Auditing Essentials
for Small Provider Organizations

By
Kenneth G. Hartman, CISSP, CPHMIS

Introduction

The very idea of an information systems security audit is likely to conjure up feelings of dread and an overwhelming desire to procrastinate. Perhaps images of an IRS personal tax audit come to mind, or experiences with JACHO or State Medicare Surveys. However, auditing has a vital role in security governance. This paper will provide essential understanding of the role of security audits and how to leverage auditing to promote more focused progress toward your organization's security and HIPAA compliance goals.

An information systems security audit is an assessment of how well the confidentiality, availability, and integrity of the information of the organization is assured by the security management program (Hayes).

Because an organization does not have unlimited resources, it must prioritize its efforts. Risk assessments support the prioritization effort while security audits provide the feedback mechanism for ongoing improvement.

Why Audit?

Healthcare providers are subject to various laws requiring the protection of personally identifiable information. In the United States, the primary laws are HIPAA and HITECH. A common theme in all modern security compliance legislation is the continuous monitoring of the adequacy and effectiveness of the security control measures. Security audits are the primary method "used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives" (SP 800-53A ix).

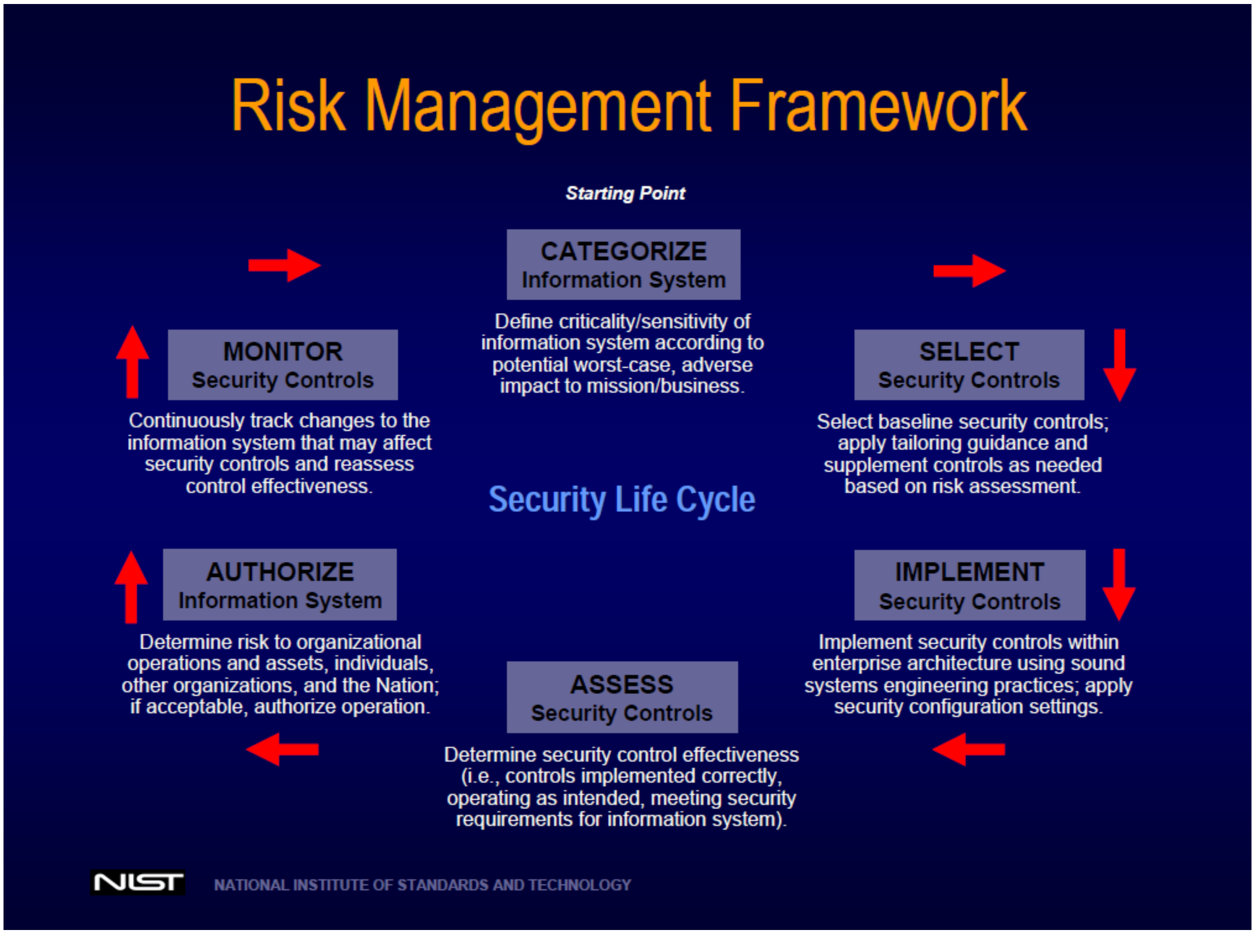
The security and privacy laws in the United States are strongly influenced by the Risk Management Framework (RMF) that has been developed by the National Institute of Standards and Technology (SP 800-37 2). The Risk Management Framework provides a risk-based methodology for identifying, prioritizing, and securing the information that an organization needs to protect. Figure 1 contains a diagram of the RMF.

While HIPAA does not mandate the use of the Risk Management Framework, the RMF is a useful tool to understand the theory behind the compliance requirements. In particular, auditing activities map to the ASSESS and MONITOR steps depicted in Figure 1 (SP 800-53A ix).

John Edwards makes a great case for security audits in an article that he wrote for ITSecurity.com.

> *"Security audits are typically conducted for the purposes of business-information security, risk management and regulatory compliance. If performed correctly, a security audit can reveal weaknesses in technologies, practices, employees and other key areas. The process can also help companies save money by finding more efficient ways to protect IT hardware and software, as well as by enabling businesses to get a better handle on the application and use of security*

technologies and processes. As bothersome as security audits are, business owners, executives and IT managers who truly understand them realize that periodic examinations can actually help ensure that security strategies are in sync with overall business activities and goals (Edwards).”



Risk Management Framework

Starting Point

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Figure 1 – The NIST Risk Management Framework (NIST HIPAA Workshop).

What is an Information Systems Security Audit?

Auditing is really the implementation of the management principle of “inspect what you expect.” That being said, auditing professionals will typically follow a very well-defined audit methodology that is tailored to the scope of the engagement.

An audit is a repeatable process used by an independent and competent professional to systematically evaluate one or more controls. The auditor will obtain and analyze evidence and then prepare a written opinion on the effectiveness of the implemented controls (Gregory).

Conceptually, an audit uses the *scientific method*. To follow this analogy, the hypothesis is that the security control is adequate and effective. Next, the auditor will examine evidence that the hypothesis is either true of false, impartially documenting the findings such that another “investigator” would draw the same conclusion.

Who Should Perform an Information Systems Security Audit?

Small provider organizations may feel as if they face a dilemma regarding security audits. The organization may not have the internal expertise to perform an audit and may not have extensive budgets to allocate towards auditing. Risk-based decision making, guided by compliance requirements, will ensure that the scope of the audit is appropriate to the size of the organization. An organization that does not have an internal IS auditor on staff should consider contracting with a professional Information systems security auditor and jointly working to develop a statement of work that defines the scope and deliverables of the audit.

If the organization decides to conduct the audit internally, it is critical that the auditor have independence from the organizational departments implementing the security controls. In other words, do not have your system administrators audit themselves, because there will naturally be a conflict of interest. No matter how well-intentioned the implementers of the security controls may be, you will not achieve the level of transparency that your organization will need to properly assess risk without separation of duties.

What Is Involved in a Security Audit?

It is best to think of an audit as a project, with a specific set of objectives and scope, schedule, and cost. The *CISA Certified Information Systems Auditor All-in-One Exam Guide* states that a typical audit plan will include the following components:

- **Purpose** – A discussion of why the audit is to be performed.
- **Scope** – A list of which systems, departments, time periods, or specific security controls are to be audited.
- **Risk Analysis** – The RA allows the auditor to focus on historically problematic areas or areas that pose the highest risk to the organization.
- **Audit Procedures** – Specific procedures as to how the audit will be performed, including criteria as to what constitutes a deficiency or not.
- **Resources** – This is a list of skills, tools, and budget that will be required to perform the audit. The scope of the audit and the objectives will naturally have bearing on the resources needed.
- **Schedule** – The timeline for the audit should specify the data collection, analysis, and report generation phases.

The *NIST SP 800-53A Guide to Assessing Security Controls in Federal Information Systems and Organizations* provides a very helpful diagram that illustrates the audit process. This diagram is reproduced in Figure 2.

What to Expect After the Audit?

The audit findings will typically be reported in a formal document that complies with all applicable standards that pertain to the auditor's professional credentials (Gregory). For example, the ISACA Standards apply for an auditor with the *Certified Information Systems Auditor (CISA)* professional designation.

The auditor should schedule a meeting with the appropriate representatives of management to discuss the result of the audit and to determine the corrective action plan and corresponding milestones. Expectations of how the auditor will be involved in the post-audit follow-ups will typically be discussed.

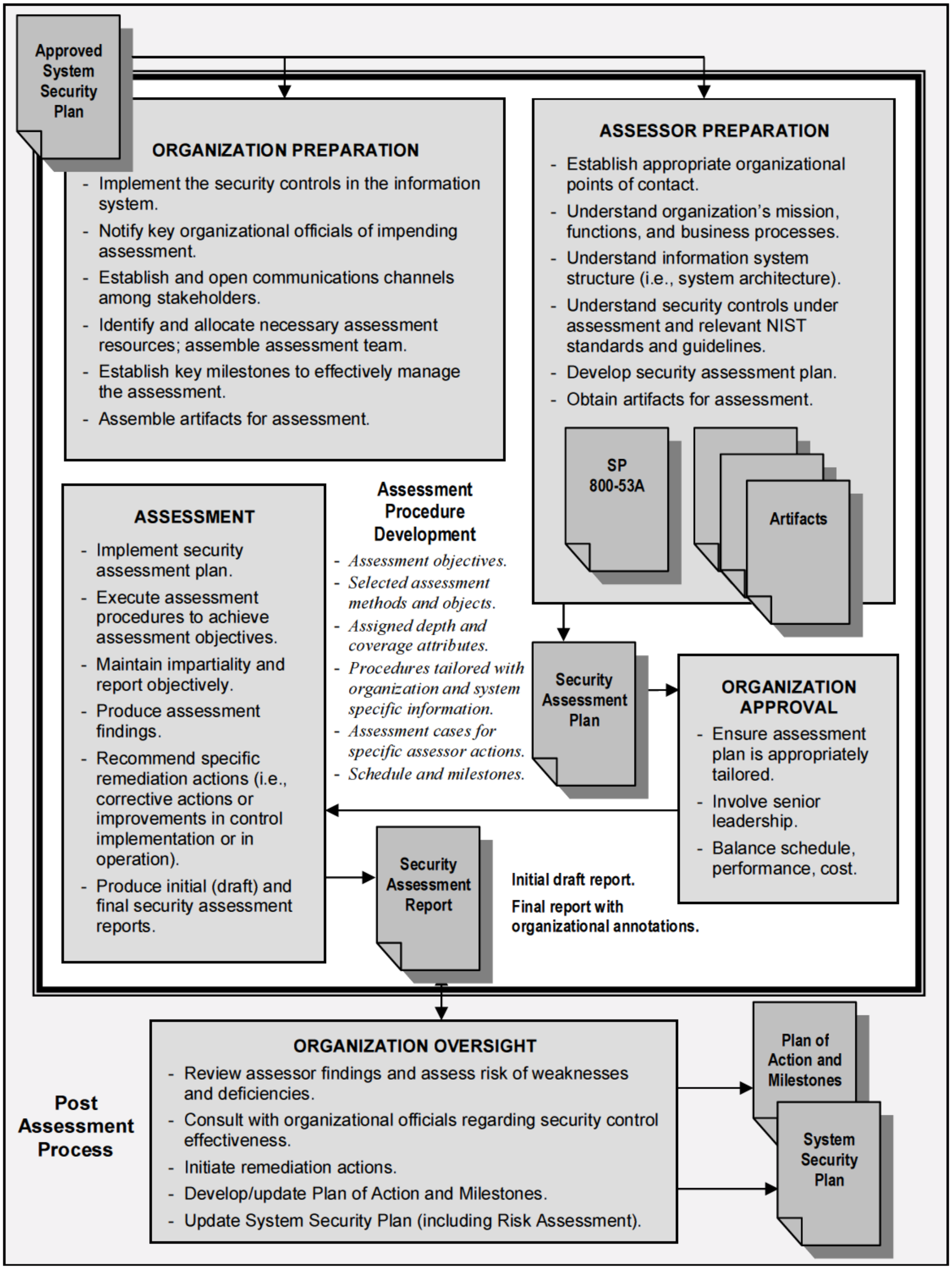

Approved System Security Plan
ORGANIZATION PREPARATION
- Implement the security controls in the information system.
- Notify key organizational officials of impending assessment.
- Establish and open communications channels among stakeholders.
- Identify and allocate necessary assessment resources; assemble assessment team.
- Establish key milestones to effectively manage the assessment.
- Assemble artifacts for assessment.
ASSESSOR PREPARATION
- Establish appropriate organizational points of contact.
- Understand organization's mission, functions, and business processes.
- Understand information system structure (i.e., system architecture).
- Understand security controls under assessment and relevant NIST standards and guidelines.
- Develop security assessment plan.
- Obtain artifacts for assessment.
SP 800-53A
Artifacts
ASSESSMENT
- Implement security assessment plan.
- Execute assessment procedures to achieve assessment objectives.
- Maintain impartiality and report objectively.
- Produce assessment findings.
- Recommend specific remediation actions (i.e., corrective actions or improvements in control implementation or in operation).
- Produce initial (draft) and final security assessment reports.
Assessment Procedure Development
- Assessment objectives.
- Selected assessment methods and objects.
- Assigned depth and coverage attributes.
- Procedures tailored with organization and system specific information.
- Assessment cases for specific assessor actions.
- Schedule and milestones.
Security Assessment Plan
ORGANIZATION APPROVAL
- Ensure assessment plan is appropriately tailored.
- Involve senior leadership.
- Balance schedule, performance, cost.
Security Assessment Report
Initial draft report.
Final report with organizational annotations.
Post Assessment Process
ORGANIZATION OVERSIGHT
- Review assessor findings and assess risk of weaknesses and deficiencies.
- Consult with organizational officials regarding security control effectiveness.
- Initiate remediation actions.
- Develop/update Plan of Action and Milestones.
- Update System Security Plan (including Risk Assessment).
Plan of Action and Milestones
System Security Plan

Figure 2 – The NIST SP 800-53A "Security Control Assessment Process Overview" illustrates a typical audit process.

Additional Audits

The initial audit sets the baseline for measurable improvement. The audit is not as much about passing or failing as much as it is about prioritizing your vulnerabilities and refining your processes to demonstrate continuous improvement (Hengst). All organizations evolve, especially healthcare organizations, with the rapidly changing compliance requirements. Because of this, the organization's security controls will need to adapt and auditing is the best way to demonstrate due diligence in the face of change.

Conclusion

This paper discusses the benefits of an information systems security auditing program and why it should be incorporated into the security management program of every small provider organization. The paper also highlights the importance of auditor independence and provides insight into the auditing process. Lastly, it concludes with a reminder that auditing is a an on-going process because healthcare is constantly evolving.

Audit Methodologies

- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- ISACA – IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals
- ISSAF – Information Systems Security Assessment Framework
- OSSTMM – Open Source Security Testing Methodology Manual
- IIA GTAG - Global Technology Audit Guide

Further Reading

- Conducting a Security Audit: An Introductory Overview
- How to Clear a Security Audit with Flying Colors
- So You Failed A Security Audit, now what?

References

Edwards, John. The Essential Guide to Security Audits. n.d. 16 January 2011 <http://www.itsecurity.com/features/security-audit-essentials-042908/>.

Gregory, Peter H. CISA Certified Information Systems Auditor All-in-One Exam Guide. New York: McGraw Hill, 2010.

Hayes, Bill. "Conducting a Security Audit: An Introductory Overview." 25 May 2003. Symantec. 16 January 2011 <http://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview>.

Hengst, Amy. So You Failed a Security Audit, Now What? 7 May 2007. 17 January 2011 <http://www.itsecurity.com/features/failing-a-security-audit-050707/>.

National Institute of Standards and Technology. "Assessment Framework and Methodologies." 18 May 2009. 2009 HIPAA Workshop Presentations. 16 January 2011 <http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/3-051809-assessment-methods.pdf>.

—. "SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." February 2010. Computer Security Resource Center. 16 January 2011 <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.

—. "SP 800-53 A Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans." June 2010. Computer Security Resource Center. 16 January 2011 <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>.

—. "SP 800-66 Rev 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." October 2008. Computer Security Resource Center. 16 January 2011 <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.