Audit Evidence Refresher

Audit evidence supports the conclusions of an auditor during the audit process. It attests that management follows the right procedures to account for the internal controls within the IT environment. When audit evidence is thought of, usually the first two ideas that come to mind are professional skepticism (not to take things at face value) and paying attention to detail.

Audit evidence is a component of the audit program execution process, which starts with audit objective identification, control selection, documentation of audit procedures (test of controls) and audit evidence evaluation, as depicted in figure 1.

The quality of audit evidence is determined by its relevance, reliability and sufficiency. Relevancy relates to applicability of the evidence. For instance, if the evidence is for the period under review (e.g., year-end), then when receiving documents, it is imperative to review the contents and pay attention to the dates. One should also verify the source of the information, and if there are any signatures, one should inquire who signed off. Reliability, simply put, is how trustworthy the evidence is. Written information is more reliable than oral, and original documents are more reliable than photocopies. Sufficiency refers to how well the evidence addresses the control activity in its entirety. For example, when testing whether password controls in a Windows 2003 server are set to be strong, reviewing only the password policy (e.g., minimum password length, minimum password age in days) might not be sufficient evidence for this control because although password policy is set at the server level, the system administrator has rights to change password settings for each user. Some of the changes that can be made include setting the user to access the network without a password or setting the user's password to never expire. Such changes will take precedence over the policy set at server level. Therefore, apart from the review of the password policy, the information systems (IS) auditor should additionally review:

- Users without passwords
- Users whose passwords have been set to never expire
- Users who have not changed their passwords or logged on in days exceed the company's policy for password change, which is intended to ensure that evidence is gathered sufficiently to address the control.

Different types of audit evidence are gathered during the audit process, for example:

- Inquiry—Inquiry alone is regarded as the least creditable audit evidence. This is especially true if the source of the information is from the auditee who performs or supervises the function about which one is inquiring. If inquiry is the only way to get the evidence, it is advisable to corroborate the inquiry with an independent source. If one is auditing proprietary software and the IT officer has no access to the source code and cannot demonstrate from the system configurations that there were no upgrades carried out in the year under review, one can corroborate the inquiry with the users of the applications. Although inquiry is the least creditable when carrying out control adequacy testing, it is deemed sufficient during the planning stage.

Ookeditse Kamau, CISA, CIA, has more than five years of experience in IT audit, and has worked as a senior IT auditor at Deloitte. She recently joined the Office of Auditor General Botswana, where she is working as principal auditor—IT audit.
• **Confirmation**—Audit evidence that is from an external independent source is more creditable than evidence from an internal source. Most financial auditors confirm balances (e.g., creditor’s balances and debtor’s balances) by sending out confirmation letters to external independent sources such as banks and vendors. However, in the majority of IT audits, audit evidence is derived from the system configurations. Configurations obtained by an auditor through observation of the system or via a reliable audit software tool are more reliable than data received from the auditee.

• **Inspection of records**—The reliability of the records depends on the source. Information obtained directly from the system is more reliable than information obtained from the system and then customized by the auditee. For example, most system administrators would rather purge backup status results every three months due to system capabilities. The intention is to free up server space. They usually record the backup results in a spreadsheet that they retain to show that the control has been operating throughout the year. An example of such a form is depicted in figure 2.

<table>
<thead>
<tr>
<th>Day</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Successful</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>Failure</td>
<td>The files that failed to back up were for user folders and, therefore, have no implication.</td>
</tr>
<tr>
<td>3</td>
<td>Successful</td>
<td>None</td>
</tr>
<tr>
<td>4</td>
<td>Successful</td>
<td>None</td>
</tr>
<tr>
<td>5</td>
<td>Successful</td>
<td>None</td>
</tr>
</tbody>
</table>

Tasked performed by: BK
Task reviewed by: RS

Figure 2—Example of a Control Operation Form

The information in figure 2 is less reliable than if the system administrator had saved the results in PDF format in a folder and recorded the data only for monitoring purposes. Using figure 2 would enable confirmation of the recordings.

• **Inspection of tangible assets**—This type of evidence involves verifying the existence of an asset and the condition of the asset. It is important to record the asset name or model, serial number, or product ID, and compare it to the asset register.

• **Observation**—It is suggested that observation should be carried out by two auditors. This is to corroborate what the auditor observed and to avoid instances in which management refutes the findings of the observation. In addition, observation is key in establishing segregation of duties. When auditing, where possible, the auditor should spend some time with the auditees. This will afford the auditor the opportunity to see exactly what is happening, not what should happen.

• **Reperform**—This form of audit evidence involves verifying an activity by reperforming the procedures carried out. For example, an auditor could confirm that the system can successfully recover the backup by observing system administrators as they reperform the recovery procedures and recording the results. This form of audit evidence can be used when verifying the adequacy of a control.

• **Recalculation**—This form of audit evidence is reliable because the auditor reaches the same conclusion as the auditee by independently carrying out the calculation. It is important for the auditor to confirm the calculation formula where possible with an external party (e.g., using a government web site to verify pay-as-you-earn [PAYE] calculations).

• **Scanning**—This form of audit evidence involves searching for large or unusual items to detect error. For example, if there is a maximum or minimum loan amount, one can scan through the loan book for amounts outside the stated range.
TECHNIQUES OF GATHERING AUDIT EVIDENCE

The following are possible techniques for gathering audit evidence:

- **Interviews**—This is an interactive process of gathering data by asking the IS personnel open and closed questions. It is important to determine the right person to interview who has knowledge of the process of the area being audited.

- **Questionnaire**—This is a process of gathering data by allowing the IS personnel to answer predetermined questions. This technique is usually used to collect data during the planning phase of the audit. Information gathered through this process has to be corroborated through additional testing.

- **Benchmarking**—This is a process of comparing an IS department against a similar organization or a well-accepted standard in the industry. Examples of benchmarking evidence include, but are not limited to, comparisons of ITIL process maturity framework (PMF) reports, COBIT® maturity model assessments and the newly introduced COBIT® Assessment Programme reports.

- **Data interrogation**—This is a process of analyzing data usually through the use of computer-aided audit tools (CAATs). Generalized audit software can be embedded within an application to review transactions as they are being processed, and exception reports showing variances or anomalies are produced and used for further audit investigations. The most commonly used CAATs method involves downloading data from an application and analyzing it with software such as ACL and IDEA. Some of the tests include journal testing, application input and output integrity checks (e.g., duplicate numbers), gaps on invoices/purchase orders, and summarization of vendors by amounts paid.

- **Extraction of system parameter**—This is a process of reviewing system configuration and user account details through the use of manual or utility tools/scripts, which are available either freely online, developed in-house or obtained off the shelf on the market. The available software includes, but is not limited to, Microsoft Baseline Security Analyzer (free), Dumpsec (free), Sekchek, IDEA examiner, ACL CaseWare and in-house-developed visual basic scripts. Alternatively, the IS auditor can read system manuals for the system being audited for guidance on how to retrieve system configurations and user accounts manually. For example, to get administrator access on a Windows 2003 server, the IS auditor would follow this procedure: Start > administrative tools > active directory users and computers > built in > select administrator > right click > select properties > select member.

SAMPLING

Sampling is an audit procedure that tests less than 100 percent of the population. There are different types of sampling methods that an IS auditor can apply to gather sufficient evidence to address the audit objectives and the rate of risk identified. Sampling methods can be statistical or nonstatistical. Statistical sampling involves deriving the sample quantitatively. The statistical methods commonly used are random sampling and systematic sampling. Nonstatistical sampling involves deriving the sample qualitatively. Commonly used nonstatistical methods are haphazard and judgmental sampling.

The sampling size applied depends on the type of control being tested, the frequency of the control and the effectiveness of the design and implementation of the control.

TYPE OF CONTROLS AND SAMPLE SIZE

The following are the two types of controls:

- **Automated controls**—Automated controls generally require one sample. It is assumed that if a program can execute a task—for example, successfully calculate a car allowance due based on a base percentage of an employee’s salary—and the program coding has not been changed, the system should apply the same formula to the rest of the population. Therefore, testing one instance is sufficient for the rest of the population. The same is true for the reverse; if the system incorrectly calculates the allowance, the error is extrapolated to the rest of the population.

- **Manual controls**—Depending on which sampling method an IS auditor uses to calculate the sample size, the following factors should be taken into consideration to determine the sample size:

1. Reliance placed on the control
2. The risk associated with control
3. The frequency of the control occurrence

Examples of manual controls include review of audit log monitoring, review of user authorization access forms, and review of daily IT procedures, server monitoring procedure
and help-desk functions. Figure 3 provides examples of IT controls, the technique that can be used to gather evidence and the sampling method that can be used.

**CONCLUSION**

Quality evidence collected during the audit process enhances the overall quality of the work performed and significantly reduces audit risk. Failure to collect quality evidence may result in the auditor or company facing litigation, loss of reputation and loss of clientele. It is important to ensure that the audit evidence obtained from the auditee is of high quality and supports the understanding of the IT control environment.

**ENDNOTES**

6 ISACA, COBIT Assessment Programme, www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Assessment-Programme.aspx