IT AUDIT CHECKLIST SERIES

ComplianceINSIGHT

Information Security

Practical guidance on how to prepare for successful audits

www.ITCinstitute.com

IT Compliance Institute™

ComplianceINSIGHT

IT AUDIT CHECKLIST SERIES

Information Security

About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today's regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi's primary goal is to be a useful and trusted resource for IT professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

For more information, please visit: www.itcinstitute.com

Comments and suggestions to improve the IT Audit Checklists are always encouraged. Please send your recommendations to editor@itcinstitute.com.

All design elements, front matter, and content are copyright © 2006 IT Compliance Institute, a division of 1105 Media, Inc., unless otherwise noted. All rights are reserved for all copyright holders.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under § 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the copyright holder.

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be usable for your situation. You should consult with a professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

All trademarks cited herein are the property of their respective owners.

Table of Contents

Executive Overview

What Is the IT Audit Checklist Series?

The ITCi IT Audit Checklists are a series of topical papers that provide practical guidance for IT, compliance, and business managers on preparing for successful internal audits of various aspects of their operations. In addition to helping managers understand what auditors look for and why, the IT Audit Checklists can help managers proactively complete self assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of an actual audit.

What is this paper about?

This paper, "IT Audit Checklist: Information Security," supports an internal audit of the organization's information security program with guidance on improving information security programs and processes, as well as information on assessing the robustness of your organization's security efforts. The paper is intended to help IT, compliance, audit, and business managers prepare for an audit of information security and, ultimately, to ensure that the audit experience and results are as productive as possible.

Paper Contents

- According to the Information Security Forum, security management means "keeping the business risks associated with information systems under control within an enterprise." Requirements for security management include "clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the enterprise, and the establishment of a secure environment."[1]

- The information security program is a critical component of every organization's risk management effort, providing the means to protect the organization's information and other critical assets.

- A well-managed information security program has robust plans, procedures, goals, objectives, trained staff, performance reporting, and ongoing improvement efforts. The audit team looks for evidence that the information security program is well organized and well managed. The security program must also specifically mitigate risks in satisfying key business objectives, and this traceability must be clear.

- Your information security audit should confirm that key risks to the organization are identified, monitored, and controlled; that key controls are operating effectively and consistently; and that management and staff have the ability to recognize and respond to new threats and risks as they arise.

- Audits and reviews of your information security program and its management advance the goal of program oversight and ensuring continuous improvement and success.

- The information security audit's goals, objectives, scope, and purpose will determine which actual audit procedures and questions your organization requires. This document provides a foundational IT audit checklist you can use and modify to fit your specific situation.

- Additional resources that complement the content of this paper are provided in the appendices.

[1] Standard of Good Practice for Information Security. February 2005. Information Security Forum. http://www.isfsecuritystandard.com/index_ie.htm

Introduction to Information Security

Over the past few years, the importance to corporate governance of effectively managing risk has become widely accepted. The information security program is a critical component of every organization's risk management effort and provides the means for protecting the organization's digital information and other critical information assets. With the increased importance of the information security program in protecting sensitive corporate and personal information, the internal audit function has increased the frequency and comprehensiveness of its assessment of information security processes and efforts.

What Is Information Security Management?

According to the Information Security Forum, security management means "keeping the business risks associated with information systems under control within an enterprise." Requirements for security management include "clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the enterprise, and the establishment of a secure environment."[1]

An effective information security management program promotes and assures a broad understanding of security and security management, establishes policies and procedures that highlight the organization's key security risks and the steps being taken to address and mitigate them, and identifies emerging security threats early. The information security program must reflect the organization's needs and risk tolerance; that is, how much risk it is willing and able to accept, given the cost of mitigation.

What Are the Benefits of Information Security?

An information security management program is necessary because threats to the availability, integrity, and confidentiality of the organization's information are great and, apparently, ever increasing. All companies possess information that is critical or sensitive, ranging from personal data to financial and product information and customer, brand, and IP information. An information security program implements protective measures to ensure corporate information is not illicitly or improperly accessed, modified, or used.

The benefits of an effective information security program include:

1. The ability to systematically and proactively protect the company from the dangers and potential costs of computer misuse and cybercrime
2. The ability to make informed, practical decisions about security technologies and solutions and thus increase the return on information security investments
3. The management and control of costs related to information security
4. Greater organizational credibility with staff, customers, and partner organizations
5. Better compliance with regulatory requirements for security and privacy
6. Implementation of best practices in risk management in regard to information assets and security

The Auditor's Perspective on Information Security

Why Audit?

Audits are opportunities for companies to improve, based on auditor analysis and advice. To preserve the integrity and authority of audits, auditors maintain a delicate balance between offering advice and making decisions.

For each organization, the scope of auditor responsibility should be documented in the company's internal audit charter and be approved by the audit committee. Because every organization has different goals and objectives—and certainly different issues and challenges—there is no one-size-fits-all audit process, nor one audit approach that fits all situations.

Historically, information security audits have focused primarily on the enterprise infrastructure (router locations, what kinds of servers are involved, how servers are protected, how management assigns and enforces system access permissions, how managers assess staff competence and trustworthiness, etc.). Increasingly, however, information security audits also have a significant external component. For example:

- How are backup tapes transferred, and where are they stored?
- Does the company have confidence that storage vendors are competent and maintain information securely?
- How much should the company trust customers, suppliers, and partners that have access to sensitive internal data?
- What is the company's exposure to local, state, federal, and international regulatory or law enforcement issues? Do laws demand policies or processes the company would rather not provide; if so, can the company defend its position?

> Historically, information security audits have focused on the enterprise infrastructure... Increasingly, however, audits also have a significant external component.

The size and complexity of various organizations' audit efforts differ due to variations in operating environments, risk priorities and thresholds, and business and audit objectives. In addition, the scope of audits can vary from project to project, depending on auditor's focus (for example, on various business processes, management controls, and technical controls). Ensuring appropriate audit focus is another reason management should communicate with auditors, and vice versa, early and often for every audit project.

Internal auditors should perform organizational risk assessments and evaluate the audit universe and supporting audit plans at least annually, and sometimes more frequently.[2] At the micro level, an audit risk assessment of the various entities being audited is completed to support the audit project (sometimes also referred to as the audit "terms of reference"). Planning for each audit requires serious consideration of the organizations's many risks and opportunities. Finally, in many companies, continuous auditing (ongoing audit evaluations) is being implemented for key systems and/or key transactions.

[2] For more information, refer to Swanson, Dan. "Ask the Auditor: Business Risk vs. Audit Risk." IT Compliance Institute. May 2, 2006. http://www.itcinstitute.com/display.aspx?id=1673.

Who Is Responsible for Information Security?

The board of directors, management (of IT, information security, staff, and business lines), and internal auditors all have significant roles in information security assurance and the auditing of information security efforts. The big question for many companies is how these stakeholders should work together to ensure that everything that should be done to protect sensitive information is being done—and that the company's information assets are protected appropriately.

1. The **board of directors** must provide oversight at a level above other business managers. The director's role in information security is to ask managers the right questions and encourage the right results. Directors must set appropriate tone at the top, communicating to executive management the business imperative of effective information security management. The board also has a role in establishing and overseeing security policy and defining the corporate security culture—which includes security assurance and ethics attitudes.

2. **Executive management** must provide leadership to ensure that information security efforts are supported and understood across the organization, demonstrating by example the mandate of security policies. Executive management must also dedicate sufficient resources to allow controls to be effective.

   Finally, by ensuring that the information security program and its management are subject to audit and reviewed by qualified professionals, corporate leaders advance the goal of security oversight and promote continuous improvement and success.

3. **Staff and line-of-business managers** must have a voice in the design and implementation of information security programs, since the managers are held accountable for protecting and enhancing the value of the organization's assets, including information assets. Managers must also review and monitor security controls to ensure they are appropriate, despite ever-changing risks and business requirements. This is, in fact, a form of auditing information security.

   And, finally, managers who own business-unit information should also help define their security requirements, based on business objectives, the significance of the information involved, legal requirements, and the seriousness of threats to data integrity and disclosure (privacy).

Although business managers often try to relegate security responsibilities to an information security management function, all parts of the organization have security responsibilities.

Many companies have a separate managerial structure with wholly dedicated information security executives, managers, and technical staff. Collectively, this information security function must organize, oversee, implement, test, and monitor the organization's technical information security program.

Although business managers often try to relegate information security responsibilities to an information security management function, all parts of the organization have information security responsibilities. Security goals include a mixture of technical, procedural, and oversight controls, all of which should be reviewed or tested by all appropriate staff and management to ensure they are (a) adequate, as defined to mitigate information security risks, and (b) reasonably efficient and effective in practice.

4. The **internal audit function** provides strategic, operational, and tactical value to an organization. For example, internal auditing:

    - Informs the board and management as to whether business units understand the importance of security and are adhering to policies, whether key information assets and systems are sufficiently secure, whether programs are in place for continually updating and strengthening safeguards against internal and external security threats, and whether the policies are reasonable. In brief, internal audits assess the state of the information control environment and recommend improvements.

    - Independently validates that the organization's information security efforts are proactive and effective against current and emerging threats. To provide this level of assurance, internal auditors may compare current organizational practices with industry practices and regulatory guidelines.

Notably, auditing provides only a reasonable level of assurance. Auditors cannot provide an insurance policy against any fault or deficiency, particularly in regard to activities that cannot be totally controlled, such as collusion and management override.

To fulfill an audit's potential, however, the internal auditors need to: 1) know what they are doing (i.e., have the skills to perform appropriate security audits), 2) have a strong understanding of both the technical and the business environment, 3) know what to ask for, and 4) complete regular and ongoing training to keep on top of new guidance and standards of practice. In addition, the auditing function should "complement," but never replace, management's responsibility to ensure their IT security controls are operating properly.

INFORMATION SECURITY RESPONSIBILITIES

BOARD OF DIRECTORS

- Provide oversight
- Communicate business imperative
- Establish and oversee security policy
- Define corporate security culture

EXECUTIVE MANAGEMENT

- Provide leadership
- Ensure information security efforts are supported and understood across the organization
- Dedicate sufficient resources to be effective
- Advance the goal of security oversight and promote continuous improvement and success

STAFF AND LINE-OF-BUSINESS MANAGERS

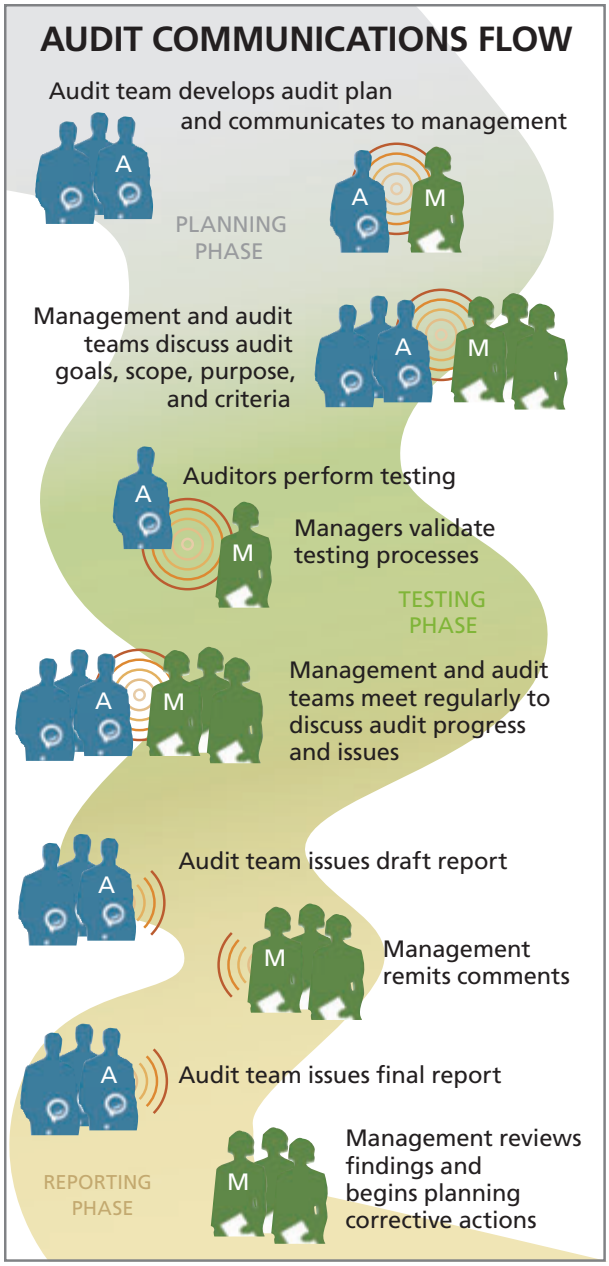
- Contribute to design and implementation of information security programs
- Review and monitor security controls
- Define security requirements
- Monitor control environments, including understanding, adoption, and effectiveness
- Implement a continuous improvement program

INTERNAL AUDITORS

- Assess information control environments, including understanding, adoption, and effectiveness
- Validate information security efforts and compare current practices to industry standards
- Recommend improvements

Management's Role in the Audit Process

An internal audit engagement typically has three phases: planning, testing, and reporting. Management has an important role in each phase:



Managers and auditors should work together throughout the audit process to ensure that auditors pursue appropriate goals and have proper insight into IT and business processes. Good communication throughout the audit process helps ensure that audit findings are relevant and can be used to benefit the company.

- ☐ **During planning**, management should first focus on the audit plan (the auditor's "road map") and ensure that managers understand and are in general agreement with the audit purpose, focus, and approach. An open, positive discussion with the audit team regarding these defining factors helps management and the audit team communicate their expectations up front. Audit planning should focus on critical or sensitive risks, but all risks should be considered. To this end, active involvement by management in audit planning is vital to the overall success of an internal audit.

  Management should also discuss the evaluation criteria auditors will use in assessing the risk management program. Finally, managers and auditors should broadly discuss planned audit testing, although auditors must have the authority and discretion to select tests they deem appropriate.

- ☐ **During testing**, management facilitates the auditors' access to appropriate people and systems. Management confirms the audit results, not re-performing the actual tests, but verifying processes and data in order to gain confidence in the audit findings. The audit team leader and senior executives of the areas being audited should meet regularly throughout the audit process—usually weekly and at least once a month—to discuss audit progress, identified issues, and potential actions.

  An open, transparent dialogue between senior members of both management and the audit team does much to avert misunderstandings or resolve disputed findings before the audit team issues its draft report. The audit team should communicate critical findings to management as early as possible, even outside of the established meeting schedule. These findings may also be reviewed during regular meetings, but prompt notice is necessary and usually appreciated.

- ☐ **During reporting**, management receives and reviews the findings of auditors, plans and develops corrective actions, and implements change.

What Auditors Want to See

Audits exist to assess how well a business unit or program meets the performance goals of the organization, as dictated by the CEO, CFO, board, and investors. Accordingly, the managerial goal in auditing is not simply to make auditors happy, but to demonstrate how well operations, controls, and results meet the needs of the business. During audit planning, managers help auditors to design an audit process that truly reflects business strategies and goals. Thus, the managerial response to auditors throughout the audit process—planning, testing, and reporting—is for the benefit of the business, not its auditors.

Auditors exist to provide the board and senior management with an objective, independent assessment of a business unit or program (such as information security), including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors need to review and assess evidence of the risk management program and its performance. If auditors are able to demonstrate performance and show that accountability has been established and is working, they should produce a positive audit report—it's that simple.

Accordingly, auditors and managers should work to help each other reach common goals—auditors striving to earnestly, honestly, and completely assess program effectiveness, and management working to help auditors make valid assessments. In that vein, there are some typical program characteristics and managerial processes that auditors do and don't like to see. As in all aspects of audit and risk management programs, auditor likes and dislikes vary by company; however, the following list itemizes typical indicators of good and bad audits.

Auditors Like...

- ☐ Good management practices: planning, direction, monitoring, reporting, etc.
- ☐ Proactive management, including frequent operational monitoring
- ☐ Supervisory review of key performance reports
- ☐ Supervisory review of operating results (especially exception reports and analyses)
- ☐ Organized, clear, and up-to-date documentation
- ☐ Well-documented policies and procedures
- ☐ Managerial actions based on facts, not habits
- ☐ A documented chain of command, roles, accountability, and responsibilities (e.g., organization charts, job descriptions, separation of duties)
- ☐ Consistent adherence to policy and procedures, from senior management through frontline staff
- ☐ Good staff management, including workforce development (bench strength and cross training), assurance that absences do not compromise controls, and policies for secure staff turnover
- ☐ A balance between short- and long-term focus, for both objectives and results
- ☐ Managerial willingness to embrace new ideas

Auditors Don't Like...

- ☐ Interviewing defensive or uninformed managers and executives
- ☐ Wading through piles of disorganized analyses
- ☐ Managers who can't or won't comprehend the level of risk they are incurring
- ☐ The opposite of the "like" items listed above

How Companies (Inadvertently or Intentionally) Help or Hinder Auditors

Both the audit team and managers should approach every audit process in a positive and open manner. If management and staff are defensive, negative, or even hostile, an audit project can quickly evolve into a no-win, give-no-quarter type of evaluation that ultimately damages every party involved. Even well intentioned management can inadvertently hinder the audit process, however. Management can either help or hinder the audit process by:

- ☐ (Not) having requested documentation available at the prearranged time
- ☐ (Not) meeting deadlines and (not) stonewalling
- ☐ (Not) communicating at an appropriate managerial level
- ☐ (Not) ensuring key staff are available to auditors, especially at critical milestones
- ☐ (Not) informing relevant staff about the audit and its goals, impacting the time and effort auditors must spend to explain the audit to affected personnel
- ☐ (Not) having administrative support where needed
- ☐ (Not) providing accurate documentation
- ☐ (Not) having an audit charter for the internal audit function

Who Should Talk to the Auditors?

An efficient audit process depends on effective communication between auditors, managers, and workers. Management and auditors should strive to balance efficiency (having a minimal number of staff dealing directly with the auditors) with the need for "open access" to management and staff by the audit team (when needed).[3] Obviously, it is impractical and unproductive for both teams to put too many staff in front of auditors. Instead, management should:

- ☐ Provide knowledge of operations through several informed point people to interact with auditors. A "short list" of interviewees within the program area being audited can more quickly answer auditor queries and provide better continuity of audit support.
- ☐ Allow ready access to all management and staff, if required by the audit team to gain a clearer picture of overall operations
- ☐ Work with the audit team to draw up a staff interview schedule as part of the planning effort. Update the schedule as necessary during the audit fieldwork phase, if circumstances change.

In many situations, a single point of contact for each audited program will provide the vast majority of documentation to the audit team. The role of that individual—and, indeed, for all auditor contacts—is to ensure that the audit team receives accurate and adequate information for the task. Auditors will still use their professional judgment to determine if and when additional sources of information (other staff interviews) are required. The audit team will also conduct a variety of audit tests, if necessary, to confirm their audit analysis.

[3] The audit team is always expected to ensure all interactions (with all staff) are professional and result in minimal disruption.

Information Security Audit Checklist

Your audit's goals, scope, and purpose determine the appropriate audit procedures and questions. An audit of information security should determine that key risks to the organization are being controlled, that key controls are operating effectively and consistently, and that management and staff have the ability to recognize and respond to new threats and risks as they arise.

The following checklist generally describes information security audit steps that management might follow in preparation for and during an audit. The list does not attempt to itemize every possible information security objective, but rather to provide general guidance on defensible controls and a logical control hierarchy.

Audit Planning

- ☐ The audit team develops an initial draft of the internal audit plan
- ☐ Managers of the information security program and other appropriate executives meet with the audit team to review audit program steps and define key players and necessary resources
- ☐ Management collects program documentation in preparation for audit
- ☐ Management supports a preliminary survey of the information security program (by the internal audit team)
- ☐ The audit team drafts the internal audit program plan
- ☐ Management and board members provide feedback on the draft plan

Audit Testing

Management has a responsibility to ensure that audit testing is productive. The audit team performs tests to independently assess the performance of the information security program and, while the audit team ultimately determines the nature of these tests and the extent of testing (e.g. the sample sizes to use), management should engage auditors in discussions about their testing methods and goals.

In tone, management should try to strike a balance, neither entirely deferring to the audit team nor micro-managing the internal audit efforts. The key is to provide productive input on the evaluation methodology before audit management signs off on it.

As the testing phase winds up, the audit team will prepare summaries of its key findings. Information security managers should be prepared to provide feedback and comments on audit summaries, prior to the more final, formal audit report.

Proactive communication, candor from all parties, and thorough documentation can prevent many surprises and conflicts that might otherwise arise during the testing phase; however, managers might still disagree from time to time with audit results. Management should strive to provide solid evidence—not just argument—that supports its contrasting position. Facts are the most successful tool for swaying an adverse opinion before the audit report is finalized.

Since the audit report often forms the basis of future security focus and investment, management should ensure that every audit point raised—and its related recommendation—is relevant and valid. Likewise, every action plan proposed by managers or auditors should be achievable, appropriate, cost effective, and able to produce lasting effect.

Audit Testing Processes

- ☐ Managers and auditors complete a "kick-off" meeting
- ☐ Managers support auditors' high-level assessment of the information security program with interviews and documentation of:
  - ___ Scope and strategy, including how thoroughly the program addresses potential risks and compares with industry best practices
  - ___ Structure and resources, reflecting managerial commitment to effective information security management and the program's robustness relative to the potential impact of adverse events
  - ___ Management of policies and related procedural documentation
  - ___ Communication of program policies and expectations to stakeholders
  - ___ Impact of program efforts on organizational culture
  - ___ Internal enforcement processes and consistency
  - ___ Ongoing improvement efforts
- ☐ Managers support more detailed audit analysis of the information security program
- ☐ Auditors complete the evaluation of design adequacy
- ☐ Auditors complete the evaluation of control effectiveness

Audit Testing Steps

The following activities may be repeated in each of the aforementioned audit processes.

- ☐ Auditors evaluate information on information security processes and procedures
- ☐ Managers assist auditors with walkthroughs of selected processes; documentation of the controls
- ☐ Auditors evaluate the quality of information generated by the information security program; the ease, reliability, and timeliness of access to such information by key decision makers; and the operational consistency with which such information is generated
- ☐ Auditors assess information security performance metrics: existence, usefulness, application, monitoring, and responses to deviation
- ☐ Auditors evaluate whether risk management controls are sufficiently preventive, as well as detective
- ☐ Auditors define tests to confirm the operational effectiveness of information security activities. Tests might include management and staff interviews, documentation and report review, data analysis, and result sampling for recent initiatives
- ☐ Managers provide requested data, documentation, and observations
- ☐ Auditors identify (or recommend) opportunities for improvement of information security activities
- ☐ Managers and auditors complete an exit meeting to discuss audit findings, auditor recommendations, and managerial response

Controls for Information Security

In general, auditors look at three types of controls: management, operational, and technical. Within these categories, auditors may review the controls listed in this section (and potentially others, depending on the audit's purpose and focus). The following list represents the full spectrum of information security controls, as defined by the US government's National Institute of Standards and Technology (NIST); however, auditors should not weight and review all controls equally.

As stated earlier, the actual information security controls to be audited are determined during the audit planning phase. Controls are assessed during the audit testing phase. Management should determine which information security controls are appropriate for each organizational environment, based on the corporate risk profile, and compare the list to the controls in this section, which reflect audit best practices and US federal guidance on information security management.

According to the US Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems,"[4] information security controls fall into 17 categories, ranging from access control to system and information integrity. The US NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems,"[5] further defines specific information security controls for each category.[6] The descriptive tables in this section reflect information from both FIPS 200 and NIST 800-53.

Management Controls

Management controls ensure a well-run and effective information security program. In general, management controls assess whether:

- ☐ Information security program policies and procedures have been established
- ☐ Performance is measured
  - — Performance metrics are established and documented
  - — Management regularly monitors performance results
- ☐ A business plan exists
- ☐ A budget exists
- ☐ A continuous improvement program is in place and operates effectively

[4] US Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems. March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[5] US NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. February 2005. http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf.

[6] NIST 800-53, FIPS 200, and an additional publication, FIPS 199 ("Standards for Security Categorization of Federal Information and Information Systems." February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) provide much more guidance on the listed controls than is reproduced in this paper. Of particular note are the three control impact ratings or "baselines" defined in FIPS 199 and specified for individual controls in NIST 800-53. The NIST documents do not simply assign each control a baseline; rather, they provide guidance on how controls must be implemented to meet the criteria for increasingly stringent levels of control baselines.

Management Controls

Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

	Number	Description
☐	CA-1	**Certification, Accreditation, and Security Assessment Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
☐	CA-2	**Security Assessments:** The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
☐	CA-3	**Information System Connections:** The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.
☐	CA-4	**Security Certification:** The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
☐	CA-5	**Plan of Action and Milestones:** The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
☐	CA-6	**Security Accreditation:** The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency]. A senior organizational official signs and approves the security accreditation.
☐	CA-7	**Continuous Monitoring:** The organization monitors the security controls in the information system on an ongoing basis.

Management Controls

Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

	Number	Description
☐	PL-1	**Security Planning Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
☐	PL-2	**System Security Plan:** The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.
☐	PL-3	**System Security Plan Update:** The organization reviews the security plan for the information system [Assignment: organization-defined frequency] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
☐	PL-4	**Rules of Behavior:** The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.
☐	PL-5	**Privacy Impact Assessment:** The organization conducts a privacy impact assessment on the information system.

Risk Assessment (RA)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

	Number	Description
☐	RA-1	**Risk Assessment Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
☐	RA-2	**Security Categorization:** The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.
☐	RA-3	**Risk Assessment:** The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

Management Controls

Risk Assessment (RA) *(continued)*

	Number	Description
☐	RA-4	**Risk Assessment:** The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.
☐	RA-5	**Vulnerability Scanning:** Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities affecting the system are identified and reported.

System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

	Number	Description
☐	SA-1	**System and Services Acquisition Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
☐	SA-2	**Allocation of Resources:** The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.
☐	SA-3	**Life Cycle Support:** The organization manages the information system using a system development life cycle methodology that includes information security considerations.
☐	SA-4	**Acquisitions:** The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.
☐	SA-5	**Information System Documentation:** The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
☐	SA-6	**Software Usage Restrictions:** The organization complies with software usage restrictions.
☐	SA-7	**User Installed Software:** The organization enforces explicit rules governing the downloading and installation of software by users.
☐	SA-8	**Security Design Principles:** The organization designs and implements the information system using security engineering principles.

Management Controls

System and Services Acquisition (SA) *(continued)*

	Number	Description
☐	SA-9	**Outsourced Information System Services:** The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.
☐	SA-10	**Developer Configuration Management:** The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
☐	SA-11	**Developer Security Testing:** The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.

Operational Controls

Operational controls ensure the effective performance of the information security program. Operational controls assess whether:

- Controls exist to meet regulatory requirements[4]
- Rules and requirements exist and are documented
- Staff performance appraisals are completed regularly
- Supervisory review of key management reports and operating results occurs regularly

[4] For a control-by-control comparison of information security regulations and standards, see ITCi's Unified Compliance Project, Technical Security Control Matrix. http://www.itcinstitute.com/ucp/impactZone.aspx?id=9.

Operational Controls

Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

	Number	Description
☐	AT-1	**Security Awareness and Training Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
☐	AT-2	**Security Awareness:** The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and [organization-defined frequency, at least annually] thereafter.
☐	AT-3	**Security Training:** The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and [organization-defined frequency] thereafter.
☐	AT-4	**Security Training Records:** The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

	Number	Description
☐	CM-1	**Configuration Management Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
☐	CM-2	**Baseline Configuration:** The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.
☐	CM-3	**Configuration Change Control:** The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.
☐	CM-4	**Monitoring Configuration Changes:** The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.

Operational Controls

Configuration Management (CM) *(continued)*

	Number	Description
☐	CM-5	**Access Restrictions for Change:** The organization enforces access restrictions associated with changes to the information system.
☐	CM-6	**Configuration Settings:** The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.
☐	CM-7	**Least Functionality:** The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

	Number	Description
☐	CP-1	**Contingency Planning Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
☐	CP-2	**Contingency Plan:** The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
☐	CP-3	**Contingency Training:** The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].
☐	CP-4	**Contingency Plan Testing:** The organization tests the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.
☐	CP-5	**Contingency Plan Update:** The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
☐	CP-6	**Alternate Storage Sites:** The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
☐	CP-7	**Alternate Processing Sites:** The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.

Operational Controls

Contingency Planning (CP) *(continued)*

	Number	Description
☐	CP-8	**Telecommunications Services:** The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.
☐	CP-9	**Information System Backup**: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and stores backup information at an appropriately secured location.
☐	CP-10	**Information System Recovery and Reconstitution**: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

	Number	Description
☐	IR-1	**Incident Response Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
☐	IR-2	**Incident Response Training:** The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].
☐	IR-3	**Incident Response Testing:** The organization tests the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and exercises] to determine the incident response effectiveness and documents the results.
☐	IR-4	**Incident Handling:** The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
☐	IR-5	**Incident Monitoring:** The organization tracks and documents information system security incidents on an ongoing basis.
☐	IR-6	**Incident Reporting**: The organization promptly reports incident information to appropriate authorities.
☐	IR-7	**Incident Response Assistance:** The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Operational Controls

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

	Number	Description
☐	MA-1	**System Maintenance Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
☐	MA-2	**Periodic Maintenance:** The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
☐	MA-3	**Maintenance Tools:** The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.
☐	MA-4	**Remote Maintenance:** The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
☐	MA-5	**Maintenance Personnel:** The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.
☐	MA-6	**Timely Maintenance:** The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.

Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

	Number	Description
☐	MP-1	**Media Protection Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
☐	MP-2	**Media Access:** The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.
☐	MP-3	**Media Labeling:** The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [Assignment: organization-defined list of media types and hardware components].
☐	MP-4	**Media Storage:** The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.

Operational Controls

Media Protection (MP) *(continued)*

	Number	Description
☐	MP-5	**Media Transport:** The organization controls information system media (paper and digital) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.
☐	MP-6	**Media Sanitization:** The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.
☐	MP-7	**Media Destruction and Disposal:** The organization sanitizes or destroys information system digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using the information contained on the media.

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

	Number	Description
☐	PE-1	**Physical and Environmental Protection Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
☐	PE-2	**Physical Access Authorizations:** The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].
☐	PE-3	**Physical Access Control:** The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
☐	PE-4	**Access Control for Transmission Medium:** The organization controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.
☐	PE-5	**Access Control for Display Medium:** The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Operational Controls

Physical and Environmental Protection (PE) *(continued)*

	Number	Description
☐	PE-6	**Monitoring Physical Access:** The organization monitors physical access to information systems to detect and respond to incidents.
☐	PE-7	**Visitor Control:** The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.
☐	PE-8	**Access Logs:** The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the access logs [Assignment: organization-defined frequency] after closeout.
☐	PE-9	**Power Equipment and Power Cabling:** The organization protects power equipment and power cabling for the information system from damage and destruction.
☐	PE-10	**Emergency Shutoff:** for specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.
☐	PE-11	**Emergency Power:** The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
☐	PE-12	**Emergency Lighting:** The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.
☐	PE-13	**Fire Protection:** The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.
☐	PE-14	**Temperature and Humidity Controls:** The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.
☐	PE-15	**Water Damage Protection:** The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
☐	PE-16	**Delivery and Removal:** The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.
☐	PE-17	**Alternate Work Site:** Individuals within the organization employ appropriate information system security controls at alternate work sites.

Operational Controls

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

	Number	Description
☐	PS-1	**Personnel Security Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
☐	PS-2	**Position Categorization:** The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].
☐	PS-3	**Personnel Screening:** The organization screens individuals requiring access to organizational information and information systems before authorizing access.
☐	PS-4	**Personnel Termination:** When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.
☐	PS-5	**Personnel Transfer:** The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).
☐	PS-6	**Access Agreements:** The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.
☐	PS-7	**Third-Party Personnel Security:** The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.
☐	PS-8	**Personnel Sanctions:** The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Operational Controls

System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

	Number	Description
☐	SI-1	**System and Information Integrity Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
☐	SI-2	**Flaw Remediation:** The organization identifies, reports, and corrects information system flaws.
☐	SI-3	**Malicious Code Protection:** The information system implements malicious code protection that includes a capability for automatic updates.
☐	SI-4	**Intrusion Detection Tools and Techniques:** The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.
☐	SI-5	**Security Alerts and Advisories:** The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.
☐	SI-6	**Security Functionality Verification:** The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.
☐	SI-7	**Software and Information Integrity:** The information system detects and protects against unauthorized changes to software and information.
☐	SI-8	**Spam and Spyware Protection:** The information system implements spam and spyware protection.
☐	SI-9	**Information Input Restrictions:** The organization restricts the information input to the information system to authorized personnel only.
☐	SI-10	**Information Input Accuracy, Completeness, and Validity:** The information system checks information inputs for accuracy, completeness, and validity.
☐	SI-11	**Error Handling:** The information system identifies and handles error conditions in an expeditious manner.
☐	SI-12	**Information Output Handling and Retention:** The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.

Technical Controls

Technical controls ensure that information security enactment is effective and efficient.

Access Control (AC)

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

	Number	Description
☐	AC-1	**Access Control Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
☐	AC-2	**Account Management:** The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts.
☐	AC-3	**Access Enforcement:** The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.
☐	AC-4	**Information Flow Enforcement:** The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
☐	AC-5	**Separation of Duties:** The information system enforces separation of duties through assigned access authorizations.
☐	AC-6	**Least Privilege:** The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
☐	AC-7	**Unsuccessful Login Attempts—Control:** The information system enforces a limit of [organization-defined number] consecutive invalid access attempts by a user during a [organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [organization-defined time period], delays next login prompt according to [organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.
☐	AC-8	**System Use Notification:** The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.
☐	AC-9	**Previous Logon Notification:** The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Technical Controls

Access Control (AC) *(continued)*

	Number	Description
☐	AC-10	**Concurrent Session Control:** The information system limits the number of concurrent sessions for any user to [organization-defined number of sessions].
☐	AC-11	**Session Lock:** The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
☐	AC-12	**Session Termination:** The information system automatically terminates a session after [organization-defined time period] of inactivity.
☐	AC-13	**Supervision and Review:** The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.
☐	AC-14	**Permitted Actions without Identification or Authentication:** The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.
☐	AC-15	**Automated Marking:** The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.
☐	AC-16	**Automated Labeling—Control:** The information system appropriately labels information in storage, in process, and in transmission.
☐	AC-17	**Remote Access:** The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, broadband, Internet) to the information system. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.
☐	AC-18	**Wireless Access Restrictions:** The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.
☐	AC-19	**Access Control For Portable And Mobile Devices:** The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.
☐	AC-20	**Personally Owned Information Systems:** The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information

Technical Controls

Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

	Number	Description
☐	AU-1	**Audit and Accountability Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
☐	AU-2	**Auditable Events:** The information system generates audit records for the following events: [Assignment: organization-defined auditable events].
☐	AC-3	**Content of Audit Records:** The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.
☐	AU-4	**Audit Storage Capacity:** The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.
☐	AU-5	**Audit Processing:** In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: [organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
☐	AU-6	**Audit Monitoring, Analysis, and Reporting:** The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
☐	AU-7	**Audit Reduction and Report Generation:** The information system provides an audit reduction and report generation capability.
☐	AU-8	**Time Stamps:** The information system provides time stamps for use in audit record generation.
☐	AU-9	**Protection of Audit Information:** The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
☐	AU-10	**Non-repudiation:** The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).
☐	AU-11	**Audit Retention:** The organization retains audit logs for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Technical Controls

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

	Number	Description
☐	IA-1	**Identification and Authentication Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
☐	IA-2	**Auditable Events:** The information system generates audit records for the following events: [Assignment: organization-defined auditable events].
☐	IA-3	**Device Identification and Authentication:** The information system identifies and authenticates specific devices before establishing a connection.
☐	IA-4	**Identifier Management:** The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.
☐	IA-5	**Identifier Management:** The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.
☐	IA-6	**Authenticator Feedback:** The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.
☐	IA-7	**Cryptographic Module Authentication:** for authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.

System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

	Number	Description
☐	SC-1	**System and Communications Protection Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
☐	SC-2	**Application Partitioning:** The information system separates user functionality (including user interface services) from information system management functionality.

Technical Controls

System and Communications Protection (SC) *(continued)*

	Number	Description
☐	SC-3	**Security Function Isolation:** The information system isolates security functions from nonsecurity functions.
☐	SC-4	**Information Remnants:** The information system prevents unauthorized and unintended information transfer via shared system resources.
☐	SC-5	**Denial of Service Protection:** The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].
☐	SC-6	**Resource Priority:** The information system limits the use of resources by priority.
☐	SC-7	**Boundary Protection:** The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
☐	SC-8	**Transmission Integrity:** The information system protects the integrity of transmitted information.
☐	SC-9	**Transmission Confidentiality:** The information system protects the confidentiality of transmitted information.
☐	SC-10	**Network Disconnect:** The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.
☐	SC-11	**Trusted Path:** The information system establishes a trusted communications path between the user and the security functionality of the system.
☐	SC-12	**Cryptographic Key Establishment and Management:** The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.
☐	SC-13	**Use of Validated Cryptography:** When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2
☐	SC-14	**Public Access Protections:** for publicly available systems, the information system protects the integrity of the information and applications.
☐	SC-15	**Collaborative Computing:** The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).
☐	SC-16	**Transmission of Security Parameters:** The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.
☐	SC-17	**Public Key Infrastructure Certificates:** The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.
☐	SC-18	**Mobile Code:** The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.
☐	SC-19	**Voice Over Internet Protocol:** The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.

Audit Reporting

During the reporting phase, management and the board of directors receive formal feedback from the audit team. This knowledge transfer should be an open and transparent process.

Almost every audit identifies opportunities for improvement. The primary goal of management and auditors should be to address critical issues first, followed by important issues. Both management and auditors should work to ensure that, whatever action plans they agree to, the goals are achievable and beneficial to the organization.

During the reporting phase, management must determine which corrective actions it will implement and when, based on audit findings. Mangers will provide oversight and support to ensure the timely resolution of found issues. Although the audit team may make recommendations based on its assessments of risks and consequences, it cannot make or dictate managerial decisions.

The following are typical steps an audit team takes to confirm and release the audit results.[8]

- ☐ Auditors debrief management, formally discussing significant audit findings and conclusions before they issue the final audit report
- ☐ Managers receive a written draft report from auditors
  - — The report communicates audit results clearly and precisely
  - — Results are presented in an unbiased tone, noting where management has taken actions to correct deficiencies and acknowledging good performance
- ☐ Management and auditors discuss the draft report
- ☐ Management provides feedback on the draft report
- ☐ Auditors review managerial comments and action plan(s)
- ☐ Auditors finalize and distribute the final audit report
- ☐ Auditors close out the internal audit project and plan any necessary follow-up efforts regarding management's action plans

Auditors might also choose to communicate some audit findings that might be useful for information security efficiency and effectiveness, but do not warrant inclusion in the formal report. This type of communication should be documented, if only as a note in audit findings that the topic was verbally discussed.

[8] In organizations with established internal audit functions, there may be standard operating procedures (SOP) for audit reporting (and other audit activities). If so, these audit SOPs should be reviewed and understood by management.

Preparing for an Audit

A well-managed business unit or information security program includes robust plans, procedures, goals, objectives, trained staff, performance reporting, and ongoing improvement efforts. The internal audit team looks for evidence that the business unit and information security program are well organized and well managed. The security program must also specifically and traceably mitigate risks related to key business objectives. Managerial preparation should mainly be routine, day-to-day practices.

Management's ultimate goal in the audit process is not to make the auditors happy, but rather to demonstrate that information security efforts meet the demands of the CEO, board of directors, regulators, and investors. Likewise, auditors' requests should be aligned with these overarching needs; that is, to support responsible program performance within a sound, ethical business environment.

While the audit is in the planning phase, management should proactively work with the audit team and "educate" the auditors. As a rule, business or security managers should provide constructive input on the evaluation methodology before audit management approves it. Expectations are a two-way street: management must help auditors ensure that audit expectations are aligned and that participants understand each other.

Prior to the audit, managers should collect the information and documentation necessary to demonstrate how well they manage their operations in concert with the overall organizational business objectives. They should be prepared to provide auditors with evidence of well-managed security efforts and results. This might include documentation of security plans, supporting budgets, policy and procedure manuals, assignments of responsibilities (such as up-to-date job descriptions), results reporting and other trending information, and finally, any other relevant guidance (to management and staff) that demonstrates a "well-run" and performing program.

In selecting documentation, management should not try to overload the audit team with information, but to provide genuine insight into how the information security program is run and how well it is doing. An information security management periodic risk assessment and the organizational business impact analysis (BIA) are two key management efforts to share with auditors.

Management steps prior to an audit:

- ☐ Learn early and contribute often to the internal audit goals, objectives, purpose, approach, and procedures (audit tests). In particular, setting an appropriate purpose and the audit approach are the two most important elements of every successful audit.
- ☐ Discuss with audit management the evaluation criteria and standards and how the audit will actually be conducted, in order to ensure that you'll receive a quality audit. Ask whether they audit in accordance with international standards for the professional practice of internal auditing.
- ☐ Learn who is on the audit team and their qualifications, talents, and motivations. The audit team exists to help make your operations more efficient and effective, but they are also individuals with strengths and weaknesses common to many employees. It pays to know the experience of your auditors, whether they're rookies or veterans (and perhaps to push for the latter). Showing an interest in their work can also influence and increase the benefits from the audit—within reason. At the end of the day, auditors still need to be independent and objective.

Throughout its discussion with the audit team prior to the audit, management should try to strike a balance between influence and deference. Managers should neither yield entirely to the audit team nor micromanage its efforts.

Communicating with Auditors

Like any interaction between people, but particularly in the work environment, a professional and trusting relationship is a strong precursor to successful collaboration.

When managers interact with the auditors in a professional manner, they tell the audit team that its function is respected and supported. Likewise, lackadaisical efforts by managers and staff reflect poorly on the business unit or process, its capabilities, and its performance. Managers should also expect professional interaction from the audit team and push back whenever they see an exception to this practice.

To contribute to a successful and accurate audit report, managers should be receptive to auditor observations and the audit team's recommendations. Managers should also be firm when discussing anything they see as incorrect, in order to ensure there are no misunderstandings.

Finally, always remember: managers, not auditors, are responsible for defining and implementing solutions to issues raised by the audit. Thus, it is in everyone's best interest to have a cooperative, collaborative audit process that respects the independence and discretion of all participants. Auditors should listen to management. And for its part, management should encourage staff to be open and honest with auditors.

APPENDIX A—
Information Security Resources

1. The Computer Emergency Response Team (CERT)—part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University: http://www.cert.org

   - Evaluations & Practices for Insider Threat: http://www.cert.org/nav/index_green.html
   - Computer security incident response team (CSIRT) development: http://www.cert.org/csirts/
   - Governing for Enterprise Security (PDF): http://www.cert.org/archive/pdf/05tn023.pdf
   - Build Security In Initiative (sponsored by the Department of Homeland Security Cyber Security Division): https://buildsecurityin.us-cert.gov/

2. National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC): http://csrc.nist.gov/

   - US Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems" (PDF): http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
   - NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems" (PDF): http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf
   - NIST Special Publication (SP) 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems" (PDF): http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf
   - Federal Information Security Management Act (FISMA) Implementation Project: http://csrc.nist.gov/sec-cert/

3. Corporate Information Security Working Group (CISWG): http://infotech.aicpa.org/Resources/ (under Security Standards, Frameworks and Guidelines) [Documents archived by the American Institute of Certified Public Accountants (AICPA): http://www.aicpa.org/]

   - CISWG Best Practices and Metrics Teams: http://infotech.aicpa.org/Resources/ (under Security Standards, Frameworks and Guidelines; CISWG)
   - Information Security Management References (PDF): http://reform.house.gov/UploadedFiles/Best%20Practices%20Bibliography.pdf

4. ISO 27001 in North America: http://www.27001.com

5. US General Accounting Office, "Executive Guide: Information Security Management: Learning from Leading Organizations": http://www.gao.gov/cgi-bin/getrpt?AIMD-98-21

6. Microsoft Security Risk Management Guide: http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/default.mspx

7. The International Systems Security Engineering Association (ISSEA): http://www.issea.org/

8. U.S. Security Awareness, Information Security Auditing page: http://www.ussecurityawareness.org/highres/infosec-auditing.html

9. The Center for Internet Security (CIS): http://www.cisecurity.org/

10. The Information Systems Security Association (ISSA): http://www.issa.org/

APPENDIX B—
Information Security Auditing Resources

1. The Institute of Internal Auditors, IT Security: http://www.theiia.org/index.cfm?doc_id=3061

    - Global Technology Audit Guide (GTAG) Series: http://www.theiia.org/index.cfm?doc_id=4706

    - "Information Security Management and Assurance: A Call to Action for Corporate Governance" (PDF): http://www.theiia.org/download.cfm?file=22398

    - "Information Security Governance: What Directors Need to Know": http://www.theiia.org/download.cfm?file=7382

    - "Building, Managing, and Auditing Information Security": http://www.theiia.org/download.cfm?file=33288

2. US General Accounting Office (GAO), "Management Planning Guide for Information Systems Security Auditing" (PDF): http://www.gao.gov/special.pubs/mgmtpln.pdf

4. Open Compliance and Ethics Group (OCEG), "Internal Audit Guide (IAG)": http://www.oceg.org/view/IAG

5. National Association of Corporate Directors (NACD), "Information Security Oversight: Essential Board Practices": http://www.nacdonline.org/publications/pubDetails.asp?pubID=138

6. Information Systems Audit and Control Association (ISACA), "Control Objectives for Information and related Technology (COBIT)": http://www.isaca.org/cobit

7. Treasury Board of Canada, Internal Audit: http://www.tbs-sct.gc.ca/ia-vi/home-accueil_e.asp

    - Information Technology Security—Audit Guide: http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TB_H4/01guid01_e.asp

    - Guide to the Audit of Security: http://www.tbs-sct.gc.ca/ia-vi/policies-politiques/gas-gvs/gas-gvs_e.asp

8. The Center for Education and Research in Information Assurance and Security: http://www.cerias.purdue.edu/

ABOUT THE AUTHOR

Dan Swanson, CMA, CIA, CISA, CISSP, CAP

Dan Swanson is a 24-year internal audit veteran who was most recently director of professional practices at the Institute of Internal Auditors. Prior to his work with the IIA, Swanson was an independent management consultant for over 10 years. Swanson has completed internal audit projects for more than 30 different organizations, spending almost 10 years in government auditing at the federal, provincial, and municipal levels, and the rest in the private sector, mainly in the financial services, transportation, and health sectors. The author of more than 75 articles on internal auditing and other management topics, Swanson is currently a freelance writer and independent management consultant. Swanson recently led the writing of the OCEG internal audit guide for use in audits of compliance and ethics programs (www.oceg.org) and participated in the COSO small business task force efforts to provide guidance for smaller public companies regarding internal control over financial reporting (www.coso.org). Swanson is a regular columnist for *ComplianceWeek* and also writes the ITCi "Auditor Answers" column.

If you have ideas for improving the IT Audit Checklists, please write editor@itcinstitute.com.