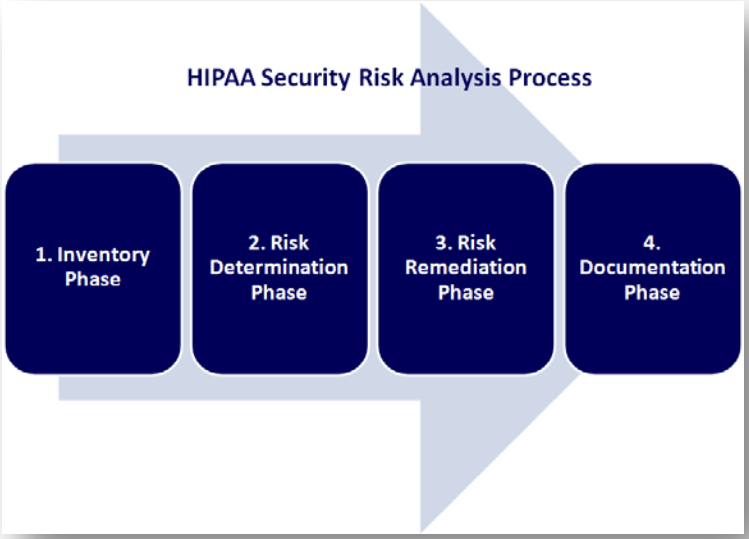
A White Paper for Healthcare Professionals

HIPAA Security Risk Analysis and Risk Management Methodology

Background and Requirements



Bob Chaput, MA, CHP, CHSS, MCSE

Table of Contents

Introduction

This document provides background about and specific requirements regarding a HIPAA Risk Analysis. It describes our Security Risk Analysis and Management Methodology and the rationale behind our approach.

The HIPAA Security Final Rule[8] requires every covered entity (CE) and now, due to The HITECH Act, every Business Associate (BA) to conduct a risk analysis (§164.308(a)(1)(ii)(A)) to determine security risks and implement measures *"to sufficiently reduce those risks and vulnerabilities to a reasonable and appropriate level."* The HITECH Act requires every business associate (BA) to implement all applicable standards and specifications in the Security Rule.

This document also briefly reviews the HIPAA-HITECH regulatory requirements for security risk analysis and risk management and describes a practical methodology for completing a Risk Analysis according to the latest Health and Human Services (HHS) and Office for Civil Rights (OCR) Risk Analysis guidelines, entitled "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[1].

This Risk Analysis and Methodology has been used by organizations of all sizes and is purposefully designed to be able to be able to be used by the largest CEs and BAs (e.g., hospitals, insurors, care management firms, etc) to the smallest CEs and BAs (e.g., small medical practices, clinics, dental offices, medical billing companies etc.).

From a very practical perspective, what one ultimately seeks to develop by completing a risk analysis is a prioritized list of security risks that need to be addressed with a risk mitigation action based on an informed decision. The classic formula for calculating risk is:

Risk = Impact * Likelihood

These terms (risk, impact, likelihood and many others) will be explained in detail in this document. A classic categorization of risks is shown in the following matrix. Our process helps you determine your risks, categorize them as Low, Medium, High or Critical and then develop a risk remediation action plan.

Overall Risk Value				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Low	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Regulatory Requirement

The HIPAA Security Final Rule[8], reinforced by the HITECH Act, requires every CE and BA, in accordance with the security standards general rules (§164.306), to have a security management process in place *"to implement policies and procedures to prevent, detect, contain, and correct security violations."*

The security standards include general requirements to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the CE or BA creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy rule
- Ensure compliance with this law by its workforce

The standards are flexible in regards to approach:

- CEs and BAs may use any security measures that allow the CE to reasonably and appropriately implement the standards and implementation specifications as specified in this law
- In deciding which security measures to use, a CE or BA must take into account the following factors:
  - The size, complexity, and capabilities of the CE or BA
  - The CE's or BA's technical infrastructure, hardware, and software security capabilities
  - The costs of security measures
  - The likelihood and impact of potential risks to electronic protected health information

In applying flexibility, however, the preamble to the Security Rule states, *"Cost is not meant to free covered entities from this [adequate security measures] responsibility."*

As required by The HITECH Act, the Office for Civil Rights, within the Department of Health and Human Services (HHS), has issued final "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[1]. The following excerpts provide an overview of this guidance:

> *The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (ePHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.*
>
> *We [OCR] begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A).*

Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements. An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

Specific Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to *"[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."* (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard.

Section 164.308(a)(1)(ii)(A) states:

> *RISK ANALYSIS (Required).*
> *Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].*

Risk Analysis Approaches

Risk analysis and risk management are two of the required implementation specifications within the security management process standard. The Security Rule does not specify exactly how a risk analysis should be conducted, but it does reference the National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information Technology Systems." The NIST publication offers a comprehensive approach to incorporating risk management into the system or project development life cycle. Threats in the environment are identified, and then vulnerabilities in information systems are assessed. Threats are then matched to vulnerabilities to describe risk.

The NIST document includes a description of the roles of various persons in risk analysis and management. It emphasizes the key role senior management plays in understanding security risk, establishing direction, and supplying resources. HIPAA requires assigning responsibility to the security official for the development and implementation of security policies and procedures.

This individual may lead the team that actually performs the risk analysis, do much of the policy and procedure writing, and recommend or even select many of the controls.

The fact that NIST identifies the chief information officer, system and information owners, business and functional managers, information technology (IT) security analysts, and trainers recognizes the importance of a team that extends beyond IT and encompasses users. In a clinical setting, users of information systems not only can assist in providing application and data criticality information, but must also be involved in determining which mitigation strategies will work.

Because many small clinics, medical practices or business associates do not have a full-time information technology person not to mention a chief information officer, system and information owners, business and functional managers, information technology (IT) security analysts, etc., the risk analysis should be completed by a combination of outside HIPAA-HITECH Security specialists, practice management staff, the clinical staff and business leaders and managers.

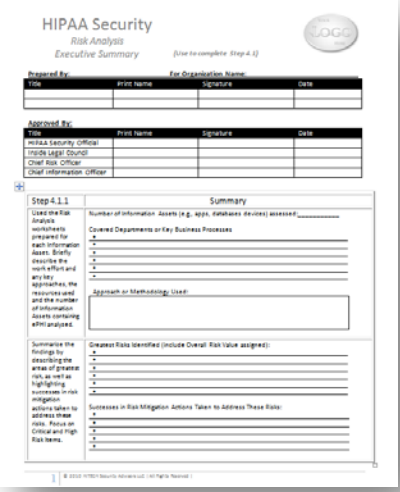
Specific Elements a Risk Analysis Must Incorporate

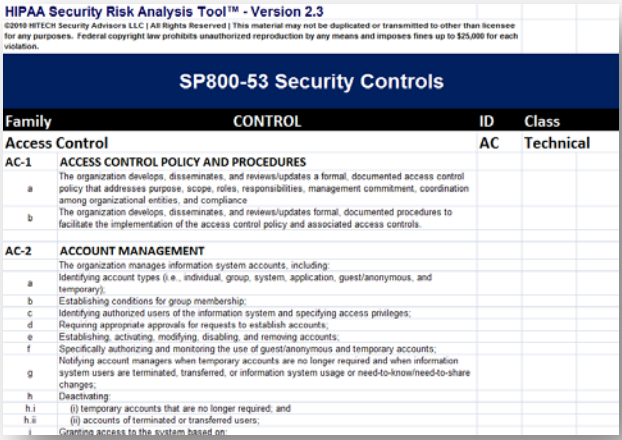
The "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[1] describes nine (9) essential elements a Risk Analysis must incorporate, regardless of the risk analysis methodology employed. These elements are as follows:

1. **Scope of the Analysis** - all ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (45 C.F.R. § 164.306(a).)
2. **Data Collection** - The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316 (b)(1).)
3. **Identify and Document Potential Threats and Vulnerabilities** - Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)
4. **Assess Current Security Measures** - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)
5. **Determine the Likelihood of Threat Occurrence** - The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)
6. **Determine the Potential Impact of Threat Occurrence** - The Rule also requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)
7. **Determine the Level of Risk -** The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

8. **Finalize Documentation -** The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).)
9. **Periodic Review and Updates to the Risk Assessment -** The risk analysis process should be ongoing. In order for an entity to update and document its security measures "as needed," which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).)

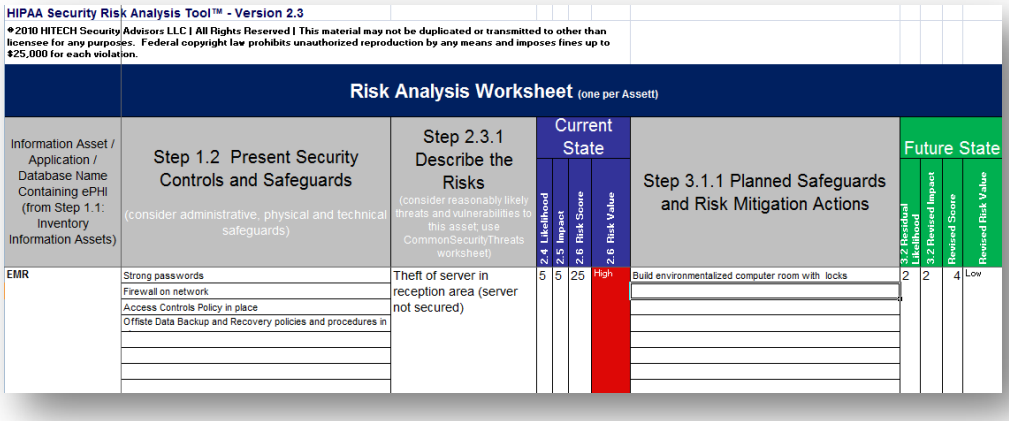
In our risk analysis methodology, as shown in the section below entitled "How Our Risk Analysis Methodology Meets/Exceeds All HHS/OCR Guidance", we help you complete the risk analysis implementation specification (45 C.F.R. § 164.308(1)(ii)(A)) and make substantial progress in meeting the requirements of the risk management implementation specification (45 C.F.R. § 164.308(1)(ii)(B)). In a separate HIPAA Security Risk Analysis ToolKit™, we make available to CEs and BAs, we provide forms, templates and specific Step-by-Step instructions.


HIPAA Security
Risk Analysis
Executive Summary


HIPAA Security Risk Analysis Tool™ - Version 2.3

SP800-53 Security Controls

Family	CONTROL	ID	Class
Access Control		AC	Technical
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		
a	The organization develops, disseminates, and reviews/updates a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance		
b	The organization develops, disseminates, and reviews/updates formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.		
AC-2	ACCOUNT MANAGEMENT		
	The organization manages information system accounts, including:		
a	Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);		
b	Establishing conditions for group membership;		
c	Identifying authorized users of the information system and specifying access privileges;		
d	Requiring appropriate approvals for requests to establish accounts;		
e	Establishing, activating, modifying, disabling, and removing accounts;		
f	Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;		
g	Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;		
h	Deactivating:		
h.i	(i) temporary accounts that are no longer required; and		
h.ii	(ii) accounts of terminated or transferred users;		
i	Granting access to the system based on:		


HIPAA Security Risk Analysis Tool™ - Version 2.3

Risk Analysis Worksheet (one per Assett)

Information Asset / Application / Database Name Containing ePHI (from Step 1.1: Inventory Information Assets)	Step 1.2 Present Security Controls and Safeguards (consider administrative, physical and technical safeguards)	Step 2.3.1 Describe the Risks (consider reasonably likely threats and vulnerabilities to this asset; use CommonSecurityThreats worksheet)	Current State: 2.4 Likelihood	2.5 Impact	2.6 Risk Score	2.6 Risk Value	Step 3.1.1 Planned Safeguards and Risk Mitigation Actions	Future State: 3.2 Residual Likelihood	3.2 Revised Impact	Revised Score	Revised Risk Value
EMR	Strong passwords Firewall on network Access Controls Policy in place Offsite Data Backup and Recovery policies and procedures in	Theft of server in reception area (server not secured)	5	5	25	High	Build environmentalized computer room with locks	2	2	4	Low

Security Risk Analysis and Management Methodology

The principles behind our methodology are sound, incorporate all of the key essential elements indicated in the HHS/OCR final guidance and include industry best practices at the core of quantitative risk analysis approaches.

Our practical approach to conducting and documenting a risk analysis for the HIPAA Security Rule involves these four major phases:

1. **Inventory Phase**
   1.1. Inventory information assets, especially those handling ePHI
   1.2. Document their present security controls and criticality of the applications and their data

2. **Risk Determination Phase**
   2.1. Identify threats in the environment
   2.2. Identify vulnerabilities that threats could attack
   2.3. Describe the risks based on threats and vulnerabilities
   2.4. Determine the likelihood of the risk
   2.5. Determine the severity of the impact
   2.6. Determine and summarize the risk level

3. **Risk Remediation Phase**
   3.1. Recommend risk mitigation strategies for each risk
   3.2. Implement applicable controls to mitigate risk
   3.3. Determine residual likelihood that a threat could attack a vulnerability
   3.4. Analyze the residual severity of the impact
   3.5. Determine and report residual risk to senior management

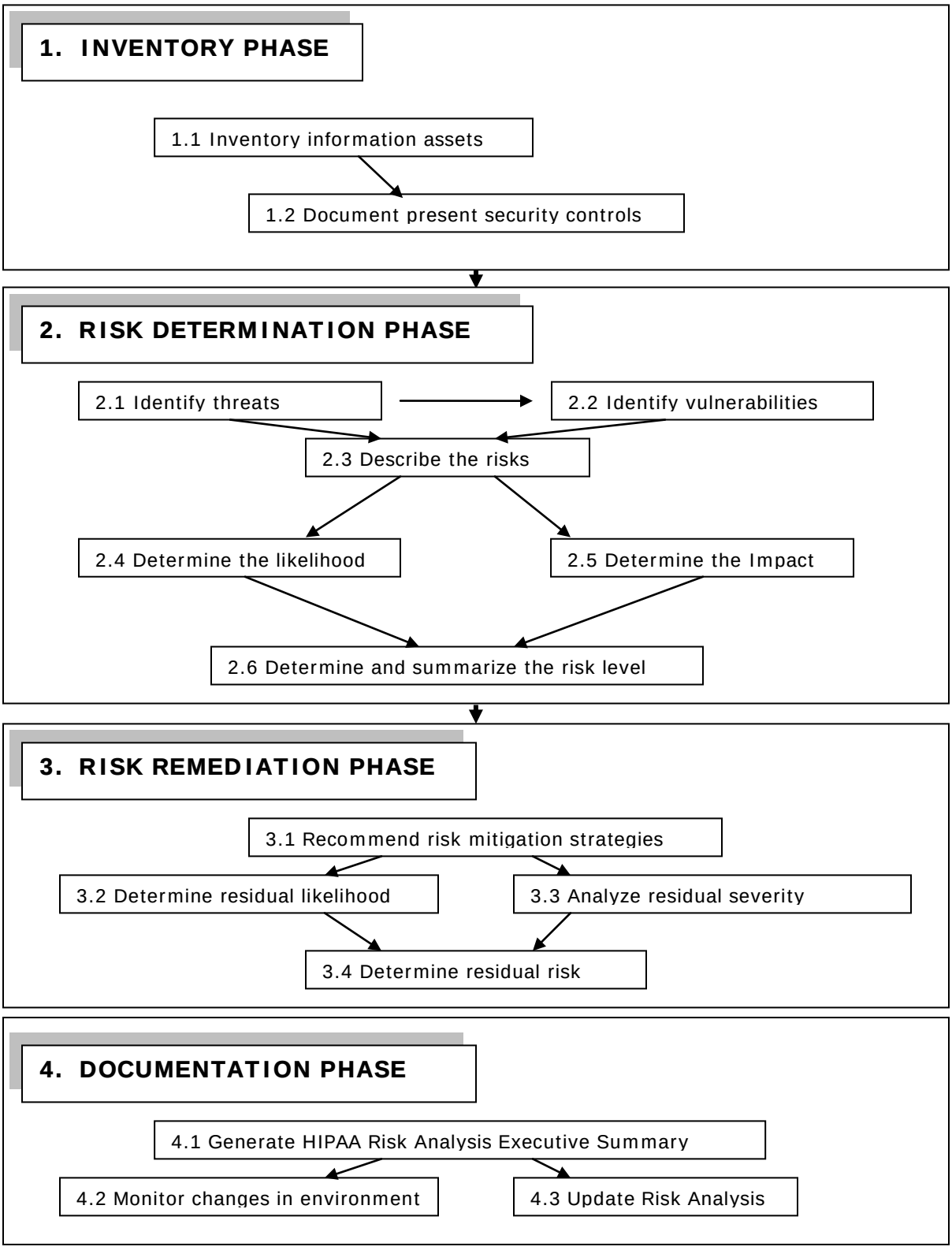
4. **Documentation Phase**
   4.1. Generate HIPAA Risk Analysis Executive Summary
   4.2. Monitor changes in the environment, information systems, and security technology
   4.3. Update the risk analyses; and implement any other controls

How Our Risk Analysis Methodology Meets/Exceeds All HHS/OCR Guidance

Our Risk Analysis methodology incorporates all essential HHS/OCR-specified elements of a risk analysis and extends beyond these requirements in several areas. Below, our Risk Analysis Phases and sub-phases are mapped to the nine (9) HHS/OCR essential elements:

Our Risk Analysis	HHS/OCR elements of a risk analysis
1. Inventory Phase 1.1. Inventory information assets, especially those handling ePHI 1.2. Document their present security controls and criticality of the applications and their data	1. **Scope of the Analysis** 2. **Data Collection** *Our Risk Analysis methodology includes inventory forms and instructions for capturing all relevant details about ePHI.*
2. Risk Determination Phase 2.1. Identify threats in the environment 2.2. Identify vulnerabilities that threats could attack 2.3. Describe the risks based on threat/vulnerability pairings 2.4. Identify existing controls 2.5. Determine the likelihood that a threat could attack a vulnerability 2.6. Analyze the severity of the impact 2.7. Determine and summarize the risk level	*In addition to addressing all the HHS/OCR requirements, our Risk Analysis methodology iterates through the risk planning process taking into account implementing controls or safeguards and recalculating risk.* 3. **Identify and Document Potential Threats and Vulnerabilities** 4. **Assess Current Security Measures** 5. **Determine the Likelihood of Threat Occurrence** 6. **Determine the Potential Impact of Threat Occurrence** 7. **Determine the Level of Risk**
3. Risk Remediation Phase 3.1. Recommend risk mitigation strategies for each risk 3.2. Implement applicable controls to mitigate risk 3.3. Determine residual likelihood that a threat could attack a vulnerability 3.4. Analyze the residual severity of the impact 3.5. Determine and report residual risk to senior management	*Our Risk Analysis methodology facilitates informed decision making about risk management actions. Forms and instructions capture essential documentation throughout the process.*
4. Documentation Phase 4.1. Generate HIPAA Risk Analysis Executive Summary 4.2. Monitor changes in the environment, information systems, and security technology 4.3. Update the risk analysis; and implement any other controls	8. **Finalize Documentation** 9. **Periodic Review and Updates to the Risk Assessment** *Our Risk Analysis methodology includes forms, templates and instructions to create appropriate documentation and management reporting.*

Our Security Risk Analysis Process Flow



Our Security Risk Analysis ToolKit™ Contents

For those who acquire our HIPAA Risk Analysis ToolKit™ directly or through a HIPAA Risk Analysis WorkShop™ engagement, you will find the ToolKit™ contents include, but are not limited to:

- HIPAA Risk Analysis Excel Workbook Tool™, which in turn includes
  - Information Asset Inventory worksheet / form
  - Risk Analysis worksheet / form
    - Current State Risk Determination
    - Future State Residual Risk Determination
  - Remediation Project Tracking worksheet / form
  - NIST Special Publication 800-53 Security Controls resource worksheet
  - Risk Ratings resource worksheet
  - Common Security Risks resource worksheet
  - Types of Threats resource worksheet
  - Glossary of HIPAA-HITECH Privacy and Security resource worksheet
  - References resource worksheet
- HIPAA Security Risk Analysis Executive Summary form/template
- HIPAA Security Final Rule
- Health and Human Services – Office for Civil Rights, “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”
- National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information Technology Systems"

Summary

To say, there is some debate in the security community among the experts surrounding the definitions of Risk, Threats and Vulnerabilities and how to conduct a Risk Analysis is a slight understatement. Prestigious organizations such as ISO, IEC, NIST and ENISA seem to disagree, and the Information Security industry also offers various definitions.

A primary focus of our risk analysis methodology is to make it practical, tangible and actionable… and as fast as possible. Therefore, we have worked to simply the process while not compromising the ultimate outcomes. Remember, security safeguards must be designed to be reasonable and appropriate and, ultimately, manage risk.

Risk management does not mean finding 100 safeguards that are missing and drumming up a $1 million budget to address them all. Risk management means making informed decisions about which risks to mitigate and which risks to accept. There are many options for risk mitigation including, but not limited to:

1. **Risk assumption**
2. **Risk avoidance**
3. **Risk limitation**
4. **Risk planning**
5. **Research and acknowledgement**
6. **Risk transference**

Making informed decisions which options are optimal for your organization should be based on a sound Risk Analysis, one that is based on the NIST standards, industry best practices and, most importantly for healthcare organizations, the final "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"[1] issued by OCR.

A successful risk analysis and management program depends on people—people given the authority and assuming responsibility for complying with policy and following procedure, for awareness and reporting incidents, and for offering suggestions for mitigating risk.

The Security Rule contains many more administrative and physical safeguard standards than technical standards. Even as it only addresses protected health information in electronic form, it is people that make security happen.

Benefit from our experience and expertise.

References

1. Health and Human Services – Office for Civil Rights, “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”, (http://www.datamountain.com/wp-content/uploads/OCR_Risk-Analysis_Final_guidance.pdf)

2. National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

3. National Institute of Standards and Technology (NIST) Special Publication 800-33, " Underlying Technical Models for Information Technology Security" (http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf)

4. National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1, "A Resource Guide for Implementing The HIPAA Security Rule" (http://csrc.nist.gov/publications/PubsSPs.html)

5. National Institute of Standards and Technology (NIST) Special Publication 800-14, “Generally Accepted Principles and Practices for Securing Information Technology Systems” (http://csrc.nist.gov/publications/nistpubs/800-14/Planguide.PDF)

6. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 Final, "Recommended controls for Federal Information Systems and Organizations" (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)

7. Notice of Public Rulemaking (NPRM) – “Modifications to HIPAA Privacy, Security and Enforcement Rules under The Health Information Technology for Economic and Clinical Health Act (HITECH)” (http://hipaasecurityassessment.com/wp-content/uploads/2010/07/Modifications-to-the-HIPAA-Privacy-Security-and-Enforcement-Rules-under-HITECH.pdf)

8. “HIPAA Security Final Rule” (http://www.datamountain.com/files/HIPAA_Security_Final_Rule.pdf)

How to Purchase Our HIPAA Risk Analysis ToolKit™

An End-to-End Solution for Completing Required HIPAA Security Risk Analysis

Buy Now at: http://hipaasecurityassessment.com/estore/hipaa-hitech-security-risk-analysis-toolkit/

What You Receive – HIPAA Security Risk Analysis ToolKit™

- HIPAA Security Risk Analysis ToolKit™ Contents document
- How to Use the HIPAA Security Risk Analysis ToolKit™ document
- **Comprehensive HIPAA Security Risk Analysis Excel Workbook Tool™,** HIPAA Compliance Software
- HIPAA-HITECH Security Compliance Roadmap™
- Comprehensive HIPAA Security Glossary of Terms, included with Excel Tool™
- HIPAA Security Risk Analysis and Risk Management Methodology with Step-by-Step Instructions
- Executive Summary – Risk Analysis template
- HHS/OCR Final Guidance on Risk Analysis
- NIST Special Publication 800-30, "Risk Management Guide for Information Technology
- NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations”
- **60 minutes of complimentary email, telephone or web-meeting support**
- **Very Latest Updates on HITECH Act and NPRM Changes**

How You Benefit by Using the HIPAA Security Risk Analysis ToolKit™

- Avoid re-inventing forms, templates, worksheets and references
- Use Step-by-Step instructions to complete a thorough Risk Analysis
- Complete Risk Analysis faster, better and cheaper
- Meet key Meaningful Use core objective
- Determine specific information assets and all associated ePHI
- Determine and document present security controls
- Assess threats and vulnerabilities to your information assets and ePHI
- Determine gaps in security controls and make plans to remediate them
- Make informed decisions, based on data, facts and current risks
- Develop solid documentation of HIPAA Risk Analysis process and controls for audits

Buy Now at: http://hipaasecurityassessment.com/estore/hipaa-hitech-security-risk-analysis-toolkit/