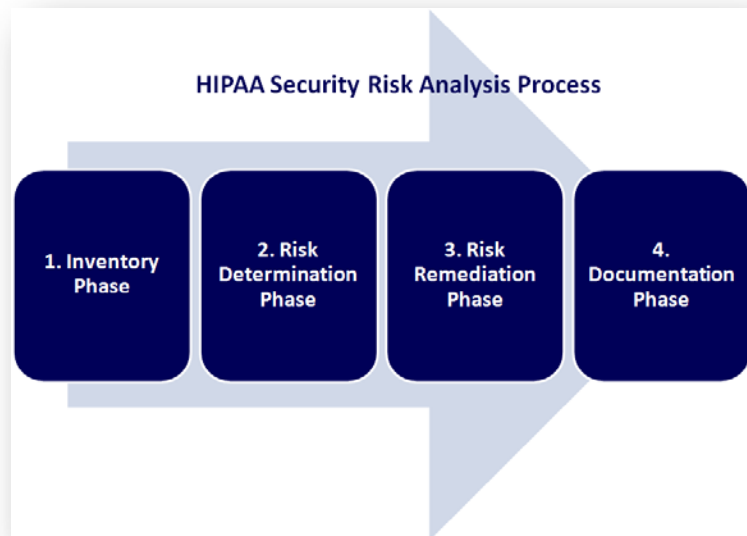




HIPAA Security Risk Analysis and Risk Management Methodology

with Step-by-Step Instructions



Bob Chaput, MA, CHP, CHSS, MCSE



Table of Contents

Table of Contents	2
Introduction	3
Regulatory Requirement	4
Specific Risk Analysis Requirements under the Security Rule	5
Risk Analysis Approaches	5
Specific Elements a Risk Analysis Must Incorporate	6
Security Risk Analysis and Management Methodology	8
How Our Risk Analysis Methodology Meets/Exceeds All HHS/OCR Guidance	9
Our Security Risk Analysis Process Flow	10
Our Security Risk Analysis ToolKit™ Contents	11
Our Security Risk Analysis Step-by-Step Instructions	12
Keys for Success	30
References	Error! Bookmark not defined.
How to Purchase Our HIPAA Risk Analysis ToolKit™	32



Introduction

This document describes our Security Risk Analysis and Management Methodology and the rationale behind this approach. It also includes Step-by-Step Instructions

The HIPAA Security Final Rule⁸ 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 provides a practical methodology and step-by-step instructions for completing a Risk Analysis according to the latest Health and Human Services (HHS) and Office of 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 used by the largest CEs and BAs (e.g., hospitals, insurers, 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:

$$\text{Risk} = \text{Impact} * \text{Likelihood}$$

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 Security Rule⁸, reinforced by the HITECH Act, requires a CE and a 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 of 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)). We provide forms, templates and specific Step-by-Step instructions.

HIPAA Security Risk Analysis Tool™ - Version 2.3

©2010 HITECH Security Advisors LLC | All Rights Reserved | This material may not be duplicated or transmitted to other than licensee for any purposes. Federal copyright law prohibits unauthorized reproduction by any means and imposes fines up to \$25,000 for each violation.

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	Obtaining 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; 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;		
g	Deactivating		
h	(i) temporary accounts that are no longer required; and		
h.i	(ii) accounts of terminated or transferred users;		
i	Granting access to the system based on:		

HIPAA Security Risk Analysis Tool™ - Version 2.3

©2010 HITECH Security Advisors LLC | All Rights Reserved | This material may not be duplicated or transmitted to other than licensee for any purposes. Federal copyright law prohibits unauthorized reproduction by any means and imposes fines up to \$25,000 for each violation.

Risk Analysis Worksheet (one per Asset)										
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 Common Security Threats worksheet)	Current State			Step 3.1.1 Planned Safeguards and Risk Mitigation Actions	Future State			
			2.4 Likelihood	2.5 Impact	2.6 Risk Score		3.2 Residual Likelihood	3.2 Revised Impact	4 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 this 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

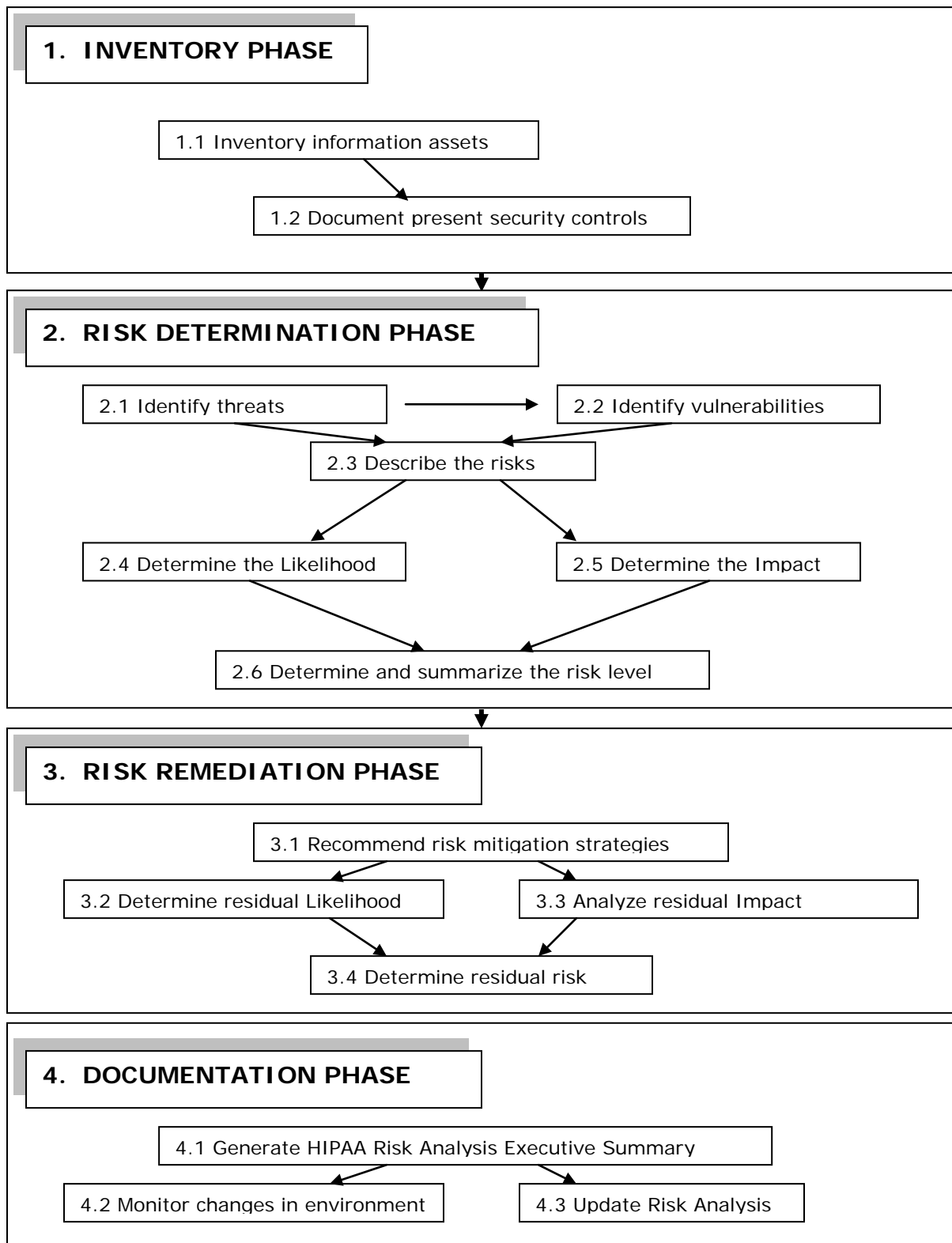


How Our Risk Analysis Methodology Meets/Exceeds All HHS/OCR Guidance

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 <i>Our Risk Analysis methodology includes inventory forms and instructions for capturing all relevant details about ePHI.</i>
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	<i>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.</i> 3. Identify and Document Potential Threats and Vulnerabilities 4. Assess Current Security Measures 5. Determine the Likelihood of Threat Occurrence
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	6. Determine the Potential Impact of Threat Occurrence 7. Determine the Level of Risk <i>Our Risk Analysis methodology facilitates informed decision making about risk management actions. Forms and instructions capture essential documentation throughout the process.</i>
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 <i>Our Risk Analysis methodology includes forms, templates and instructions to create appropriate documentation and management reporting.</i>

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 of 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"



Our Security Risk Analysis Step-by-Step Instructions

The following procedures detail the steps, within major phases, to complete the HIPAA Security Risk Analysis using our Risk Analysis methodology.

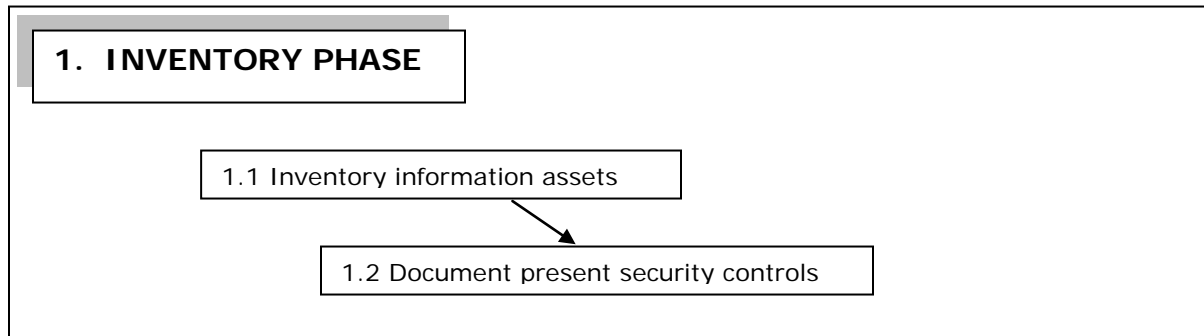
These Step-by-Step Instructions require the HITECH Security Advisors Risk Analysis Tool™ which is an Excel macro-enabled workbook with key worksheets / forms including, but not limited to:

- **Information Asset Inventory** – the worksheet / form is used to gather relevant data about information assets with electronic Protected Health Information (ePHI) that an organization creates, receives, maintains or transmits.
- **Risk Analysis** – the worksheet used to analyze current state threats and vulnerabilities, determine risk, assess current safeguards, plan mitigating actions and assess residual risks.
- **Types of Threats** – the worksheet used to assist in brainstorming reasonably anticipated vulnerabilities and threats that may affect the organizations information assets and ePHI.
- **Risk Ratings** – the worksheet containing definitions of likelihood and impact (i.e., criticality) used in determining both current state risk and residual or future state risk after mitigating safeguards have been implemented.
- **NIST Special Publication 800-53 Security Controls resource worksheet** – this worksheet may be used in assessing current controls in place and potential security controls which may be implemented to mitigate risks.
- **Risk Ratings resource worksheet** - this worksheet includes the ratings used to assess likelihood and impact of various threats and vulnerabilities and shows how the overall Risk Score is determined
- **Common Security Risks resource worksheet** - this worksheet contains a list of common security risks faced by organizations today and may be used in assessing threats and vulnerabilities an organization may have.
- **Types of Threats resource worksheet** - this worksheet contains a categorized list of human, natural and environmental threats and may be used to stimulate thinking about threats your organization may encounter.
- **Glossary of HIPAA-HITECH Privacy and Security resource worksheet** - this worksheet contains a comprehensive list of terms and associated definitions in the domain of privacy, security, HIPAA and HITECH.
- **References resource worksheet** - this worksheet contains a list of useful resources and websites, both private and government, that may assist you with HIPAA and HITECH compliance.

Equivalent worksheets / forms and templates may be developed and used by anyone using our step-by-step instructions. The Risk Analysis Excel Workbook Tool™ along with several other useful reference and guidance documents are available in our HIPAA Risk Analysis ToolKit™.

1. Inventory Phase

1.1. Inventory Information Assets



Use the blank **Information Asset Inventory** worksheet inside the **Risk Analysis Excel Workbook Tool™** for this step.

An information asset is any software, hardware, network or computing component that creates, receives, maintains, or transmits ePHI. For example, the asset may be an electronic medical record system, an email system, a laptop computer, a PDA, etc. This step and the resulting completed inventory form the basis of completing your Risk Analysis for each individual asset identified in this step. Information assets identified here are then subjected to a detailed risk analysis either one-by-one or by class of asset (e.g., all the laptops that store ePHI).

For each information asset (database, major hardware, network equipment, operating systems, and application software) fill in the following columns/fields, as appropriate and available, the following in the **Information Asset Inventory** worksheet:

- 1.1.1. **Information Asset / Application / Database Name Containing ePHI** - provide a name for the information asset, application or database containing ePHI. This may be an acronym or a few words that describe a computer system through which data is created, received, maintained or transmitted to support a business function.
- 1.1.2. **Information Asset Owner** – indicate the name and/or title of the individual who is ultimately responsible for the confidentiality, integrity and availability of this information asset or ePHI.
- 1.1.3. **Description of Information Asset / Application / Database Name Containing ePHI** – describe the type of ePHI, including how it is collected or received, who has appropriate access to it, to whom it may be transmitted, the types of data elements beyond ePHI that may be located here.
- 1.1.4. **Location of ePHI** – indicate in the columns shown by making an “X”, on what types of devices or media is the ePHI created, received, maintained or transmitted. For example, network server, desktop, laptop, backup media, etc,



- 1.1.5. **ePHI Data Source** - Describe the source of the data as specifically as possible; e.g., created internally, received from other department, from an external business associate, vendor, etc).
- 1.1.6. **ePHI Data Sharing** - Describe any other entities with whom the data is shared; (e.g., other department, with an external business associate, another covered entity, subcontractor, vendor, etc).
- 1.1.7. **Business Processes Supported** - Describe the key business process supported or enabled by this information asset (e.g., patient treatment, patient billing, healthcare operations, communications, etc.)
- 1.1.8. **Asset Importance to Business** – Using a simple High (H), Medium (M), Low (L), characterize the asset's or ePHI's criticality to the business thinking in terms of how its loss or unavailability would affect the business.
- 1.1.9. **Estimated Number of Records** - Estimate the volume of data based on the subject of the data (i.e. number of patients, claims records, plan members, employees, research subjects, etc).
- 1.1.10. **Planned Risk Analysis Completion Date** - For each inventory item, a risk analysis will be completed. Indicate the month and year when that analysis will be completed.

The information gathered in these inventory data elements (1.1.1 to 1.1.10) will help inform and guide the risk analysis steps that follow. Such an inventory should encompass all information assets, wherever they are located.

A note about Planned Risk Analysis Completion Date: Use this Information Asset Inventory worksheet as a planning tool. That is, create a written schedule for conducting detailed risk analyses on each information asset or instance of ePHI. Based on completion of the Information Asset Inventory worksheet, you will likely have a strong sense as to which information assets containing ePHI should be assessed first. Prioritize those assets you believe (without the benefit of a detailed analysis) may be at significant risk and/or would have the greatest adverse effect on the organization if lost or breached and/or those assets of greatest importance to the business and/or those about which very little is known.

Consider ePHI criticality, based on the nature and use of that information, when setting your priorities. Think carefully about the following two questions when setting your priorities:

1. What would be the impact on the patient or member, the business, business partners, etc, if the ePHI were breached or lost?
2. What would be the impact on the business' operation if the information were no longer available or its accuracy compromised?



NOTE: STEP 1.2 (Document their present security controls and criticality of the applications and their data) THROUGH STEP 3.5 (Determine and report residual risk to senior management) IN THE PROCESS WILL BE REPEATED FOR EACH INFORMATION ASSET LISTED IN THE "ASSET INVENTORY".

That is, the Risk Analysis worksheet will be used multiple times; one time for each information asset containing ePHI, listed in the Information Asset Inventory. Prepare to copy/paste multiple copies of the Risk Analysis worksheet/form within the workbook.

1.2. Document present security controls

Use ONE blank **Risk Analysis** worksheet for each item listed in the **Information Asset Inventory** worksheet for this step. The Risk Analysis worksheet will be used in subsequent steps.

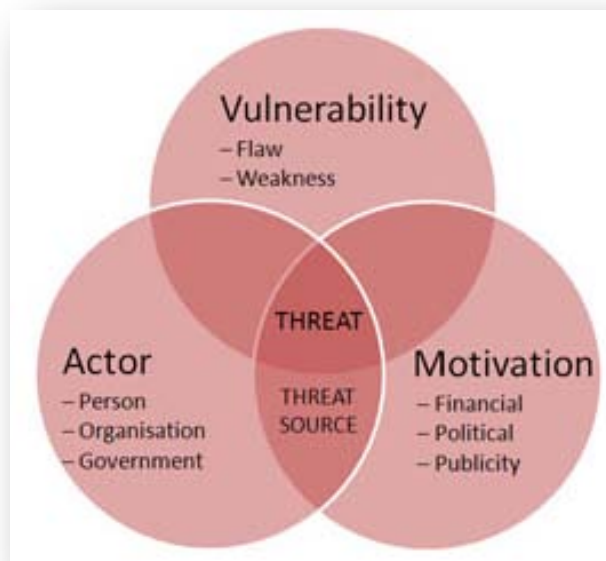
For each information asset listed in the Information Asset Inventory (database, major hardware, network equipment, operating systems, and application software), create a new Risk Analysis worksheet in the workbook. You will use this same Risk Analysis worksheet for this Asset for each of Steps 1.2 (Document their present security controls and criticality of the applications and their data) THROUGH 3.5 (Determine and report residual risk to senior management)

Fill in the following columns/fields, as appropriate and available, the following in the **Risk Analysis** worksheet:

- 1.2.1. **Information Asset / Application / Database Name Containing ePHI** – transcribe the name of the information asset, application or database containing ePHI from the Information Asset Inventory.
- 1.2.2. **Present Security Controls and Safeguards** – in this column, list as best as possible, any and all security controls that you believe to be in place for this Asset. In other words, describe how the confidentiality, integrity and availability of this Asset are being protected presently. These should include consideration of all administrative, physical and technical safeguards. Reference the worksheet entitled "SP800-53 Controls" as an aid / guide / memory prompt. From this worksheet, you may wish to copy/paste security controls from the "SP800-53 Controls" worksheet into the Risk Analysis worksheet.

After reading the brief background information on risks, threats and vulnerabilities immediately below, proceed to the next section on Risk Determination.

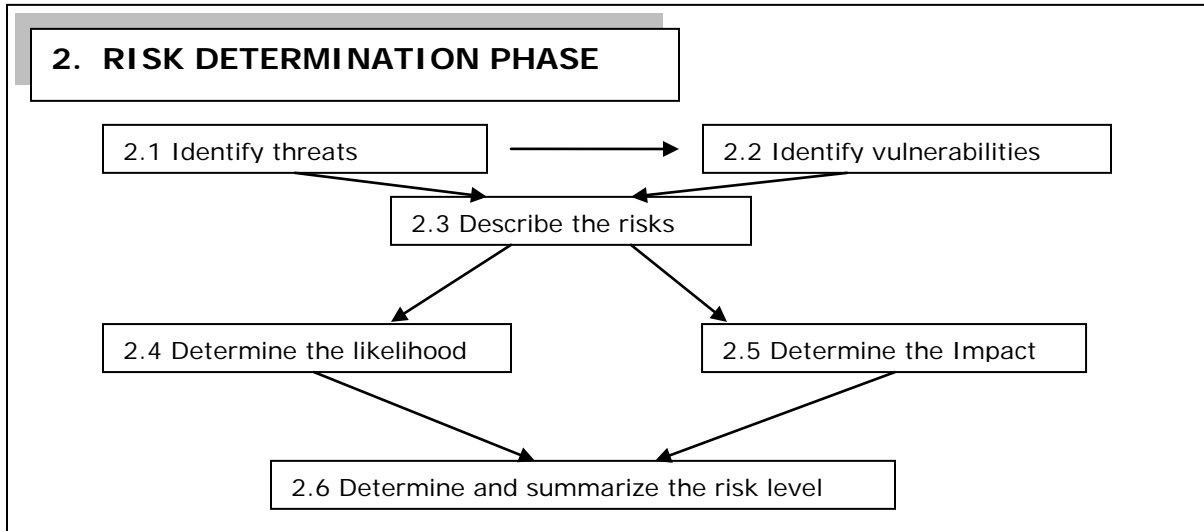
Brief Background Information on Risk, Threats and Vulnerabilities: To say, there is some debate in the security community among the experts surrounding the definitions of Risk, Threats and Vulnerabilities is a slight understatement. Prestigious organizations such as ISO, IEC, NIST and ENISA seem to disagree, and the Information Security industry also offers various definitions. The graphic below illustrates how fine-tuned the definitions and discussion may get...vulnerabilities, threats, threat-sources, actors, motivation, etc can make for lengthy intellectual discussions. A primary focus of our risk analysis methodology is to make it practical, tangible and actionable... fast. Therefore, we have worked to simply the process while not compromising the ultimate outcome.



We start where there is agreement: security safeguards must be designed to manage risk, and risk exists as a function of at least threat and vulnerability.

It is true that a threat-source does not represent a risk when there is no vulnerability that can be exercised or exploited. It is also true that in determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls. At the same time, we do not want you to become bogged down on definitional debate that may cause you to miss the mission at hand which is to ultimately develop a prioritized list of security risks that need to be addressed with a risk mitigation action, based on an informed decision.

In the following phase on Risk Determination, we have purposefully worked to simplify the matter of risk versus threat versus vulnerability by focusing on reasonably likely threats to ePHI and the risks they create without compromising the ultimate outcome of the Risk Analysis process. Your goal is to determine risks to information assets that create, receive, maintain and transmit ePHI, then prioritize those risks from highest-to-lowest and, ultimately, take risk mitigation actions that include implementing reasonable and appropriate safeguards.



2. Risk Determination Phase

Use the **Risk Analysis** worksheet from the previous step 1.2 (Document Present Security Controls) for each Asset from **Information Asset Inventory** worksheet.

Read Sections 2.1 and 2.2 below for background information. Then, fill in the columns/fields indicated, and as instructed, in the **Risk Analysis** worksheet to complete the steps in 2.3 through 2.6.

2.1. Identify Threats

An adapted definition of threat, from NIST SP 800-30, is “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

- Natural threats such as floods, earthquakes, tornadoes, and landslides.
- Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to ePHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

In security, therefore, a threat is anything that could harm information or systems creating, receiving, maintaining or transmitting that information by exercising a vulnerability.



Example - Laptop: As an example, theft of a laptop containing ePHI is a threat.

For the Asset under analysis, consider various threats to that asset. Use the worksheet entitled “Types of Threats” to identify possible threats that may be reasonably likely to this asset.

2.2. Identify Vulnerabilities

Vulnerability is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of ePHI.

Vulnerabilities may be grouped into two general categories, technical and nontechnical.

- Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines.
- Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

External sources of information about vulnerabilities include hardware and software vendor Web sites that might describe incidents others have had and provide patches or service packs to mitigate some of these. Many security associations produce online and print newsletters. Even local business groups, colleges or universities, and the police department may be good sources of information. Review of the Health and Human Services Data Breach Notification website (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>) should provide ideas about vulnerabilities that may exist to various information assets.

Example - Laptop: Using the threat of the theft of a laptop, as an example again, a vulnerability or weakness may be that the ePHI is not encrypted.

For the Asset under analysis, consider various security weaknesses or flaws in design that make this asset vulnerable. Use the external resources mentioned in the previous paragraph to prompt consideration of a wide range of vulnerabilities. Err on the side of considering more rather than fewer.

2.3. Describe the risks

Describe the risks in the asset under review in terms of confidentiality, integrity and/or availability elements that may result in a compromise of the system and the ePHI data it handles.



An adapted definition of risk, from NIST SP 800-30, is:

“The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . [R]isks arise from legal liability or mission loss due to—

- 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
- 2. Unintentional errors and omissions*
- 3. IT disruptions due to natural or manmade disasters*
- 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.”*

Risk can be understood as a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

- 2.3.1. **Describe the Risks** – consider all possible risks to the Asset being analyzed in the context of known vulnerabilities and common security threats. Use the “Common Security Threats” worksheet and the “Types of Threats” worksheet as a source of ideas and guidance. Create a separate row for each Risk to the Asset being analyzed. (Note: If you have multiple applications/databases that you believe are managed and secured identically, you may combine them when analyzing them against the various risks and threats listed in the tool). When evaluating each risk and threat against your application/database, first consider what controls you have already implemented and as documented in the column completed in Step 1.2 Present Security Controls and Safeguards.

2.4. Determine the Likelihood

The likelihood is an estimate of the frequency or the probability of such an event. Likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access and existing controls; the presence, motivation, tenacity, strength and nature of the threat; and the presence of vulnerabilities; and the effectiveness of existing controls.

- 2.4.1. **Indicate the Likelihood** – taking into account the factors list above, use the drop-down menu in the **Risk Analysis** worksheet to indicate on a scale of 0-5, the likelihood of this risk occurring.



Score The Likelihood:

- 0 = Risk/threat does not apply to this ePHI/application/database.
- 1 = Rare – The event would only occur under exceptional circumstances.
- 2 = Unlikely – The event could occur at some time, but probably will not.
- 3 = Moderate – The event should occur at some time.
- 4 = Likely – The event will probably occur at some time.
- 5 = Almost Certain – The event is expected to occur in most circumstances.

Example - Laptop: Because there are approximately 12,000 laptops that are lost or stolen in the US every week (~1 every 43 seconds), the likelihood is arguably moderate.

2.5. Determine the Impact

Determine the magnitude or severity of impact on the system's operational capabilities and ePHI data if the risk is realized. The impact can be measured by loss of system functionality, degradation of system response time or inability to meet a business mission, dollar losses, and loss of public confidence, legal liability, regulatory fines or unauthorized disclosure of data.

- 2.5.1. **Indicate the Impact** – taking into account the factors list above, use the drop-down menu in the **Risk Analysis** worksheet to indicate on a scale of 0-5, the impact on the organization were this risk to occur.

Score The Impact:

- 0 = Threat is not applicable to this application.
- 1 = Insignificant** – Negligible impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Very limited or no financial/political/legal/regulatory/operational impact.
- 2 = Minor** – Minor impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Minimal financial/political/legal/regulatory/operational impact.
- 3 = Moderate** – Medium impact on ability to plan and conduct business activities with a moderate reduction in customer service, operational efficiency and staff morale. Some financial/political/legal/regulatory/operational is experienced.
- 4 = Major** – Major impact on ability to plan and conduct business activities with significant reduction in customer service, operational efficiency and staff morale. Considerable financial/political/legal/regulatory/operational impact.
- 5 = Disastrous** – Comprehensive impact on ability to plan and conduct business activities with total disruption in customer service, operational efficiency and staff morale. Devastating financial/political/legal/regulatory/operational impact.

Example - Laptop: Depending on the number of individuals' records that may be breached, the impact may be minor, moderate, major or even disastrous.



2.6. Determine and summarize the risk level

Once the Likelihood and Impact scores are entered for each threat, the Risk Analysis worksheet automatically calculates a Risk Score and a Risk Value.

The Risk Score is computed using the basic risk equation:

Risk Score = Impact * Likelihood, with scores ranging from 0-25

The Risk Value provides an overall risk severity rating and is computed using the basic risk equation:

Risk Value = Critical, High, Medium, or Low, and is assigned based on the Risk Score as follows:

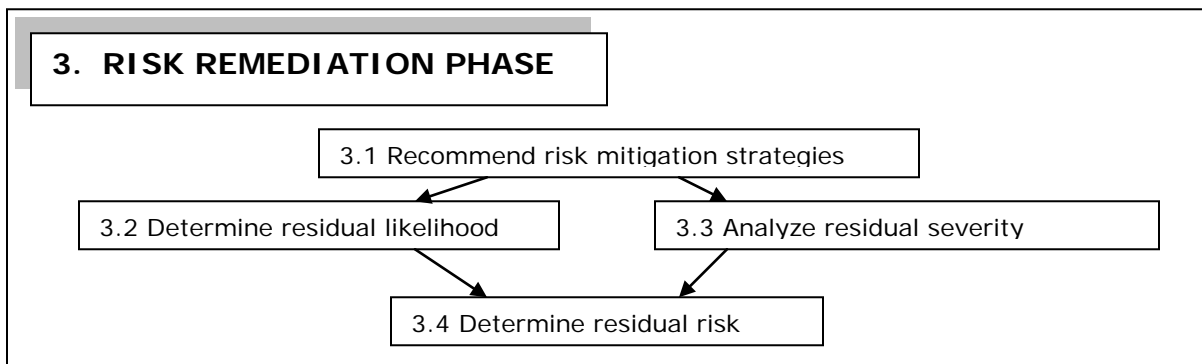
- Risk Score > 19 → Critical
- Risk Score > 13 and < 19 → High
- Risk Score > 5 and < 13 → Medium
- Risk Score < 5 → Low

Once completed, one can visualize the various risks that have been analyzed for each asset falling into one of the categories in this risk matrix.

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

Example - Laptop: Because there are approximately 12,000 laptops that are lost or stolen in the US every week (~1 every 43 seconds), the likelihood is arguably moderate. Depending on the number of individuals' records that may be breached, the impact may be minor, moderate, major or even disastrous. For the sake of discussion, assume the laptop stored ePHI related to 100,000 individuals. Arguably, the impact would be major, if not disastrous, in which case the overall Risk Value would be either High or Critical.

3. Risk Remediation Phase



Use the **Risk Analysis** worksheet from the previous step 2.6 (Determine and Summarize the Risk Level) for each Asset from **Information Asset Inventory** worksheet to complete risk remediation planning for each Asset.

Read Sections 3.1 below for background information and guidance, then complete Step 3.1.1 below. Fill in the columns/fields indicated, and as instructed, in the **Risk Analysis** worksheet.

3.1. Recommend risk mitigation strategies for each risk and implement applicable controls

Once each risk is understood for that Asset, risk mitigation strategies can be developed and controls implemented. The NIST Special Publication 800-33 “Risk Management Guide for Information Technology Systems²” lists six options for risk mitigation:

1. **Risk assumption**—the acceptance of the potential for risk. Controls may be used to lower risk, but not to the extent they could be if more resources are applied. This may be an acceptable strategy if risk is determined to be low and the cost of mitigation is high
2. **Risk avoidance**—the act of eliminating the risk cause. Generally this means forgoing certain functions in the system or shutting the system down. This strategy is not often used, but may be necessary on a temporary basis
3. **Risk limitation**—the implementation of controls that minimize the adverse impact of a threat exploiting a vulnerability. These controls would help deter, detect, and react to a potential threat.
4. **Risk planning**—the management of risk by prioritizing, implementing, and maintaining controls. This is essentially the process of conducting risk analysis and risk remediation as outlined here.
5. **Research and acknowledgement**—the acknowledgement that a vulnerability exists and the process to research appropriate controls. This should be considered a temporary strategy reserved for use during the implementation phase of the security



rule, the implementation of a new information system, or when a completely new threat becomes known

6. **Risk transference**—the selection of other options to compensate for loss, such as purchasing insurance or outsourcing certain business functions. This generally will be used in combination with other strategies.

The options above recognize that controls cannot totally eliminate risk. 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 application, such as backup systems, contingency plans

In addition to what the security controls address, control strategies should include administrative, physical, and technical components. The HIPAA Security Rule standards themselves offer guidance on what general types of controls are required. Furthermore, the Security Rule also references two other NIST Special Publications, “Generally Accepted Principles and Practices for Securing Information Technology Systems⁴” (800-14) and “Underlying Technical Models for Information Technology Security³” (800-33). Additionally, “Recommended Security Controls for Federal Information Systems and Organizations⁷” (800-53) includes over 170 specific controls in 17 different families of controls.

The NIST Web site (<http://csrc.nist.gov/publications/>) features many other helpful special publications. Many information system vendors have also posted information about what plans they have for enhancing security features.

Policy provides the overall direction for the controls. If senior management directs that controls should be preventive to the extent possible, then controls must necessarily be stronger than those where management indicates deterrent or detective controls are adequate.

Procedures will spell out the details of how specific controls will be implemented. While security policies should be known by all members of the work force, some security procedures may need to be considered sensitive information. In this case, only a limited number of persons with a need to know should have access to procedures such as how to set passwords or the encryption methodology employed. While procedures may be sensitive and the number of persons with a need to know limited, there should always be more than one



person who knows each procedure (backup) and no one person should know all procedures for all controls (separation of duties).

- 3.1.1. **Planned Safeguards and Risk Mitigation Actions** – For each risk, review those safeguards and controls listed in the “Common Security Controls” worksheet in the Risk Analysis worksheet that you have not already implemented.

The task here is to populate the worksheet with risk mitigation actions you plan to take. From the “Common Security Controls” worksheet, you may wish to copy/paste security controls into this column in the Risk Analysis worksheet. Reminder: This step does not necessarily mean that you are implementing the safeguard immediately. You are identifying which safeguards your organization plans to implement in the future, and in comments, you can describe what those plans are.

- 3.1.2. **Comments / Supporting Documentation / Plans** – For each risk mitigation action, as/if appropriate, make notes regarding the plans, resources assigned, timing and work products related to that risk mitigation action.

3.2. Determine residual Likelihood

A final step in risk mitigation is to determine and report residual risk to senior management. Because no system can be made risk free, residual risk is that risk remaining after the implementation of new or enhanced controls. In an age of due care and ultimate responsibility for mission accomplishment, an estimate of residual risk should be made and presented to senior management. If the residual risk has not been reduced to an acceptable level, the risk analysis cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

- 3.2.1. **Indicate the Residual Likelihood** – taking into account the factors list above, use the drop-down menu in the **Risk Analysis** worksheet to indicate on a scale of 0-5, the likelihood of this risk occurring.

Score The Likelihood:

- 0 = Risk/threat does not apply to this ePHI/application/database.
- 1 = Rare – The event would only occur under exceptional circumstances.
- 2 = Unlikely – The event could occur at some time, but probably will not.
- 3 = Moderate – The event should occur at some time.
- 4 = Likely – The event will probably occur at some time.
- 5 = Almost Certain – The event is expected to occur in most circumstances.



3.3. Determine the Revised Impact

Determine the residual severity of impact on the system's operational capabilities and data if the threat is realized and exploits the associated vulnerability. As above, with current state impact, the impact can be measured by loss of system functionality, degradation of system response time or inability to meet a business mission, dollar losses, loss of public confidence, legal liability, regulatory fines or unauthorized disclosure of data.

- 3.3.1. **Indicate the Residual Impact** – taking into account the factors list above, use the drop-down menu in the **Risk Analysis** worksheet to indicate on a scale of 0-5, the impact on the organization were this risk to occur.

Score The Impact:

0 = Threat is not applicable to this application.

1 = Insignificant – Negligible impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Very limited or no financial/political/legal/regulatory/operational impact.

2 = Minor – Minor impact on ability to plan and conduct business activities with minimal reduction in customer service, operational efficiency and staff morale. Minimal financial/political/legal/regulatory/operational impact.

3 = Moderate – Medium impact on ability to plan and conduct business activities with a moderate reduction in customer service, operational efficiency and staff morale. Some financial/political/legal/regulatory/operational is experienced.

4 = Major – Major impact on ability to plan and conduct business activities with significant reduction in customer service, operational efficiency and staff morale. Considerable financial/political/legal/regulatory/operational impact.

5 = Disastrous – Comprehensive impact on ability to plan and conduct business activities with total disruption in customer service, operational efficiency and staff morale. Devastating financial/political/legal/regulatory/operational impact.



3.4. Determine and summarize the revised risk level

Once the Revised Likelihood and Revised Impact scores are entered for each threat, the Risk Analysis worksheet automatically calculates a Risk Score and a Risk Value.

The Revised Risk Score is computed using the basic risk equation:

Revised Risk Score = Impact * Likelihood, with scores ranging from 0-25

The Risk Value provides an overall risk severity rating and is computed using the basic risk equation:

Revised Risk Value = Critical, High, Medium, or Low, and is assigned based on the Risk Score as follows:

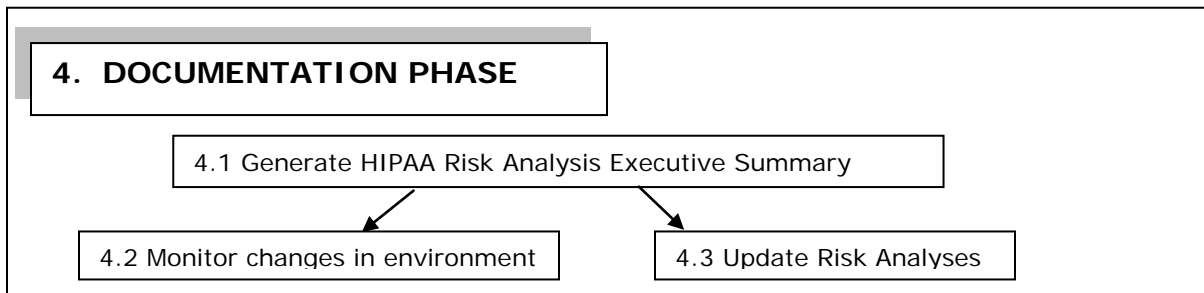
- Risk Score > 19 → Critical
- Risk Score > 13 and < 19 → High
- Risk Score > 5 and < 13 → Medium
- Risk Score < 5 → Low

Once completed, one can visualize the various risks that have been analyzed for each asset falling into one of the cells in this risk matrix.

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

With completion of this step, the Risk Analysis worksheet is complete for this Asset.

4. Documentation Phase



Use the **Executive Summary_Risk Analysis** Word document / template for this Step 4.1

Read Section 4.1 below for background information and guidance, then complete Step 4.1.1 below. Complete the form as instructed.

4.1. Generate HIPAA Risk Analysis Executive Summary

HIPAA requires documentation of the risk analysis process; and it requires that it be retained for six years. Documentation is critical in proving that the analysis was performed and to manage the ongoing Risk Management process. Even if you are in the “research and acknowledgment” phase, it is good practice to document all risks and remediation plans.

Once again, HIPAA does not specify the form of documentation a risk analysis should take. In this process, retain all individual Risk Analysis worksheets for each Asset analyzed. Additionally, prepare an executive summary for management reporting, documentation and project management purposes.

- 4.1.1. **Prepare the Executive Summary** – Use the **Executive Summary_Risk Analysis** Word document / template and enter the information required, including, but not limited to:
- 4.1.1.1. A summary of the Information Assets included in this Risk Analysis.
 - 4.1.1.2. A description of the approach used.
 - 4.1.1.3. A summary of the Critical and High risks identified, along with risk mitigation actions taken.
 - 4.1.1.4. A description of the most significant remediation projects undertaken or planned, including expected reduction in risk.
 - 4.1.1.5. Key Lessons Learned and Planned improvements in the process.
 - 4.1.1.6. An update in prior year / prior period risk remediation projects.



4.2. Monitor changes in the environment, information systems, and security technology

Risk management is the act of implementing the security measures. It also entails monitoring for changes and responding with enhanced strategies. The security standards general rules also address maintenance (§164.306(e): *“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.”*)

4.2.1. **Update the Risk Analysis Project Tracking worksheet** – Use the Risk Analysis Project Tracking worksheet / form to capture a summary of the status of detailed risk analyses for all information assets. Enter the information required, including, but not limited to:

- 4.2.1.1. Organizational Unit / Business Process Area
- 4.2.1.2. Name of Inventoried Information Asset (e.g., Application, Database, device, etc)
- 4.2.1.3. Fiscal Year for Risk Analysis
- 4.2.1.4. Detailed Risk Analysis Completed?
- 4.2.1.5. Executive Summary Covering Application/ Database Submitted?
- 4.2.1.6. Executive Summary Author
- 4.2.1.7. Notes/Comments

Additionally, the Information System Activity Review implementation specification under the security management process standard requires records of audit logs, access reports, and incident tracking reports. These and other internal and external documents should be periodically reviewed to determine if risk has increased. In addition, technology itself changes. Where it may have been difficult and costly in the past to institute single sign-on, new standards may make it easier to implement this measure that helps users manage their authentication process.

If specific reports do not trigger a review of risk, it may be suitable to institute specific indicators or future review dates. Federal government agencies are required by law to reassess risk to information systems every three years. This is a good benchmark from which to determine an appropriate time frame.

4.3. Update the risk analysis; and implement any other controls



One measure that the final Security Rule does not explicitly address is configuration management. The rule's preamble explains this was eliminated as a separate standard (previously included in the proposed security rule) because it was believed to be incorporated in other standards. Configuration management is essentially change control. Many organizations apply configuration management to information technology to manage versions of software and prioritize requests for changes to systems. A formal change control procedure should also address security. Any time a change in an Information Asset takes place; two key elements should be reviewed:

1. Are security controls in place? Were any security controls temporarily shut off to install an upgrade? Have they been reinstated? Are there default controls in the new system that should be customized to your environment?
2. Should new controls be adopted? Are changes to the system or new systems such that old controls don't work or newer controls will apply? Are there additional controls that are needed for the upgrade or new system?



Keys for Success

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.



References

1. Health and Human Services – Office of 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/>