Security Risk Analysis and Management: An Overview (2013 update)

Save to myBoK

Editor's note: This update replaces the January 2011 practice brief "Security Risk Analysis and Management: An Overview."

Managing risks is an essential step in operating any business. It's impossible to eliminate all threats; however, healthcare organizations typically conduct a periodic risk analysis to determine their potential exposure. A risk analysis allows organizations to develop strategies to manage those risks appropriately.

The concept of risk management is not new to healthcare, but conducting a risk analysis for information technology can be challenging.

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

Clarifying Key Terms

When thinking about risk analysis, it's helpful to first sort out key terminology. For the purposes of this practice brief, the following terms are clarified below:

- **Assessment**—A judgment based on an understanding of the situation; a method of evaluating performance
- **Analysis**—The close examination of something (i.e. an application or information system) to understand it more effectively or to draw conclusions from it; the separation of something (i.e. an application or information system) into its constituents to determine what it contains; to examine individual parts or to study the structure of the whole Source: Encarta Dictionary
- **Risk Analysis**—A systematic and ongoing process of identifying threats, controls, and vulnerabilities—as well as their likelihood of impact—to arrive at an overall rating of risk

Regulatory Requirements

The HIPAA Security Rule and Meaningful Use require covered entities to perform a risk analysis. An assessment must address the following HIPAA Security Rule standard:

- **§164.308(a)(8),** Evaluation, which states that organizations must "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."

Refer to the Office of the National Coordinator's (ONC) *Guide to Privacy and Security of Health Information* for information about what does and does not qualify as a risk analysis. Specifically, refer to the table entitled **Security Risk Analysis Myths and Facts** for specific examples. One example is provided below.For example, p. 11 of the guide states the following:

A checklist will suffice for the risk analysis requirement.	**False**. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed[1].

The HIPAA Security Rule requires covered entities and business associates as well as 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, the rule requires compliance with the following:

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

The security rule applies to a variety of organizations ranging from large healthcare systems to small physician practices as well as their business associates.[2] Thus, the standards for how an organization must approach a risk analysis are flexible. An organization must base its decision on several factors, including:

- 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 electronic protected health information (ePHI)

The final security rule includes the word 'reasonable' 51 times. It includes the word 'reasonably' 21 times(including the preamble). What is considered reasonable for one organization may not be for another. Some organizations may be more comfortable accepting certain levels of risk based on their own unique analysis.

A risk analysis determines how to meet the security rule's implementation specifications and whether an alternative security measure appropriately meets the intent of an implementation specification. However, the HIPAA Security Rule's 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 striving to meet the Meaningful Use criteria must conduct a risk analysis.[3] The Stage 1 criteria include 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."

Stage 2 criteria specifies: "Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's [eligible provider] risk management process."

Risk Analysis: Framework

The HIPAA Security Rule does not require a specific methodology or process for conducting a risk analysis. However, it does reference the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems. This publication provides a comprehensive framework that both the Department of Health and Human Services (HHS) and CMS reference in the following publications:

- The HIPAA Security Rule[4]
- *6 Basics of Risk Analysis and Risk Management*[5]
- *HIPAA Compliance Review Analysis and Summary of Results*[6]
- *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*[7]

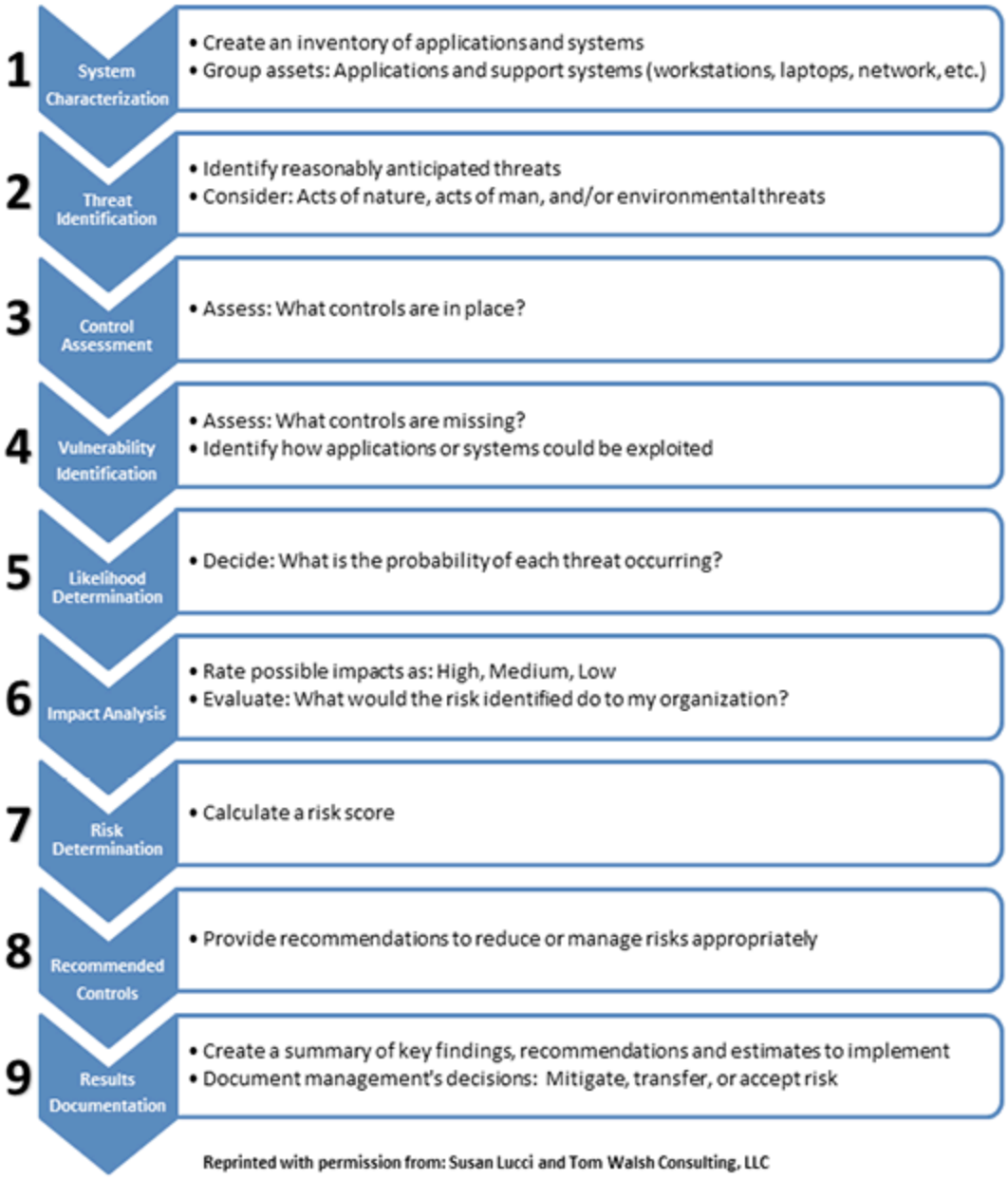
The original NIST SP 800-30 was retired and replaced with the following publications:

- 800-30 *Guide for Conducting Risk Assessments*, Revision 1 (September 2012)
- 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011)

Note: Because this practice brief is intended to provide a high-level overview, AHIMA recommends that the reader download NIST SPs 800-30 and 800-39 for a more detailed explanation of risk analysis.9

Figure 1 illustrates the nine risk analysis process steps as detailed in this practice brief.

Figure 1 - Risk Analysis Methodology Flowchart



Reprinted with permission from: Susan Lucci and Tom Walsh Consulting, LLC

Step 1. System Characterization

System characterization is the process of identifying the information assets that require a risk analysis. The information assets require protection either because of their criticality to the business and/or because the systems process and store ePHI. System characterization requires an inventory of major applications and general support systems—that is, any systems that process or store PHI. A major application is one that is critical to an organization or that stores PHI. Generally, the 'owner' of a major application is the director of the department that primarily uses that application. Following are some examples of major applications and their probable owners:

- Electronic health record (EHR) [chief operating officer and/or chief information officer]
- Laboratory information system [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 information technology (IT) department. Following are some examples of general support systems:

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

An organization's risk analysis should initially focus on systems that have the greatest effect on healthcare operations as well as 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.10

Another method for identifying the systems on which the healthcare organization should focus is to rank applications systems based on risk factors, such as:

- Number of users (i.e., the greater the number of users, the higher the risk)
- Type of information (i.e., the more sensitive the information, the higher the risk – Social Security Numbers, HIV data, bank account numbers, credit card data, etc.),
- Use of the information (i.e., patient care, research, business intelligence, patient accounting, etc.)
- Availability of the information (e.g., hosted in the cloud via the Internet, standalone system, virtualized servers, mirrored SAN, etc.)
- Mobility of the information (i.e., the more mobile, the greater the risk – portable media, smartphone, tablet, laptop, etc.)
- Effects on the organization and patients if the system is not available
- Other factors that might indicate that a system has a higher relative risk for the organization (i.e., system frequently goes down, system provide interconnectivity to other applications and system such as an interface engine, etc.

A risk analysis can be time-consuming. Therefore, healthcare organizations should initially focus should be on the 'critical few' versus the 'trivial many.' However, all applications and systems (including biomedical devices) containing ePHI must eventually be assessed.

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.

There are three types of threats:

- **Acts of nature** (e.g., lightning, earthquakes, hurricanes, and tornadoes)
- **Acts of humans** (e.g., carelessness, human errors, unauthorized access, identity theft; tampering; hacking into data; and theft of equipment by internal workforce members, external hackers, and visitors)
- **Environmental** (e.g., hardware failure, power outage, inoperable air conditioning that leads to overheating, break in the network cable, and water leaking from the ceiling)

Conducting a thorough risk analysis does not imply that organizations must 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. Instead, they should consider these factors:

- Statistics (i.e. HHS website for reported breaches affecting over 500 patients)
- Geographical location (i.e. hurricane for coastal areas, tornado for the Midwest, volcano for Hawaii)
- Past experiences (i.e. incident reports indicate areas of vulnerability that have been exploited before – theft of equipment in public areas)

- Industry trends (i.e. surveys, reports, security alerts, patches or system updates)

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. Alternatively, theft may not be a reasonably anticipated threat for a large rack-mounted server in a data center.

System characterization divides information assets into manageable pieces and helps healthcare organizations identify the unique threats that may exist at each layer of an information system, including the application, the operating system, any software, the server, the network, and desktop and laptop levels of use.

Steps 3 and 4. Control Assessment and Vulnerability Identification

Vulnerabilities and controls should go hand in hand, and it's often easier to combine the identification of both into one step. If a major application or general support system is already in use, then a healthcare organization should first conduct a control analysis. If an application or system is new and not currently active, then the healthcare organization should perform a vulnerability identification first because some of the security controls may not have been implemented fully yet.

A *vulnerability* is as an inherent weakness or absence of a safeguard that a threat could exploit. Vulnerabilities may be attributed to people, processes, or technologies. The absence of a functioning control often represents 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 vulnerability. Sometimes a control may be present but inadequate. Using the same example, if the antivirus software is present but does not get updated regularly, this is also a vulnerability.

Typically, threats are correlated 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, 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 (e.g., virus, worm, Trojan horse, spyware)	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 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

In addition to 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 whether a breakdown or flaw in a security control exists
- 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 the HHS Web site, that post breaches[8] affecting more than 500 individuals

Step 5. Likelihood Determination

The next step in the risk analysis process is to determine the probability or likelihood that a potential threat will successfully exploit vulnerabilities. The likelihood determination must be made with consideration of the existing security safeguards and controls. Example definitions of likelihood ratings are described in Figure 3.

Figure 3 – Likelihood Definition

Likelihood Level	Likelihood Definition
Very High (4)	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
High (3)	The threat-source is motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium (2)	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (1)	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 that successfully exploit vulnerabilities. Figure 4 includes example definitions of different types of threats. Figure 5 includes impact ratings of those threats.

Figure 4 - Impact Definition

Magnitude of Impact	Impact Definition
Very High (16)	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.
High (8)	Exploitation of the vulnerability (1) may result in the 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 serious human injury.
Medium (4)	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 (2)	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 these 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 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

Step 7. Risk Determination

The purpose of this step is to assign a risk score that is based on **likelihood** of the threat being realized, considering the current controls in place and **impact** to the organization if the threat was successful in exploiting a vulnerability. The scoring of risks allows healthcare organizations to prioritize resources and focus on the areas of greatest risk.

Regardless of the method used, the primary goal for conducting a risk analysis is to prioritize risks. This prioritization ensures that limited resources (i.e., money, people, and time) may be applied to the areas of greatest risk so vulnerabilities can be addressed and reduced.

Healthcare organizations use two approaches to determine risk: qualitative and quantitative. See Figure 6 below.

Figure 6 - Risk Determination: Two Common Approaches

Qualitative Approach

The qualitative approach rates the likelihood (probability) that a threat will cause an effect as very high, high, medium, or low. The qualitative approach also rates the impact of that threat as very high, high, medium, or low.In this scale, as outlined in the table below, a low likelihood rating is equivalent to a numerical value of 1; medium, a value of 2; high, a value of 3; and very high, a value of 4. A low impact rating is equivalent to a numerical value of 2; medium impact, a value of 4; high impact, a value of 8; and very high impact, a value of 16.

The overall risk score is determined by multiplying the likelihood value by the impact value.

	Likelihood (Probability)			
	Very High (4)	**High (3)**	**Medium (2)**	**Low (1)**
Very High Impact (16)	Very High (64)	Very High (48)	High (32)	High (16)
High Impact (8)	High (32)	High (24)	High (16)	Medium (8)
Medium Impact (4)	High (16)	Medium (12)	Medium (8)	Low (4)
Low Impact (2)	Medium (8)	Low (6)	Low (4)	Low (2)

Controls are implemented to either reduce the probability that a threat will cause an effect or to reduce the impact of that effect, thereby reducing risks.

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 harm to a healthcare organization's reputation.

Factors to consider 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 a 100-year timeframe. A 100-year flood is one in which the extreme water level is expected only once every 100 years.
- An approximate cost (i.e., 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 are 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 a cost-benefit analysis of recommended controls. For example, if an 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 is generally 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

A control recommendation is plan to address a vulnerability. Figure 7 includes 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.

Note that there may not always be a specific control recommendation for a given vulnerability. For example, when employees have remote access or work from home, there is a threat that someone else (i.e., family member, friend, neighbor) may have access to confidential information. There is no way for an organization to technically secure an employee's home environment. The recommendation to stop allowing remote access from home may not be a viable option for most organizations. The risk remains without a direct technical control recommendation. Other administrative safeguards might be recommended, such as enhanced awareness for remote access.

Step 9. Results Documentation

The final step in the risk analysis process is the results documentation. The HIPAA Security Rule does not specify the format for documentation of a risk analysis. Many organizations 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 stored in a Word document, an Excel spreadsheet, or a database. The risk profile below 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	8	Require power-on passwords (i.e., Windows boot-up password). Consider the cost-effectiveness of tracking controls.
Malicious code (virus, worm, Trojan horse, spyware)	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	8	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.

A risk analysis report includes the key findings or vulnerabilities as well as the control recommendations for reducing risks. The application or system owners should sign off on this report so that they are aware of the residual risks (i.e., the risks that remain even with the current safeguards and controls applied). Application or system owners typically address risks in one of the three following ways:

1. **Mitigate**—reduce risks by implementing the recommended controls
2. **Transfer**—outsource or insure against loss (not always a viable option)
3. **Accept**—recognize the residual risk but hold off on implementing any controls

Healthcare organizations should address risks in a cost-effective manner relative to the value of the asset and the criticality and sensitivity of the data. Of course, if the risk could be avoided altogether (which is seldom the case), it is also an option. For example, a risk analysis conducted prior to the purchase of an application or system may result in the organization deciding to avoid the risks inherent in the application or system altogether by not purchasing it.

This final step of the risk analysis process is often incomplete because some of the information technology (IT) staff might find it difficult to complete the necessary paperwork and reports. It can also be challenging to obtain a decision from the application or system owner regarding how residual risks will be managed.

HIPAA requires healthcare organizations to retain documentation of the risk analysis 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:

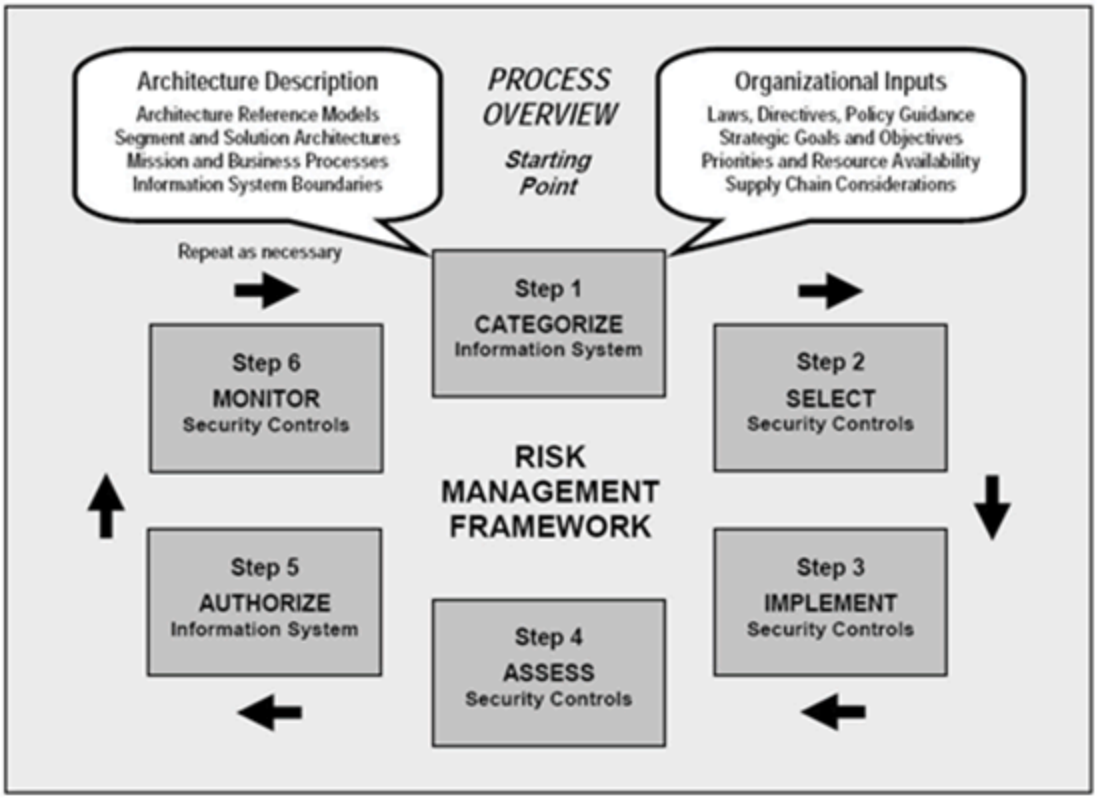
- **§164.306(e)€,** which requires organizations to ensure the following: “Security measures implemented to comply with standards and implementation specifications adopted...must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information.”
- **§164.308(a)(1)(ii)(D),** Information system activity review, which requires organizations to “implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”
- **§164.308(a)(8),** Evaluation, which requires organizations to “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."

The success of a risk management process depends heavily on the commitment of those involved with safeguarding an application or system. These individuals must implement the approved control recommendations. Therefore, it is strongly suggested that some type of follow-up be scheduled approximately 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 to 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 healthcare organizations can determine an appropriate time frame. Figure 9 illustrates the ongoing risk management process as described in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Revision 1 February 2010).

Figure 9 - A Security Life-Cycle Approach



Notes

1. The Office of the National Coordinator for Health Information Technology. *Guide to Privacy and Security of Health Information*. Available online at http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
2. Business associates are now required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule because of the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and as amended by the Omnibus Rule (released January 25, 2013) [Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; and Other Modifications to the HIPAA Rules]
3. 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.

4. U.S. Department of Health and Human Services. “The Security Rule.” Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html.
5. U.S. Department of HHS. “Security Rule Guidance Material.” Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.
6. Centers for Medicare and Medicaid Services, Office of E-Health Standards and Services . “HIPAA Compliance Review Analysis and Summary of Results.” 2008. Available online at www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf.
7. U.S. Department of HHS. 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.
8. Office for Civil Rights. Breaches Impacting More than 500 Individuals available online at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
9. NIST SPs in the 800 series are available online at: http://csrc.nist.gov/publications/PubsSPs.html.
10. 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).”
11. Alberts, Christopher, and Audrey Dorofee. *Managing Information Security Risks– The OCTAVESM Approach*. Boston, MA: Addison-Weley, 2002.

Reference

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

Prepared by (2013)

Tom Walsh, CISSP

Assisted by (2013)

William Miaoulis, CISA, CISM

Acknowledgments (2013)

Becky Buegel, RHIA, CHP, CHC
Marlisa Coloso, RHIA, CCS
Julie A. Dooling, RHIA
Katherine Downing, MA, RHIA, CHPS, PMP
Sharon Easterling, MHA, RHIA, CCS, CDIP, CPHM
Lesley Kadlec, MA, RHIA
Michele Kruse, MBA, RHIA, CHPS
Kelly McLendon, RHIA CHPS
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA
Jane DeSpiegelaere, MBA, RHIA, CCS, FAHIMA

Prepared by (2011)

Tom Walsh, CISSP

Acknowledgments (2011)

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 (2013 update)" (AHIMA Practice Brief, November 2013)