IT AUDIT CHECKLIST SERIES

ComplianceINSIGHT

Logging, Monitoring, and Reporting

Practical guidance for management on how to prepare for successful audits

Research Sponsor

LogLogic

www.ITCinstitute.com

IT Compliance Institute™

ComplianceINSIGHT

IT AUDIT CHECKLIST SERIES

Logging, Monitoring, and Reporting

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 Information Technology 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@itcinsititute.com.

Table of Contents

EXECUTIVE OVERVIEW

What Is the IT Audit Checklist Series?

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 also help managers proactively complete self assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of actual audit.

What Is This Paper About?

This paper supports an internal audit of the organization's logging, monitoring, and reporting policies and procedures as a function of compliance, risk management, and governance. The recommendations herein are intended to help management ensure the overall confidentiality, integrity and availability of IT systems and infrastructure.

This paper includes advice on assessing the existence and robustness of logging, monitoring, and reporting functions; guidance on how management and auditors can support effective assurance; and information on promoting the continual improvement of IT governance efforts through improvement of critical logging, measurement, and reporting functions. The paper is intended to help IT, compliance, audit, and business managers prepare for an audit of high-level processes and resources and to provide concrete tools managers can use to ensure that the audit experience and results are as beneficial as possible to both IT leaders and the company as a whole.

Paper Contents

- All audits are opportunities for companies to improve, based on auditor analysis and advice. But 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. In response to various regulatory requirements, auditors will look for documentation of control existence and effectiveness provided by logging, monitoring, and reporting documentation, as well as evidence of controls around the log management, monitoring, and reporting processes themselves.
- All regulations require some degree of logging, monitoring, and/or reporting. Reporting is intrinsic to compliance and is generally based on some level of monitoring. Monitoring, in turn, usually relies on an audit trail—often provided by logs. Broadly accepted standards, such as ISO 27001/27002 (formerly ISO 17799:2005) and ITIL, also prescribe logging, monitoring, and reporting guidance.
- On the surface, logging, monitoring, and reporting might seem like mundane, even rote, compliance exercises. In reality, however, these processes are often the workhorses of managerial oversight--providing baselines, test results, and even surprising insight that shapes IT and business management across the enterprise.
- This document provides a "base-level" IT audit checklist that is generic enough to be applicable across a broad range of user environments and regulatory demands, yet specific enough to provide actionable guidance. Controls cited in this paper are derived from ISACA's CobiT; ITIL from the UK Office of Government Commerce (OGC); Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" from the National Institute of Standards and Technology (NIST); ISO 27002, (formerly ISO 17799:2005) from the International Organization for Standardization; and the authors' own experience.

INTRODUCTION TO LOGGING, MONITORING AND REPORTING

Logging, monitoring, and reporting practices and requirements transcend compliance regimes. They are the primary vehicle of assurance for management, auditors, and regulators that control objectives are being met—or, if not fully met, then progressively improved.

From Sarbanes-Oxley (SOX) to Gramm-Leach-Bliley (GLB), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the PCI Data Security Standard (PCI DSS), and Basel II, the need for measurable assurance is built into most major regulations. Specific requirements are explored in more detail later in this paper.

This paper focuses on the aspects of reporting most clearly related to IT—both as a subject of monitoring and a tool of reporting. The heart of the paper is a list of controls related to logging, monitoring, and reporting functions that are necessary for compliance. To provide a logical order and hierarchy for this extensive number of recommended controls, the paper loosely refers to the control groupings and hierarchy suggested by NIST guidance on log management. However, the full content of the control checklist goes beyond NIST recommendations to incorporate CobiT and ISO guidance, as well.

What Is Logging, Monitoring, and Reporting?

Logging provides a record of events related to IT systems and processes. Each recorded event is a log entry, denoting information such as what occurred, when it occurred, and who or what caused it. A log might be as simple as a text list of application logons for a service host or as complex as a description of transactions across an ERP system. Logs provide a record that is the foundation of effective monitoring, which provides the fodder for managerial reporting. Without reporting there is no compliance.

Logs are both inputs and outputs of monitoring, providing the data record through which managers can examine IT systems and processes. Managers monitor logs to look for state changes, exceptions, and other significant events. If monitoring produces records, those are also logs that might be subject to further analysis or simply fulfill a compliance documentation requirement. Within the scope of this paper, monitoring generally refers to IT controls that are put in place for the purpose of compliance.

Reporting, for the purposes of this paper, refers to the generation (automatic or manual) of reports that indicate the status of IT controls designed to meet compliance goals. Reporting is intermeshed with both monitoring and logging, since reports can be based on the output of both monitoring and logging activities. To complicate the mix, some authorities—such as ISO 27002—require management to report on the effectiveness of reporting and monitoring controls.

What Are the Benefits of Logging, Monitoring, and Reporting?

On the surface, logging, monitoring, and reporting might seem like mundane, even rote compliance exercises. In reality, however, these processes are often the workhorses of managerial oversight—providing baselines, test results, and even surprising insight that shapes IT and business management across the enterprise. Logging, monitoring, and reporting are key elements of IT governance that meet the needs of a variety of enterprise stakeholders and provide the tools to resolve a broad range of IT problems. They provide the data and diagnostic tools that allow managers to identify and respond to significant events and process exceptions in order to reduce business risk.

- **Logging**—Successful logging offers value beyond compliance that includes support of overall IT

functions including performance management, change management, security management, and project planning.

- **Monitoring**—Monitoring is the window into IT operations for both managers and auditor. Good monitoring provides historical and realtime views of IT control performance. Good monitoring also supports overall IT functions including performance management, change management, training, security management, and project planning.
- **Reporting**—Reports are the currency of compliance for auditors. Without reliable, accurate, consistent, and verifiable reporting, there can be no compliance assurance. Good reporting also helps IT managers to evaluate system and employee performance over time and provides input for balanced scorecards and other managerial mechanisms.

Benefits of logging, monitoring, and reporting include:

- **Stronger IT governance**—Logging, monitoring, and reporting are the information lifeblood of compliance, risk management, and governance. They reveal problems, put performance indicators behind managerial decisions, and supply evidence for control assurance, and provide evidence for risk analyses.
- **Better managerial oversight**—By providing a record of real-world events, logs provide invaluable information that can validate or dispel managerial assumptions, reveal unrecognized performance issues, point to problem-specific solutions, and provide case studies for staff training.
- **Support of corporate information security**—Logs can provide a record of access and authentication events, note configuration or application changes that could compromise system integrity, record details of inbound and outbound information traffic, and provide a corpus of evidence for forensic investigation of security breaches.
- **Stronger service-level agreements (SLAs)**—Logs monitoring is a critical component of SLA assurance, revealing service interruptions, threats to network stability, and other critical evidence that support troubleshooting efforts.
- **Performance validation**—Logs and monitoring provide the basis for performance measurement, while reporting requirements ensure that managers have the information they need to make intelligent decisions about process changes that impact performance outcomes.
- **More effective change control**—Logs provide a record of configuration, application, network, and other types of changes that might otherwise go unnoticed by management.[1]
- **Regulatory Compliance**—Logging, monitoring, and reporting provide both the means and data for auditing, intrusion monitoring, compliance monitoring, and ensuring adherence to segregation of duties.
- **More consistent problem identification, monitoring, and resolution**—Logs have conventionally been used to troubleshoot IT operational and process failures. Consistent log monitoring can also provide an early warning system for system problems, revealing network instability and changes before they impact IT systems. Most recently, IT best-practice standards and regulatory requirements have put parameters around the logging, monitoring, and reporting controls, as well as the retention of records and reports that evidence control effectiveness.

[1] For more information on measurement and monitoring controls related to change management, read ITCI's IT Audit Checklist for Change Management, available at http://www.itcinstitute.com/display.aspx?id=2499.

THE AUDITOR'S PERSPECTIVE ON LOGGING, MONITORING, AND REPORTING

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.

In response to various regulatory requirements, auditors will look for documentation of control existence and effectiveness provided by logging, monitoring, and reporting documentation, as well as evidence of controls around the log management, monitoring, and reporting processes themselves. Some of the key regulations that require measurement and reporting policies and procedures include:

- **SOX**—Although the SOX act does not contain any specific IT requirements, Auditing Standard No. 2 (AS 2), the primary audit guidance for Sarbanes-Oxley published by the Public Company Accounting Oversight Board (PCAOB), states, "The auditor's understanding of management's monitoring of controls extends to and includes its monitoring of all controls, including control activities, which management has identified and designed to prevent or detect material misstatement in the accounts and disclosures and related assertions of the financial statements." Specific indications related to this sweeping directive include proof of control over access to financial data, including logging, monitoring, and reporting the status of and changes to system-user privileges, duties, and activities. Auditors might also require proof of other monitoring efforts, such as anti-virus logs, under the broad umbrella of "IT general controls."

- **HIPAA, FISMA, GLB, state and international privacy and data protection laws, etc.**—For all regulations and standards that require the protection of integrity, availability, and confidentiality of personally identifiable data, auditors may require log- and report-based evidence of effective IT controls. Most US federal requirements for log management are aligned with the log management recommendations published by NIST.[2]

- **ISO 27002**—Section 9.7.2.3 of the international data security standard requires the organization to monitor logs to identify security events. Section 10.10 addresses the need for audit logs and system activity logs, log information and communication faults, and the protection of "logging facilities and log information."

- **PCI DSS**—The PCI DSS, which is based on ISO 17799 (the precursor to ISO 27002), contains fairly explicit log management requirements. Requirement 10 of the DSS requires organizations to "Track and monitor all access to network resources and cardholder data," and encompasses seven subsections of logging and monitoring specifications. Since the PCI DSS is concerned with a fairly narrow subset of sensitive cardholder data, its requirements do not necessarily apply to all enterprise systems, but may be limited to applications, operating systems, network technologies, and database technologies related to PCI in-scope systems. The objective of these requirements is both reactive and forensic: first, to alert IT managers if unauthorized access occurs; second, to provide forensic evidence in case of a breach.

2 Several NIST publications reference logging and log management. NIST's seminal guidance on the topic is Special Publication 800-92, "Guide to Computer Security and Log Management." NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," also contains log management recommendations.

The size and complexity of various organizations' audit efforts in response to these requirements 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.[3] 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 organization's many risks and opportunities. Finally, in many companies, continuous auditing (ongoing audit evaluations) is being implemented for key systems and/or key transactions.

Who Is Responsible for Logging, Monitoring, and Reporting?

Executive management (of IT and business lines), and internal auditors all have significant roles in logging, monitoring, and reporting assurance and the auditing of related 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) **Executive management** must help other levels of management understand the types of reporting it needs to feel confident in its attestations. Executives must also provide leadership to ensure that logging, monitoring, and reporting efforts are appropriate, supported, and understood across the organization. And they must ensure that sufficient resources are dedicated to enable controls to be effective.

   Finally, by ensuring that logging, monitoring, and reporting efforts and their management are subject to audit and reviewed by qualified professionals, corporate leaders advance the goal of corporate oversight and promote its continuous improvement and success.

2) **IT, security, and line-of-business managers** must have a voice in the design and implementation of logging, monitoring, and reporting policies and procedures, since those managers are held accountable for protecting and enhancing the value of the organization's assets, including information assets. Managers must also review and monitor logging, monitoring, and reporting controls to ensure they are appropriate, despite ever-changing risks and business requirements. This is, in fact, a form of auditing. And, finally, managers who own business-unit information should also help define their logging, monitoring, and reporting requirements, based on business objectives, regulatory mandates, operational constraints, and the overall level of competence with regard to logging, monitoring, and reporting.

   Under a separate aspect of management, information security managers should have direct input into the organization's logging, monitoring, and reporting controls, since so many of the controls are driven by information-protection requirements.

   Although business managers often try to relegate compliance measurement and reporting responsibilities to a narrow IT function, all parts of the organization have some responsibility for related controls. Logging, monitoring, and reporting 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

3 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

ensure they are (a) adequate, as defined to mitigate oversight risks, and (b) reasonably efficient and effective in practice.

3) The **internal audit function** provides strategic, operational, and tactical value to the control process. For example, internal auditing:

   - Informs the board and management as to whether business units understand the importance of logging, monitoring, and reporting and are adhering to policies; whether key information assets and systems are sufficiently managed, protected and monitored; whether programs are in place for continually updating and strengthening safeguards against information security breach, system failure, and employee misdeeds; and whether policies are reasonable. In brief, internal audits assess the state of the information control environment and recommend improvements.
   - Independently validates that the organization's logging, monitoring, and reporting efforts are proactive and effective in detecting current and emerging threats. To provide this level of assurance, internal auditors might compare current organizational practices with industry best practices and regulatory guidelines.

Of course, 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, internal auditors need to: 1) know what they are doing (have the skills to perform appropriate logging, monitoring, and reporting 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 audit function should complement, but never replace or overpower, management's responsibility to ensure its logging, monitoring, and reporting controls are operating effectively.

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:

☐ **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 logging, monitoring, and reporting 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 logging, monitoring, and reporting), including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors need to review and assess evidence of the logging, monitoring, and reporting 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.

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, if not continuous, operational monitoring
- ☐ Supervisory review of key reports and operating results
- ☐ 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
- ☐ 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 ...

- ☐ Managers who adopt the "letter" of requirements in order to satisfy audit requirements, rather than embracing the "spirit" of the controls for the full risk mitigation they can offer
- ☐ 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 Help (or Hinder) Auditors

- ☐ (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). 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.

Logging, Monitoring, and Reporting Audit Checklist

Your audit's goals, scope, and purpose determine the appropriate audit procedures and questions. An audit of logging, monitoring, and reporting 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 logging, monitoring, and reporting audit steps that management might follow in preparation for and during an audit. The list does not attempt to itemize every possible control objective that might fall under the topic of this paper, 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 with oversight of logging, monitoring, and reporting controls meet with the audit team to review audit program steps and define key players and necessary resources
- ☐ Management collects documentation in preparation for audit
- ☐ Management supports a preliminary survey of logging, monitoring, and reporting efforts (by the internal audit team)
- ☐ The audit team drafts the internal audit program plan
- ☐ Management and board members provide feedback on the draft audit program plan

Audit Testing

Management has a responsibility to ensure that audit testing is productive. The audit team performs tests to independently assess the logging, monitoring, and reporting controls. Although the audit team ultimately determines the nature of these tests and the extent of testing (e.g. 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 micromanaging 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. logging, monitoring, and reporting 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 powerful tool for swaying an adverse opinion before the audit report is finalized.

Since the audit report often forms the basis of future logging, monitoring, and reporting efforts and investments, 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 logging, monitoring, and reporting practices 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 logging, monitoring, and reporting, as well as 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 logging, monitoring, and reporting 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 logging, monitoring, and reporting policies and procedures
- ☐ Managers assist auditors with walkthroughs of selected processes and control documentation
- ☐ Auditors evaluate the quality of information generated by the logging, monitoring, and reporting 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 logging, monitoring, and reporting performance metrics: existence, usefulness, application, monitoring, and responses to identified exceptions
- ☐ Auditors evaluate whether logging, monitoring, and reporting controls are sufficiently preventive, as well as detective
- ☐ Auditors define tests to confirm the operational effectiveness of logging, monitoring, and reporting 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 and recommend opportunities for improvement of logging, monitoring, and reporting activities
- ☐ Managers and auditors complete an exit meeting to discuss audit findings, auditor recommendations, and managerial response

Controls for Logging, Monitoring, and Reporting

Although the actual controls to be audited are determined during the audit planning phase, controls are assessed during the audit testing phase. Management should determine which 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 generally accepted guidance on on logging, monitoring, and reporting management.

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). As a frame of reference, the following controls section also refers to CobiT categories as a baseline for defining management, operational. and technical controls. The rationale for this approach is:

- CobiT as control framework ties together IT governance and business processes. Therefore, each identified control may be linked to both an IT governance and business process requirement. This approach provides focus so that controls are not discussed only in relation to meeting a specific mandate, such as HIPAA, but rather are considered in relation to broader governance and risk management requirements.
- This approach extends the discussion of controls even beyond IT governance and compliance, tying control objectives to business value. This is a subtle point, but one worth considering—particularly when discussing processes that can support both compliance and performance improvement.
- As described earlier, some logging, monitoring, and reporting requirements are actually about reporting on the effectiveness of logging, monitoring, and reporting controls. Because the apparent circularity of this requirement can lead to confusion, it helps to map the controls discussion back to a higher-level framework.

CobiT defines four control domains:[4]

- **Plan and Organize (PO)**—This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives
- **Acquire and Implement (AI)**—To realize the IT strategy, IT solutions need to be identified, developed, or acquired, as well as implemented and integrated into the business process
- **Deliver and Support (DS)**—This domain is concerned with the actual delivery of required services, which includes service delivery, management of IT security and continuity, service support for users, and management of data and operational facilities
- **Monitor and Evaluate (ME)**—All IT processes must be regularly assessed over time for quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance.

Of the four domains, the critical IT controls related to logging, monitoring, and reporting mostly map into the DS and ME domains. In addition to drawing from CobIT, IT controls in the following tables represent ISO 27002, ITIL, NIST 800-53, NIST 800-92, the PCI DSS, and the authors' experience.

4 CobiT 4.0 (2005). ISACA. http://www.isaca.org/AMTemplate.cfm?Section=Overview&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22940 (PDF)

Management Controls

Management controls ensure a well-run and effective logging, monitoring, and reporting program. In general, management controls assess whether:

- ☐ Logging, monitoring, and reporting policies and procedures have been established
- ☐ Performance logging, monitoring, and reporting are measured
  - __ Performance metrics are established and documented
  - __ Management regularly monitors performance results
- ☐ The budget supports appropriate logging, monitoring, and reporting
- ☐ A continuous improvement program is in place and operates effectively

Management controls include:

Service-Level Management

	CONTROL DESCRIPTION
☐	**Definition and Management of Service Levels:** The organization ensures the alignment of IT services and business strategy by 1) identifying service requirements, 2) defining service levels, and 3) measuring service performance to goals. (Source=CobiT DS 1)
☐	**Service-Level Monitoring Plan:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented policy for service performance monitoring, and 2) procedures to facilitate the implementation of service performance monitoring policies and associated controls. (Source: ITIL SD/SLM 4.3.2)

Management Controls

IT Performance Evaluation

CONTROL DESCRIPTION

- ☐ **IT Performance Measurement Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, IT performance measurement policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the performance measurement policy and associated audit and accountability controls. (Source: CobiT ME 1.1)
- ☐ **IT Performance Measurement Framework:** The organization follows a performance monitoring framework and approach that defines performance measurement scope, methodology and process. (Source: CobiT ME 1.1)
- ☐ **Managerial Reporting on IT Performance:** The organization provides IT performance reports for senior management. Management reviews reports to assess the organization's progress toward established goals, specifically in terms of IT investments and initiatives, as well as IT service contributions and levels within specific programs. Management reviews any deviations from expected performance and responds with an appropriate action to close the gap. The organization records managerial responses. (Source: CobiT ME 1.5)

Information Security Strategy

CONTROL DESCRIPTION

- ☐ **Information Security Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) formal, documented, information security management policy that addresses security policy, procedures, standards, monitoring, detection, reporting, and incident resolution; and 2) documented procedures to facilitate the implementation of system security policy and associated controls. (Source: CobiT DS 5, DS 5.5, NIST 800-53; ISO 27002 5.1)
- ☐ **Compliance Assurance:** The organization implements policies and procedures to: 1) confirm regulatory compliance, 2) identify areas of control deficiency, and 3) describe remediation and improvement status for identified control deficiencies. The organization integrates IT control reporting with complementary reports from business units. (Source: CobiT 3.4, 3.5; ISO 27002 15.2.1)

Access Control Policy and Procedures

CONTROL DESCRIPTION

- ☐ **Access control policies and procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. (Source: NIST 800-53, ISO 27002 10.10.2, CobiT DS 5.5)
- ☐ **Account Management Review:** Management reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently, the activities of users with significant information system roles and responsibilities. (Source: NIST 800-53, ISO 27002 10.10.2)

Management Controls

Audit and Accountability

CONTROL DESCRIPTION

- ☐ **Audit and Accountability Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. (Source: NIST 800-53, CobiT DS 5.5, ISO 27002 15.3.1)
- ☐ **Audit Group:** The organization develops an auditor's group, whose members can view and archive the event logs. (Source: NIST 800-53)

System Security Assessment and Accreditation

CONTROL DESCRIPTION

- ☐ **Deficiency Remediation Plan and Milestones:** The organization develops and periodically updates 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 reported during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. (Source: NIST 800-53, CobiT DS 5.5)

Change and Configuration Management

CONTROL DESCRIPTION

- ☐ **Change Management Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, change management policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the change management policy and associated monitoring and management controls. (Source: NIST 800-53, CobiT DS 9, ISO 27002 10.1.2)
- ☐ **Configuration Management Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the configuration management policy and associated monitoring and management controls. (Source: NIST 800-53, CobiT DS 9)

Management Controls

Identification and Authentication

CONTROL DESCRIPTION

☐ **Identification and Authentication Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. (Source: NIST 800-53)

Incident Response

CONTROL DESCRIPTION

☐ **Incident Response Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. (Source: NIST 800-53, PCI 12.9, CobiTDS 5.5)

☐ **Help/Service Desk Policies and Procedures:** The organization develops and documents policies and procedures for monitoring trends related to the IT help desk function. (Source: NIST 800-53, CobiT DS 8)

System Maintenance

CONTROL DESCRIPTION

☐ **System Maintenance Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. (Source: NIST 800-53)

Media Protection

CONTROL DESCRIPTION

☐ **Media Protection Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. (Source: NIST 800-53)

Management Controls

Physical Protection

CONTROL DESCRIPTION

☐ **Physical Protection Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. (Source: NIST 800-53)

Risk Assessment

CONTROL DESCRIPTION

☐ **Risk Assessment Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. (Source: NIST 800-53, CobiT PO 9)

Systems Acquisition

CONTROL DESCRIPTION

☐ **Systems Acquisition Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. (Source: NIST 800-53)

Systems and Communications Protection

CONTROL DESCRIPTION

☐ **Systems and Communications Protection Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. (Source: NIST 800-53, CobiT DS 5.5)

Systems and Information Integrity

CONTROL DESCRIPTION

☐ **Systems and Information Integrity Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Operational Controls

Operational controls ensure the effective performance of the logging, monitoring, and reporting efforts. Operational controls assess whether:

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

Operational controls include:

Service-Level Management

CONTROL DESCRIPTION
☐ **Service-Level Monitoring and Reporting:** The organization continuously monitors identified service-level performance criteria and provides status reports to stakeholders. (Source: CobiT DS 1.5)
☐ **Service-Level Analysis:** The organization analyzes audit statistics and identifies trends in individual services and overall service performance. (Source: CobiT DS 1.5)

Access Control

CONTROL DESCRIPTION
☐ **Information Access Tracking:** The organization monitors and controls all access to data. (NIST 800-53, PCI 12.5.5)
☐ **Account Management:** The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Account management includes 1) monitoring of guest/anonymous account usage, 2) reporting to account managers when information system users are terminated or transferred, 3) when users' information system usage or need-to-know changes. (Source: NIST 800-53, NIST 800-125; ISO 27002 11.5)
Access Control continued
☐ **Account Change Notification:** The organization ensures that reports of all account modifications and terminations go to appropriate individuals. (Source: NIST 800-53, NIST 800-12)
☐ **Account Access Supervision and Review:** The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. (Source: NIST 800-53)
☐ **Remote Access Tracking:** The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method. (Source: NIST 800-53)

[5] NIST Special Publication 800-12 "An Introduction to Computer Security – The NIST Handbook"

Operational Controls

Access Control *(continued)*

- ☐ **Wireless Access Tracking:** The organization documents, monitors, and controls wireless access to the information system. (Source: NIST 800-53) The organization copies logs for wireless networks onto a log server on the internal LAN. (Source: PCI 10.5.4)
- ☐ **Access Tracking for Portable and Mobile Devices:** The organization documents, monitors, and controls device access to organizational networks. (Source: NIST 800-53)
- ☐ **System Use Notification:** The restricted information system displays an approved system use notification message before allowing access. The notification informs potential users that: 1) they are accessing restricted information system; 2) system usage might be monitored, recorded, and subject to audit; 3) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4) that use of the system indicates consent to monitoring and recording. The notification also 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. (Source: NIST 800-53)

System Logging and Monitoring

CONTROL DESCRIPTION

- ☐ **Log Monitoring, Analysis, and Reporting:** The organization regularly: 1) reviews and analyzes audit records for indications of inappropriate or unusual activity; 2) investigates suspicious activity or suspected violations, 3) reports findings to appropriate officials, and 4) takes necessary actions. (Source: NIST 80-53; CobiT DS 2, DS 5.5)

  The organization reviews logs for all PCI in-scope system components at least daily. Log reviews include servers that perform security functions, such as intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers. (Source: PCI 10.6)

  The organization periodically reviews outsourced service records and reports for indications of exceptional or suspicious activity and service violations. The organization reports findings to appropriate stakeholders and respond appropriately. (Source: CobiT DS 2.4, DS 5.5)
- ☐ **Log Retention:** The organization retains audit logs for a management-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. (Source: NIST 800-53) Generally, security logs are retained for at least a few weeks, preferably a few months (Source: NIST 800-61, CobiT DS 5.5)

  The organization retains audit trails for PCI in-scope systems for at least one year, with a minimum of three months online availability. (Source: PCI 10.7)

Security Assessment and Accreditation

CONTROL DESCRIPTION

- ☐ **Periodic Reaccreditation:** The organization periodically retests and reaccredits systems. (Source: NIST 800-37, CobiT DS 5.5)
- ☐ **Security-Control Measurement and Monitoring:** Management continually assesses security-control effectiveness using industry best practices and benchmarks, when available. The organization maintains records of security control effectiveness, demonstrating that the organization: 1) assesses security controls; 2) analyzes and reports control weaknesses and changes; and 3) adjusts the information system security plan to support control remediation and performance. (Source: CobiT ME 2.1, DS 5.5; ISO 27002 15.2.1, 15.2.2)

Operational Controls

Security Assessment and Accreditation *(continued)*

- ☐ **System Connection Tracking:** 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. (NIST 800-53)

Contingency and Continuity Management

CONTROL DESCRIPTION

- ☐ **Threat Tracking:** The organization uses logging, monitoring, and reporting to identify potential sources of IT service interruptions, threats to network stability, and other critical evidence that support troubleshooting efforts. (Source: CobiT DS 4)
- ☐ **Contingency Plan Testing:** The organization's business contingency/continuity plan addresses the need to monitor and report on critical-resource availability, access and processing alternatives, and effectiveness of offsite backup and recovery procedures. (Source: NIST 800-53)

Change and Configuration Management

CONTROL DESCRIPTION

- ☐ **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. (Source: NIST 800-53)
- ☐ **Monitoring Configuration Changes:** Control: The organization monitors additions, modifications, and deletions to information systems and conducts security impact analyses to determine the effects of the changes. After the information system is changed, the organization checks the security features to ensure the features are still functioning properly. (Source: NIST 800-53)
- ☐ **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. (Source: NIST 800-53, ISO 27002 12.5)
- ☐ **Software and Information Change Detection:** The information system detects and protects against unauthorized changes to software and information. (Source: NIST 800-53, , CobiT DS 9, ISO 27002 10.1.2)

  The organization installs file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts—although new data being added should not trigger an alert. (Source: PCI 10.5.5)

Identification and Authentication

CONTROL DESCRIPTION

- ☐ **Authenticator Management:** The organization manages information-system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by:1) defining initial authenticator content; 2) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and 3) changing default authenticators upon information system installation. (Source: NIST 800-53)

Operational Controls

Incident Response

CONTROL DESCRIPTION

- ☐ **Incident Tracking:** The organization tracks and documents information system security incidents on an ongoing basis. (Source: NIST 800-53, CobiT DS 5.5)
- ☐ **Incident Response Scope:** Incident response includes alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems for PCI in-scope systems (Source: PCI 12.9.5)
- ☐ **Incident Reporting:** The organization promptly reports incident information to appropriate authorities. (Source: NIST 800-53, CobiT DS 5.11, ISO 27002 13.1)
- ☐ **Incident Response Support:** The organization provides an incident response support (or help desk) 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. (Source: NIST 800-53)
- ☐ **Incident Response Support Monitoring:** The organization monitors and reports trends related to incident response support. (Source: CobiT DS 8, ISO 27002 13.2)

System Maintenance

CONTROL DESCRIPTION

- ☐ **System Maintenance-Tool Tracking:** The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis. The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications. The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system. The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception. (Source: NIST 800-53)
- ☐ **Remote Maintenance Monitoring:** The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities. The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions. (Source: NIST 800-53)

Media Protection

CONTROL DESCRIPTION

- ☐ **Media Access Monitoring and Control:** The organization monitors access to media and ensures that only authorized users have access to information in printed form or on digital media removed from the information system. (Source: NIST 800-53)
- ☐ **Media Preservation:** The organization chooses storage media and systems to facilitate the retrieval of stored data, if required, in an optimal time frame and format. (Source: CobiT DS 11)
- ☐ **Media Sanitization Monitoring:** The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance. (Source: NIST 800-53)

Operational Controls

Infrastructure Protection

CONTROL DESCRIPTION

- ☐ **Infrastructure Monitoring:** The organization monitors the IT infrastructure and maintains a log with sufficient detail to enable investigators to understand sequences of operations, impacting events, and other activities related to operational management. (Source: CobiT DS 13.3)

Physical Protection

CONTROL DESCRIPTION

- ☐ **Physical Access Tracking:** The organization monitors physical access to information systems to detect and respond to incidents. The organization reviews physical access logs periodically, investigates apparent security violations or suspicious physical access activities, and takes remedial actions. The organization monitors real-time intrusion alarms and surveillance equipment. (Source: NIST 800-53,CobiT DS 12, ISO 27002 9.1.2)
- ☐ **Visitor Tracking:** The organization logs and authenticates visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. The organization monitors visitor activity to the degree indicated by the situation and required by managerial policy. (Source: NIST 800-53, CobiT DS 12.3)
- ☐ **Visitor Access Log Reviews:** Designated officials within the organization periodically review visitor access logs after closeout. (Source: NIST 800-53, CobiT DS 12.3)
- ☐ **Internal Climate Control:** The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems. (Source: NIST 800-53)
- ☐ **Third-Party Security Monitoring:** The organization establishes service-level agreements and personnel security requirements for third-party service providers. The organization monitors provider compliance and service levels to ensure adequate security and overall supplier performance. Third-party service managers provide performance reports to business management. (Source: NIST 800-53, CobiT DS 2)

Systems Acquisition

CONTROL DESCRIPTION

- ☐ **Software Usage Monitoring:** The organization complies with software usage restrictions. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. If the organization hosts a publicly accessible peer-to-peer file sharing technology, the organization controls and documents its use to ensure that it is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. (Source: NIST 800-53)
- ☐ **Outsourced Information Services Tracking:** The organization monitors security controls to ensure that third-party providers of information system services employ adequate security controls in accordance with applicable laws, policies, standards, and service-level agreements. Third-party providers are required to conform to the same security control and documentation requirements as would apply to the organization's internal systems. The organization explicitly tracks information on outsourced providers, including hirer, service provider, and end user security roles and responsibilities, and any service level agreements. (Source: NIST 800-53, ISO 17799 10.2.2, CobiT DS 2.4)

  The organization periodically reviews outsourced service records and reports for indications of exceptional or suspicious activity and service violations. The organization reports findings to appropriate stakeholders and respond appropriately. (Source: CobiT DS 2.4)

Operational Controls

Systems and Communications Protection

CONTROL DESCRIPTION

- ☐ **Boundary Monitoring:** The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. (Source: NIST 800-53)
- ☐ **Mobile Code Monitoring:** The organization documents, monitors, and controls the use of mobile code within the information system. (Source: NIST 800-53)
- ☐ **VOIP Monitoring:** The organization documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP. (Source: NIST 800-53)

Systems and Information Integrity

CONTROL DESCRIPTION

- ☐ **Flaw Remediation:** The organization identifies, reports, and corrects information system flaws. The organization identifies information systems containing proprietary or open source software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws. (Source: NIST 800-53, CobiT 5.5)
- ☐ **Error Handling:** The information system monitors for, identifies, and handles error conditions in an expeditious manner. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. (NIST 800-53)
- ☐ **Security Alerts:** The organization receives information system security alerts/advisories on a regular basis, documents the types of actions to be taken in response to security alerts/advisories, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response. (Source: NIST 800-53)

Technical Controls

Technical controls ensure that the implementation of logging, monitoring, and reporting is effective and efficient. Technical controls include:

Account Management

CONTROL DESCRIPTION

- ☐ **Automation of Account Management:** The organization employs automated mechanisms to support the management of information system accounts, including 1) Auditing of account creation, modification, disabling, and termination actions 2) automatic deletion of accounts after a predefined period of inactivity. (Source: NIST 800-53, CobiT DS 5.5)
- ☐ **Automation of Remote Access Monitoring:** The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (Source: NIST 800-53)
- ☐ **Automation of Wireless Access Monitoring:** The organization employs automated mechanisms to facilitate the monitoring and control of wireless access methods. (Source: NIST 800-53)

Technical Controls

Account Management *(continued)*

☐ **Automation of Access from Portable and Mobile Devices:** The organization employs automated mechanisms to facilitate the monitoring and control of network access from portable and mobile devices. (Source: NIST 800-53)

☐ **Protection of Cardholder Data:** Monitor access attempts and prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files). (Source: PCI 4.1)

Systems Performance Management

CONTROL DESCRIPTION

☐ **Capacity and Performance Modeling:** The uses results from testing and tracking system capacity, availability, and performance to build predictive models and forecasts for performance scenarios. (Source: CobiT DS 3; ITIL SD/AM 8.7, SD/CM 6.3.1)

Education and Training

CONTROL DESCRIPTION

☐ **Training Records:** The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. The organization tests and measures the effectiveness of training efforts. (Source: NIST 800-53, CobiT DS 7)

Log and Audit records

CONTROL DESCRIPTION

☐ **Auditable Events:** The information system generates audit records for organizationally defined events, such as logins and login types, modification of system configuration or elements, password modification, and access violation: Audit records are adequate to support after-the-fact investigations of security incidents. (Source: NIST 800-53, CobiT 5.5, ISO 27002 10.10.2)

The organization generates audit trails and logs for all in-scope PCI-system components to reconstruct the following events:

- All individual user accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects.

(Source: PCI 10.2 and subparts)

Technical Controls

Log and Audit records *(continued)*

☐ **Log / Audit Record Content:** 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. The information system allows staff to add additional detail to audit records. (Source: NIST 800-53) The organization sets the level of required logging according to a risk assessment of the relevant systems. (Source: NIST 800-53, CobiT DS 5.5)

Logs for PCI in-scope systems do not include Personal Account Numbers (PANs). (Source: PCI 3.4)

The organization records at least the following audit trail entries for all in-scope PCI-system components for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource.

(Source: PCI 10.3 and subparts)

☐ **Centralized Log Management:** The information system enables staff to centrally manage the content of audit records generated by individual components throughout the system.

☐ **Log Storage Capacity:** The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded. (Source: NIST 800-53)

☐ **Log Processing:** In the event of an audit failure or overflow of audit storage capacity, the information system alerts appropriate organizational officials and automatically reacts in an appropriate matter designed by managerial staff. (Source: NIST 800-53)

☐ **Automation of Log Monitoring:** The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. (Source: NIST 800-53)

☐ **Automation of Alerts:** The organization employs automated mechanisms to immediately alert personnel of inappropriate or exceptional activities with risk implications. (Source: NIST 800-53)

☐ **Audit Report Generation:** The information system generates audit reports that support after-the-fact investigations of incidents without altering original audit records. Audit records can be automatically processed for events of interest based upon selectable event criteria. (Source: NIST 800-53)

☐ **Log Time Stamps:** The information system time stamps audit records generation. Time stamps of records are generated using internal system clocks that are synchronized system-wide. (NIST 800-53, PCI 10.4)

☐ **Protection of Logs and Audit Information:** The information system protects audit information and audit tools from unauthorized access, modification, and deletion. (Source: NIST 800-53; PCI 10.5, 10.5.2, CobiT DS 5.5, ISO 27002 10.10.3)

The organization limits access to audit trails to those with a job-related need. (Source: PCI 10.5.1) and promptly backs-up audit trail files to a centralized log server or media that is difficult to modify (Source: PCI 10.5.3)

☐ **Non-Repudiation:** The information system can determine whether a given individual took a particular action. (Source: NIST 800-53)

The organization establishes a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. (Source: PCI 10.1)

Technical Controls

Security Assessment and Accreditation

CONTROL DESCRIPTION

☐ **Continuous Monitoring:** The organization monitors the security controls in the information system on an ongoing basis. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring.1 (Source: NIST 800-53; CobiT ME 2, ME 3; ISO 27002 15.2.1)

Change and Configuration Management

CONTROL DESCRIPTION

☐ **Automation of Configuration Change Control:** The organization uses automated mechanisms to: 1) document proposed changes to the information system; 2) notify appropriate approval authorities; 3) highlight approvals that have not been received in a timely manner; 4) inhibit change until necessary approvals are received; and 5) document completed changes to the information system. (Source: NIST 800-53)

☐ **Automation of Change Monitoring:** The organization employs automated mechanisms to facilitate the monitoring changes across information systems. (Source: NIST 800-53)

☐ **Automation of Software and Information Change Detection:** The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions and uses tools to automatically monitor the integrity of the information system and the applications it hosts. (Source: NIST 800-53)

The organization deploys file integrity monitoring software to alert personnel to unauthorized modification of critical PCI in-scope systems or content files. The organization configures the software to perform critical file comparisons at least weekly. (Source: PCI 11.5)

Incident Response

CONTROL DESCRIPTION

☐ **Automation of Incident Monitoring:** The organization employs automated mechanisms to facilitate the tracking of security incidents and in the collection and analysis of incident information. (Source: NIST 800-53)

☐ **Automation of Incident Reporting:** The organization employs automated mechanisms to assist in the reporting of security incidents. (Source: NIST 800-53) The organization employs automated mechanisms to generate exception reports. (Source: CobiT DS 3.5)

☐ **Automation of Incident Reporting Assistance:** The organization employs automated mechanisms to increase the availability of information related to incident response and reporting. (Source: NIST 800-53)

System Maintenance

CONTROL DESCRIPTION

☐ **Automation of System-Maintenance Tool Monitoring:** The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools. (Source: NIST 800-53)

Technical Controls

Systems Performance Management

CONTROL DESCRIPTION

☐ **Capacity and Performance Assessment:** The organization continuously tests and tracks system capacity, availability, and performance. Management uses measurements and reports to improve current performance and address such issues as resilience, stress response, storage and archiving capacity, and procurement planning. (Source: CobiT DS 3.5)

The monitoring statistics are analyzed and acted upon to identify negative and positive trends for individual services as well as for services overall. (Source: CobiT DS 3; ITIL SD/AM 8.7, SD/CM 6.3.1)

Media Protection

CONTROL DESCRIPTION

☐ **Automation of Media Access Tracking:** Unless the organization provides personnel guards to control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas. The organization maintains a log of access attempts and access granted. (Source: NIST 800-53)

☐ **Automation of Media Sanitization and Disposal Tracking:** The organization employs automated mechanisms to track, document, and verify the sanitization of digital media, such that information recovery is not possible.

☐ **Media Disposal Tracking:** The organization tracks, documents, and verifies media destruction and disposal actions. (Source: NIST 800-53, ISO 27002 10.7)

Physical Protection

CONTROL DESCRIPTION

☐ **Automation of Physical Access Tracking:** The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated. (Source: NIST 800-53)

☐ **Physical Access Logging:** The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: 1) name and organization of the person visiting, 2) signature of the visitor, 3) form of identification, 4) date of access, 5) time of entry and departure, 6) purpose of visit, and 7) name and organization of person visited. Organization retains the physical access log for a minimum of three months, unless otherwise restricted by law. (Source: NIST 800-53, ISO 27002 9.1, PCI 9.4)

Risk Assessment

CONTROL DESCRIPTION

☐ **Risk Evaluation:** The organization takes a risk-based approach to security tracking and testing, including remediation plans for identified control deficiencies and incident response procedures. The organization assesses potential security scenarios and risk weights, including negative effects from system breaches; unauthorized use of information, service disruption, and unmanaged changes. (Source: CobiT 5.5, ISO 27002)

Technical Controls

Risk Assessment *(continued)*

☐ **Vulnerability Scanning:** The organization scans the information system for vulnerabilities, periodically or when significant new vulnerabilities affecting the system are identified and reported. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. (Source: NIST 800-53, ISO 27002 12.6)

Systems and Information Integrity

CONTROL DESCRIPTION

☐ **Automation of Flaw Remediation:** The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention. The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation. (Source: NIST 800-53)

☐ **Intrusion Detection:** The organization monitors events on the information system, detects attacks, and provides identification of unauthorized use of the system. The information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware. (Source: NIST 800-53)

The organization uses and regularly updates anti-virus software or programs. Anti-virus software is deployed on all systems at risk for virus infections, especially staff computers and servers. The organization ensures that antivirus programs can detect, remove, and protect against common forms of malware. Antivirus software generates logs. (Source: PCI 5, 5.1, 5.1.1, 5.2)

The organization uses network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises of PCI in-scope systems. The organization keeps all intrusion detection and prevention engines up-to-date. (Source: PCI 11.4)

The organization connects individual intrusion detection tools into a systemwide intrusion detection system using common protocols. (Source: NIST 800-53)

☐ **Protection of Cardholder Data:** Monitor access attempts and prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files). Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic. Restrict outbound traffic from payment card applications to IP addresses within the DMZ. (Source: PCI 1.4, 1.4.1, 1.4.2)

☐ **Automation of Intrusion Detection:** The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (Source: NIST 800-53)

☐ **Automation of Security Alerts:** The organization employs automated mechanisms to make security alert and advisory information available throughout the organization, as needed. (NIST 800-53, PCI 12.5.2)

☐ **Error Reporting Parameters:** The organization carefully considers the structure and content of error messages. User error messages generated by the information system provide timely and useful information without revealing information that could be exploited by adversaries. System error messages are revealed only to authorized personnel. Sensitive data is not listed in error logs or associated administrative messages.

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 reporting, 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:

- ☐ 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 logging, monitoring, and reporting 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 has been verbally discussed.

Preparing for an Audit

A well-managed business unit or governance 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 governance program is well organized and well managed. Logging, monitoring, and reporting efforts 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 auditors happy, but rather to demonstrate that logging, monitoring, and reporting efforts meet the demands of the CEO, board of directors, regulators, and investors. Likewise, auditor's 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, 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 logging, monitoring, and reporting efforts and results. This might include documentation of system tracking and reporting 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 logging, monitoring, and reporting is performed and whether it is meeting organizational requirements and needs.

Other steps management should take to prior to the audit:

- ☐ 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

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 found in 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: Logging, Monitoring, and Reporting Resources

National Institute of Standards and Technology (NIST) Special Publication 800-53–Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf (PDF)

National Institute of Standards and Technology (NIST) Special Publication 800-92– Guide to Computer Security Log Management http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf (PDF)

National Institute of Standards and Technology (NIST) Special Publication 800-12–An Introduction to Computer Security–The NIST Handbook http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter10.html

ISO 27002 in North America http://www.27001.com

Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 (AS 2) http://www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx

Office of Government Commerce (OGC) IT Infrastructure Library (ITIL) http://www.itil.co.uk/

The Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/tech/

SANS Institute Guide to Security Metrics http://www.sans.org/reading_room/whitepapers/auditing/55.php

Office of Government Commerce (OGC) Best Management Practice for Project, Programme, Risk and Service Management http://www.best-management-practice.com/officialsite.asp

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/

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

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

Research Sponsors

LogLogic

LogLogic™ provides the world's leading enterprise-class platform for collecting, storing, reporting, and alerting on 100 percent of IT log data from virtually any device, operating system, or application. LogLogic 4 LX and ST systems address the compliance, operations, and risk mitigation needs of the most demanding Fortune and Times 1000 companies globally. LogLogic's innovations include creating the world's first search engine for fast-moving IT log data and Compliance Suites that automate using that data to enforce critical controls and regulations. LogLogic has established a position as the market visionary and leader, as evidenced by awards and accolades including Gartner SIEM Magic Quadrant "Leader," 2006 AlwaysOn Top 100 Private Company, Best of Interop 2005, SC Magazine's "Best Computer Forensics," Infosecurity's "Hot Company 2006," and the Red Herring 100.

For more information, visit www.loglogic.com and http://blog.loglogic.com.

About the Authors

Ted Ritter, CISSP
Ted Ritter has more than 20 years of experience in information assurance, telecom technology management, business development, marketing, and sales. Before founding iTRitter he built a Cyber Security practice at Intelligent Decisions, a federal systems integrator; growing the security business from less than $200K to more than $8M in two years. A published author and international speaker, he is currently focusing on regulatory compliance tools and their value (or cost) to in corporate governance, risk, and compliance (GRC) processes. Ritter's education includes a BA in Neuroscience from Oberlin College and a MA in Telecommunications Management from The George Washington University. He is a Certified Information Systems Security Professional (CISSP

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.

Series editor: Cass Brewer, Editorial and Research Director, IT Compliance Institute

If you have suggestions for improving this IT Audit Checklist, please write editor@itcinstitute.com.

Legal Notice

When assessing any legal matter, do not rely solely on materials published by third parties, including the content in this paper, without additionally seeking legal counsel familiar with your situation and requirements. The information contained in this IT Audit Checklist is provided for informational and educational purposes and does not constitute legal or other professional advice. Furthermore, any applicability of any legal principles discussed in this paper will depend on factors specific to your company, situation, and location. Consult your corporate legal staff or other appropriate professionals for specific questions or concerns related to your corporate governance and compliance obligations.

ITCi makes every effort to ensure the correctness of the information we provide, to continually update our publications, and to emend errors and outdated facts as they come to our attention. We cannot, however, guarantee the accuracy of the content in this site paper, since laws change rapidly and applicability varies by reader.

The information in this publication is provided on an "as is" basis without warranties of any kind, either expressed or implied. The IT Compliance Institute disclaims any and all liability that could arise directly or indirectly from the reference, use, or application of information contained in this publication. ITCi specifically disclaims any liability, whether based in contract, tort, strict liability, or otherwise, for any direct, indirect, incidental, consequential, punitive or special damages arising out of or in any way connected with access to or use of the information in this paper.

ITCi does not undertake continuous reviews of the Web sites and other resources referenced in this paper. We are not responsible for the content published by other organizations. Such references are for your convenience only.