From: www.csoonline.com

Information Systems Audit: The Basics

Jennifer Bayuk, CSO

May 18, 2009

In the early days of computers, many people were suspicious of their ability to replace human beings performing complex tasks. The first business software applications were mostly in the domain of finance and accounting. The numbers from paper statements and receipts were entered into the computer, which would perform calculations and create reports. Computers were audited using sampling techniques. An auditor would collect the original paper statements and receipts, manually perform the calculations used to create each report, and compare the results of the manual calculation with those generated by the computer. In the early days, accountants would often find programming errors, and these were computer audit findings.

However, these exercises also sometimes yielded findings of fraud. Fraud activities ranged from data entry clerks changing check payees to programmers making deliberate rounding errors designed to accumulate cash balances in hidden bank accounts. [Editor's note: For more, see Essential Reading on Fraud.] As auditors recognized repeating patterns of fraud, they recommended a variety of security features designed to automatically prevent, detect, or recover from theft of assets.

As computers became more sophisticated, auditors recognized that they had fewer and fewer findings related to the correctness of calculations and more and more on the side of unauthorized access. Moreover, the checks and balances that were devised to maintain correctness of calculations were implemented as software change control measures. These rely heavily on security to enforce controls over segregation of duties between programming, testing, and deployment staff. This meant that even programming changes relied in some measure for their effectiveness on computer security controls. Nowadays, information systems audit seems almost synonymous with information security control testing.

The Scope of an IS Audit

However, the normal scope of an information systems audit still does cover the entire lifecycle of the technology under scrutiny, including the correctness of computer calculations. The word "scope" is prefaced by "normal" because the scope of an audit is dependent on its objective. Audits are always a result of some*concern* over the management of assets. The concerned party may be a regulatory agency, an asset owner, or any stakeholder in the operation of the systems environment, including systems managers themselves. That party will have an *objective* in commissioning the audit. The objective may be validating the correctness of the systems calculations, confirming that systems are appropriately accounted for as assets, assessing the operational integrity of an automated process, verifying that confidential data is not exposed to unauthorized individuals, and/or multiple combinations of these and other systems-related matters of importance. The objective of an audit will determine its scope.

It is sometimes a challenge for auditors representing management interests to map the audit objective onto technology. They first identify business activity that is most likely to yield the best type of evidence to support the audit objective. They identify what application systems and networks are used to handle the information that supports the business activity. For example, an audit may focus on a given IT process, in which case its scope will include the systems used to create input for, to execute, or to control the IT process. An audit focused on a given business area will include the systems necessary to support the business process. An audit that focuses on data privacy will cover technology controls that enforce confidentiality controls on any database, file system, or application server that provides access to personally identifiable data.

From the point of view of the IT Manager, scope should be clear from the outset of the audit. It should be a well-define set of people, process, and technology that clearly correspond to the audit objective. If an auditor does not understand the technology environment prior to the beginning of an audit, there may be mistakes in scope definition. Where such mistakes happen, they are often caught in the course of the audit, and systems that previously were not

in scope may be declared to be in scope. The audit professional calls this "scope creep." They generally try to avoid it, because the consequence is that more resources than planned will be necessary to meet the audit objective.

Once a scope is determined, an auditor will be provided with a contact for the review. In some organizations, the role of audit liaison is formally assigned. This role often falls to an information security professional, but there is no expectation on the part of audit that it would be someone in security. By default, it would be the highest ranking person in the IT management chain whose responsibilities fully cover the systems within the scope of the audit. This contact will be requested to provide background information on the systems that an auditor can use to plan the audit. Policies, architecture diagrams, systems manuals, and other sorts of documentation will often be requested in advance of an audit.

Management Practices and the Control Environment

The preliminary data gathering effort allows the auditor to verify that the scope has been set correctly, and also to form a set of control objectives, which will be the basis for audit testing. Control objectives are management practices which are expected to be in place in order to achieve control over the systems to the extent required to meet the audit objective. Auditors will repeatedly emphasize that control objectives are *management practices*. It is expected that the control objectives have been consciously established by management, that management provides leadership and resources to achieve control objectives, and that management monitors the environment to ensure that control objectives are met. *Control environment* is management behavior that provides leadership and accountability for controls; it is synonymous with the succinct phrase:*the tone is set at the top*. It is an absolute and nonnegotiable requirement for every audit that management responsibility with respect to system operation be undeniably clear to all within the organization under review.

The control objectives serve as a checklist to ensure that the auditor has covered the complete scope of the audit, while the planned technology tests may change during the course of the audit. In advance of any on-site meeting with an auditee, an auditor will associate each control objective with a set of activities that would provide evidence that the control objective is met. As far as possible, they will devise tests in advance that should yield evidence that the activities are well established and produce reliable results. The control objectives and associated test plans are referred to as the *audit program*.

When the auditor is ready to begin actual audit testing, the management contact will be requested to schedule an *opening meeting*. The contact is expected to meet the auditor upon arrival, and to facilitate auditor communication with other IT personnel whose services may be required to assist in the performance of audit tests. If at all possible, the contact should obtain a copy of the audit program prior to the opening meeting in order to schedule resources adequate to support the audit process. If not, the auditor should be requested to bring it to the opening meeting so that the affected management can review it at that time, and use it to schedule resources with the auditor (or audit team) accordingly.

Fieldwork, Findings and Compensating Controls

Audit *fieldwork* is the process of identifying the people, process, and technology within a given systems environment that correspond to expected control activities. Management accountable for audit results should do their best to ensure that an auditor is always speaking with the expert in the area under review. They should caution personnel not to make guesses in responses to audit questions, but instead to refer the auditor to the appropriate subject matter expert, or back to the accountable management contact.

As every security professional knows, it is extremely difficult to keep abreast of all the new management tools and techniques required to control IT, much less to determine which is the best fit to meet a given control objective. In recognition of this difficulty, audit programs are usually quite well established and uncontroversial. They are stated in general terms and can be supported with a wide variety of technology tools and techniques.

Where auditors cannot find evidence that a control objective is met, they will circle back to the accountable manager to see if there is some activity with the organization that qualifies as meeting the objective which was not anticipated

by the auditor, due to inexperience or unfamiliarity with the control environment. If they find it, they may refer to it as a "*compensating control*." This allows them to conclude that the control objective is met even though the control activity they expected does not exist, because the newly found activity *compensates* for the lack of the expected one.

In the event that an auditor can find no evidence corresponding to a given control objective, this issue will be labeled as a *finding*. A documented audit finding should have four or five parts. These are:

Condition: a factual description of audit evidence
Criteria: some standard that indicates why the condition impairs management ability to achieve control objectives
Cause: the root cause of the situation that introduced the control weakness
Effect: the risk that the condition presents to the audited organization, stated in terms of potential business impact
Recommendation: an appropriate management response (optional)

At any given point during the fieldwork, an auditor will have a list of potential findings. They may not yet be fully documented, but the condition may be known. The IT management contact for the audit should frequently touch base with the auditor during the fieldwork, and ask whether there are any potential findings. It is the role of the IT contact to assist both management and the auditor in the quest for evidence that would provide assurance that the control objective is met, and thus eliminate the finding.

The Assessment Report

Whether or not there are any audit findings, an audit will conclude with an *assessment report*. This is the formal opinion of the auditor with respect to the topic of the management concern driving the audit objective. The audit objective will be stated, the audit methodology will be briefly described, and there will be a statement with respect to the auditor's professional opinion on whether the management concern is adequately addressed. Where there are findings, these will be listed. The report may also include recommendations for management activity that would reduce the impact of the findings. In cases where auditors are permanent employees of the organization, or on retainer to monitor recurring management concerns (such as financial statement generation), they may request formal management commitment to a specific plan designed to eliminate the finding. This *remediation* activity is often formally tracked to completion. The audit is often considered to remain "open" until the remediation activity is complete.

An IT manager whose work is within the scope of an audit has a responsibility to cooperate with the auditor's quest to validate a management concern. The audit should precede smoothly to the extent that the accountable IT manager has a complete understanding of the source of the management concern, is satisfied with translation of that concern into an audit objective, agrees that the scope maps directly to the objective, maintains evidence that control objectives are met, and fully understands the auditor's reasoning with respect to findings. Where there is disagreement with the auditor on any of these key aspects of the audit, the issue should be escalated through the IT management chain. This internal IT management communication may or may not have any effect on the audit process, but it will serve to demonstrate that the auditee fully understands the audit process, and is willing to open discuss and informed debate on audit issues.

Jennifer Bayuk is an information security consultant and former CISO. She has written or co-edited several books including Enterprise Information Security and Privacy, Stepping Through the IS Audit, 2nd Edition,Stepping Through the InfoSec Program, and a forthcoming work on Security Leadership.