PacificCPE

COURSE
60454A

Building AI-Powered Audit Function: Part 2

Once planning wraps up, the real work begins—and AI has a growing role to play throughout fieldwork and reporting. This course walks through how intelligent automation applies to internal controls assessment, substantive and analytical procedures, and post-audit management. You'll gain a clearer picture of where technology can reduce manual effort, improve consistency, and strengthen documentation. Whether you're managing a team or doing hands-on audit work, this course offers actionable insight into building a more efficient, technology-enabled engagement process.

CREDIT HOURS 2 | FIELD OF STUDY BUSINESS | EXAM QUESTIONS 10

Start Course ↓ | Final Exam Copy ↓

Assignment

- Study the full course materials included here.
- Complete the review questions after each chapter.
- Answer 10 final exam questions.
- Final exam is scored immediately, 70% or better passes.
- Certificate of completion is available in your account.
- Failed exams can be retaken free of charge.

Course Objectives

- Identify the four principles of risk assessment as defined by the COSO 2013 framework.
- Recognize the standard tools of audit inquiries.
- Identify the characteristics of the maturity models for audit firms.

Copyright Notice

© 2026 Pacific CPE, LP. All rights reserved.

The materials in this course — including the text, illustrations, exhibits, examples, exam questions, and review questions — are the copyrighted property of Pacific CPE, LP. No portion of this course may be reproduced, stored in a retrieval system, distributed, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Pacific CPE, LP, except for the personal, non-commercial use of the registered learner.

Pacific CPE, LP grants the registered learner a single-seat, non-transferable license to access this course for the purpose of completing the associated continuing professional education credit. Account credentials may not be shared. Group access requires a separate enterprise license.

This course is provided "as is" for educational purposes. While Pacific CPE, LP makes a reasonable effort to ensure the content is current and accurate, the materials should not be relied upon as a substitute for professional advice. Pacific CPE, LP disclaims all liability for any error, omission, or loss arising from the use of, or reliance on, the course content.

Questions about reproduction, licensing, or use of these materials should be directed to support@pacificcpe.com.

Publication Date: May 2026

TABLE OF CONTENTS

CHAPTER 01

Automating Internal Controls Assessment 5

1.01 Automating Internal Controls Assessment 6

1.02 Automated Control Environment 8

1.03 ***Figure 9.2 Automated Environment Evaluation*** 9

1.04 Control Activities 19

1.05 Automated Monitoring 23

1.06 Control Risk And Next Steps 25

Test Your Knowledge 26

CHAPTER 02

Automated Procedures 30

2.01 Accumulating Evidence 32

2.02 ***Figure 10.1 The Audit Automation Map*** 34

2.03 ***Figure 10.2 Audit Procedures And Testing*** 34

2.04 Automated Reconciliation 38

2.05 Automated Journal Entries 39

2.06 Putting It All Together 40

Test Your Knowledge 42

CHAPTER 03

Reporting And Post-Audit Management 44

3.01 ***Figure 11.1 The Audit Automation*** 44

3.02 Post-Audit Management 46

3.03 ***Figure 11.2 Data Classes*** 47

3.04 Challenges In Achieving The Maturity 52

3.05 Building An In-House Architecture For An Audit Firm (Or Internal Audit) 53

3.06 A Few Important Things To Consider 53

Test Your Knowledge 55

Final Exam Copy 61

Glossary 57

Index .....

Chapter 1: AUTOMATING INTERNAL CONTROLS ASSESSMENT

Chapter Objective

After completing this chapter, you should be able to:

- Identify the four principles of risk assessment as defined by the COSO 2013 framework.

Recently, PricewaterhouseCoopers (PWC) settled two major high-profile malpractice lawsuits in the UK. In the two cases (MF Global and Taylor Bean & Whitaker), the allegations against PwC indicated that the plaintiffs expected the audit firm to go beyond the management assertions and include management decision-making in the scope of the audit.

Another firm, travel company Thomas Cook, was also audited by PwC between 2007 and 2016. Between 2017 and the collapse of Thomas Cook in 2019, Ernst & Young (EY) took over as the auditors. Upon investigation it was discovered that PwC provided remuneration advice to Thomas Cook, and that while both firms, PwC and EY, had information about the deep problems facing Thomas Cook, both gave clean audit reports to Thomas Cook. Commenting on audit failures, Bob Moritz, global chairman of PwC, said, “The expectations of the market is above the regulatory requirement. When big failures happen, it is not necessarily an audit failure. The controls might be appropriate, but the continuation of the business, its financial position and long-term sustainability can still be in question” (Kinder, 2019).

- Would it be possible for PwC and EY to gain deeper insights about their clients’ material weaknesses in internal controls, even before an audit is launched?
- Is it possible for PwC to develop greater insights into the business operations of a firm?
- How can management, board, and the audit committee receive continuous evaluation of audit controls?
- How can new and emerging risks be identified and mitigated?
- Can audit expand its scope without incurring greater cost?

Answers to these and many other similar questions greatly depend upon the automation strategy of internal controls. In this chapter we develop a comprehensive strategic approach to automate internal controls assessment and audit.

AUTOMATING INTERNAL CONTROLS ASSESSMENT

Unlike the inherent risk, which is embedded in the strategic choices made by the firm due to its business model, industry, etc., the internal controls risk is a function of actions of management teams and boards. In 1993, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) presented a framework, which has become the standard for internal controls. COSO defined internal control as (COSO, 2013):

> Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three categories:
>
> - Reliability of financial reporting.
> - Effectiveness and efficiency of operations.
> - Compliance with applicable laws and regulations.

The COSO standard is based upon three objectives – effectiveness and efficiency of operations, reliable financial reporting, and compliance with laws and regulations. This means that the controls exist to achieve the three objectives. The first objective of effectiveness and efficiency of operations is based upon the corporate objectives as determined by the board and the senior leadership teams and constitute the primary goals that the firm must achieve to fulfill its strategy. The second objective of reliable financial reporting is based upon the assertions made by the firm and the numbers and disclosures reported about the financial performance of the firm. The third objective aims to ensure that the firm abides by the laws and regulations applicable to its business and industry.

For each objective, internal controls are built with the following five components: (1) control environment, (2) risk assessment, (3) control activities, (4) monitoring, and (5) information and communication. Each of the components is supported by principles and, as of 2013, 17 principles are part of the framework.

At this point it is important to note that audit automation can be viewed as a combination of tool-driven (where auditors don't rely upon any human-provided information) and human-based evidence collection. Auditees provide information in the form of data requests, access to systems and information, and responses to specific informational requests in the form of reports, questions and answers, forms, etc.

Automated tools do not rely upon human-provided information and instead they directly access evidence from the source such as data, the databases, and the applications. Human-based evidence collection relies upon surveys and questionnaires. Artificial intelligence (AI) has a role to play in both areas and while this chapter primarily focuses upon the tools, the human-centric surveys and questionnaires automation involves the ability to generate and analyze surveys and questionnaires. We will cover human surveys and questionnaires in a following chapter.

Previous studies using AI methods of self-organizing maps (SOMs) based clustering techniques have suggested that internal controls form a complex nexus of capabilities where a firm may have one or more strong components (e.g., control activities and monitoring) but not all areas. Furthermore, firms may have strong components for one objective but not all three (Länsiluoto et al., 2016). Recall that there are three objectives: effectiveness and efficiency of operations, reliable financial reporting, and compliance with laws and regulations. To design an automated system, our strategy needs to cover all three COSO objectives and the related five components.

When designing an automated internal control system, our broad strategy is as follows:

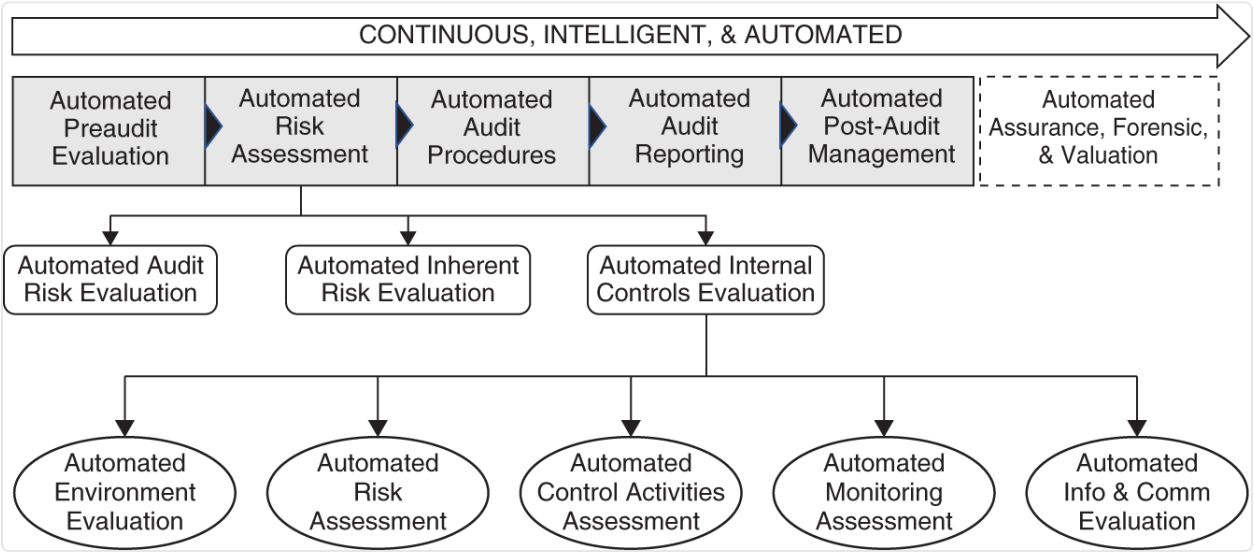
- Approach the problem as an integrated interaction of various agents (both deterministic and stochastic).
- Use a variety of technologies, including process mining, machine learning, RPA, and expert systems.
- Check for internal control weaknesses that are embedded in the design of the client firm and hence create an environment ripe for errors and frauds, and to predict if a fraudulent activity is taking place.
- Use integrated internal controls system to perform continuous assessment.
- Apply integrated internal controls system to create an exhaustive assessment (i.e., the entire population is analyzed vs. a sample).
- Evolve and grow the system with business.

Automated risk assessment is composed of three areas: audit risk evaluation, inherent risk evaluation, and internal controls evaluation. Audit risk is a function of inherent risk, controls risk, and detection risk. In the previous chapter we covered the inherent risk. Inherent risk is the risk that exists in the absence of any internal controls. Internal controls risk happens when a firm does not have proper internal controls to manage and control the inherent risks. The lack of controls can be due to a firm’s practices or design. It can happen intentionally or unintentionally. Internal controls can be evaded, overridden, or bypassed when management engages in fraud. Thus, while inherent risk is embedded in the nature of the business, internal controls risk is very

much a product of how a firm is managed. When auditors observe gaps in internal controls, they are supposed to increase their substantive procedures to reduce or minimize the chances of misstatement.

As shown in Figure 9.1, to automate the internal controls evaluation, we follow the COSO model and break it down into five capability areas of automated environment evaluation, automated risk assessment, automated control activities assessment, automated monitoring assessment, and automated information and communications evaluation. Each of the areas is automated with various agents that work in a coordinated and collaborative manner to achieve total automation.

FIGURE 9.1 AUTOMATION OF INTERNAL CONTROLS EVALUATION

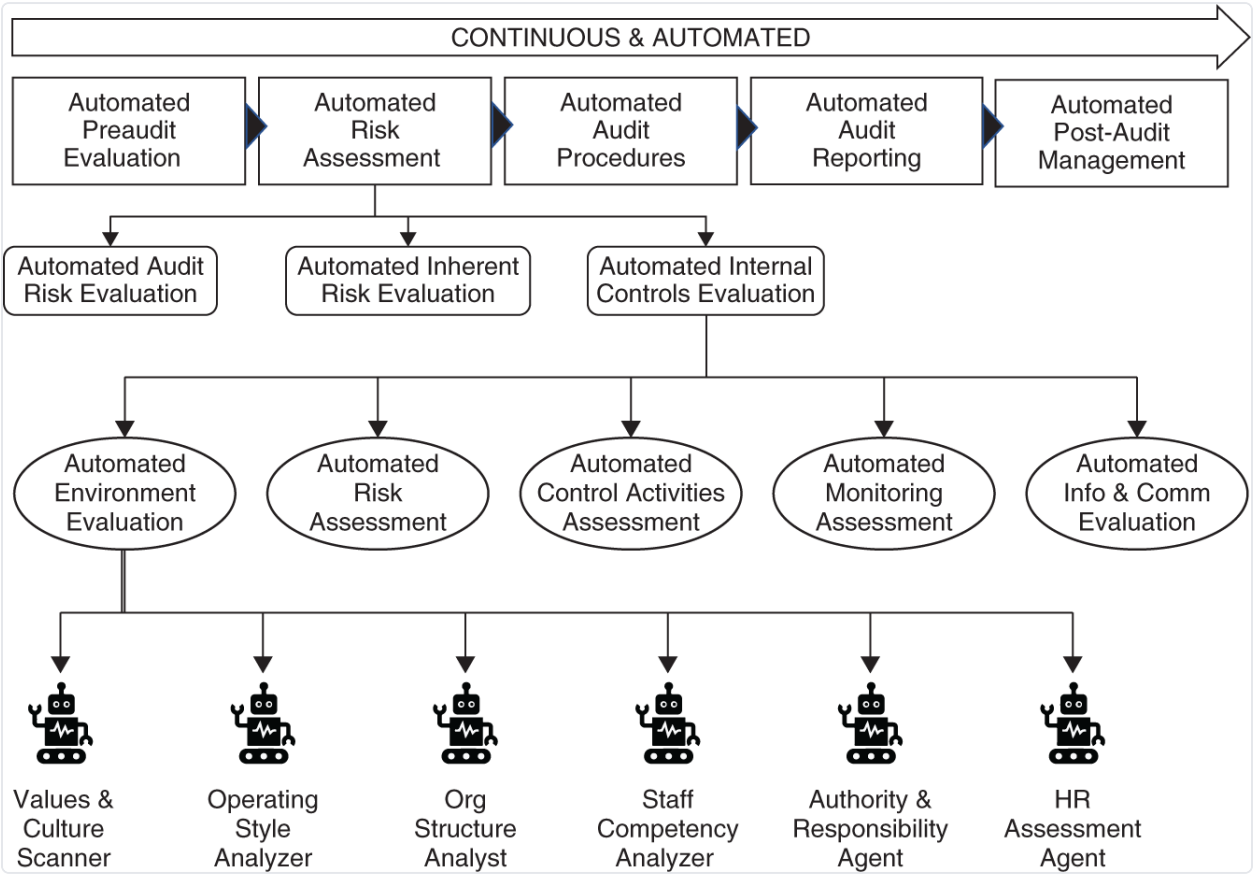


AUTOMATED CONTROL ENVIRONMENT

The principles of control environment (Figure 9.2) are

- The organization demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

FIGURE 9.2 AUTOMATED ENVIRONMENT EVALUATION



The assessment of control's environment is an inquiry about the patterns of human values and actions. For example, the word "organization" in the first principle implies there are one or more humans who demonstrate commitment to integrity and ethical values. Commitment is a cognitive construct and manifests via human communications and actions. At this time, we do not have reliable technology to observe what transpires in people's minds, but we can observe patterns about humans and human behavior that can provide us information about their mental or cognitive constructs. For example, speech, choice of words, gestures, and body language (including physiological information) can give us clues about the cognitive constructs. These could be general – or specific to a domain. For example, a general assessment can reveal the personality of a person and can be classified as aggressive versus passive. A specific assessment will search for speech (verbal, written) for values.

Thus, designing a system to assess the controls environment will be composed of:

- An agent that gauges the cognitive constructs of management teams (values, ethics, personalities, integrity, and others).

- An agent that gauges the cognitive constructs of management teams and boards specific to the task structure (e.g., values or personality types to function during a specific challenge for a firm or for the specific objective of financial reporting).
- An agent that determines if the board has undertaken the responsibility of the oversight, structures, responsibilities, and authorities.
- An agent that determines that Board separation with the management team, and exercises oversight over the development and performance of internal controls.
- An agent that measures and provides feedback on the firm's commitment to attract, develop, and retain competent individuals.
- An agent that evaluates accountability.

The above agents, once trained, form the integrated control environment system.

Integrity, Ethics, Personality, and Values

This system was explained in the audit preplanning chapter. We will reexamine it here from an internal (vs. external) system perspective. The auditor has access to significantly more documents internally than analyzing a company from the outside. In today's world, pictures, voice, and video data can also be requested and obtained. The core version of this system is natural language processing, which analyzes the written communications of the management team and the board members to search for words that signify integrity, ethics, values, and personality. As previously mentioned, this approach has been deployed to study the fraud risk from linguistic and vocal patterns of earnings calls (Throckmorton et al., 2015) as well as from documents (Management's Discussion and Analysis (MD&A) section of the Form10-K) (Humpherys et al., 2011). The agent is expected to evaluate how much of management and board communication is applied to values and ethics. The input documents used for these analyses may include reports, messages, board meeting minutes, emails, and other communications. Using that as input, a classification engine is deployed that, based upon words, evaluates the presence, depth, and frequency of ethics and integrity-related discussions in the normal course of business operations.

Another, more complicated, way is to get data from communications of leaders of a firm that engaged in fraud and study the patterns of their expression versus the patterns of the firms that provided proper returns and met the fiduciary obligations.

Board of Directors