Security Risk Analysis and Management: an Overview (2011 update)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: This update replaces the October 2003 practice brief "Security Risk Analysis and Management: An Overview."

Managing risks is an essential step in operating any business. Because eliminating all threats is impossible, businesses will periodically conduct a risk analysis to determine their possible exposure and how best to manage risks appropriately to an acceptable level.

The concept of risk management is not new to healthcare, but conducting a risk analysis for information technology can be challenging. Reporting on the compliance audits it conducted in 2008, the Centers for Medicare and Medicaid Services (CMS) wrote, "CEs [covered entities] did not understand the key elements of an effective risk assessment. CEs did not conduct a documented analysis targeted at risks to the confidentiality, integrity, and availability of ePHI [electronic protected health information]. In some cases, although management had identified certain risks within the organization, no formally documented risk assessment covering ePHI risks throughout the organization existed."[1]

This practice brief reviews the regulatory requirements of an effective security risk analysis and provides an overview of one approach on how to conduct a risk analysis.

Regulatory Requirement

The HIPAA security rule requires covered entities and business associates, their agents, and subcontractors to conduct a risk analysis and implement measures "to sufficiently reduce those risks and vulnerabilities to a reasonable and appropriate level." Specifically, it has two required implementation specifications on risk analysis and risk management:

- "…conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information…" **Risk Analysis §164.308(a)(1)(ii)(A)**
- "…implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level…" **Risk Management §164.308(a)(1)(ii)(B)**

Because the security rule applies to a variety of organizations ranging from large healthcare systems to small physician practices, as well as various business associates, the standards are flexible in regard to the approach an organization takes based on several factors:

- The organization's size, complexity, and capabilities
- The organization's technical infrastructure, hardware, and software security capabilities
- The costs of security measures
- The probability and criticality of potential risks to ePHI

The word "reasonable" appears 51 times and the word "reasonably" appears 21 times in the final security rule (including the preamble). What is reasonable for one organization may be different from what is reasonable for another because of their risk analysis and their management's comfort level with accepting those risks.

A risk analysis helps determine how best to meet the security rule's implementation specifications and whether an alternative security measure appropriately meets the intent of an implementation specification. However, regarding the flexibility of applying the HIPAA security rule's implementation specifications, the preamble states, "Cost is not meant to free covered entities from this [adequate security measures] responsibility." If the cost is reasonable and a security measure or control would reduce risk significantly, then an organization of any size should consider implementing the control, especially if the risks are high or moderate.

In addition, healthcare organizations that wish to meet the meaningful use criteria must conduct a risk analysis.[2] The stage 1 meaningful use criteria includes the following measure: "Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process."

Risk Analysis: Framework

The HIPAA security rule does not specify a method or process for conducting a risk analysis. Therefore, this practice brief will follow the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Risk Management Guide for Information Technology Systems," because it is a comprehensive framework and is referenced by the Department of Health and Human Services (HHS) and/or CMS in the following publications:

- The HIPAA security rule[3]
- "6 Basics of Risk Analysis and Risk Management," in the *HIPAA Security Series*[4]
- "HIPAA Compliance Review Analysis and Summary of Results"[5]
- "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[6]

Figure 1, "Risk Analysis Process as Outlined in NIST SP 800-30," illustrates the risk analysis process as detailed in NIST SP 800-30. There are nine process steps, identified in the rectangular boxes in the center of the illustration. The rounded boxes to the left of a process step are the inputs, and the rounded boxes to the right represent the possible outputs of a process step. The next sections of this practice brief will provide additional information about each of the nine steps.

Note: To make it easier to follow the text in the next sections, refer back to this figure as needed. Because this practice brief is intended to be a high-level overview, AHIMA recommends that the reader download NIST SP 800-30 "Risk Management Guide for Information Technology Systems" for a more detailed explanation of risk analysis.[7]

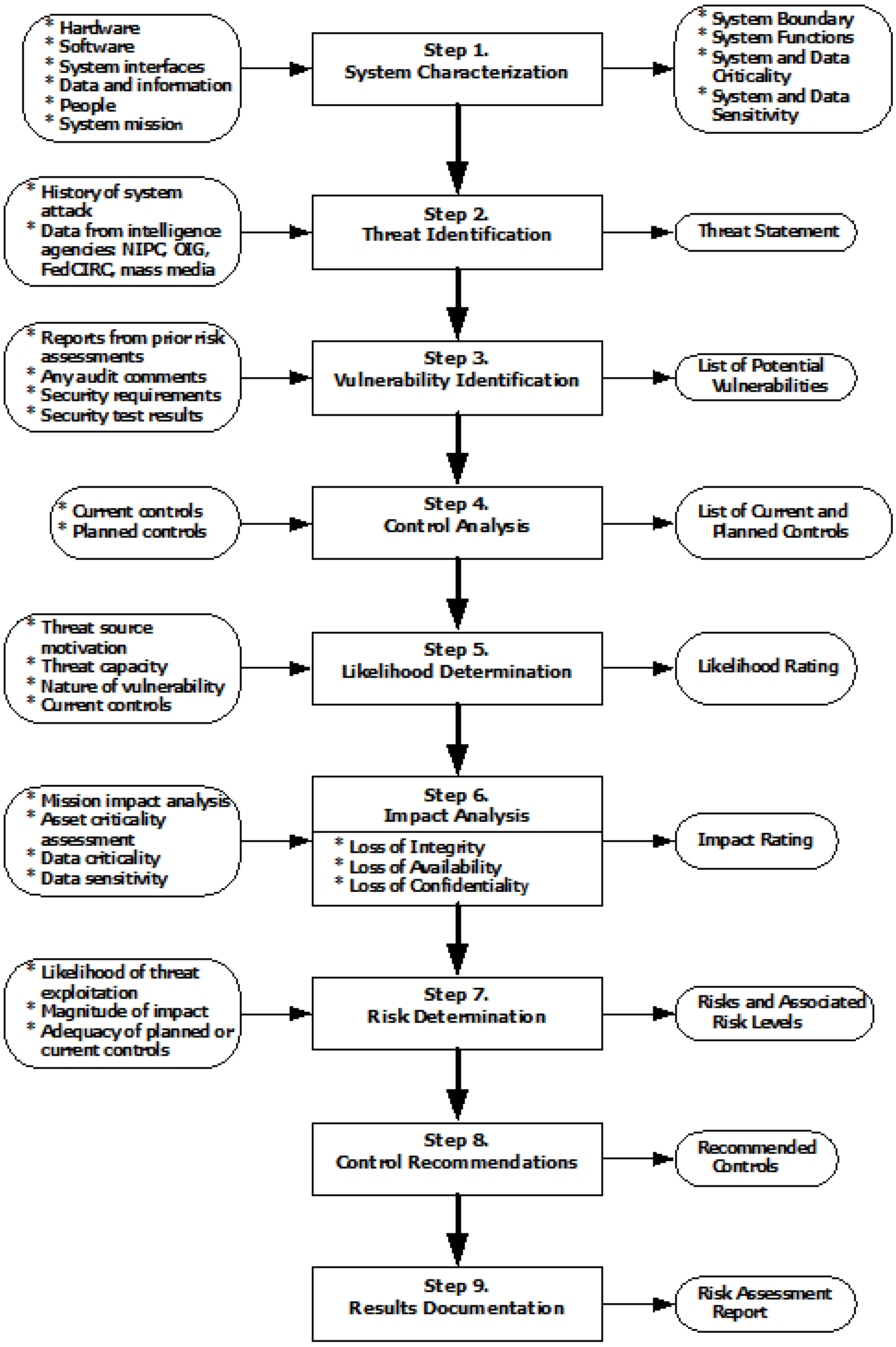


Figure 1 – Risk Analysis Process as Outlined in NIST SP 800-30

Step 1. System Characterization

System characterization is used to expedite the risk analysis. It is the process of identifying which information assets need protecting either because of their criticality to the business and/or because ePHI is processed and stored on the system. This process includes conducting an inventory of major applications and general support systems-any systems that process or store PHI. A major application is an application that is critical to an organization or stores PHI. Generally, the “owner” for a major application is the director of the department that is the primary user of the application. Listed below are some examples of major applications, with the probable owner in square brackets:

- Electronic health record (EHR) [chief operating officer]

- Laboratory information system (LIS) [director of laboratory]
- Pharmacy system-medication dispensing carts [director of pharmacy]

General support systems are the systems used throughout the organization to support one or more applications. They are usually “owned” by the IT department. Listed below are some examples of general support systems:

- Computer workstations
- Laptops and tablets
- Smartphones and other mobile devices
- Network (wired and wireless)
- E-mail system

The initial focus of the organization’s risk analysis should be on systems that have the greatest effect on healthcare operations and systems that pose the greatest risk for the organization. A business impact analysis, often conducted before creating a disaster recovery plan, is one method used to determine information system criticality.[8]

Another method for identifying which systems to focus on is to rank applications systems based on risk factors, such as the number of users, the type of information, the use of the information (patient care, etc.), the availability of the information (Internet, etc.), the mobility of the information, the effects on the organization and patients if the system is not available, and other factors that might indicate that a system has a higher relative risk for the organization.

Step 2. Threat Identification

Once major applications and general support systems have been categorized, the next step is to identify threats. From an information security perspective, a threat is anything that could affect the confidentiality, integrity, or availability of information or an information system.

For simplicity, three groups of threats can be identified:

- **Acts of nature**-Lightning, earthquakes, hurricanes, and tornadoes are examples of acts of nature threats.
- **Acts of man**-Carelessness, errors, unauthorized access, identity theft, tampering, hacking, and theft of equipment by internal workforce members, external hackers, and visitors are examples of acts of man threats.
- **Environmental**-Hardware failure, power outage, air conditioning not working, break in the network cable, and water leaking from the ceiling are examples of environmental threats.

Conducting a thorough risk analysis does not imply that organizations need to identify every possible threat. The term “reasonably anticipated” is used three times within the HIPAA security rule (twice in the preamble and once in the actual rule) as it pertains to threats or hazards. Factors for determining what could be reasonably anticipated includes statistics, geographical location, past experiences, or industry trends. Once identified, the reasonably anticipated threats are matched to a particular application or general support system. For example, the probability of theft is more likely for a laptop or a smartphone that is transported daily in and out of an organization than for a large rack-mounted server in a data center.

System characterization is useful for dividing information assets into manageable pieces, like a puzzle, identifying the unique threats that may exist at each layer that constitutes an information system. However, the overall risk to a system will be the combination of the risks at each layer: the application, operating system, software, server, network, and desktop and laptop layers.

Steps 3 and 4. Vulnerability Identification and-Control Analysis

Because of the close relationship between vulnerabilities and controls, it is often easier to combine these two steps. If the risk analysis is being conducted on a major application or general support system that is already being used, then conducting a control analysis first usually makes more sense. If an application or system is brand-new, then the vulnerability identification should occur first because some of the security controls may not yet have been implemented fully.

A *vulnerability* can be described as an inherent weakness or absence of a safeguard that could be exploited by a threat. Vulnerabilities may be attributed to people, processes, or technologies. The absence of a functioning control often represents a vulnerability in an application or system. For example, antivirus software is used to prevent or detect malicious code. If this control is missing, it represents a vulnerability. Sometimes a control may be present but inadequate. Using the same example, if the antivirus software is present (control) but does not get updated regularly, then that is also a vulnerability.

Typically, threats are paired with vulnerabilities, although it is not necessarily a one-to-one relationship. Many threats may exploit a single vulnerability. One threat source may exploit more than one vulnerability. Conversely, a single control may be used to address multiple threats. Figure 2, "Sample of Threats, Controls, and Vulnerabilities" below offers samples of controls and vulnerabilities based on a specific threat for laptops.

Figure 2 - Sample of Threats, Controls, and Vulnerabilities

Threat	Control	Vulnerability
1. Theft or loss	• File encryption is used to protect some of the data stored on the hard drive.	• Power-on passwords and other access control devices are not being used. • Security devices (physical or technical) for tracking lost or stolen laptops are lacking.
2. Malicious code (virus, worm, Trojan horse, spyware, etc.)	• Antivirus software is loaded on laptops.	• Antivirus software does not get updated regularly. • Users have local administrator rights and can disable or turn off the antivirus software and download executable programs.

In general, controls may be categorized as:

- **Preventive**-Inhibiting a threat, such as by access controls, encryption, and authentication requirements
- **Deterrent**-Keeping the casual threat away, such as strong passwords, two-tiered authentication, and Internet use policies
- **Detective**-Identifying and proving when a threat has occurred or is about to occur, such as audit trails, intrusion detection, and checksums
- **Reactive**-Providing a means to respond to a threat that has occurred, such as an alarm or penetration test
- **Recovery**-A control that helps retrieve or recreate data or applications, such as backup systems and contingency plans

NIST SP 800-53 Rev. 3, "Recommended Security Controls for Federal Information Systems and Organizations," may be used as a means for assessing information security safeguards and controls.[9] This document was created for agencies of the federal government and may specify controls that are not used commonly in many healthcare organizations.

Besides the control analysis, other sources for determining vulnerabilities include reports or results from:

- Past incidents or data breaches, including news stories about reported data breaches at other organizations
- Audits or evaluations conducted by external or internal auditors
- A compliance gap analysis or privacy and security assessment
- Patient complaints to determine if there is a breakdown or flaw in a security control
- A walk-through inspection (e.g., workstations being left unattended while logged on to an information system containing confidential information)
- A network vulnerability scanning or penetration test
- Web sites, such as HHS's, that post breaches affecting more than 500 individuals

Step 5. Likelihood Determination

The next step in the risk analysis process is to determine the probability or likelihood of a potential threat being successful in exploiting vulnerabilities. The likelihood determination must be made with consideration of the existing security safeguards and controls. The definitions of likelihood ratings are described in "NIST SP 800-30 Likelihood Definition," below.

Figure 3 - NIST SP 800-30 Likelihood Definition

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.

Step 6. Impact Analysis

The next step in the process is to determine the potential impact resulting from threats successfully exploiting vulnerabilities. Some examples of possible impacts are listed in figure 5, "Possible Impacts." The definitions of impact ratings are described in figure 4, "NIST SP 800-30 Impact Definitions."

Figure 4-NIST SP 800-30 Impact Definition

Magnitude of Impact	Impact Definition
High	Exploitation of the vulnerability (1) may result in the high costly loss of major tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest significantly; or (3) may result in human death or serious injury.
Medium	Exploitation of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exploitation of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may affect an organization's mission, reputation, or interest noticeably.

Healthcare organizations are encouraged to edit the NIST definitions or create their own definitions for likelihood and impact. An accurate description of what constitutes a rating of high, medium, or low is important for maintaining consistency when evaluating risk scores. A consistent standard for scoring risks ensures a better prioritization of risk.

Figure 5-Possible Impacts

Confidentiality

Disclosure of protected health information (PHI)
Access to credit card data used for committing financial fraud
Access to Social Security numbers used for identity theft
Disclosure of sensitive or proprietary research information

Integrity

Data entry errors
Data alteration (intentional or unintentional)
Data synchronization errors

Availability

Business interruption
Denial of service
Loss of productive time and operational delays
Replacement of lost information

Opportunity (financial)

Loss of business
Loss of competitive advantage or research grant
Equipment repair or replacement
Increase in insurance premiums

Reputation

Loss of patient confidence
Decreased employee morale
Loss of faculty confidence

Litigation

Criminal or civil case
Regulatory fines or criminal punishment for noncompliance

Source: Adapted from Alberts, Christopher, and Audrey Dorofee. *Managing Information Security Risks – The OCTAVE*^{SM} *Approach*. Boston, MA: Addison-Weley, 2002.

Step 7. Risk Determination

The purpose of this step is to assign a risk score that is based on likelihood and effect. The scoring of risks provides for appropriate prioritization of resources and focus on the areas of greatest risk. Risk can be determined by using one of the two common approaches described in the figure 6.

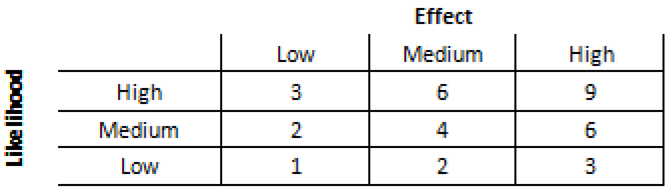
Regardless of the method used, prioritization of risks is the primary goal for conducting a risk analysis. This prioritization ensures that limited resources (money, people, and time) may be applied where the greatest risk reduction may be realized.

Figure 6 - Risk Determination: Two Common Approaches

Two approaches commonly are used in risk analysis for determining risks: qualitative and quantitative.

Qualitative Approach

In the qualitative approach, the likelihood (or probability) of the threat being realized and the effect it would have are rated as high, medium, or low. The ratings may be combined to create a numeric risk score as shown below.



		Effect		
		Low	Medium	High
Likelihood	High	3	6	9
	Medium	2	4	6
	Low	1	2	3

In this scale, a low rating is equivalent to a numerical value of 1; medium, a value of 2; and high, a value of 3. The overall risk score is determined by multiplying the likelihood value by the effect value. NIST SP 800-30, *Risk Management Guide for Information Technology Systems* has descriptions for each of the categories of ratings for likelihood and effect.

Quantitative Approach

A quantitative risk analysis is an attempt to assign monetary values to the potential losses that might occur. A quantitative evaluation is difficult because it is not easy to determine an accurate monetary value for information or intangible effects, such as the reputation harm an organization would experience if a threat successfully circumvented existing controls and exploited a vulnerability.

Examples of factors considered when determining the magnitude of effect include:

- The value of the asset being protected. For example, a critical application or system used enterprise-wide that costs $10 million to implement has a greater organizational value than a departmental system used by a small population of the workforce that was purchased and implemented for $50,000.
- An estimate of the frequency that a threat may occur across a specified time. For example, flooding is a threat that is often calculated and expressed in terms of 100-year flood, which is the extreme water level expected only once every 100 years.
- An approximate cost (measureable costs and intangible costs) resulting from each occurrence of the threat being realized. For example, measurable costs include replacement equipment, labor for repair work, loss of business revenue because systems were unavailable, and fines or penalties. Intangible costs include damaged reputation, loss of patient confidence or trust, and lost market share.

The primary benefit for using the qualitative method is cost-benefit analysis of recommended controls. For example, if the organization estimates that the realization of a particular threat may cause $500 worth of damage every 10 years, and the cost to implement a control to prevent the threat costs $100,000, then the cost-benefit analysis may indicate that it is more cost-effective for the organization to accept the risk rather than implement the recommended control.

The NIST approach to risk analysis generally is considered qualitative because it relies heavily on narrative descriptions of risk. The NIST approach also addresses cost-benefit analysis but not as an integral determinant of risk. Although a systematic procedure is followed for conducting a risk analysis, there is a certain amount of good judgment in play in the analysis part of the process of both methods.

Step 8. Control Recommendations

Wherever a vulnerability exists, the control recommendation is essentially what to do to counteract the missing control. For example, figure 7 lists some samples of how a stated vulnerability can be translated into a control recommendation.

Figure 7 - Creating Control Recommendations

Vulnerability	Control Recommendation
Audit logs are not reviewed regularly and are used primarily for problem solving.	Create procedures to audit users randomly; formalize log review responsibilities and procedures.
User's account is not disabled after a predetermined number of unsuccessful log-on attempts.	Consider locking out a user's account after five consecutive unsuccessful log-on attempts.

However, there may not always be a specific control recommendation for a given vulnerability.

Step 9. Results Documentation

The final step in the risk analysis process is the results documentation. The HIPAA security rule does not specify the form of documentation a risk analysis should take. Many organizations will use some type of spreadsheet or a summary report.

Figure 8 is a sample of a risk profile for a risk analysis conducted on laptops. A *risk profile* is one way to generalize and document risks efficiently. A risk profile can be done in a Word document, an Excel spreadsheet, or a database. In the sample in figure 8, this risk profile covers most laptops routinely carried in and out of the organization by its workforce. Although there may be some variations in individual configurations, management by exception is a far simpler approach than trying to conduct and document a risk analysis for every laptop used within the organization.

Figure 8 - Sample Risk Profile

Threats	Current Controls	Vulnerability	Like	Impt	Risk	Suggested Controls

Theft or loss	File encryption is used to protect some of the data stored on the hard drive.	• Power-on passwords and other access control devices are not being used. • Security devices (physical or technical) for tracking lost or stolen laptops are lacking.	M	M	4	• Require power-on passwords (i.e., Windows boot-up password). • Consider the cost-effectiveness of tracking controls.
Malicious code (virus, worm, Trojan horse, spyware, etc.)	Antivirus software is loaded on laptops.	• Antivirus software does not get updated on a regular basis. • Users have local administrator rights and can disable or turn off the antivirus software and download executable programs.	L	H	3	• Configure laptops to check for antivirus software updates automatically when the laptop connects to the internal network or the Internet. • Configure antivirus software so that a user cannot disable it.

Appendix B of NIST SP 800-30, "Risk Management Guide for Information Technology Systems," provides a sample report outline. A risk analysis report contains the key findings or vulnerabilities and the control recommendations for reducing risks. The application or system owners should sign off on this report to make them aware of the *residual risks*-the risks that remain even with the current safeguards and controls applied-and their decision about what to do. To simplify things, there is usually one of three possible decisions by owners on how risks will be addressed:

1. **Mitigated** or reduced by implementing the recommended controls
2. **Transferred** by either outsourcing or insuring against loss
3. **Accepted** and the recommended controls are not implemented, but at least the owner is recognizing the residual risk-the risks that remain even with the current safeguards and controls inherent in the application or system

Risks should be handled in a cost-effective manner relative to the value of the asset and the criticality and sensitivity of the data.

Often, this final step of the risk analysis process is incomplete because some technical people find completing the necessary paperwork and reports difficult. Obtaining a decision from the owner on how residual risks will be managed also can be challenging.

HIPAA requires documentation of the risk analysis be retained for six years. Documentation is critical in proving that the analysis was performed.

Risk Management

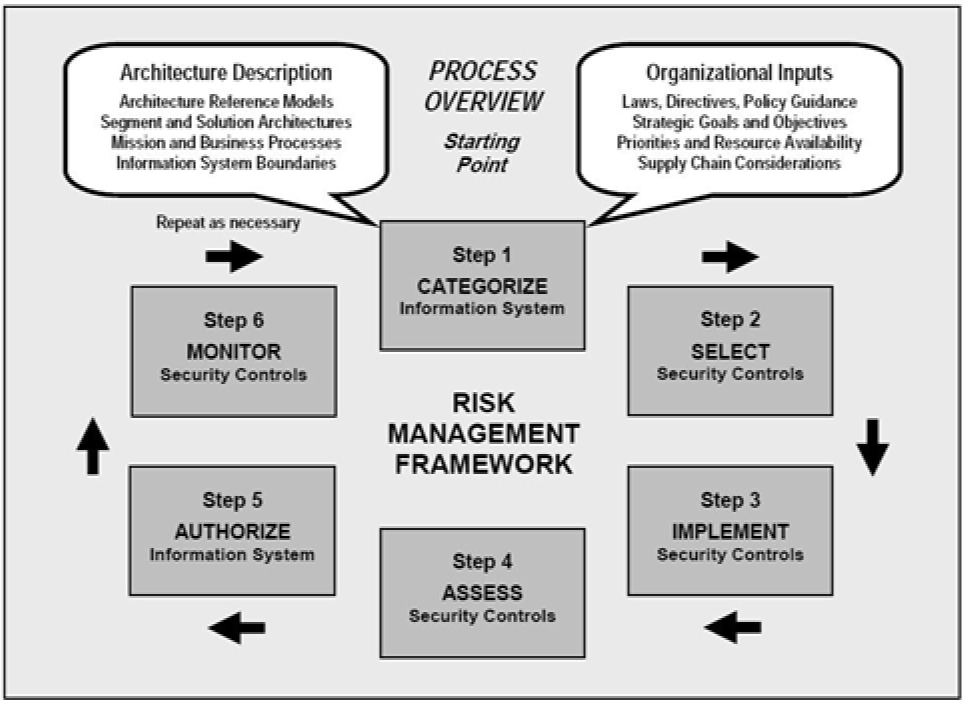
Risk management is the act of implementing security safeguards and controls. It also entails monitoring for changes and responding with enhanced strategies. The HIPAA security rule addresses the ongoing management of risks in several areas:

- "Security measures implemented to comply with standards and implementation specifications adopted...must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information." **§164.306(e)**
- "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." **Information system activity review §164.308(a)(1)(ii)(D)**
- "Perform a periodic technical and nontechnical evaluation, based initially upon the standards and implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart." **Evaluation §164.308(a)(8)**

The success of the risk management process depends heavily on the commitment of those involved with safeguarding an application or system to implement the approved control recommendations. Therefore, it is strongly suggested that some type of follow-up be scheduled around two to three months after the final risk analysis report is delivered and signed. The purpose of the follow-up is to verify progress on risk reduction and maintain open communications when obstacles are encountered.

Risk analysis and risk management are ongoing processes. Federal government agencies are required by law to reassess risk to information systems every three years. This reassessment is a good benchmark from which to determine an appropriate time frame. NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach", has a diagram that illustrates this ongoing risk management process, as illustrated in figure 9.

Figure 9 - A Security Life-Cycle Approach from NIST SP 800-37


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Notes

1. Centers for Medicare and Medicaid Services (CMS), Office of E-Health Standards and Services (OESS). "HIPAA Compliance Review Analysis and Summary of Results." 2008. Available online at www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf.
2. The Office of the National Coordinator for Health Information Technology, "Electronic Health Records and Meaningful Use." Available online at http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2.
3. US Department of Health and Human Services. "The Security Rule." Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html.
4. US Department of Health and Human Services. "Security Rule Guidance Material." Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.
5. Centers for Medicare and Medicaid Services, Office of E-Health Standards and Services (OESS). "HIPAA Compliance Review Analysis and Summary of Results." 2008. Available online at www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf.
6. US Department of Health and Human Services. "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." July 14, 2010. Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.
7. National Institute of Standards and Technology. "Risk Management Guide for Information Technology Systems." Special Publication 800-30. Available online at http://csrc.nist.gov/publications/PubsSPs.html.
8. Under the HIPAA security rule provision for the addressable implementation specification, "Applications and data criticality analysis" §164.308(a)(7)(ii)(E) is essentially a Business Impact Analysis (BIA)."

9. National Institute of Standards and Technology. "Recommended Security Controls for Federal Information Systems and Organizations." Special Publication 800-53, Rev. 3. Available online at http://csrc.nist.gov/publications/PubsSPs.html.

Reference

Herzig, Terrell. *Information Security in Healthcare: Managing Risk*. Chicago: HIMSS, 2010.

Prepared by

Tom Walsh, CISSP

Acknowledgments

Angela K. Dinh, MHA, RHIA, CHPS
Margaret M. Foley, PhD, RHIA, CCS
Judi G. Hofman, CAP, CHSS
John T. Jensen, CHPS, CIPP
William Miaoulis, CISA, CISM
Margaret Schmidt, RHIA
Mary C. Thomason, II, RHIA, CHPS, CISSP
LaVonne Wieland, RHIA, CHP

Prepared by (original)

Margret Amatayakul, RHIA, CHPS, FHIMSS

Article citation:
Walsh, Tom. "Security Risk Analysis and Management: an Overview (2011 update)" (AHIMA Practice Brief, January 2011)