THE HITRUST CSF & CSF ASSURANCE

Why the HITRUST Risk Management Framework is the Best Approach for the Healthcare Industry

Introduction

Our Target Audience

Healthcare organizations that need an industry-accepted approach to information security risk management, which can easily integrate into their existing programs, provide an appropriate level of due diligence and due care, and satisfy their regulatory, compliance and related business requirements for the protection of sensitive health information

What We Want to Accomplish

Facilitate the ability of a healthcare organization's management or staff to make an informed decision about the approach they take to the HIPAA risk analysis and the risk management framework it adopts, and help ensure an industry acceptable level of protection against reasonably anticipated threats to sensitive health information

Topics

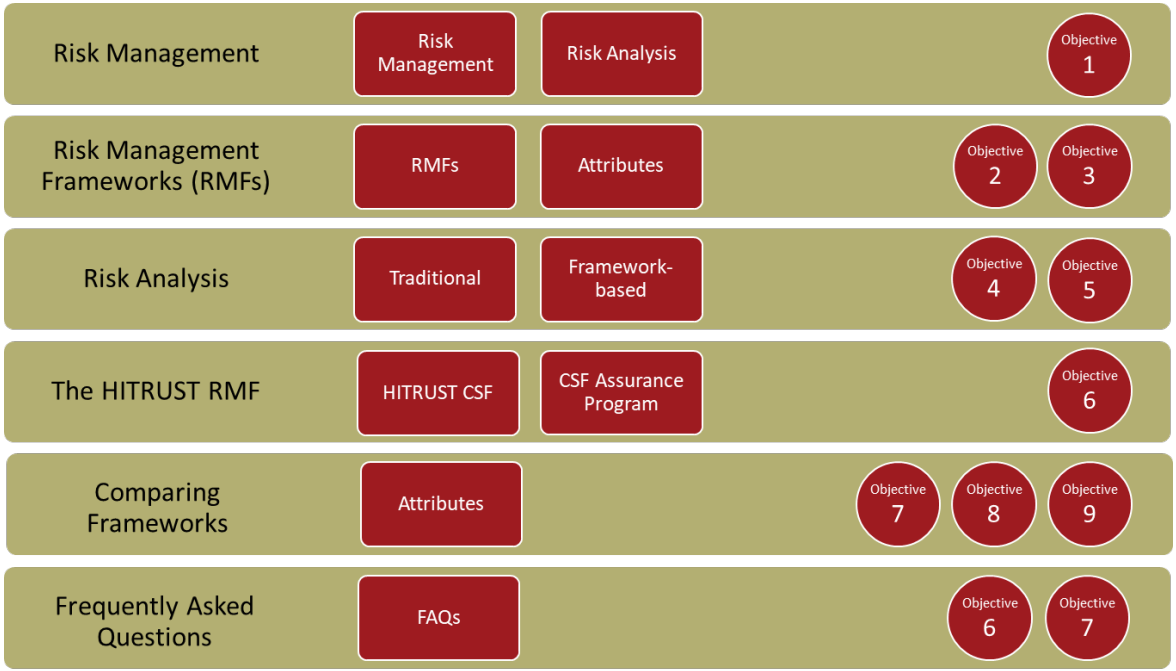
1. Overview
2. Risk Management
3. Risk Management Frameworks
4. Risk Analysis
5. The HITRUST Risk Management Framework
   - HITRUST CSF
   - The HITRUST CSF Assurance Program
6. Selecting a Framework
7. Frequently Asked Questions
8. About HITRUST

Objectives

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

1. Identify HIPAA requirements for risk management and analysis
2. Describe the risk management process
3. Discuss risk management frameworks and the attributes of a good framework
4. Describe the role of risk analysis in the risk management process
5. Compare and contrast traditional and framework-based approaches to risk analysis
6. Discuss the HITRUST approach to risk management
7. Compare and contrast HITRUST with commonly used risk management frameworks
8. Explain why controls are needed to support the NIST Cybersecurity Framework
9. Describe how the HITRUST RMF supports the NIST Cybersecurity Framework

Topical Relationship to the Objectives



HIPAA Requirements for Risk Management

§ 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.

§ 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).

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 Analysis

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

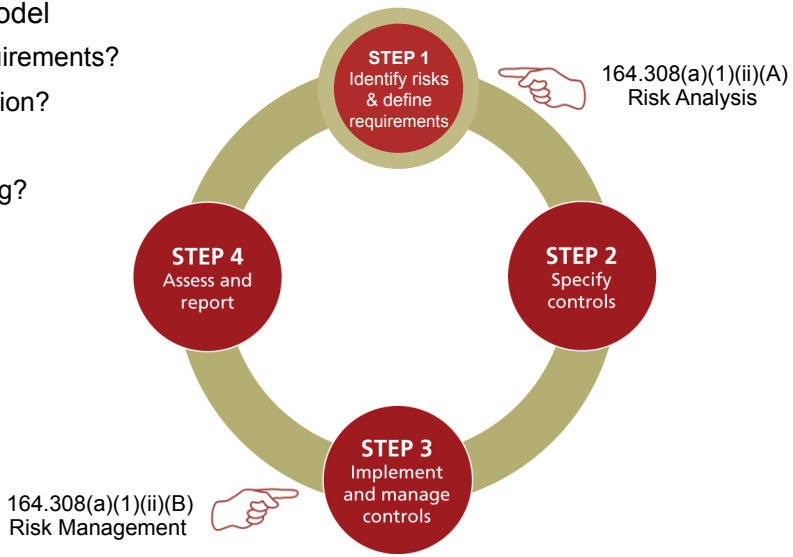
Risk Management

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.

- 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 or "life cycle" 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"



Section 3

RISK MANAGEMENT FRAMEWORKS

Risk Management Frameworks

- A risk management framework (RMF) provides an overall approach to managing information security risk throughout the information and information system life cycle and typically includes:
  - Lexicon (vocabulary) and taxonomy (classification/structure) for information security risk management
  - Methodology for evaluating and treating information security risk
- A control-based risk management framework (RMF) provides an overall approach to managing information security risk **via the design, implementation, monitoring/assessment, review and improvement of security controls** throughout the information and information system lifecycle and typically includes:
  - Lexicon (vocabulary) and taxonomy (classification/structure) for information security risk management
  - Methodology for evaluating and treating information security risk
  - **Set of security controls from which to choose/implement**
  - **Methodology for the selection and implementation of security controls**
  - **Methodology for the evaluation, review and improvement of security controls**

When referring to RMFs throughout the rest of the presentation, we refer specifically to control-based RMFs

Common Risk Management Frameworks

Examples include but are not limited to:

- The HITRUST CSF and supporting publications: used extensively by commercial entities in the healthcare industry and increasingly by non-healthcare organizations

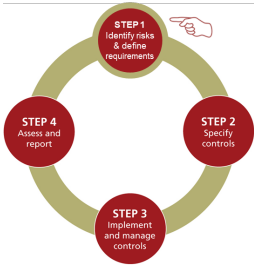
- National Institute of Standards & Technology (NIST)
  - Framework for Improving Critical Infrastructure Cybersecurity, more commonly known as the NIST Cybersecurity Framework: intended to be an overarching framework for understanding and communicating information (cyber) security in the public and private sectors
  - NIST SP 800-series publications: typically used by U.S. federal agencies to support FISMA-compliance, but also used by other governments and commercial entities

- Organization for International Standards (ISO) 27000-series publications: used by some governments and commercial entities, mostly non-U.S.

Attributes of a Good Risk Management Framework

- The framework should provide **comprehensive coverage** of general security requirements and provide **prescriptive controls** (safeguards), i.e., the control requirements should be detailed support implementation in the intended environment and adequately address the threat(s)
- The framework's controls should be **practical** for an organization to implement and maintain, and **scalable** based on the size and type of organization or information system being protected
- The controls and implementation, assessment and reporting methodologies should be vetted by organizations and industry experts such as leading professional services firms via an open and **transparent** development and update process
- The controls specified in the framework should be supported by detailed audit or assessment guidance that helps ensure **consistency** and **accuracy** in evaluation and reporting regardless of the specific assessor used
- The framework should be **efficient** and allow an organization to assess once and report many, i.e., an assessment must address multiple compliance and best practice requirements and support the reporting of assurances tailored to each requirement
- Evaluation of the framework's implementation should be **reliable**, i.e., organizations should be able to rely on the assurances provided by internal and external assessments

“Traditional” Risk Analysis



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

Step 1. Identify Risks & Define Requirements

Classify Information Assets | Inventory & Categorize Assets | Identify Threats | Assess Vulnerabilities | Determine Impact | Assess & Rank Risks | Develop Risk Strategies / Plan

STEP 2 Specify Controls

164.306(a)(1)
… All ePHI

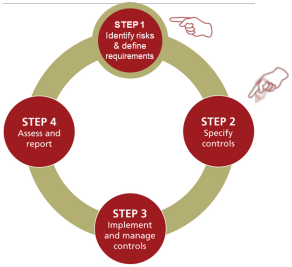
164.306(a)(1)(ii)(A)
… Potential Vulnerabilities

164.306(a)(2)
… Any Reasonably Anticipated Threats

164.306(a)(1)(ii)(A)
… Potential Risks
(Incl Threats, Vulnerabilities, Impact)

Supports
164.306(a)(1)(ii)(A)
… (Implement)
Security Measures

“Framework-based” Risk Analysis



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

Step 1. Identify Risks & Define Requirements

Classify Information Assets

Inventory & Categorize Assets

Identify Threats

Assess Vulnerabilities

Determine Impact

Assess & Rank Risks

Develop Risk Strategies / Plan

Step 2. Specify Controls

NIST Security Controls

164.306(a)(1)
… All ePHI

164.306(a)(1)(ii)(A)
… Potential Vulnerabilities

164.306(a)(2)
… Any Reasonably Anticipated Threats

164.306(a)(1)(ii)(A)
… Potential Risks

Supports 164.306(a)(1)(ii)(A)
… (Implement) Security Measures

Example is based on the NIST RMF, which provides 3 minimum security control baselines in NIST SP 800-53, which are selected based on FIPS Pub 199

Tailoring

- Once a NIST SP 800-53 control baseline is selected, it **must** be tailored* to organizational needs **before** it can be applied
- Tailoring includes but is not limited to the following:
  - Adding to or enhancing controls in the selected baseline, e.g., to address unique threats to or vulnerabilities within the organization **based on a targeted risk analysis**
  - Specifying alternative controls for those that cannot be implemented, e.g., due to technical or architectural reasons
  - Defining parameters for each control, e.g., a 5-minute screen timeout
  - Reviewing the tailored control baseline periodically to ensure risks remain adequately addressed

*See NIST SP 800-53 r4, §3.2 for more information on the tailoring process

Comparing the Approaches to Risk Analysis

Traditional Approach

Considerations:

- Must be applied to all assets where ePHI "lives"
- Must ensure a complete enumeration of anticipated threats & known vulnerabilities to design a comprehensive set of information security controls **(difficult)**
- Must be applied intelligently to specific assets or "scopes" within the organization

Takeaways:

- **Difficult to perform** comprehensively/correctly … generally results in a "20%" solution set
- Provides a custom set of information security controls IF performed correctly **(difficult)**
- No additional tailoring of the controls required

Control-based Approach

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

- 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 **(relatively easy)**
- Requires some additional tailoring of the controls

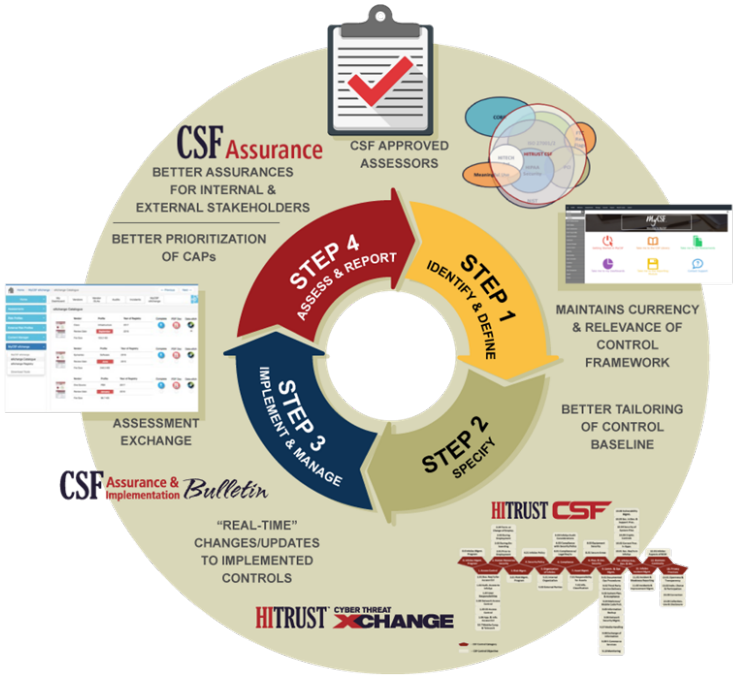
The HITRUST Risk Management Framework

Major Components

- HITRUST CSF
- CSF Assurance Program

Supported by

- CSF Assessor Program
- HITRUST Assessment Exchange
- HITRUST CTX
- HITRUST Threat Bulletins
- HITRUST De-ID Framework
- HITRUST Academy

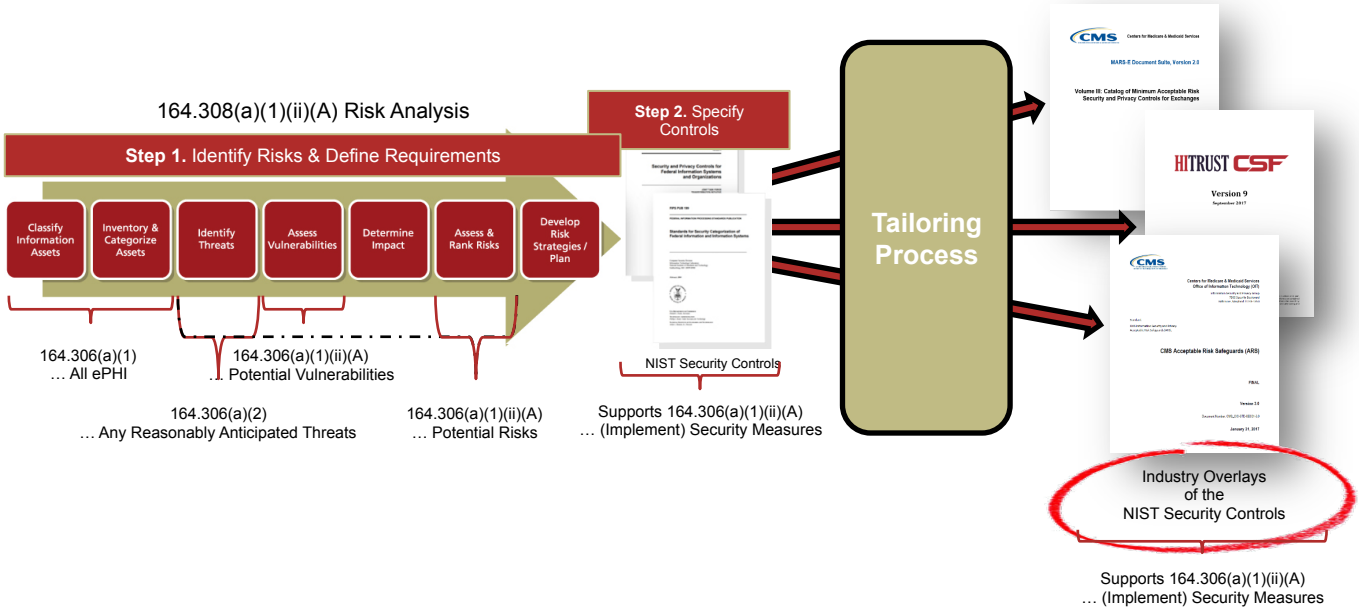


Organizational & Industry Overlays

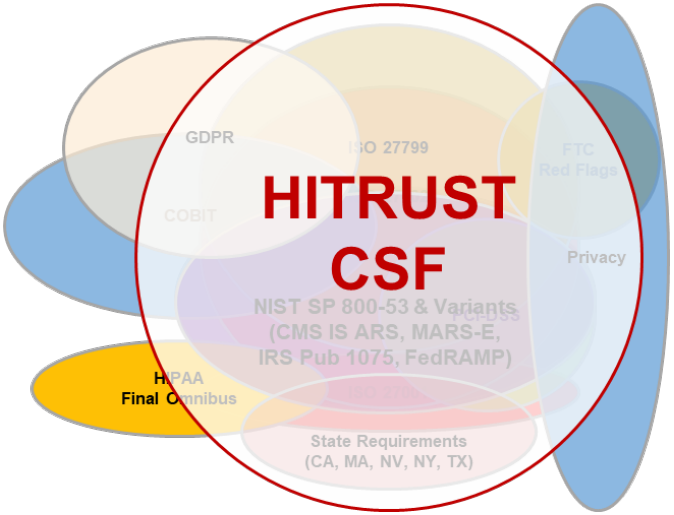
- An overlay* is a fully specified set of security controls, enhancements and supplemental guidance
  - Derived through the tailoring process
  - Intended for community-wide use
- Overlays help organizations achieve standardized security capabilities, consistency of implementation, and cost-effective 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)

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

Existing Overlays in the Healthcare Industry

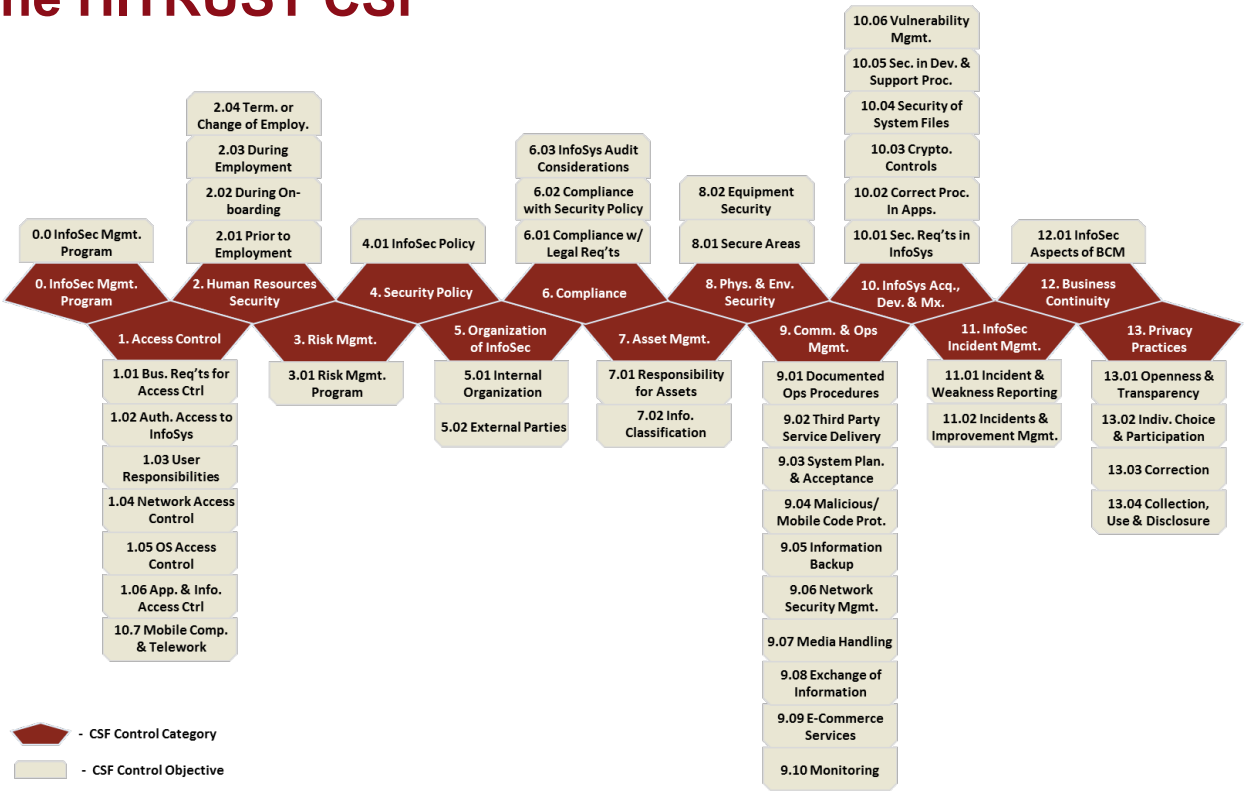


The HITRUST Approach



- A comprehensive, industry-level overlay of the NIST RMF
  - Structured on ISO/27001
  - Built on NIST SP 800-53
  - Integrates many other relevant sources
- Designed by healthcare and security professionals to address:
  - Risk Management Requirements
  - Security Requirements
  - Compliance Needs
- Provides the requirements and practices necessary to help ensure information and cybersecurity-related risks are managed smartly and consistent with business, risk and compliance objectives

The HITRUST CSF

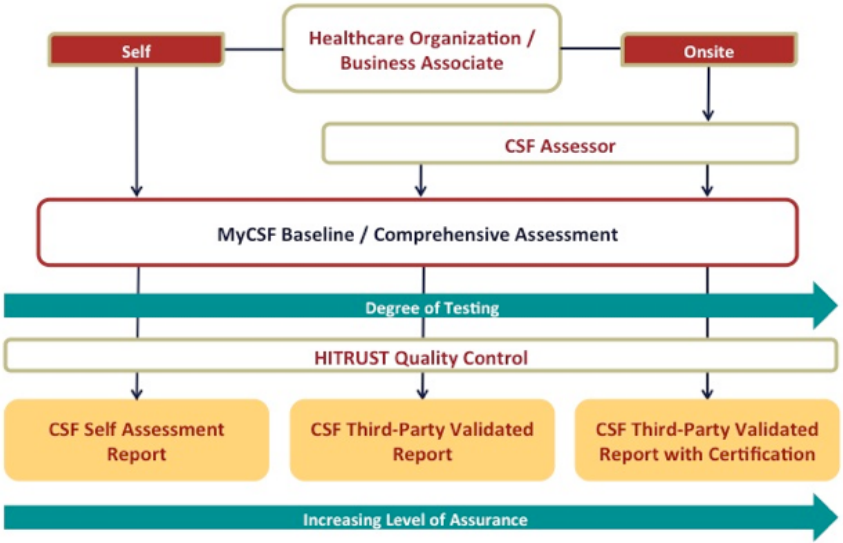


Section 5.2

THE HITRUST CSF ASSURANCE PROGRAM

The HITRUST CSF Assurance Program

The HITRUST CSF Assurance Program leverages the CSF for a common set of requirements and a standardized assessment and reporting process to improve efficiency and lower costs



Third Party Assurance

The oversight and governance provided by HITRUST supports a process whereby organizations can trust that their third parties have essential security and privacy controls in place and can understand their effectiveness

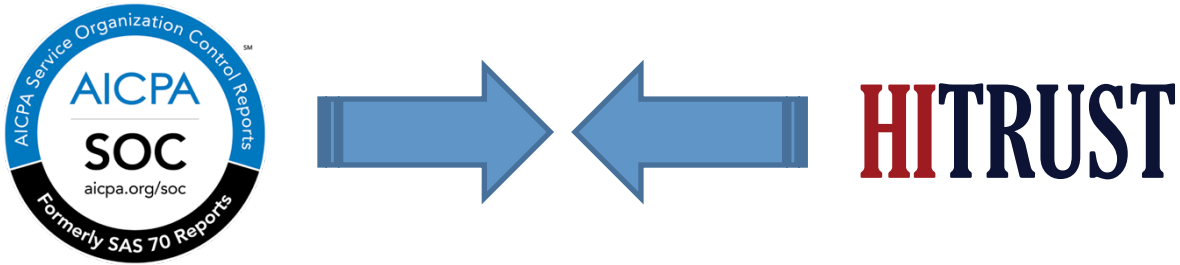
One Assessment, Three Options/Views

- In addition to the ability to obtain a SOC 2 report if assessed by a CPA firm, assessments used for HITRUST CSF certification also provide a:
  - NIST Cybersecurity Framework Scorecard, and
  - NIST Cybersecurity Framework Certification (if scoring requirements are met)
- A NIST Cybersecurity Framework Scorecard provides:
  - Compliance ratings for each NIST CsF Core Subcategory
  - Approximate NIST CsF Tiers by Core Subcategory, Category and Function
  - Consistent reporting across all critical infrastructure industries

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

HITRUST CSF Assurance and the AICPA SOC 2

- Leverage the HITRUST CSF controls in SOC 2 engagements
- Realize significant time efficiencies and cost savings by synergies between the CSF controls and Trust Services Principles and Criteria
- Reduce the inefficiencies and costs associated with multiple reporting requirements
- Consider a service organization's controls both from the SOC 2 criteria and HITRUST CSF
- Provide additional details to customers around how a service organization is addressing internal control



HITRUST/AICPA Reporting Options

Consideration	HITRUST CSF Report	SOC 2 Report with HITRUST CSF	SOC 2 + HITRUST CSF Report
Type of report (Relevant Standard)	CSF Assurance	AT101	AT101 + CSF Assurance
Scope of report	CSF controls (may or may not be limited to those required for certification)	Security, availability, confidentiality Trust Services Principles; CSF controls (may or may not be limited to those required for certification)	Security, availability, confidentiality Trust Services Principles; CSF controls (may or may not be limited to those required for certification)
Intended Users	Unlimited distribution	Limited distribution	Limited distribution
Resulting Deliverable	HITRUST CSF report with background, mgmt. rep., scope, results of maturity scores, CAPs, **NIST CsF scorecard/certification**	Attest Opinion with description of systems & service auditor test/ results against selected Trust Services Principles; HITRUST CSF controls (suitable criteria)	Attest Opinion with description of systems & service auditor test/ results against selected Trust Services Principles, HITRUST CSF controls (suitable criteria); HITRUST CSF report with background, mgmt. rep., scope, scores, CAPs, **NIST CsF scorecard/certification**
Report issued by	HITRUST	Independent CPA firms	Independent CPA firms, HITRUST
Report Addresses	HITRUST CSF, **NIST CsF**	HITRUST CSF, AICPA Trust Services Principles	HITRUST CSF, AICPA Trust Services Principles, **NIST CsF**

Attributes of a Good Risk Management Framework

- The framework should provide **comprehensive coverage** of general security requirements and provide **prescriptive controls** (safeguards), i.e., the control requirements should be detailed support implementation in the intended environment and adequately address the threat(s)
- The framework's controls should be **practical** for an organization to implement and maintain, and **scalable** based on the size and type of organization or information system being protected
- The controls and implementation, assessment and reporting methodologies should be vetted by organizations and industry experts such as leading professional services firms via an open and **transparent** development and update process
- The controls specified in the framework should be supported by detailed audit or assessment guidance that helps ensure **consistency** and **accuracy** in evaluation and reporting regardless of the specific assessor used
- The framework should be **efficient** and allow an organization to assess once and report many, i.e., an assessment must address multiple compliance and best practice requirements and support the reporting of assurances tailored to each requirement
- Evaluation of the framework's implementation should be **reliable**, i.e., organizations should be able to rely on the assurances provided by internal and external assessments

Transparency

The approach should be open and transparent

Requirements are agnostic for similar types of sensitive information

- Integrates relevant federal control baselines
- Incorporates industry leading practices
- Leverages threat-to-control relationships*

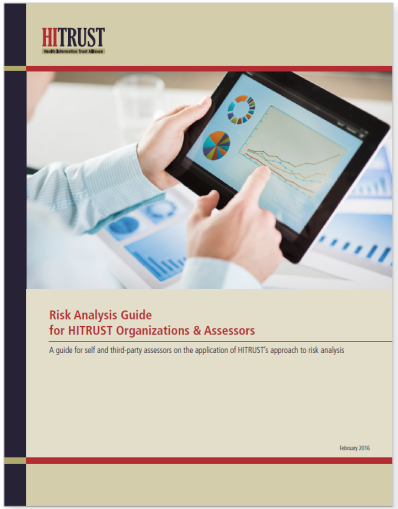
Entire program is publicly available and commonly understandable

- Control framework / requirements
- Assessment methodology / procedures
- Scoring model

**Leveraging HITRUST Threat Catalogue*

Accuracy

The approach should ensure accuracy in evaluation and reporting of the implemented controls



HITRUST uses a 5x5 control maturity and scoring model to evaluate the CSF's control requirements

- 5 maturity levels for each control requirement
- 5 scoring levels for each control maturity level

HITRUST also provides a scoring rubric for each maturity level

Consistency

The approach should ensure consistency in evaluation and reporting regardless of the specific assessor used

Extensive assessment guidance

- General guidance for each maturity level
- Specific guidance for each control

HITRUST quality assurance review process

- Applies to all 3rd Party assessments

Standardized reporting format

Scalability

The approach should be scalable enough to address the needs of the entire industry, while maintaining consistency and accuracy.

Formal CSF Assessor Program

- CSF trained staff
- Experience/capabilities vetted by HITRUST

Choose from a pool of certified CSF Assessors to ensure

- The best fit
- The best price

Program is market-based

- As demand for assurances increase, so does the pool of CSF Assessor organizations

Efficiency

The approach should allow an organization to assess once and report many, i.e., an assessment must address multiple compliance and best practice requirements and support the reporting of assurances tailored to each requirement.

HITRUST fully leverages the 'Assess Once, Report Many' approach

- Multiple security requirements (e.g., legal, regulatory)
- One cybersecurity program
- One targeted, cost-effective assessment that provides a reasonable level of assurance at a reasonable cost
- Multiple reporting options from a single assessment

Reliability

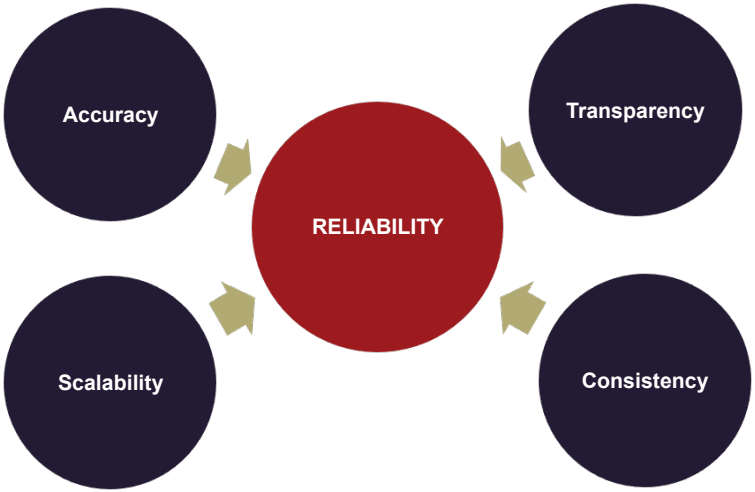
The approach should provide a high degree of assurance for relying parties, such as internal stakeholders (e.g., audit, management, Board of Directors) and external stakeholders (e.g., customers, business partners, vendors, and regulators).

Obtained through:

- Transparency
- Accuracy
- Consistency
- Scalability

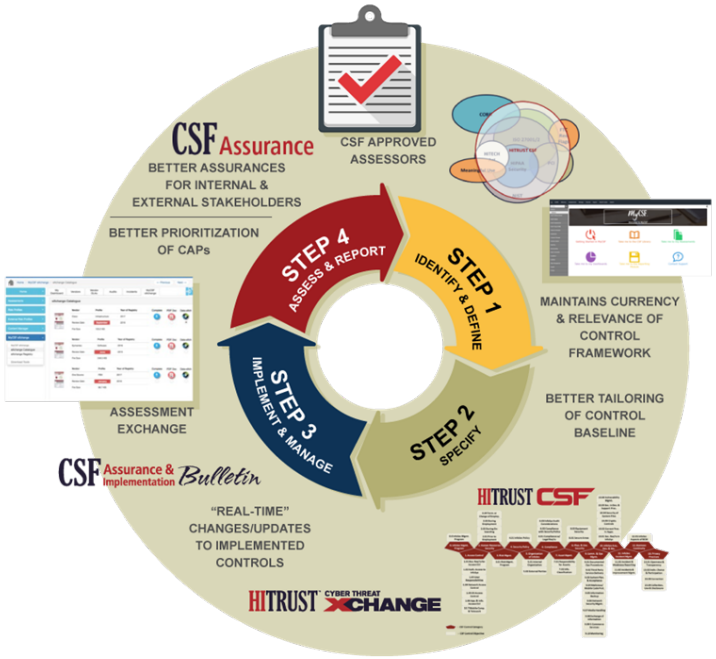
Provided by:

- HITRUST CSF
- CSF Assurance Program
- CSF Assessor Program



The Value of the HITRUST RMF

- Comprehensive Coverage
- Prescriptive Controls
- Practical Controls
- Scalable Implementation
- Transparent Update Processes
- Transparent Evaluation & Scoring Methodology
- Consistent Results
- Accurate Results
- Efficient Assessment (“Assess Once, Report Many”)
- Reliable Results (“Rely-ability”)
- Certifiable for implementing entities



The NIST Cybersecurity Framework + HITRUST

It's not a choice between the HITRUST CSF and NIST Cybersecurity Framework: you need both! The HITRUST CSF provides the foundation needed to implement the NIST framework.

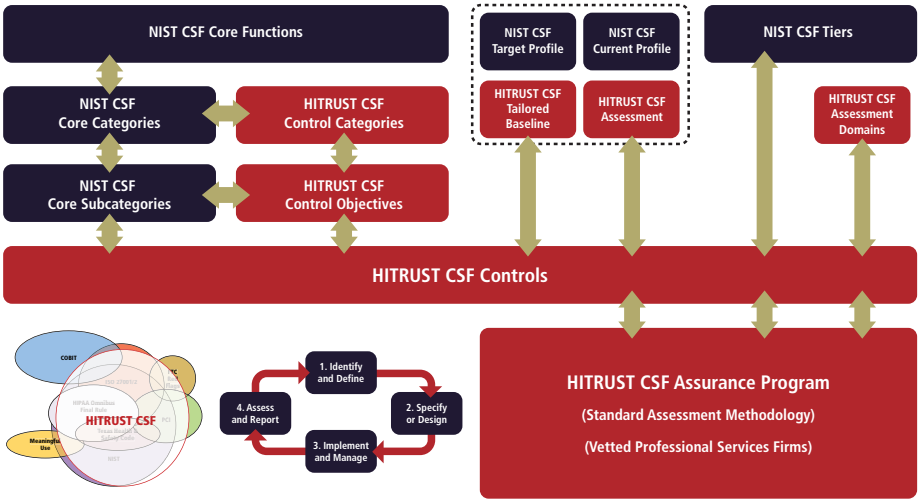
The NIST CSF lacks prescription in:

- Requirements
- Assessment methodology

Subsequently lacks:

- Transparency
- Accuracy
- Consistency
- Efficiency
- Reliability

Healthcare Sector Implementation of the NIST Cybersecurity Framework (CsF)



Comparing HITRUST with Other Approaches

The HITRUST RMF integrates and harmonizes multiple other RMFs (e.g., NIST and ISO), maximizing their strengths and minimizing their weaknesses. And the resulting ability to use the HITRUST CSF for a single information protection program that can be used to report against widely used regulations, standards and best practice frameworks, makes the HITRUST RMF the best choice for the healthcare industry.

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

Isn't the HITRUST CSF only for healthcare?

- The HITRUST CSF provides coverage across multiple regulations and includes significant components from other well-respected IT security standards bodies and governance sources.
- It is scalable, risk based, industry agnostic and certifiable

Legislative, Regulatory, and 'Best Practice" Standards and Frameworks include, but are not limited to:

ISO/IEC 27001:2005 2013, 27002:2005, 2013, 27799:2008
CFR Part 11
COBIT 4.1
NIST SP 800-53 Revision 4
NIST Cybersecurity Framework (CsF)
DHS Cyber Resilience Review

NIST SP 800-66 Revision 1
PCI DSS version 3
FTC Red Flags Rule
FFIEC IT InfoSec Examination
201 CMR 17.00 (State of Mass.)
NRS 603A (State of Nev.)

CSA Cloud Controls Matrix version 3.1
CIS CSC version 6 (SANS Top 20)
CMS IS ARS version 2
MARS-E version 2
IRS Pub 1075 v2014
FedRAMP, NY & GDPR

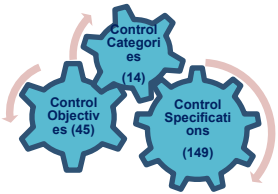
Analyzed, Rationalized & Consolidated

Scoping Factors

Regulatory
- Federal, state and domain specific compliance requirements

Organization
- Geographic factors
- Number of records processed or held

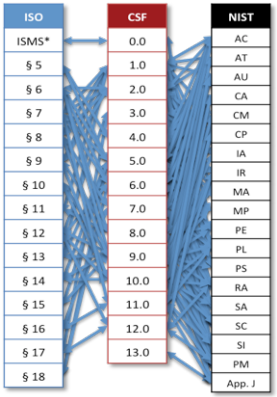
System
- Data stores
- External connections
- Number of users/transactions



Control Categories

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Info. Systems Acquisition, Development & Maintenance
11. Information Security Incident Management
12. Business Continuity Management
13. Privacy Practices

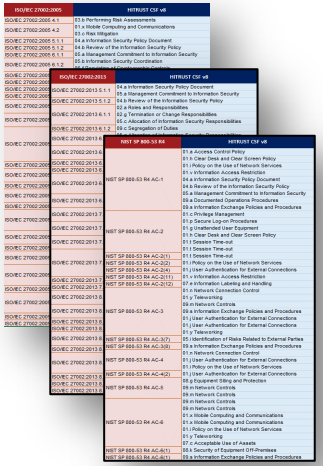
Do I have to redo my security program?



The HITRUST CSF covers 100% of the:

- ISO 27002-2005 controls (mapping is trivial, as the HITRUST CSF is built on ISO 27001-2005)
- ISO 27002-2013 controls (depicted on the left)
- NIST SP 800-53 r4 controls, moderate-level baseline (depicted on the left)

To simplify the process of aligning from a standard like ISO or NIST to the HITRUST CSF, HITRUST provides a *HITRUST CSF Standards & Regulations Cross-Reference* (X-Ref) spreadsheet with detailed mappings (depicted by the examples on the right)



*HITRUST CSF control category 0.0 addresses the original ISMS requirements in Section 4 of ISO 27001:2005

Why can't I just do a SOC 2?

HITRUST CSF meets AICPA SOC 2 reporting requirements for suitable criteria

- Realize significant time efficiencies and cost savings
- Reduce inefficiencies/costs associated with multiple reporting requirements
- Provide additional detail around how an organization is addressing internal control

Lack of uniform 'acceptable controls criteria' results in a reduction of the following when viewed across multiple entities:

- Transparency
- Accuracy
- Consistency
- Reliability

SOC 2® HITRUST CSF Version 8	Organization and Management			
	CC1.1	CC1.2	CC1.3	CC1.4
	Organizational Structure	Policy Responsibility and Accountability	Capability and Capacity of Personnel	Integrity of Personnel
03.b Performing Risk Assessments*				
03.c Risk Mitigation*				
03.d Risk Evaluation				
04.a Information Security Policy Document*		X		
04.b Review of the InfoSec Policy*				
05.a Management Commitment to InfoSec*	X	X	X	
05.b InfoSec Coordination*	X			
05.c Allocation of InfoSec Responsibilities	X	X		
05.d Authorization Process for Info Assets and Facilities				
05.e Confidentiality Agreements				

What does ‘acceptable controls criteria’ mean?

- The SOC 2 guide and Appendix C of TSP section 100 require an organization to establish controls that meet all applicable trust services criteria
- The control objectives must align with the applicable trust services criteria, and the controls must address all of the applicable trust services criteria
- AICPA requirements for suitable criteria
  - Objectivity
  - Measurability
  - Completeness
  - Relevance

SOC 2® HITRUST CSF Version 8	Organization and Management			
	CC1.1	CC1.2	CC1.3	CC1.4
	Organizational Structure	Policy Responsibility and Accountability	Capability and Capacity of Personnel	Integrity of Personnel
03.b Performing Risk Assessments*				
03.c Risk Mitigation*				
03.d Risk Evaluation				
04.a Information Security Policy Document*		X		
04.b Review of the InfoSec Policy*				
05.a Management Commitment to InfoSec*	X	X	X	
05.b InfoSec Coordination*	X			
05.c Allocation of InfoSec Responsibilities	X	X		
05.d Authorization Process for Info Assets and Facilities				
05.e Confidentiality Agreements				

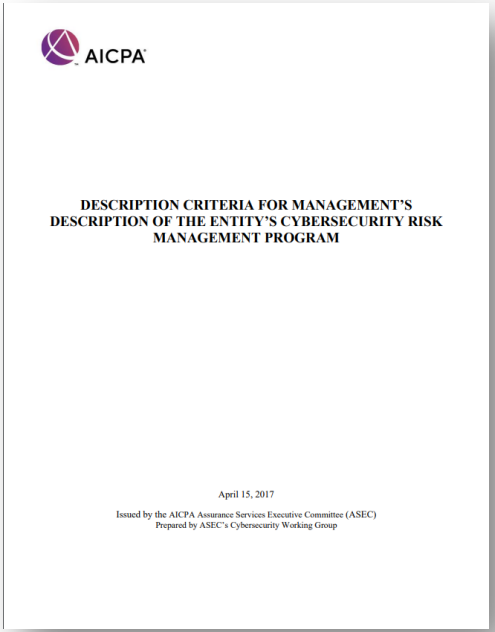
Why can't I just do an AICPA Cyber Exam?

AICPA Cyber Examination consists of two major components:

- A description of an entity's program based on new description criteria
- An assessment of control effectiveness based on its control criteria

As with the AICPA Trust Services Principles, additional information (specificity) is needed to address the criteria, and the Cyber Examination would result in a reduction of the following when viewed across multiple entities:

- Transparency
- Accuracy
- Consistency
- Reliability



How do I benefit from a HITRUST Assessment?

- **Redundant, inconsistent assessments result in lost productivity, additional costs**
- **A more efficient, streamlined approach benefits the Customer and Vendor**
- **Recommended approach leverages:**
  - A single controls framework for context
  - A strong assessment methodology that provides high assurance and consistency
  - A single assessment to provide efficient reporting
    - **HITRUST CSF** – control maturity scoring
    - **SOC 2** – HITRUST CSF provides SOC 2 the necessary prescriptiveness and transparency for availability, confidentiality and security criteria
    - **NIST Cybersecurity Framework** – HITRUST CSF provides basis for consistency, HITRUST CSF Assurance enables transparency and assurance, and scorecard enables reporting on NIST CsF Core Subcategories

How do I know what was in place and tested?

HITRUST CSF Validated and Certified Report

- Letter of Certification
- Representation Letter
- Assessment Context
- Assessment Scope
- Security Program Analysis
- Assessment Results
- Overall Security Program Summary
- Breakdown of Controls Required for Certification
- Testing Summary
- Corrective Action Plan
- Questionnaire Results (Detailed)
- System Profile

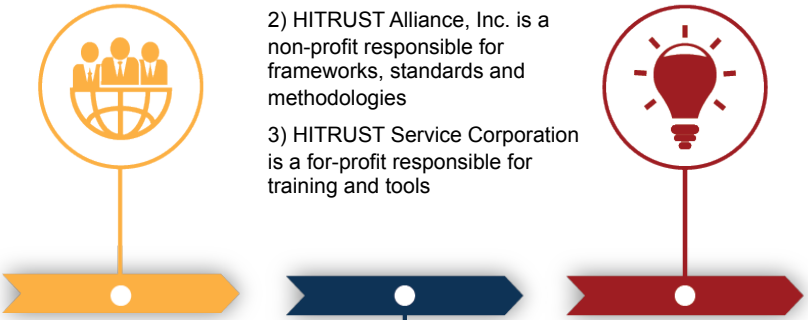
HITRUST 2018 Snapshot

Background

1) Founded in 2007

2) HITRUST Alliance, Inc. is a non-profit responsible for frameworks, standards and methodologies

3) HITRUST Service Corporation is a for-profit responsible for training and tools



Adoption

1) HITRUST CSF is utilized by 81% of US hospitals and health systems and 83% of US health plans

2) HITRUST CSF is the most widely adopted control framework in the healthcare industry, according to a 2018 HIMSS survey

3) HITRUST CSF Assurance program is the most widely adopted program for assessing third party risk

Best Known for

1) Developing the HITRUST CSF – 9th major release

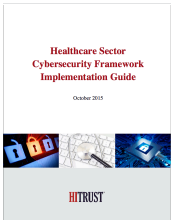
- Development guided by a CSF Advisory Council comprised of AHA, AMA, AHIP, AGMA and other security/ privacy experts
- Basis for the health and public sector implementation guidance for the NIST Cybersecurity framework, recognized by Department of Homeland Security (link) and Department of Health and Human Services (link)
- Deemed an acceptable controls by the AICPA for a SOC 2 examination
- Identified as an appropriate standard to safeguard Internet of Things (IoT) by NIST (link)

2) Operating the healthcare industry's Information Sharing and Analysis Organization (ISAO)

The HITRUST CSF and CSF Assurance

- **Comprehensive & prescriptive** – The HITRUST CSF provides an overlay of NIST's moderate-impact control baseline, tailored for the healthcare industry, that can also be used as the basis for an entity's implementation of the NIST Cybersecurity Framework
- **Practical & scalable** – The HITRUST CSF provides a custom set of security controls that can be further tailored to fit an organization's unique threat/risk environment
- **Open & transparent** – The HITRUST CSF incorporates multiple open standards and best practices, and is updated annually through an open and transparent process
- **Consistent & accurate** – HITRUST CSF assessments are supported by vetted, qualified assessors and are based upon detailed evaluation and scoring criteria to ensure consistency & accuracy of the results, regardless of the assessor used
- **Efficient** – The HITRUST CSF assurance methodology supports an 'Assess Once, Report Many' approach through a targeted, cost-effective assessment that provides a reasonable level of assurance with multiple reporting options at a reasonable cost
- **Reliable** – HITRUST provides "rely-ability" through transparency, accuracy, consistency and scalability of the HITRUST CSF and its supporting assurance and assessor programs

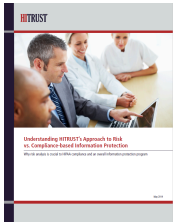
HITRUST Resources



Healthcare Sector CsF Implementation Guide

Discusses healthcare's implementation of the NIST Cybersecurity Framework based on the HITRUST CSF and CSF Assurance Program

https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf



Risk vs. Compliance-based Protection

Discusses the difference between compliance and risk-based information protection programs and shows how controls are selected based on a risk analysis, after which their implementation becomes a compliance exercise

https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf

Risk Analysis Guide

Provides a detailed discussion of HITRUST's NIST-based control implementation maturity model, HITRUST's scoring model, and additional information on risk treatments, including remediation planning for control deficiencies

https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

MyCSF vs. GRC Tools

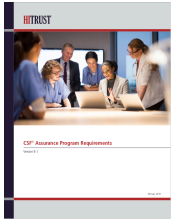
Provides a discussion of the differences between a "typical" GRC tool and MyCSF, which was primarily designed to automate HITRUST's assessment validation and certification process

https://hitrustalliance.net/documents/content/MyCSFVsGRCTool.pdf

Risk Management Frameworks Whitepaper

How HITRUST provides an efficient and effective approach to the selection, implementation, assessment and reporting of information security and privacy controls

https://hitrustalliance.net/documents/campaigns/HITRUST-RMF-Whitepaper-FM.pdf



CSF Assurance Program Requirements

Provides an overview of the CSDF Assurance Program, the various types of assessments available, and the process of obtaining and maintaining certification

https://hitrustalliance.net/documents/assurance/csf/CSFAssuranceProgramRequirements.pdf

HITRUST Blog Resources

The HITRUST CSF v9.1 Marches Forward

Discusses the incorporation of the General Data Protection Regulation (GDPR) and the New York State Cybersecurity Requirements for financial services companies into HITRUST CSF v9.1.

https://blog.hitrustalliance.net/hitrust-csf-v9-1-marches-forward/

Finding a Good Place to Start for GDPR Compliance

Discusses the General Data Protection Regulation (GDPR) and explains the challenges that organizations will face as a direct result.

https://blog.hitrustalliance.net/finding-good-place-start-gdpr-compliance/

HIPAA, HHS OCR, and HITRUST | How Do They All Fit Together?

Explains how the HITRUST CSF can help organizations build the strong HIPAA compliance program OCR is looking for when conducting an audit or investigation.

https://blog.hitrustalliance.net/hipaa-hhs-ocr-hitrust-fit-together/

Why HITRUST?

Provides the top three reasons that Premera is implementing the HITRUST framework (CSF). Written by Sean Murphy, Vice President and Chief Information Security Officer for Premera.

https://blog.hitrustalliance.net/why-hitrust/

Achieving the Benefits of the NIST Cybersecurity Framework

Provides detailed information on the relationship between the NIST CsF and the HITRUST CSF. Provides an overview of the HITRUST Assurance Program and the "assess once, report many" approach.

https://blog.hitrustalliance.net/achieving-benefits-nist-cybersecurity-framework/

HITRUST®

For more information on the HITRUST CSF and the CSF Assurance Program, visit www.HITRUSTAlliance.net

To view our latest documents, visit the Content Spotlight