

AUDIT REWIRED: TECHNOLOGY, EVIDENCE, AND THE MODERN ENGAGEMENT



● CPE Today • 2027 K2 Technology Conferences

Audit Rewired: Technology, Evidence, and the Modern Engagement

Audit Technology

June 16, 2027

Live online • Central Time

8 CPE

Credits, proposed

1 day

Group Internet Based

Proposed Agenda

Day One

8:00 AM – 9:40 AM

The Auditor's Tech Stack: What Changed and What It Means for Evidence

Audit · Intermediate · 2 CPE

Covers full-population testing, continuous auditing, and the tools now sitting between the auditor and the client's data. Explores how the shift reshapes planning, materiality thinking, and where audit effort goes when sampling stops being the constraint.

- Analyze the transition from sample-based testing to full-population analysis and its impact on audit risk models.
- Evaluate how continuous auditing tools change the timing and nature of evidence collection throughout the fiscal year.
- Identify the shifts in materiality considerations when every transaction is visible to the audit team.
- Assess the changing requirements for professional skepticism when relying on automated data intermediaries.

Prerequisites: Experience with standard financial statement audit procedures and basic familiarity with data analysis concepts. · Advance preparation: None

9:40 AM – 9:50 AM

Break

9:50 AM – 11:30 AM

CHOOSE ONE OF 2 SESSIONS

Excel and Power Query for Audit Testing

Computer Software and Applications · Basic · 2 CPE

Most audit testing still starts the same way: someone exports data from the client's accounting system, spends an afternoon cleaning it up in Excel, and repeats the whole process next quarter or next year. Power Query ends that cycle. It records every cleanup step so the same preparation runs again with a single refresh, no matter where the data came from. This session shows how to use Power Query to prepare...

- Import and clean audit data into a refreshable Power Query table
- Apply Power Query steps to test a journal entry population for gaps, duplicates, and unusual entries
- Perform a three-way match by merging purchase order, receiving, and invoice data
- Apply Benford's Law and stratification to identify transactions for further testing

Prerequisites: None. A basic working knowledge of Excel is recommended. · Advance preparation: None

Auditing Automated and Cloud Environments

Audit · Intermediate · 2 CPE

Examines testing when the process runs itself, including service accounts, segregation of duties, change management over automations, SOC reports, and evidence for controls nobody performs.

- Identify the unique risks associated with service accounts and automated system permissions.
- Evaluate the sufficiency of SOC 1 Type II reports when assessing third-party cloud environments.
- Design audit procedures to test automated controls that function without manual oversight.
- Analyze change management logs to ensure the integrity of automated financial calculations.

Prerequisites: A basic understanding of IT General Controls and experience performing substantive testing in a standard ERP environment. · Advance preparation: Review the AICPA standards regarding SOC 1 reports and internal control over financial reporting for cloud-based systems.

11:30 AM – 12:20 PM

Lunch

12:20 PM – 1:10 PM **CHOOSE ONE OF 2 SESSIONS**

Client Data Extraction: Getting Usable Files Out of the ERP

Information Technology · Intermediate · 1 CPE

Covers requesting extracts that work, validating completeness against control totals, and handling difficult exports such as 90-column crosstabs.

- Identify the specific technical requirements to include in a data request to ensure exports are compatible with audit software.
- Apply validation techniques to confirm that extracted datasets align with the general ledger and control totals.
- Determine strategies for converting complex report formats, such as wide crosstabs, into flat files suitable for testing.

Prerequisites: Experience with basic audit data requests and a working knowledge of spreadsheet software. · Advance preparation: None

ITGCs for the Non-IT Auditor: Access, Change, and Cloud

Audit · Intermediate · 1 CPE

Covers what to ask, what to look at, and what a SOC 1 report does and does not cover.

- Identify the three core domains of Information Technology General Controls that impact financial statement assertions.
- Evaluate the scope of a SOC 1 report to determine which user control considerations the audit team must test manually.
- Draft targeted inquiries for client IT personnel regarding logical access and change management procedures.
- Distinguish between effective ITGCs and manual workarounds when system-generated evidence is unreliable.

Prerequisites: A basic understanding of internal control concepts and experience performing financial statement audits. · Advance preparation: None

1:10 PM – 1:20 PM Break

1:20 PM – 2:10 PM **CHOOSE ONE OF 2 SESSIONS**

Verification Under Attack: Confirmations, Deepfakes, and Engagement Fraud

Audit · Intermediate · 1 CPE

Covers electronic confirmation platforms, identity verification when video calls are no longer proof, and fraud patterns aimed at audit procedures.

- Identify common vulnerabilities in electronic confirmation platforms that fraudsters exploit to intercept or forge evidence.
- Recognize the technical indicators of deepfake audio and video during remote client inquiries and management interviews.
- Evaluate the effectiveness of multi-factor identity verification protocols within the context of a modern audit engagement.
- Assess how social engineering tactics have evolved to target the specific workflows of external audit teams.

Prerequisites: General familiarity with electronic confirmation platforms and remote audit evidence standards. · Advance preparation: Review current firm policies regarding identity verification for remote client contacts.

Securing the Audit Firm: Client Data, Portals, and Field Devices

Information Technology · Intermediate · 1 CPE

Covers encryption, MFA and passkeys, portal hygiene, laptops at client sites, and incident response plans for lost workpaper files.

- Identify the primary security vulnerabilities associated with mobile audit devices and client-site connectivity.
- Compare the effectiveness of multi-factor authentication methods including passkeys and hardware tokens.
- Establish a protocol for client portal maintenance and user access reviews to minimize data exposure.
- Outline the essential components of an incident response plan for lost or stolen engagement files.

Prerequisites: A basic understanding of audit engagement workflows and common file-sharing tools. · Advance preparation: None

2:10 PM – 2:20 PM Break

2:20 PM – 4:00 PM AI in the Audit File: Tools, Limits, and Evidence Standards

Audit · Intermediate · 2 CPE

Covers where AI helps with document review, contract extraction, and anomaly identification, alongside standards regarding explainability, review responsibility, and relying on tool output.

- Identify specific use cases where AI tools improve the accuracy of contract extraction and document review.
- Determine the documentation requirements for AI-generated evidence to satisfy professional standards.
- Evaluate the limits of algorithmic anomaly detection when performing risk assessment procedures.
- Explain the practitioner's responsibility for reviewing and verifying the output of automated tools.

Prerequisites: A working knowledge of current GAAS and familiarity with standard electronic workpaper documentation practices. · Advance preparation: None

All times Central Time. Proposed agenda — sessions, times and credits may change before the conference.

Registration details, final credits and NASBA disclosures are published on the conference page.

<https://www.cpetoday.com/conferences/2027/audit-rewired>

