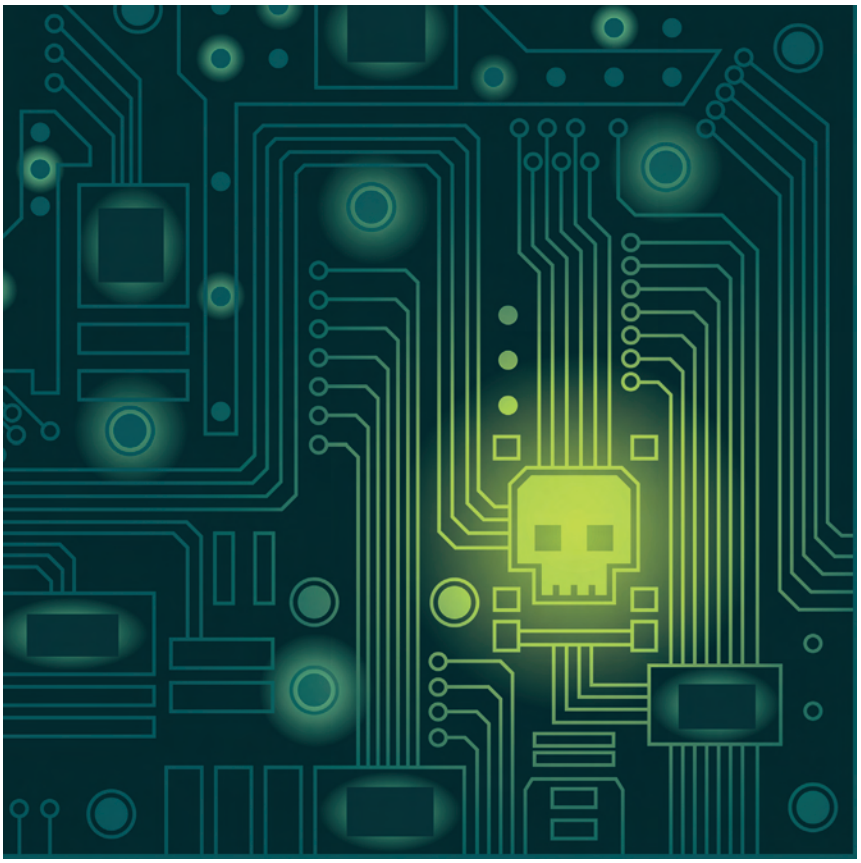
Implementing the IT-Related Aspects of Risk-Based Auditing Standards

By Dan Schroeder and Tommie Singleton



Information technology (IT) requires special consideration in the practical application of risk-based auditing, as defined under both the AICPA risk-based audit standards, Statements on Auditing Standards (SAS) 104–111, and the Public Company Accounting Board (PCAOB) Auditing Standard (AS) 5. Both SAS 104–111 and AS5 emphasize the need to establish tight linkage between audit procedures and a thorough assessment of financial statement and assertion level risk. Both standards reference the role of IT as a potentially significant source of inherent audit risk.

The risk-based audit standards adopted by the AICPA in 2006, along with AS5 released in 2007, emphasize a top-down, risk-based approach to the financial audit. The AICPA IT Executive Committee (ITEC), which includes the authors, has developed a white paper and other materials to complement those standards; these tools have been extremely well received by auditors. Their experience has affirmed the following benefits of risk-based auditing:

- The IT risk assessment procedures are necessary to completely identify and understand how IT affects financial statement assertions and the level of risk.
- By gaining an understanding of an entity's controls that exist to mitigate IT-related risks, an auditor may be able to incorporate tests of IT controls into further audit procedures (FAP) and thus improve the overall efficiency of their audit procedures.
- IT risk assessment procedures often improve the auditor's understanding of how computer-aided audit tools and techniques (CAATT) can be applied to improve the efficiency of substantive audit procedures.
- IT risk assessment procedures can usually be leveraged to provide valuable recommendations to management.

This overall approach for IT considerations in risk-based auditing, discussed in more detail below, is summarized in *Exhibit 1*.

Planning Risk Assessment Procedures: Need for an IT Specialist

Because risk-based auditing requires an auditor to understand the entity being audited, including its internal controls, the audit plan must consider how an auditor will gain this understanding. In many cases, especially in smaller entities that have a low level of IT sophistication, the role of IT for financial purposes is not complex and there is little or no dependency on IT for financial purposes—i.e., IT presents a relatively low level of risk of material misstatement. When IT does play a significant role for financial purposes, an audit plan must define how the auditor will gain an understanding of the role of IT for financial audit purposes related to material transactions, financial reporting, and material disclosures. The following are some common objectives for IT-related audit risk assessment procedures:

- Identify how IT contributes to the risk of material misstatement—i.e., identify inherent risk—at the assertion and financial statement level. An audit plan will often specify one or

more transaction classes relevant for consideration (e.g., accounts payable, or inventory and cost of goods sold, when both are material and IT plays a significant role in computation of amounts or account balances).

- Determine whether controls exist, that, if operating effectively, would provide reasonable, but not absolute, assurance that the inherent risks would be prevented or detected (i.e., assess control risk).
- Design and execute further IT-related audit procedures, as appropriate.

As IT related to financial reporting grows more sophisticated—creating greater dependence on IT for transactions and processes—the need for an IT audit specialist becomes greater (see the SAS 108 narrative in the ITEC white paper). The benefit of employing professionals possessing IT audit skills can be a significant aspect of many audit engagements in determining the impact of IT to the audit, understanding the IT controls, and designing and performing tests of IT controls and substantive procedures (e.g., using CAATTs). Depending upon the complexity of the entity's IT systems and environment, an IT audit professional will need to be an integral part of the audit team during the planning process and may also need to be involved in the planning and execution of the audit. An IT audit professional must be able to perform general auditing; understand flow of financial data, including how the system-based functions (e.g., transaction initiation, recording, processing, posting) affect accounting results; and identify IT-related risks and IT controls.

Understanding the IT Environment and Related Controls

An auditor should gather and consider for risk assessment purposes the following information:

- *The role of IT* in the initiation, authorization, recording, processing, and reporting of transactions. An auditor should gather information to understand the entity's information systems, technologies, and data for significant accounts, classes of accounts, or disclosures that are directly or indirectly used to generate financial transactions and reports. Information systems may include packaged applications, custom-developed applications, and end-user computing items (e.g., spreadsheets) that are used for accounting functions or transaction cycles (e.g., revenue recognition) and that contain relevant accounting data (e.g., accounts receivable entries).
- *Application controls* are controls that address the application level risks in the form of computerized controls built into the system, (related) manually performed controls, or a combination of both. Examples include: controls to ensure integrity of calculations and system procedures, edit checks, error handling, computerized matching of documents, and application-related access controls. Application controls should be observed and confirmed as part of normal walk-through procedures.
- *IT general controls* are not application-specific controls, but their purpose is to ensure the integrity of an entity's applications. IT general controls affect the protection of both data and programs from unauthorized change (see the Institute of Internal Auditors' "The GAIT Methodology," p. 37). They collectively provide assurance regarding the availability and reliability of the computer systems as a whole (see the Information Systems Audit and Control Association's "IT Assurance Framework," p. 31). These control functions include change management, security management, backup and recovery, operations control, and access controls. In the event auditors seek to rely on accounting-related output from one or more applications, they will need to understand whether IT general controls are effectively designed, deployed, and operating effectively so as to support the integrity of the data from those financial applications (see AS5, par. 47, and appendix B, para. 29, as well as SAS 109, para. 56).

Depending upon the circumstances of each audit team and engagement, some or all of the above may require the assistance of personnel with specialized IT audit skills. Whether the understanding of IT is performed by core audit personnel or through supplemental IT personnel, the understanding and resulting risk assessment should be integrated with the core audit process.

Because the role and significance of IT will vary from entity to entity, there is no one method for gathering information and documenting the understanding to fit every situation. An auditor should consider using a combination of methods to gather information, such as obtaining and reading written policies and procedures, survey questionnaires, interviews, walk-through reviews of processes, and walk-through reviews of observable aspects of the IT infrastructure (e.g., data centers, network closets). The use of flowcharts to depict the flow of financial information may, depending on the complexity, provide insight into the role of technology in financial processes, as well as be useful in identifying inherent risks.

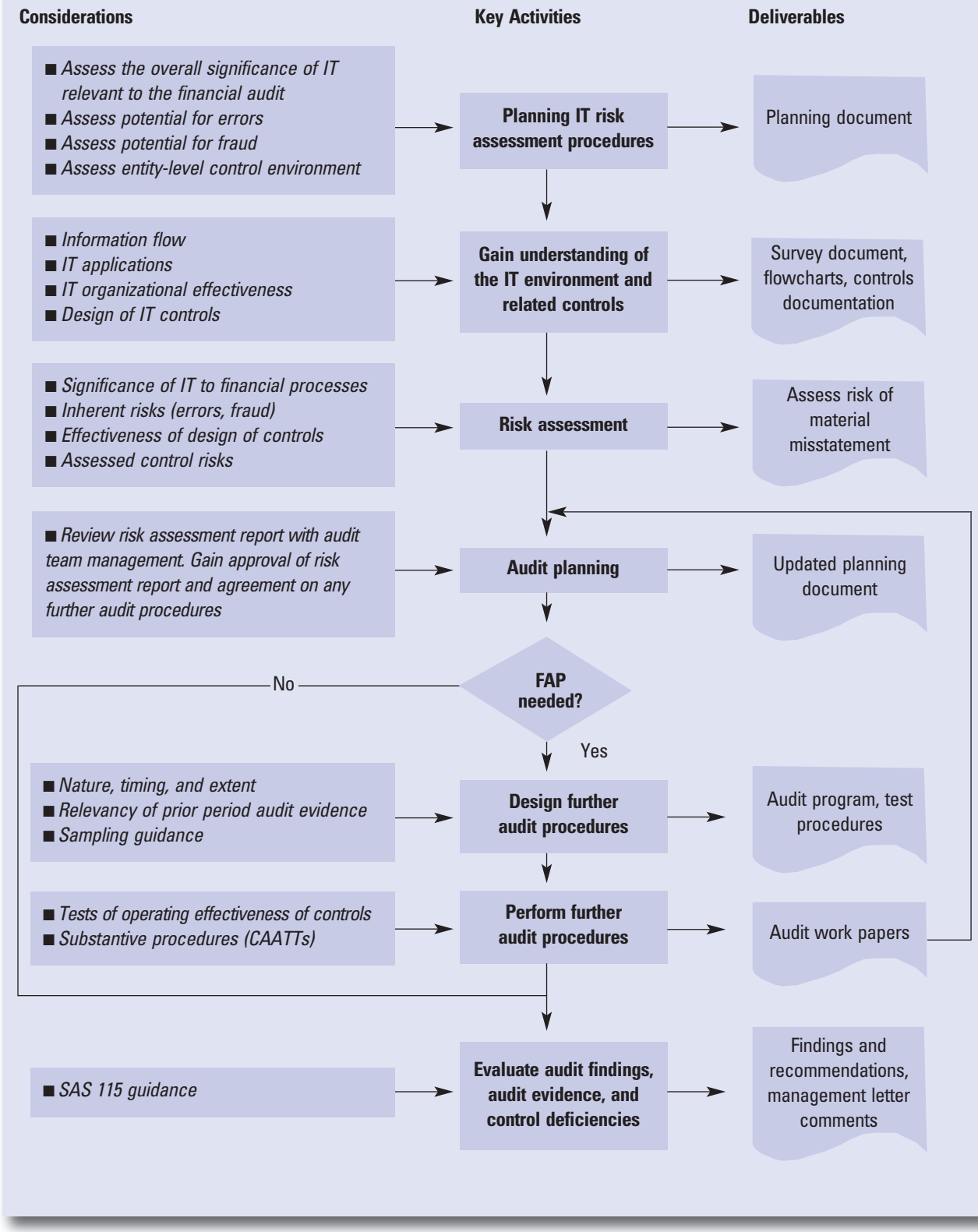
Assessing Risk of Material Misstatement

Gaining a thorough understanding of the role of IT for financial purposes will enable an auditor to effectively understand how IT impacts inherent risk and control risk (or, when combined, risk of material misstatement). In turn, understanding the risk of material misstatement is a prerequisite to enabling an auditor to design and perform further audit procedures to reduce overall audit risk to an appropriately low level. Assessing IT-related risk of material misstatement involves a consideration of the following:

- *Inherent risk:* An auditor must determine if the IT application represents a material inherent audit risk to one or more financial statement assertions or the level of financial statement risk. The affected assertions must be identified, as well as the type of risk. Inherent audit risk is affected by potential reliance on financially relevant output (e.g., report balances, journal entries uploaded to the general ledger) of the application for audit purposes. For example, if the audit team concludes there is no need to rely on the output of an application for audit purposes, the audit risk is low or nonexistent. An auditor should also determine the level (assertion or financial statement) of the inherent risk and the type of risk (error, fraud, or both).
- *Controls designed to mitigate risk:* An auditor should identify controls identified during the understanding phase that are designed and placed in operation to mitigate these inherent risks.
- *Control risk assessment:* An auditor should consider whether the identified controls (if determined to be operating effectively) would adequately prevent or detect the inherent risks identified. This assessment would consider factors for whether the controls are—
  - suitably designed to mitigate the inherent risks;
  - placed in operation.

  A control is suitably designed if it provides reasonable assurance that the risk it is intended to mitigate will be prevented or detected. A manually performed con-

EXHIBIT 1
Flowchart of IT Considerations for Risk-Based Auditing Processes



trol can be placed in operation if it can be determined that the persons responsible for execution of the control understand and are capable of fulfilling their responsibilities. For example, a walkthrough review of a standard operating procedure should confirm that the individual responsible for the control understands her control responsibilities and is capable of fulfilling those responsibilities. It can be determined that automated controls are placed in operation, by gathering evidence that the control is deployed (e.g., screenshots of persons with administrative access rights).

For more information on the risk of material misstatement formula, see Donald K. McConnell, Jr., and Charles H. Schweiger, "Implementing the New ASB Risk Assessment Audit Standards," *The CPA Journal*, June 2007.

Since the promulgation of the risk-based auditing standards, auditors can no longer choose to default an assessment of control risk at the maximum. Instead, an auditor must evaluate some key control areas in order to conclude that the current control environment, in general and specific controls, requires a maximum assessment of control risk.

One example of when IT could represent an inherent risk of material misstatement at the financial statement level would be an entity using financial applications that are highly customized and subject to frequent, significant modification. To assess control risk at the financial statement level, an auditor would determine if the entity has controls (i.e., policies and procedures) that, if deployed and operating effectively, could limit access to financial data and financial programs to authorized personnel under authorized circumstances. Control risk would be lowered by the existence of controls over administrative access to the IT environment, as well as controls over the process whereby changes are authorized, developed, and deployed to financial applications.

Controls are traditionally divided into two categories: general controls and application controls. Control activities in these two categories could be manual, automated, or a hybrid of the two. Application controls include activities such as authorization, documentation, segregation of duties, safeguarding of assets, and reviews and reconciliations. The manual procedures for these control activities often rely on automated controls (i.e., they are IT-dependent).

One example of when IT could represent an inherent risk of material misstatement at the assertion level would be when the entity uses a customized application for both service provisioning and billing as well as determining revenue recognition. To assess control risk at the assertion level (i.e., account, existence, occurrence, and accuracy), an auditor would determine if the entity has controls (policies and procedures) to limit access to all aspects of this application (database, program code, and user applications). Examples of controls to lower the assertion level risk include the following, whether automated or manual, which operate at the transaction level with the objectives of ensuring the following:

- Proper authorization is obtained to initiate and enter transactions;
- Applications are protected from unauthorized access;
- Users are only allowed access to the data and functions in an application that they are permitted to use;
- Errors in the operation of an application will be prevented or detected and corrected in a timely manner;
- Application processing operates as intended;
- Application output is protected from unauthorized access or disclosure;
- Reconciliation activities are implemented when appropriate to ensure that information is complete and accurate;
- High-risk transactions are appropriately controlled.

Other examples of application controls that affect assertions include the following:

- Input controls (e.g., edit checks, validating data inputs) for recording sales transactions affect the revenue account and assertions of existence, occurrence, and accuracy;
- Processing controls, such as automatic calculations between inventory and cost of goods sold, affect the cost of goods sold account and assertions of accuracy or valuation;
- Application controls over billing for services where invoices are automatically generated from work performed (e.g., time and billing system) affect the revenue account and assertions of existence, occurrence, and accuracy;
- Application controls for calculating commissions where the formula is complex affect the commissions expense account assertions of valuation and possibly existence or occurrence.

Determining Whether Further Audit Procedures Are Needed

Before conducting the risk assessment phase procedures and staffing the audit team, an audit partner or manager should strategically determine the need for a subject-matter expert (i.e., an IT auditor) to

EXHIBIT 2
Examples of Weaknesses that Can Potentially Lead to Material Misstatement

- The use of spreadsheets to prepare the financial statements or consolidated financial statements. Control risk is related to the ease with which errors can be made and their magnitude.
- Inventory tracking and reporting systems that calculate the cost of goods sold, where the application software has been changed, or is frequently changed, and the inventory or cost of goods sold account is material. Control risk is due to the possibility of unauthorized changes to the application, or authorized changes that could contain bugs, both of which could lead to errors.
- Third-party vendors that provide key services to an enterprise resource planning system in which the vendor has unrestricted access to data files for the supported applications. Control risk is related to the possibility of unauthorized changes to programs by the enterprise resource planning vendor and the availability of the entity's financial applications and financial reporting. Another significant risk in this scenario is disclosure risk.

adequately comply with the technical standards. Generally speaking, that decision is related to the client's level of IT sophistication, something originally described in SAS 94. When a company has a low level of IT sophistication, it is possible that the audit team does not have to employ an IT auditor. Likewise, when the level of IT sophistication is high, an IT auditor is probably necessary to comply with the risk-based auditing standards.

A central theme of the risk-based audit standards is iterative planning. A key component of risk-based audits is the IT risk assessment deliverable, which is considered by the audit team when determining what, if any, further audit procedures are needed in order to sufficiently lower audit risk to an acceptable level. The risk-based auditing standards clearly advocate continuous planning with respect to new information discovered during the audit. The risk assessment phase activities and report, however, are static. The IT risk assessment may identify controls that, if determined through testing to be operating effectively, could reduce audit risk for one or more assertions as well as the financial statement level. Therefore, if an auditor is to leverage this opportunity to gain efficiencies in further audit procedures (substantive procedures) by placing reliance on certain controls, the IT risk assessment must be produced early enough (e.g., the second or third quarter) to be considered during the audit planning process and the audit processes must be integrated.

During this step, the IT auditor's risk assessment report should become a key and active component of audit planning. The goal is to determine if any further audit procedures are needed with respect to IT and risks of material misstatement. The determination in this step is based on whether significant risks of material misstatement exist, whether they are related to IT, and whether control risk is less than the maximum (see Exhibit 1). If those conditions are met, then further audit procedures are necessary with respect to that specific set of circumstances; that specific risk, specific level of risk, or specific control; and that specific class of transactions, account balances, or presentation and disclosure.

A special case exists when the audit plan includes computer-generated information. Whenever any further audit procedures are performed using information provided by the entity's information system, an auditor should obtain adequate evidence about the accuracy and completeness of the information provided. That is, there is a need to be assured of the information provided, based on the specific controls associated with the computer-generated report that will be used in substantive procedures (e.g., a printout of accounts receivable subsidiary balances to be used in substantive procedures designed around them). In this special case, therefore, there is a need for specific and necessary tests of controls in further audit procedures, regardless of the scope of the risk assessment processes or the outcomes thereof (see SAS 110 and the ITEC white paper, section 2.2.7).

If no significant risks of material misstatement related to IT are determined to exist, then no further audit procedures are necessary (see Exhibit 1).

When Testing IT Controls Can Improve Audit Efficiency

A common source of risk of material misstatement occurs when the inventory account balance of a business is material and the business relies on its information system to determine inventory values (see the *Sidebar* for an extended treatment of such an example). Depending upon the specific functions performed by the IT system, it is possible that IT represents a risk

EXAMPLE OF RISK-BASED AUDITING: AUTOMATED CALCULATIONS AND INVENTORY VALUATION

A common source of risks of material misstatement exists for businesses where inventory amounts are material and the business relies on their IT system to calculate inventory values. Depending upon the specific functions performed by the IT system, it is possible that IT represents a risk of material misstatement at the existence and valuation assertion level. Depending upon other factors, the source of the risk could be error (e.g., related to data management and calculation accuracy) or fraud (e.g., related to unauthorized transactions, changes to programs and data). As part of the activities to understand the role of IT for the inventory transaction class (e.g., transaction walkthrough), an auditor should identify how the transactions are authorized, initiated, processed, and reported, as well as which controls are functioning within the system (i.e., application controls).

In those instances where an auditor gains evidence that relevant application controls are functioning properly—calculations are correct, access rights are validated, data entry is validated—the auditor would also inquire about supporting general controls that would protect the integrity of the applications (the inventory management application, in this case). General control dependencies will vary depending upon the nature of the application and how it is managed, but they typically involve access rights management and change management.

In this example, an auditor could achieve audit efficiencies by testing general controls for the inventory management application in conjunction with the evidence gained during the understanding of the transaction cycle, leading, when combined with substantive procedures, to a more efficient approach to lowering audit risk than if the auditor relied exclusively on substantive procedures. General controls testing will vary depending upon inherent risks, but it could include tests to confirm that changes to the application are authorized and are properly tested before being placed into production, as well as tests to confirm that only authorized personnel have access to relevant programs and data.

The test of controls related to the application could be performed in a single instance, thus potentially leading to a substantive reduction in audit costs where overlapping audit objectives exist for substantive procedures.

of material misstatement to the existence and valuation assertions; depending upon other factors, the source of the risk could be erroneous (e.g., related to data management and calculation accuracy) or fraud driven (e.g., related to unauthorized transactions, changes to programs and data). As part of the activities to understand the role of IT for the inventory transaction class (e.g., transaction walkthrough), an auditor should identify how the transactions are authorized, initiated, processed, and reported, and also which controls are functioning within the system (i.e., application controls). In those instances where the auditor gains evidence that relevant application controls are functioning properly (e.g., calculations are correct, access rights are validated, data entry is validated), an auditor would also determine which supporting general controls would protect the integrity of the application (in this case, the inventory management application).

General control dependencies will vary depending upon the nature of the application and how it is managed, but it typically involves management of the right to access and make changes. In this common example, the auditor should consider testing general controls for the inventory management application in conjunction with the evidence gained during the understanding of the transaction cycle, in conjunction with substantive procedures, as a more efficient approach to lowering audit risk than exclusively relying on substantive procedures. Control testing will vary depending upon the inherent risks, but it could include tests to confirm that changes to the application are authorized and tested before being placed into production, or tests to confirm that only authorized personnel have access to programs and data relevant to their jobs.

Designing and Performing Further Audit Procedures

Once the audit team has determined the need for further audit procedures, those procedures should be developed to directly address the specific circumstances regarding the IT-related risk of material misstatement. The procedures themselves would be tests of controls and/or substantive procedures. It is quite possible that the design of these procedures could lead to audit plan efficiencies, but it should certainly lead to audit effectiveness, as described in SAS 110, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*. There is information in the entity's systems that can be useful in the performance of substantive procedures. Thus there is an opportunity to leverage IT, such as CAATTs, in support of substantive procedures. CAATTs may be used to facilitate tests of details of transactions, account balances, and disclosures.

Basically, the audit plan addresses the nature, extent, and timing of any further audit procedures (see SAS 110). These audit procedures will be directed at those risks, and the strength or complexity of the procedure should have a composite level of strength equivalent to the assessed level of risk: If an IT-related risk of material misstatement exists at an assessed level of "high," then a high strength or complex procedure, or set of procedures, is necessary to reduce that risk to an acceptable level. For example, further audit procedures may include a test of controls combined with some substantive test in order to gain assurance that the related financial reporting information is not materially misstated. In this case, it may be that a single substantive test or test of controls would be sufficient to gain an adequate level of assurance.

In addition to the nature, extent, and timing issues, the audit team should consider the relevance of proper period audit evidence and sampling guidance when developing the audit plan.

Once the design is complete, an auditor performs those procedures, captures the audit evidence, and adds the results to the audit workpapers (see Exhibit 1).

Evaluating Audit Findings, Audit Evidence, and Control Deficiencies

During all of the above phases, an IT auditor is continually gaining an understanding of the entity's environment, especially its controls. As a function of the financial audit, SAS 112 (SAS 115 superseded 112 as of December 15, 2009) requires an auditor to report certain control deficiencies. The entire audit team should discuss the evaluation of audit findings in the risk assessment phase, audit planning phase, and further audit procedures phase, along with the audit evidence gathered during each phase, and evaluate control deficiencies. An auditor must report those assessed as material weaknesses or significant deficiencies to management and those charged with governance (SAS 112/115). A list of sample weaknesses is shown in *Exhibit 2*.

Importance of IT in Financial Reporting

Because IT is pervasive in the financial reporting of most entities today, auditors must identify the key changes that will need to be made to their audit methodology and the makeup of their audit team to ensure that IT-related risks are appropriately considered and addressed. Auditors may also use the implementation of the new risk standards as an opportunity to enhance the value they provide by helping companies identify control weaknesses and by reducing the amount of substantive procedures required by relying more on controls and the use of CAATTs.

In dealing with risk-based auditing, the following are an auditor's top priorities: Compliance with the risk-based auditing standards, opportunities for audit efficiencies, and opportunities for higher audit quality (more effectiveness, better client service). By better identifying the IT-related risks of material misstatement and designing audit procedures to address those specific risks, an auditor has a significant opportunity to perform a higher-quality, more efficient, and more cost-effective audit. ❑

Dan Schroeder, CPA, CISM, CISA, CIA, *is a partner at Habif, Arogeti & Wynne LLP, Atlanta, Ga. He is the chairperson of the AICPA IT Executive Committee.* ***Tommie Singleton, PhD, CPA/CITP, CISA,*** *is an associate professor of accounting and director of the forensic accounting program at the University of Alabama at Birmingham. He is also a scholar-in-residence at Carr, Riggs & Ingram, Enterprise, Ala., where his responsibilities include IT audit and forensic accounting.*

For more on the process and model described, read the ITEC white paper available for ITMS members only at www.aicpa.org. A practical summation of standards and best practices in risk-based auditing are discussed in more detail therein. It also includes a complete glossary of terms.