrees with the evaluation, he or she would add dissenting wording to the report, specifying the points of disagreement with it and, to the extent appropriate, with the significant findings, conclusions, recommendations, and opinions in the reports.
- Alternatively, the external assessor may prepare a separate independent validation report (concurring or expressing disagreement, as outlined above) to accompany the self-assessment report.

The **final report of the self-assessment**, validated by an external assessor, will be signed by the self-assessment team and external assessor and be issued by the CAE to senior management and the board.

Note: The individuals who perform the external assessment must be free from any conflicts of interest with the organization. It is the responsibility of the CAE to ensure that the individuals performing the external assessment are **qualified** and **independent**.

Standard 1320: Reporting on the Quality Assurance and Improvement Program

1320 – Reporting on the Quality Assurance and Improvement Program

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

Disclosure should include:

- The scope and frequency of both the internal and external assessments.
- The qualifications and independence of the assessor(s) or assessment team, including potential conflicts of interest.
- Conclusions of assessors.
- Corrective action plans.

Interpretation:

The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the board and considers the responsibilities of the internal audit activity and chief audit executive as contained in the internal audit charter. To demonstrate conformance with the Code of Ethics, and the *Standards*, the results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results include the assessor's or assessment team's evaluation with respect to the degree of conformance**.**

The Quality Assurance and Improvement Program (QAIP) analyzes the work of the IAA and makes recommendations for improvement, if appropriate. Since the CAE is in charge of the IAA, the CAE has the most to gain from the information contained in the assessment reports. Therefore, it is the CAE's responsibility to develop and maintain the QAIP for both external and internal assessments. Specific report functions are discussed below.

External assessments: Upon completing the external assessment, the assessor will send a formal communication to senior management and the board to discuss the assessment's findings. However, preliminary results of the assessment should be discussed with the CAE. The final results are communicated to the CAE with copies sent directly to senior management and the board. Based on the report, the CAE will then need to communicate specific planned actions to be taken concerning significant issues.

Internal assessments: Internal assessments are carried out to assure the CAE that subordinates are complying with the *Standards* and other applicable criteria. It is the CAE's responsibility to ensure that, at least annually, results of the internal assessments, necessary action plans, and their successful implementation are reported to senior management and the board.

Note: In a case where the CAE is grossly incompetent or has been strongly criticized in the report, a copy must also be provided to the audit committee or the board. In most cases, however, the report is provided to the CAE.

When the board is not directly copied on the report, the CAE should forward the report to the board along with the CAE's opinion as to whether or not the activities of the IAA are in compliance with the appropriate standards. If the CAE believes that the activities are in compliance with the standards, they must be able to demonstrate this compliance.

Similarly, the follow-up on the contents of the report (especially when it is an external assessment) is the responsibility of the CAE.

Implementation Guide 1320 provides an example of a rating system that may be used to identify the different levels of conformance.

Implementation Guide 1320

External assessment reports include the expression of an opinion or conclusion on the results of the external assessment. In addition to concluding on the internal audit activity's overall degree of conformance with the *Standards*, the report may include an assessment for each standard and/or standard series. The CAE should explain the rating conclusion(s) to senior management and the board, as well as the impact from the results. An example of a rating scale that may be used to show the degree of conformance is:

- **Generally conforms** – This is the top rating, which means that an internal audit activity has a charter, policies, and processes, and the execution and results of these are judged to be in conformance with the Standards.
- **Partially conforms** – Deficiencies in practice are judged to deviate from the Standards, but these deficiencies did not preclude the internal audit activity from performing its responsibilities.
- **Does not conform** – Deficiencies in practice are judged to be so significant that they seriously impair or preclude the internal audit activity from performing adequately in all or in significant areas of its responsibilities.

QAIP Comparison Table	Internal Quality Assessment	External Quality Assessment
Types of assessments	1) Ongoing monitoring of the performance of the internal audit activity 2) Periodic self-assessments	1) External Assessments 2) Self-assessment with Independent Validation
Form of report	At least annually, results of the internal assessments, necessary action plans, and their successful implementation are reported to senior management and the board.	Preliminary results discussed with CAE Final report sent to Senior Management and Board CAE must provide plan to address deficiencies
Performed by	Members of the IAA and supervised by the CAE	Qualified, independent professionals, or Reviewers from outside the organization
How often performed	Ongoing assessments performed throughout the year. Periodic assessments performed as needed	At least once every 5 years

Standard 1321: Conforming to the Standards of Internal Auditing

1321 – Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"

Indicating that the internal audit activity conforms with the *International Standards for the Professional Practice of Internal Auditing* is appropriate only if supported by the results of the quality assurance and improvement program.

Interpretation:

The internal audit activity conforms with the Code of Ethics and the *Standards* when it achieves the outcomes described therein. The results of the quality assurance and improvement program include the results of both internal and external assessments. All internal audit activities will have the results of internal assessments. Internal audit activities in existence for at least five years will also have the results of external assessments.

The CAE wants to be able to state that the internal audit activity conforms to the *International Standards for the Professional Practice of Internal Auditing.* However, the CAE may use this statement only if assessments provide information that the IAA is in compliance. Providing information about compliance requires an external assessment at least once during a five-year period, along with periodic internal assessments. Both of these assessments have to conclude that the IAA conforms to the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. It is expected that, before any use of the conformance statement, all instances of non-conformance will have been rectified.

Note: There are **only two phrases** that may be used to communicate compliance with the standards: "in conformance with the *Standards*" or "in conformity to the *Standards*." Other phrases may be similar, but these two are the only two that should be used.

Standard 1322: Disclosure of Noncompliance

1322 – Disclosure of Nonconformance

When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

There may be cases in which full compliance is not possible due to the lack of skilled and qualified people, or for other reasons. In the incidences when noncompliance impacts the overall scope of the operation, a **Disclosure of Noncompliance** statement should be made to senior management and the board.

Implementation Guide 1322 provides a list of examples of cases of nonconformance and guidance for the assessment that the CAE needs to do.

Implementation Guide 1322

If an internal audit activity fails to undergo an external assessment at least once every five years, for example, it would be unable to state that it conforms with the *Standards* (see Implementation Guide 1321 – Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"). In such a case, the CAE would evaluate the impact of this nonconformance.

Other common examples of nonconformance may include, but are not limited to, situations in which:

- An internal auditor was assigned to an audit engagement, but did not meet individual objectivity requirements (see Standard 1120 – Individual Objectivity).
- An internal audit activity undertook an engagement without having the collective knowledge, skills, and experience needed to perform its responsibilities (see Standard 1210 – Proficiency).
- The CAE failed to consider risk when preparing the internal audit plan (see Standard 2010 – Planning).

In such cases, the CAE would need to evaluate the nonconformance and determine whether it impacts the overall scope or operation of the internal audit activity. It is also important for the CAE to consider whether, and how much, a nonconformance situation may affect the internal audit activity's ability to fulfill its professional responsibilities and/or the expectations of stakeholders. Such responsibilities may include the ability to provide reliable assurance on specific areas within the organization, to complete the audit plan, and to address high-risk areas.

After such consideration, the CAE will disclose the nonconformance, as well as the impact of the nonconformance, to senior management and the board. Often, disclosures of this nature involve a discussion with senior management and communication to the board during a board meeting. The CAE may also discuss nonconformance during private sessions with the board, one-on-one meetings with the board chair, or by other appropriate methods.

Question 13: The chief audit executive should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness. All of the following are included in a quality program except:

a) Annual appraisals of individual internal auditors' performance.

b) Periodic internal assessment.

c) Supervision.

d) Periodic external assessments.

(CIA Adapted)

Question 14: Formal internal quality assessments of the internal audit activity primarily serve the needs of

a) The board of directors.

b) The internal audit activity's staff.

c) The chief audit executive.

d) Senior management.

(CIA Adapted)

Question 15: As a part of a quality program, internal assessment teams most likely will examine which of the following to evaluate the quality of engagement planning and documentation for individual engagements?

a) Project assignment documentation.

b) Weekly status reports.

c) The long-range engagement work schedule.

d) Written engagement work programs.

(CIA Adapted)

Question 16: Which of the following is the best means of aiding an internal audit activity in determining whether its goals are being met?

a) Having the board periodically review the quality of the internal audit activity's work.

b) Developing measurement criteria to accompany its goals.

c) Scheduling an external assessment every three years.

d) Having external auditors review and evaluate the work of the internal audit activity.

(CIA Adapted)

Answers to Questions

1 b – In any engagement, the deficiencies that are noted by the internal auditor should be reported to management. Choice (c) is incorrect because it may be appropriate for the audit to be conducted if management wants feedback about that at this point. It is not appropriate for the auditor to decide the appropriateness of the audit.

2 d – The four key responsibilities include (1) complies with society's legal and regulatory rules, (2) satisfies the generally accepted business norms, ethical precepts, and social expectations of society, (3) provides overall benefit to society and enhances the interests of the specific stakeholders in both the long term and short term, and (4) reports fully and truthfully to its owners, regulators, other stakeholders, and general public to ensure accountability for its decisions, actions, conduct, and performance.

3 b – Any attestation (coming to a conclusion) and risk assessment work will be done only by the external auditor. The internal auditor may do evaluating and reviewing, as long as it is the external auditor who makes the final conclusion or assessment.

4 a – This is one of the things that the CAE will do in an attempt to coordinate the internal and external audits and reduce the amount of work that is done twice.

5 b – One of the roles of the CAE is to coordinate the work of the internal and external auditors and to reduce the duplication of work.

6 d – By reviewing and testing the other departments' procedures, the internal auditor may reduce the necessary audit coverage of the function or process.

7 a – Oversight of external auditors is the responsibility of the board. The CAE should be responsible for coordinating work between internal and external auditors. However, it is possible that the board could request that the CAE provide input into the performance of the external auditor.

8 b – The policies and procedures in place are dependent upon the size and complexity of the business. Choice (a) is incorrect because policies and procedures alone cannot ensure compliance with performance standards. They only help in the process. The same is the case with choice (c): the policies and procedures only assist in the consistency effort.

9 c – A small IAA can be managed more informally because the staff may be directed and controlled through close daily supervision. In a large IAA, it is generally necessary to have more formal and comprehensive policies and procedures in order for staff to be consistent in the compliance of the *Standards*.

10 a – In order to broaden the staff auditor's knowledge, they need to be exposed to more areas. This is done through the rotation of auditors to different jobs.

11 b – In order to make certain that the internal auditors will be able to perform their duties, the CAE has a responsibility to provide counseling and training to the auditors.

12 c – The review of past risk evaluation reports is not a key objective of the risk management process. The internal auditor must determine that the organization's risk management processes address the five key objectives in order to formulate an opinion on the overall adequacy of the risk management processes.

13 a – Though this would appear to be a function of quality, the annual evaluation of the staff is an HR function. The other choices are all specifically listed as part of a quality program.

14 c – Though the assessments benefit everyone in the organization, it is the CAE who is the primary recipient of the benefit because the CAE is responsible for the performance of the IAA.

15 d – The best way to assess the quality of engagement planning and documentation is to look at the written work programs. The other choices do not give a chance to assess the documentation.

16 b – In order to determine if goals have been met, the goals need to be established and there needs to be a way to measure the achievement of that goal. Without a measurement of some sort, it is difficult to determine if the goal has been achieved.

17 b – It is important to recognize that the question is "Which of the following is least important?" Whether or not the external auditor audited the division last year is the least important of these factors listed. While the fact that it was recently audited is a good thing, it does not relieve the duty that the internal auditors have to monitor this potentially risky engagement on an ongoing basis.

18 c – In all cases, work should be assigned to managers based on their skills and the risk analysis. Personal preferences and travel desires are not the way in which engagements should be assigned.

19 c – While the board would like to think that they can determine what engagements should be performed, they cannot. The budget of the area is not a factor. Of the items listed, only the risk of financial loss or other detrimental results would be considered.

20 b – The addition of new staff is probably less important than the other factors listed. Matters to be considered in establishing the engagement should include: (a) length of time since last engagement; (b)