AUDITBOARD

CHECKLIST

Audit Evidence Collection Checklist

Collecting evidence is one of the most important elements of any audit, but it can cause confusion, frustration, and even regulatory violations if the documentation is not handled properly. While IIA Standard 2330 describes good evidence as "sufficient, reliable, relevant, and useful information to achieve the engagement's objectives," auditors also have to consider how to request, collect, and properly store the documentation. The content, organization, and format of workpapers may vary by organization and the nature of the engagement, however, it is important to achieve documentation consistency by applying best practices throughout the audit.

The checklist below includes three sections with best practices for handling evidence during different stages of the audit. Depending on your industry, you may work with both hard copies of files or electronic files. We have included recommendations for both scenarios, as well as tips for those working in a hybrid environment.

Requesting and Tracking Evidence

Requesting and tracking the status of evidence manually can be a time-intensive exercise.
Be specific when creating your tracker or use purpose-built software for the task.

- □ Identify the appropriate, reliable source for audit evidence.
- □ Decide if the evidence can be self-collected or if you will need assistance.
- □ If evidence cannot be obtained internally, determine if an external organization or third party may provide the evidence.
- □ Be specific to request evidence within date ranges in line with audit scope.
- □ Clearly communicate which data to include if the evidence is extracted from a system.
- □ Log all relevant data regarding the request.
    - □ Document name.
    - □ Description.

    - □ Contact name for the request.
    - □ Time and date sent.
    - □ Follow-up attempts.
- □ Consider jurisdictional restrictions related to data and document movement across borders.
- □ Request all screenshots to include date and timestamps.
- □ Files should be sent through approved, protected channels with encryption as needed.

Gathering and Handling Evidence

Consider the chain of custody and data security when gathering and handling either hard copy or digital evidence.

Hard Copy Evidence

- □ Pick up original documents and maintain custody.
- □ Keep documents well organized.
- □ Do not leave documents in plain view and practice maintaining a clean desk.
    - □ Protect data in open office environments.
    - □ Apply data protection to the home office as well.
- □ Store hard copy documents (original and copies) in locked drawers.
- □ When working with hard copy originals, scan or copy the documents, so these are not compromised.
- □ Redact or return any documents with personal identifiable information (PII) that are not needed as evidence.
- □ Document the methods used to gather the evidence with enough detail to facilitate reperformance.

Digital Copy Evidence

- □ When using audit management software, deliver digital evidence directly to the audit.
- □ Do not leave documents open and unattended and practice maintaining a clean desktop.
    - □ Protect data in open office environments and in your home office as well.
    - □ Consider using privacy screens for laptops.
    - □ Do not work with sensitive data on unsecured wi-fi.

- □ Data should be encrypted in transit and at rest (stored in a database).
- □ The database should be backed up, encrypted, and stored offsite in case of disaster.
- □ Evidence in the audit should be restricted to the audit team and administrators.

Using and Disposing of Evidence

When the audit is finished, make sure the final evidence is scanned into the file, originals are returned, and copies are destroyed appropriately.

- □ Update the tracking sheet/system.
- □ Evaluate the information received to determine if it is accurate and complete.
- □ Reference the evidence in context within the working papers.
- □ Remove any documents that were not needed and not referenced from the audit file.
- □ Return original documents and destroy any copies that do not need to be retained for evidence.
- □ Note if audit evidence is placed on a legal hold requiring retention.
- □ Destroy files according to the audit data retention policy (physical and digital copies).

Support Audit Evidence Collection with Technology

While managing the process manually with spreadsheets and following up through email is possible, we have more effective methods available to us today. Technology makes a huge difference in audit evidence collection and management, especially when working in a hybrid environment. Audit management systems include evidence request and management features to facilitate creating, sending, and following up on requests. Following the best practices outlined in the checklist above and enabling the process with technology will improve your ability to collect, gather, and use the documentation in the most effective way possible.