
CIA Part 2

Practice of Internal Auditing

Version 22.01

HOCK international books are licensed only for individual use and may not be lent, copied, sold, or otherwise distributed without permission directly from HOCK international.

If you did not download this book directly from HOCK international, it is not a genuine HOCK book. Using genuine HOCK books assures that you have complete, accurate and up-to-date materials. Books from unauthorized sources are likely outdated and will not include access to our online study materials or access to HOCK teachers.

Hard copy books purchased from HOCK international or from an authorized training center should have an individually numbered orange hologram with the HOCK globe logo on a color cover. If your book does not have a color cover or does not have this hologram, it is not a genuine HOCK book.

2022 Edition
CIA
Preparatory Program

Part 2

Practice of Internal Auditing

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



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 March 2022

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.

© 2022 HOCK *international*, LLC

No part of this work may be used, transmitted, reproduced or sold in any form or by any means without prior written permission from HOCK *international*, LLC.

ISBN: 978-1-934494-15-8

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.

Dear Future CIA:

Welcome to HOCK *international!* You have made a wonderful commitment to yourself and your profession by choosing to pursue this prestigious credential. The process of certification is an important one that demonstrates your skills, knowledge, and commitment to your work.

We are honored that you have chosen HOCK as your partner in this process. We know that this is a great responsibility, and it is our goal to make this process as efficient as possible for you. To do so, HOCK has developed the following tools for your use:

- **A Study Plan** that guides you, week by week, through the study process. You can also create a personalized study plan online to adapt the plan to fit your schedule. Your personalized plan can also be emailed to you at the beginning of each week.
- **The Textbook** that you are currently reading. This is your main study source and contains all of the information necessary to pass the exam. This textbook follows the exam contents and provides all necessary background information so that you don't need to purchase or read other books.
- **The Flash Cards** include short summaries of main topics, key formulas and concepts. You can use them to review whenever you have a few minutes, but don't want to take your textbook along.
- **ExamSuccess** contains original questions and questions from past exams that are relevant to the current syllabus. Answer explanations for the correct and incorrect answers are also included for each question.
- **A Mock Exam** enables you to make final preparations using questions that you have not seen before.
- **Teacher Support** via our online student forum, e-mail, and telephone throughout your studies to answer any questions that may arise.
- **Videos** using a multimedia learning platform that provide the same coverage as a live-taught course, teaching all of the main topics on the exam syllabus.

We understand the commitment that you have made to the exams, and we will match that commitment in our efforts to help you. Furthermore, we understand that your time is too valuable to study for an exam twice, so we will do everything possible to make sure that you pass the first time.

I wish you success in your studies, and if there is anything I can do to assist you, please contact me directly at brian@hockinternational.com.

Sincerely,

Brian Hock, CIA, CMA
President and CEO

Table of Contents

Part 2 Exam Introduction	1
Box Styles Used in This Book	1
Section I – Managing the Internal Audit Activity	2
1. Internal Audit Operations	3
1A. Policies and Procedures	3
1B. Administrative Activities of the Internal Audit Activity	7
2. Establishing a Risk-Based Internal Audit Plan	12
2A. Identify Potential Engagements	12
2B. Identify a Framework for Assessing Risk	13
Types of Engagements	16
2C. Assurance Engagements	17
1) Risk and Control Self-assessments	17
2) Audits of Third Parties and Contract Compliance	21
3) Quality Assurance Engagements	23
4) Due Diligence Assurance Engagements	26
5) Security Engagements	27
6) Privacy Audit Engagements	28
7) Performance Assurance Engagements	29
8) Operational Assurance Engagements	30
9) Financial Audit Engagements	31
10) Compliance Audit Engagements	37
2D. Consulting Services	39
1) Internal Control Training	43
2) Benchmarking	44
3) Business Process Mapping	46
4) Due Diligence Consulting	46
5) System Development Reviews	46
6) Privacy Consulting	47
7) Design of Performance Measurement Systems	47
8) Internal-Control Testing Consulting Engagements	48
9) Business Process Review/Re-engineering Consulting Engagements	48
2E. Coordinate Internal Audit Efforts with Other Assurance Providers	49
3. Communicating and Reporting to Senior Management and the Board	56
3A. Communicate Annual Audit Plan and Obtain Board Approval	56
3B. Identify Significant Risk Exposures to Report to the Board	56
3C. Report on the Effectiveness of the Organization’s Internal Controls & Risk Management	57
3D. Reporting Key Performance Indicators to the Board	59

Section II. Planning the Engagement	64
A. Establish Engagement Objectives/Criteria and Finalize Scope	67
B. Plan Engagement to Assure Identification of Key Risks and Controls	69
C. Complete a Detailed Risk Assessment of Each Audit Area	70
D. Determine Engagement Procedures and Prepare Work Program	71
E. Determine Level of Resources Needed	76
Section III – Conducting Internal Audit Engagements – Introduction	79
1. Information Gathering.....	79
1A. The Preliminary Survey	79
1B. Checklists and Questionnaires	85
1C. Sampling and Statistical Analysis Techniques	86
2. Analysis and Evaluation	98
2A. Computerized Audit Tools and Techniques (CAAT)	98
2B. Evaluate the Relevance, Sufficiency, and Reliability of Evidence	102
2C. Analytical Approaches and Process Mapping	105
2D. Analytical Review Techniques	110
2E. Working Papers and Documentation	129
2F. Develop Engagement Conclusions	137
3. Engagement Supervision	140
Section IV – Communicating Results and Monitoring Progress.....	143
1. Communicating Engagement Results and the Acceptance of Risk	143
1A. Initiate Preliminary Communication with Client	143
1B. Demonstrate Communications Quality and Elements	143
1C. Communicate Interim Progress	147
1D. Recommendations to Enhance and Protect Organizational Value	148
1E. Engagement Communication and Reporting Process	149
1F and G. Assessing Residual Risk and Acceptance of Risk	155
2. Monitoring Progress and Following-Up	156
Appendix A: Sample Code of Conduct.....	160

Part 2 Exam Introduction

The CIA Part 2 exam, **Practice of Internal Auditing**, is 120 minutes (2 hours) long and consists of 100 multiple-choice questions. For more information about the exams, visit the IIA's website (www.theiia.org).

The CIA Part 2 syllabus has four sections:

- **Section I:** Managing the Internal Audit Activity (20%)
- **Section II:** Planning the Engagement (20%)
- **Section III:** Performing the Engagement (40%)
- **Section IV:** Communicating Engagement Results and Monitoring Progress (20%)

Additionally, the IIA syllabus refers to **proficient** and **basic** cognitive levels:

- **Proficient.** Candidates must exhibit thorough understanding and ability to apply concepts, processes, or procedures; analyze, evaluate, and make judgments based on criteria; and/or put elements or material together to formulate conclusions and recommendations.
- **Basic.** Candidates must retrieve relevant knowledge from memory and/or demonstrate basic comprehension of concepts or processes.

In preparing for the exam, candidates need to read the textbook and use the ExamSuccess software with questions from past exams. Many of the exam topics are very large; therefore, by studying past exam questions candidates can get a feeling for the manner and depth to which a topic is tested.

As a word of caution, you might notice that the terminology used in this book may be different than what you are familiar with from your workplace. Because internal auditing is an internal activity, there are no established or standardized terms that apply in every organization. Keep in mind that the terms used in this book are the terms that appear on the exams, so you should become accustomed to them.

Box Styles Used in This Book

The following box styles used throughout this book indicate material quoted from various IIA sources. Minor changes may have been made to the formatting, but no changes have been made to the content.

Content quoted from the IIA web site appears in light grey boxes with an orange border.¹

Content quoted from the *Standards* or *Implementation Guides* appears in yellow boxes.

Content quoted from the *Practice Advisories* appears in orange boxes.

Note: Quotes may not include the entire section or may include non-sequential sections.

¹ The website is <https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx#mandatory>.

Section I – Managing the Internal Audit Activity

The first section of the Part 2 exam covers **Managing the Internal Audit Activity**, which makes up 20% of the exam. There are three topics discussed in this section:

- 1) **Internal Audit Operations.** The internal auditing activity, like any other business function, has to be properly managed. From an **operational standpoint**, the chief audit executive (CAE) has to make sure that:
 - Planned engagements are carried out in a timely manner.
 - Resources needed to carry out the planned engagements are properly allocated.
 - Results of the engagements are properly communicated to all interested parties.
- 2) **Establishing a Risk-Based Internal Audit Plan.** The CAE has a responsibility to establish risk-based audit plans. While risk is a primary factor in determining which engagements to conduct, it is not the only factor. The internal auditor must also understand how to prioritize engagements.
- 3) **Communicating and Reporting to Senior Management and the Board.** After the engagement plan has been created, it must be approved by the board.

The *Standards* and *Practice Advisories* are excellent resources to assist in your preparation for this section, but you do not need to memorize the specific *Standard* or *Practice Advisory* texts.

Note: Throughout this book, you will see the term **internal audit activity** (IAA) in reference to the internal audit department. You will also see the term **chief audit executive** (CAE) in reference to the head of internal auditing.

Note: Previously, there was a category of recommended guidance called Practice Advisories (PAs). The PAs provided detailed guidance for the application of the *Standards* and were the best practices endorsed by the IIA for applying the *Definition*, *Code of Ethics*, and *Standards*. While the PAs are no longer included in the Recommended Guidance, they are included here where appropriate. The PAs tend to be longer and more detailed than the Implementation Guides and therefore make an excellent tool when preparing for the exam.

Managing the Internal Audit Activity

Standard 2000: Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation:

The internal audit activity is effectively managed when:

- It achieves the purpose and responsibility included in the internal audit charter.
- It conforms with the *Standards*.
- Its individual members conform with the Code of Ethics and the *Standards*.
- It considers trends and emerging issues that could impact the organization.

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

Beyond accomplishing these goals and objectives, the internal audit activity must also be forward-looking, setting the groundwork both for current and future success. This section discusses the strategic and operational roles of internal auditing.

For internal auditing to remain a relevant function within an organization, the management and board must regard the IAA as a value-added activity. In its initial inception, internal auditing simply looked at processes and controls and made judgments as to whether they were effective or not. However, increased pressure for profits and a rapidly evolving business environment has meant that internal auditing is now a much more active, rather than a passive, contributor to a company's overall strategy for success.

1. Internal Audit Operations

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.

1A. 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 size, structure, and complexity of the IAA will determine the necessary extent, depth, and formalization of the policies and procedures. 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 memoranda. 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 organization, the policies and procedures of the IAA 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 and 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

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.

(continued)

- 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.

1B. Administrative Activities of the Internal Audit Activity

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. 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 sufficient and qualified 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 others.

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