HITRUST®

A Framework-based Approach to HIPAA Compliance


Module Overview

Topics

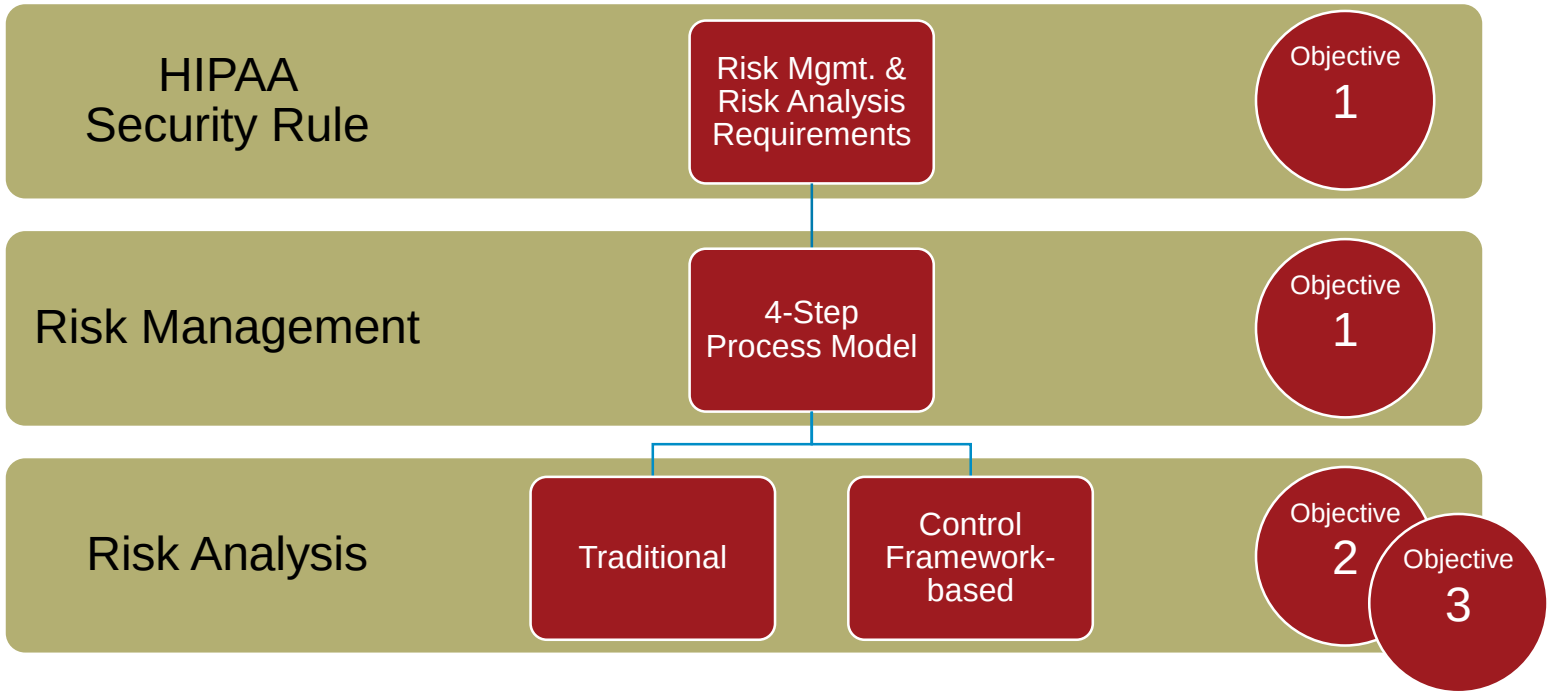
- Module Overview
- HIPAA Security Rule
- Risk Management
- Traditional Risk Analysis
- Control-based Risk Management Frameworks
- Control Framework-based Risk Analysis
- Considerations & Takeaways
- Questions & Additional Resources
- Appendices
  - A. More on the HITRUST Framework
  - B. Additional Definitions

Learning Objectives

By the end of this module, you should be able to:

1. Explain the HIPAA Security Rule's risk analysis requirement and discuss the exact role it plays in how one manages information security risk
2. Compare and contrast the two most common approaches organization's use to satisfy the HIPAA Security Rule's risk analysis requirement
   a) "Traditional" risk analysis
   b) "Control Framework-based" risk analysis
3. Select the approach most suitable to your situation based on their respective pros and cons

Topical Relationships to the Learning Objectives




HIPAA Security Rule

HIPAA Requirements for the Protection of ePHI

§ 164.306 Security Standards: General Rules.

(a) General requirements. Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

…

HIPAA Requirements for Risk Management & Analysis

§ 164.308 Administrative Safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) 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 covered entity or business associate.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).


Risk Management

What is Risk Management?

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

Risk Management

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

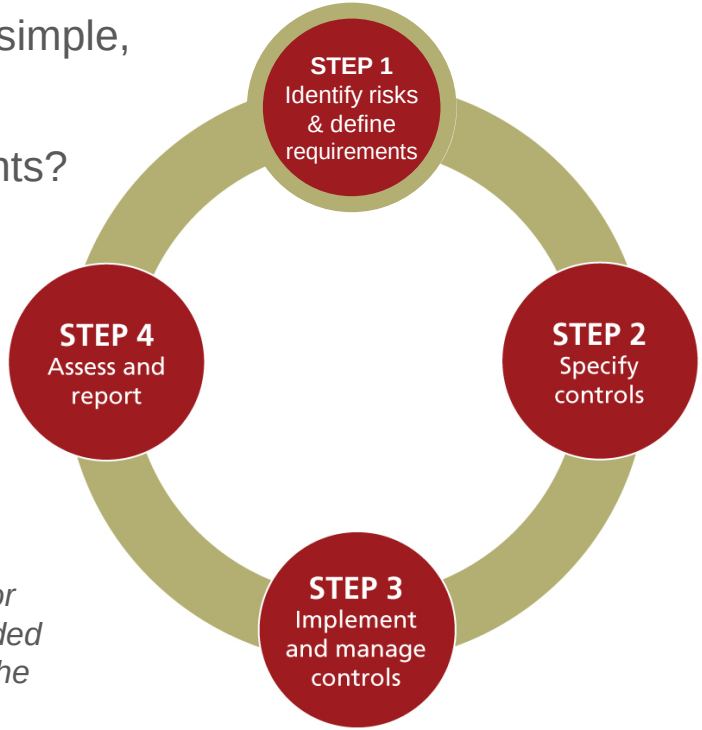
Risk Analysis

Examination of information to identify the risk to an information asset. Synonymous with risk assessment.

- NIST Interagency Report 7298 Revision 2, *Glossary of Key Information Security Terms*

Risk Management Process Model

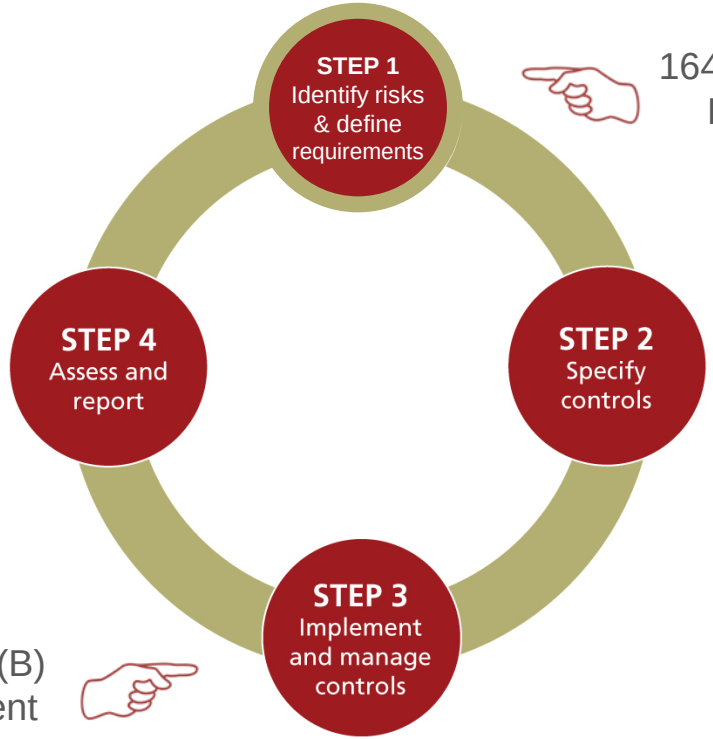
- Risk management can be represented by a very simple, 4-step process model
  - Step 1 – What are my protection requirements?
  - Step 2 – How do I provide the protection?
  - Step 3 – Provide the protection
  - Step 4 – How is my protection working?
- "Rinse & Repeat"



** Information security controls, also referred to as countermeasures or safeguards, consist of those policies, procedures and activities intended to help reduce operational and financial risk to an organization from the inappropriate disclosure, loss or corruption of information*

Example Based on Home Security

HIPAA Risk Management & Analysis in the Model



164.308(a)(1)(ii)(A)
Risk Analysis

164.308(a)(1)(ii)(B)
Risk Management

HIPAA


Control-based Risk Management Frameworks

Control-based RMFs

Control-based frameworks provide organizations with a common

- Understanding of information security risk concepts and principles
- Approach to evaluating, treating and reporting information security risk
- **“Template” of information security controls* to get one started**
- **Approach to evaluating, reviewing and improving information security controls**

Commonly Used Control-based RMFs

- National Institute of Standards & Technology (NIST) SP 800-53 and related 800-series publications

- Organization for International Standards (ISO) 27001 and related 27000-series publications

- HITRUST CSF and supporting RMF publications

- Payment Card Industry (PCI) Data Security Standard (DSS) and associated publications

Home Security Example

- The American National Standards Institute (ANSI) publishes a security standard on residential alarm and security cabling*, which includes but is not limited to the following requirements (controls):
  - Security system wiring should be installed while the building is under construction and prior to dry wall installation.
  - All low-voltage wire runs that are run parallel to AC power cables should be separated by at least 12".
  - All wiring must terminate in an alarm or a control panel grounded to a true earth ground.
  - Home run wiring is required from all sensors/detectors to the control panel.
- Many such standards would apply to home security, such as standards around doors and locks, as well as the building itself
- In all cases, terms and methods would be defined (e.g., for construction, installation and testing)

* ANSI/TIA/EIA-570A Addendum 1

Characteristics of a Control-based RMF

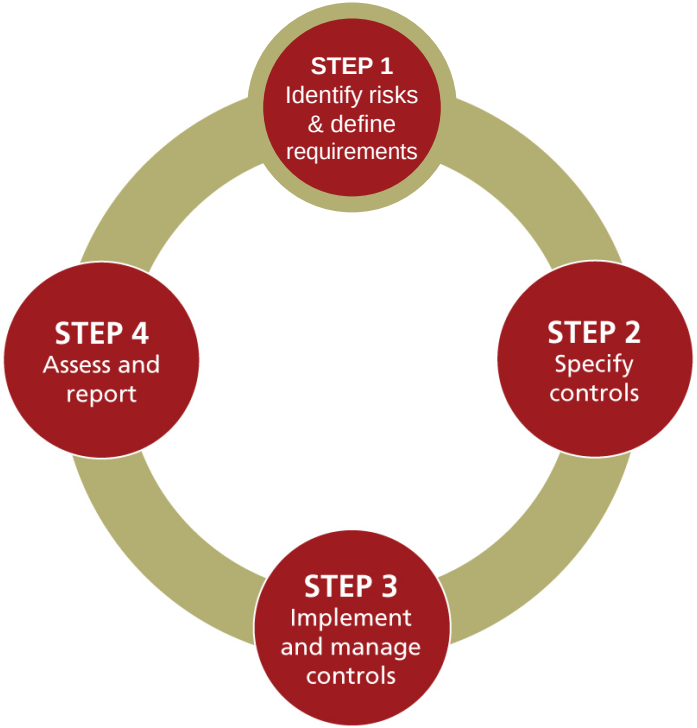
A ***good*** control-based RMF should provide:

- **Comprehensive coverage** of general security requirements
- **Practical, prescriptive, and scalable** controls
- An **open** and **transparent** process
- **Consistent** and **accurate** evaluation and reporting
- **Efficient** implementation
- **Reliable** assessment and reporting

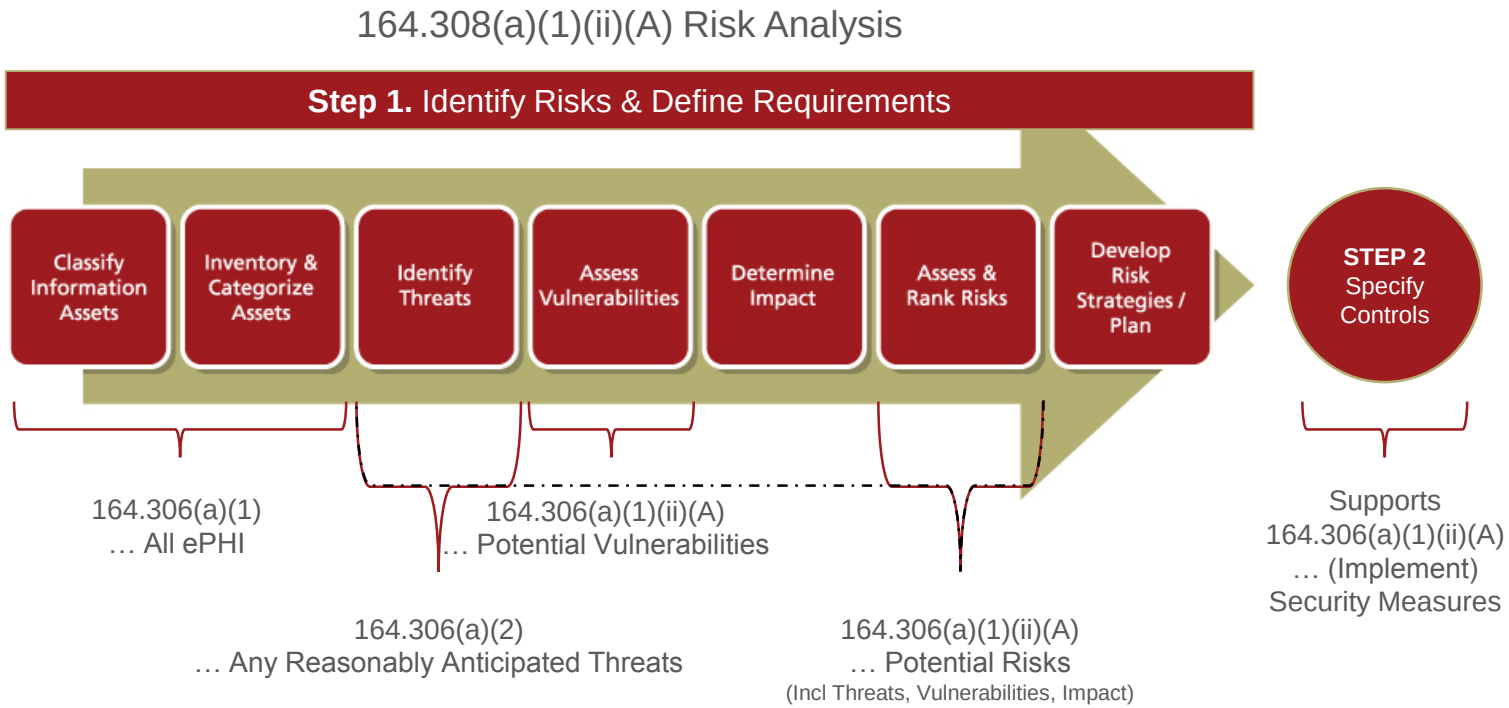

Traditional Risk Analysis

Risk Mgmt. Process Model with Traditional Risk Analysis

- *Step 1 – What are my protection requirements?*
- Step 2 – How do I provide the protection?
- Step 3 – Provide the protection
- Step 4 – How is my protection working?
- “Rinse & Repeat”



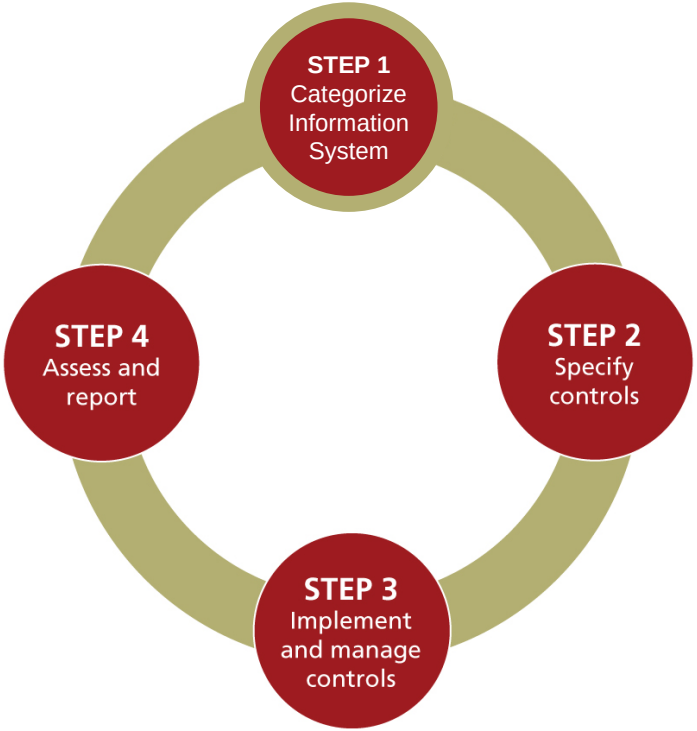
The Risk Analysis Process




Control Framework-based Risk Analysis
HITRUST®

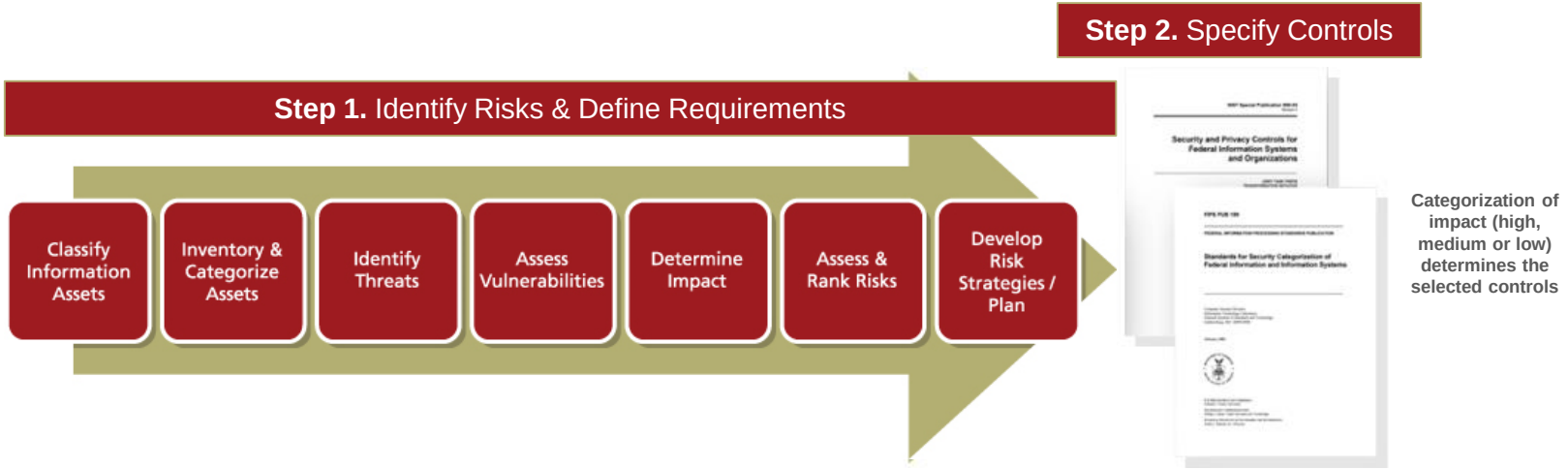
Control Framework-based Risk Analysis in the Model

- Another version of the 4-step risk management process model modifies the risk analysis in the first step
  - Step 1 – How much will it hurt if I don't protect my information?
  - Step 2 – How do I provide the protection?
  - Step 3 – Provide the protection
  - Step 4 – How is my protection working?
- "Rinse & Repeat"



Control Framework-based Risk Analysis

- Alternative approach leveraging a control framework (NIST example)



Tailoring the NIST SP 800-53 Security Controls

- Obtain a starting point by selecting a NIST minimum security control baseline, e.g., the moderate impact baseline, to provide an “80% solution”
- For the other “20%,” an organization must customize* the controls
  - Add controls to address unique threats or vulnerabilities **based on a targeted risk analysis**
  - Specify alternatives for controls you cannot implement, e.g., due to technical reasons
  - Define values for each control, e.g., a 5-minute screen timeout
- Review your customizations periodically to ensure risks remain adequately addressed

*NIST baselines **must** be tailored to organizational needs **before** they can be applied. See NIST SP 800-53 r4, §3.2 for more information on the tailoring process

Example of a NIST Security Control

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

Control Enhancements:

(1) SESSION LOCK | PATTERN-HIDING DISPLAYS The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

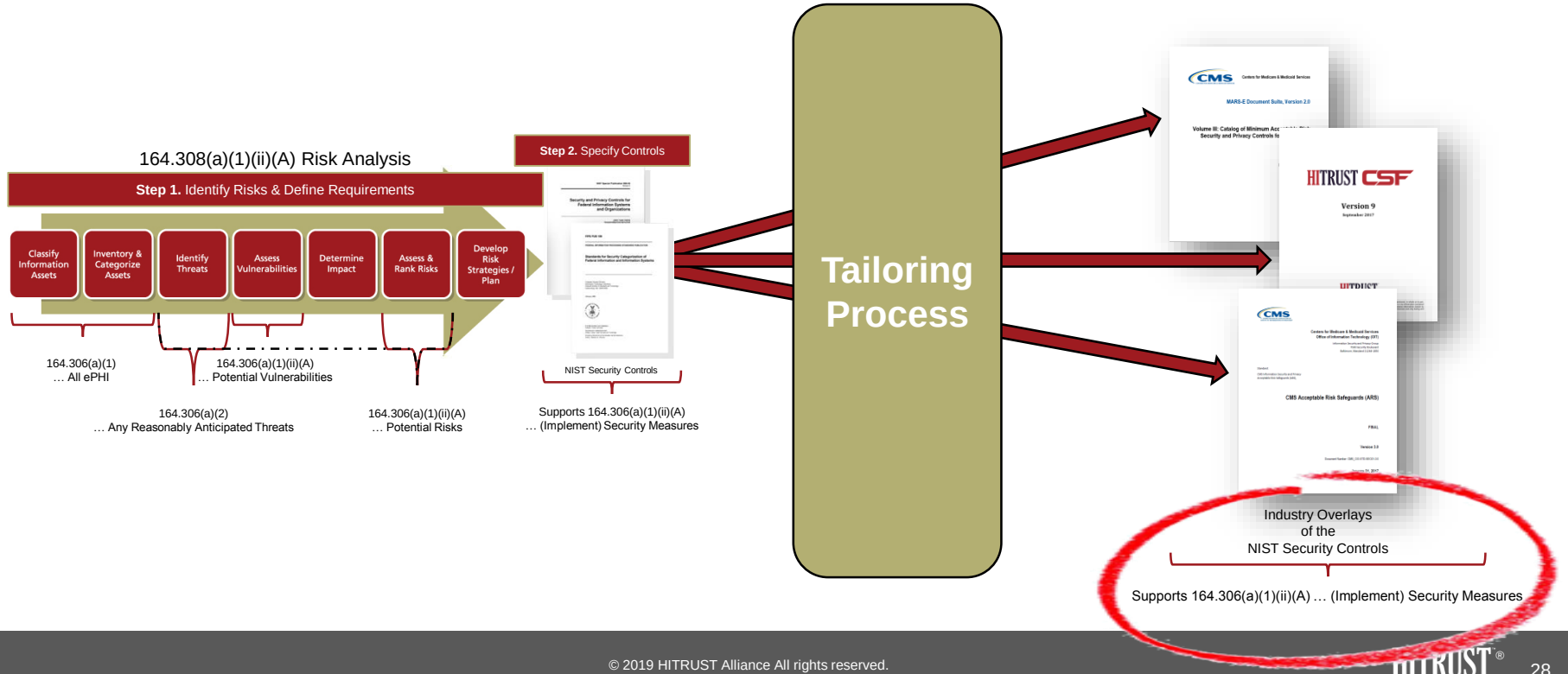
References: OMB Memorandum 06-16.

Industry-specific Overlays

- An overlay* is a fully specified set of security controls, enhancements and supplemental guidance derived through the tailoring process
- Overlays help organizations achieve standardized security capabilities, consistency of implementation, and cost-effective security solutions, and may support
  - Industry/sectors (e.g., healthcare, public health)
  - Information technology (e.g., medical devices, cloud services)
  - Coalitions/partnerships (e.g., Joint HITRUST™ certification & EHNAC accreditation)
  - Statutory/regulatory requirements (e.g., HIPAA, PCI)
- Overlays become the new “gold standard” for the intended “community-of-interest”

*See NIST SP 800-53 r4, §3.3 for more information on creating overlays

Existing Overlays in the Healthcare Industry

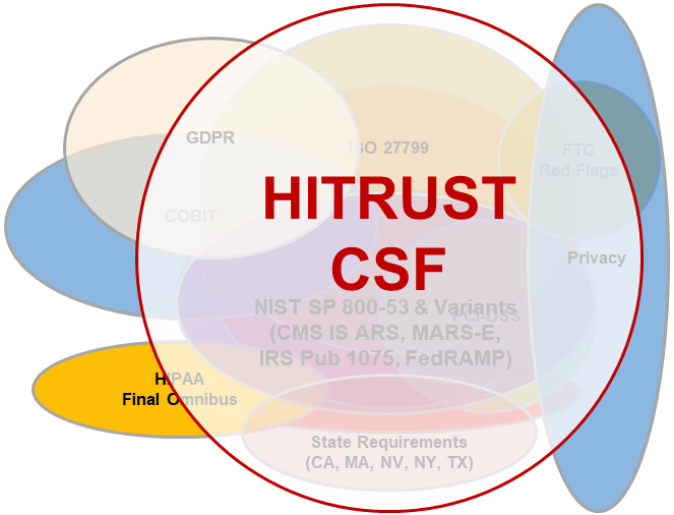


Comparing NIST, CMS & HITRUST Controls – Example

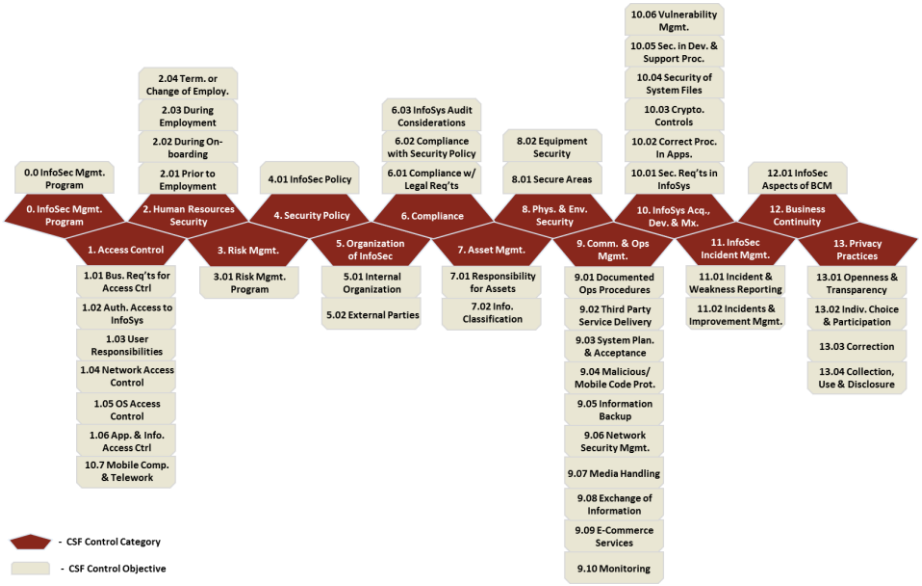
NIST SP 800-53 R4 AC-7 Unsuccessful Logon Attempts (*Moderate*)	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [**Selection:** locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.
CMS IS ARS* V3 AC-7 Unsuccessful Logon Attempts	The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and b. Automatically disables or locks the account/node until released by an administrator or after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. Implementation Standards: *High*: Std.1 - Configure the information system to lock out the user account automatically after three (3) invalid login attempts during a 120 minute time period. Require the lock out to persist until released by an administrator. *Moderate*: Std.1 - Configure the information system to lock out the user account automatically after five (5) invalid login attempts during a 120 minute time period. Require the lock out to persist for a minimum of one (1) hour. *Low*: Std.1 - Configure the information system to disable access for at least fifteen (15) minutes after five (5) invalid login attempts during a 120 minute time period.
HITRUST CSF V9.1 01.p Secure Log-on Procedures	A secure log-on procedure shall: 1. display a general notice warning that the computer shall only be accessed by authorized users; 2. limit the number of unsuccessful log-on attempts allowed to six (6) attempts; 3. enforce recording of unsuccessful and successful attempts; 4. force a time delay of thirty (30) minutes before further log-on attempts are allowed OR reject any further attempts without specific authorization from an administrator; and 5. not display the password being entered by hiding the password characters with symbols.

More on the HITRUST Overlay

Industry-specific overlay of the NIST moderate impact security controls baseline

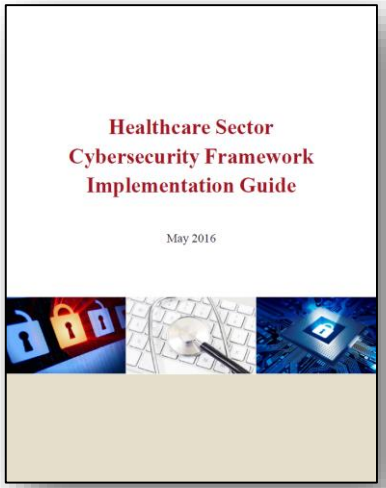


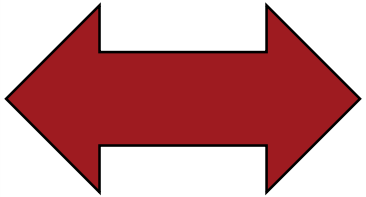
A new, comprehensive yet tailorable **control-based RMF** for the healthcare industry

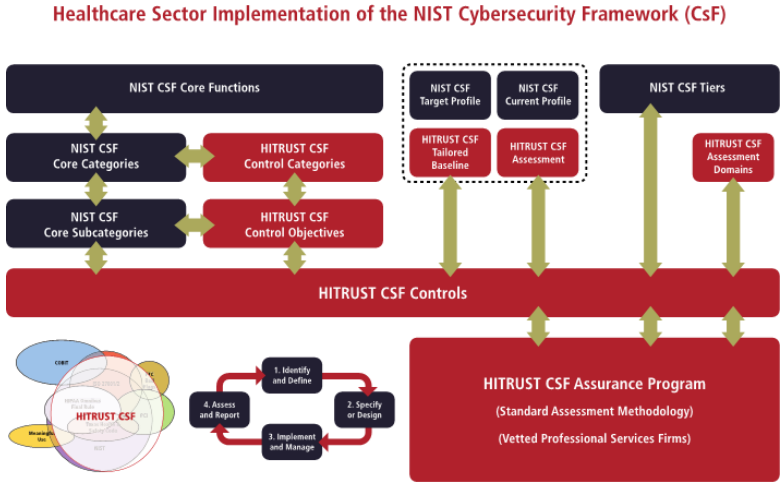


HITRUST and the NIST Cybersecurity Framework (CsF)

Guidance on implementing the NIST CsF leveraging the HITRUST RMF was developed through the Healthcare and Public Health Government and Sector Coordinating Councils, which is a public-private partnership that includes DHS, HHS and numerous industry organizations and associations





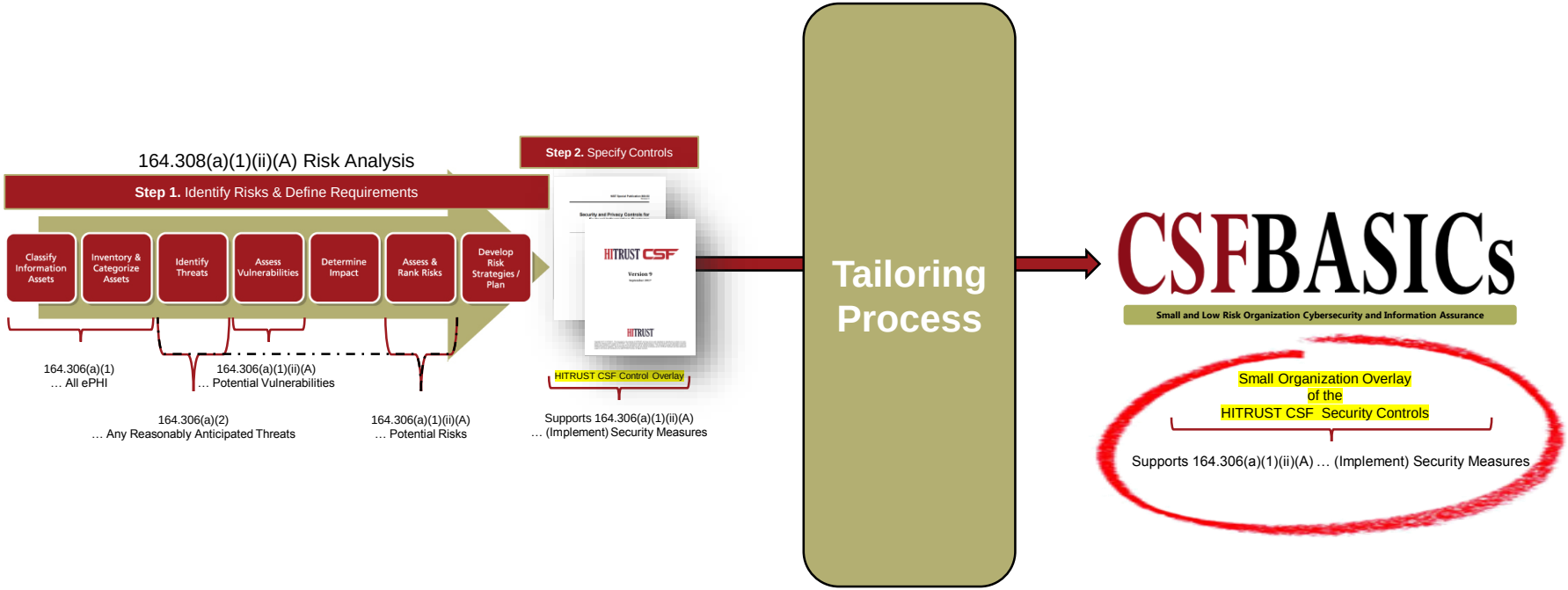


Comparing Frameworks

Requirement	Approach*					
	HITRUST (CSF)	ISO (27001)	NIST (800-53)	PCI SSC (DSS)	NIST (CsF)†	HHS (HIPAA)‡
Comprehensive Coverage	Yes	Yes	Yes	Yes	Yes	Partial
Prescriptive Controls	Yes	Partial	Yes	Yes	No	No
Practical Controls	Yes	Yes	No	Yes	Yes	Yes
Scalable Implementation	Yes	Yes	No	Partial	Yes	Yes
Transparent Update Processes	Yes	Partial	Yes	No	Yes	No
Transparent Evaluation & Scoring Methodology	Yes	Partial	Partial	Partial	No	No
Consistent Results	Yes	Partial	Yes	Partial	No	No
Accurate Results	Yes	Partial	Partial	Partial	No	No
Efficient Assessment ("Assess Once, Report Many")	Yes	Partial	Partial	No	Partial	No
Reliable Results ("Rely-ability")	Yes	Partial	Partial	Partial	No	No
Certifiable for implementing entities	Yes	Yes	Partial	Yes	Partial	No

* Since HITRUST, ISO, NIST and PCI are all RMFs, the document specifying their associated controls is used in the table to uniquely identify them
† The NIST CsF is a high-level framework that relies on the specification or design of additional controls to support the framework's recommended outcomes
‡ HIPAA specifies information security requirements (generally at a high level) but is a U.S. federal regulation and not a risk management framework

New Control Overlay for Small, Low-Risk Organizations



More on CSFBASICs

Requirements

- Program
  - Eligibility based on size (SBA criteria) & risk (# of records held/processed)
  - Covers the HIPAA Security, Data Breach Notification, and Privacy Rules
- Controls
  - 76 security controls (includes data breach notification)
  - 34 privacy controls
- Evaluation
  - Simplified 3-point maturity model (policy, process/ procedures, implementation)
  - Simplified 3-point scoring model (fully compliant, partially compliant, non compliant)
  - Separate control to address periodic monitoring of the information protection program

Control Examples

Topic: Education, Training & Awareness

- Control: *Employees receive security and privacy training*

  Guidance: Security training is provided to employees as part of their “onboarding” process within 60 days of hire and as part of an ongoing awareness program specific to their roles, which includes why it’s important, what it covers, and what they must do, what they can and cannot do with the organization’s information resources, and what will happen if they do something wrong

- Control: *The office documents what is acceptable and unacceptable uses of its information*

  Guidance: Documented rules of behavior describe users’ responsibilities and acceptable use of information resources (e.g., networks, computers, systems, and information). Acceptable use agreements address, at a minimum, rules of behavior for email, Internet, mobile devices, social media, and facilities/grounds.


Considerations & Takeaways

Considerations for Each Approach

Traditional Risk Analysis

- Must be applied to all assets where ePHI "lives"
- *Must ensure a complete evaluation of anticipated threats & known vulnerabilities (i.e., starting at 0%) to design a comprehensive set of information security controls*
- Must be applied intelligently to specific assets within the organization

Framework-based Risk Analysis

- Must be applied to all assets where ePHI "lives"
- *Although significant tailoring is done to create the overlay (starting at 80%*), the organization must perform additional tailoring via a targeted risk analysis to address any unique threats & vulnerabilities (for the additional 20%*)*
- Must be applied intelligently to specific assets within the organization

* Based on the Pareto Principle (also known as the 80/20 Rule, the law of the vital few, or the principle of factor sparsity), which states that, for many events, roughly 80% of the results (effects) come from 20% of the effort (causes). In this case, an organization must only provide a limited amount of effort to obtain a near complete specification of the security controls required to address reasonably anticipated threats to the sensitive information is uses.

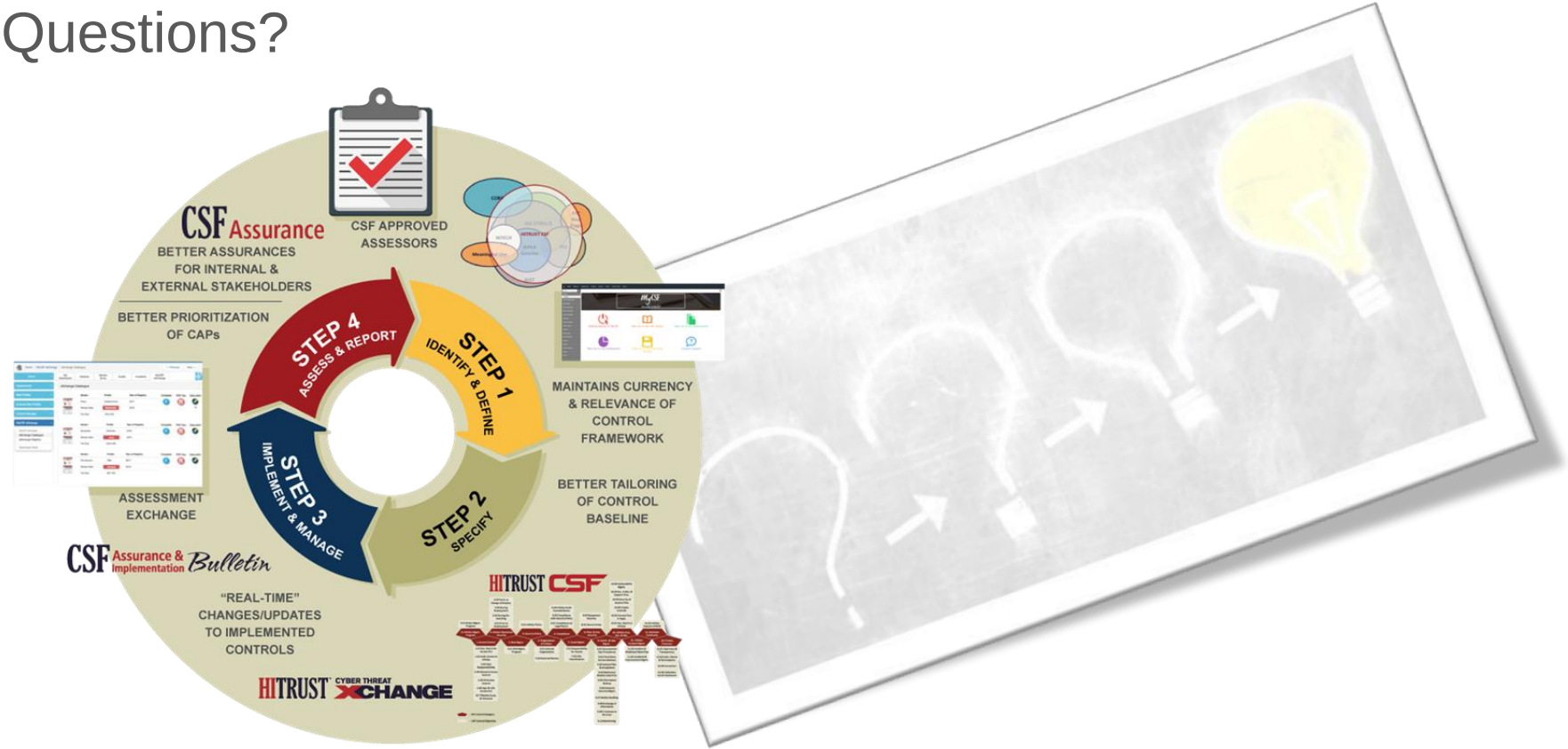
Takeaways

There are two commonly used approaches to the HIPAA risk analysis requirement

- Traditional risk analysis
  - **Difficult to perform** comprehensively/correctly … must start from a 0% solution
  - Provides a custom set of information security controls **IF** performed correctly
  - No additional tailoring of the controls required
- Framework-based risk analysis
  - Comprehensive & **very easy to perform** … leads to an "80%" solution set "out-of-the-box"
  - Provides a semi-custom set of information security controls **IF** applied correctly
  - **Requires some additional tailoring of the controls**


Questions & Additional Resources

Questions?



Additional Resources

Selecting a Healthcare Information Security Risk Management Framework in a Cyber World

An explanation by Health Care Services Corporation CISO Ray Biondo and Children's Health Dallas CIO Pamela Aurora of the criteria they used to evaluate major information protection standards and frameworks like ISO, NIST and HITRUST™ and their rationale for selecting the HITRUST™ risk management framework as the basis for their information protection and cybersecurity program.
https://hitrustalliance.net/content/uploads/2016/01/HCSC_Childrens_Health_Selecting_Healthcare_Information_Security_RMF_in_a_Cyber_World.pdf

Leveraging a Control-Based Framework to Simplify the Risk Analysis Process

This paper discusses HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.
https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf

Healthcare Sector Cybersecurity Framework Implementation Guide

Produced by the Joint Healthcare and Private Health (HPH) Cybersecurity WG under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC), this guide provides an explanation of how healthcare organizations can leverage a control framework-based approach to information security and privacy like the HITRUST CSF™ to implement the objectives outlined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, or Cybersecurity Framework (CsF).
https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

Appendix A – Additional Definitions

Additional Definitions

- [Security] Control – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an organization and/or information system(s) to protect information confidentiality, integrity, and availability. [NISTIR 7298 r2, adapted]

- Impact – The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NISTIR 7298 r2]

- Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [NISTIR 7298 r2]

- Overlay – A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. [NIST SP 800-53 r4]

Additional Definitions

- Risk Factor – A characteristic in a risk model used as an input for determining the level of risk in a risk assessment. [HITRUST]

- Risk Management Framework – A common taxonomy and standard set of processes, procedures, activities, and tools that support the identification, assessment, response, control and reporting of risk. [HITRUST]

- Risk Mitigation – Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/ countermeasures recommended from the risk management process. A subset of Risk Response. [NISTIR 7298 r2]

- Risk Model – A key component of a risk assessment methodology—in addition to the assessment approach and analysis approach—that defines key terms and assessable risk factors. [NISTIR 7298 r2]

- Risk Response – Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, or other organizations. See Course of Action. Synonymous with Risk Treatment. [NISTIR 7298 r2, adapted]

Additional Definitions

- Risk Treatment – The process of selection and implementation of measures to modify risk. Synonymous with Risk Response. [ISACA Glossary of Terms]

- Tailoring – The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation. [NISTIR 7298 r2]

- Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NISTIR 7298 r2, adapted]

- Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [NISTIR 7298 r2]