HCSC
Health Care Service Corporation

children's health℠

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

July 2015

The Need For A Healthcare Information Security Risk Management Framework

Risk Management Frameworks

Given increasing regulatory pressure to ensure the adequate protection of ePHI and a dynamic cyber threat environment that is increasingly hostile to the industry, we believe it is incumbent upon all healthcare entities to adopt a formal risk management framework to ensure all reasonably anticipated threats to ePHI are formally addressed.

An information security risk management framework provides a set of principles, tools and practices to help organizations:

- Ensure people, process and technology elements completely and comprehensively address information and cybersecurity risks consistent with their business objectives, including legislative, regulatory and best practice requirements
- Identify risks from the use of information by the organization's business units and facilitate the avoidance, transfer, reduction or acceptance of risk
- Support policy definition, enforcement, measurement, monitoring and reporting for each component of the security program are adequately addressed

However, there are multiple information security risk management frameworks from which to choose, including but not limited to:

- HITRUST CSF and supporting programs, tools and methodologies
- ISO/IEC 27001, 27002 and supporting 27000-series documents
- NIST SP 800-53 r4 and supporting 800-series documents

Healthcare Framework Requirements (1)

To aid in the selection of an appropriate information security risk management framework for healthcare entities, we believe the selected framework should meet the following requirements:

- The framework should provide **comprehensive coverage** of general security requirements for the protection of ePHI specified in the HIPAA Security Rule under § 164.306(a) and § 164.308(a)(1)(ii), including best practices such as those specified in the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)
- The framework should address and **harmonize relevant business and compliance requirements**, e.g., from applicable federal and state statues and regulations, including the HIPAA Security Rule's standards and implementation specifications. Since the HIPAA Security Rule's standards and implementation specifications are generally high-level, the framework should provide **prescriptive controls** (safeguards), i.e., the control requirements should be detailed enough for a healthcare entity to understand what must be implemented in the intended environment to adequately address the threat(s)
- The framework's controls should be **practical** for a healthcare entity to implement and maintain and **scalable** based on the size and type of organization or information system being protected
- The framework should allow for the flexibility of approach specified in the HIPAA Security Rule under § 164.306(b) and support a **risk-based** rather than a compliance-based selection of a reasonable and appropriate set of controls

Healthcare Framework Requirements (2)

Requirements (continued):

- The framework should be fully **supported and maintained** by a sponsoring third-party organization to ensure its continued relevance to the healthcare industry and the threat environment
- The controls and implementation, assessment and reporting methodologies should be **vetted by healthcare organizations and industry experts** such as leading professional services firms via an **open and transparent update process**
- The controls specified in the framework should be supported by **detailed audit or assessment guidance** that helps ensure the **consistency and accuracy** in evaluation and reporting regardless of the specific assessor used
- The framework should employ an assessment approach and scoring methodology that makes the framework **certifiable for implementing organizations**, i.e., it supports the formal certification of an implementing healthcare entity against the framework's controls
- The framework should allow an organization to **assess once and report many**, i.e., an assessment must address multiple compliance and best practice requirements (e.g., the HIPAA Security Rule and NIST) and support the reporting of assurances tailored to each requirement
- The framework should provide robust support for **third party assurance** using common, standardized assessment and reporting processes that can be tailored to the specific requirements of the requesting organization

HCSC children's health

Selecting Candidate Risk Management Frameworks for Detailed Analysis

Candidate Frameworks

Including consideration of the HIPAA Security Rule, there are six (6) generally recognized and accepted frameworks that can be considered reasonable candidates from which to build an organization-level information security risk management program:

- **COBIT:** Provides a set of recommended best practices for governance and control processes for information systems and technology, one aspect of which is the control of information system and technology risk
- **HIPAA:** Although issued as a regulation, the HIPAA Security Rule provides a series of security standards and implementation specifications, including the requirements for organizations to conduct a risk analysis and protect against all reasonably anticipated threats
- **HITRUST:** Formed specifically to support the healthcare industry, the HITRUST risk management framework is detailed in the HITRUST CSF, CSF Assurance Program and supported by multiple documents (e.g., the HITRUST Risk Analysis Guide) and tools (e.g., MyCSF)
- **ISO:** International in scope, ISO/IEC 27001 and 27002 provide a comprehensive if high-level baseline set of controls that can be implemented by any type of organization; supporting 27000-series publications provide the rest of the information security risk management framework, and healthcare specific considerations are specifically addressed in ISO/IEC 27799
- **NIST:** Although intended for federal agencies, the NIST SP 800-53 controls and supporting 800-series publications provides a comprehensive and detailed information security risk management framework and three control baselines that can be applied to low, moderate and high impact/sensitive information; healthcare specific considerations are also addressed in NIST SP 800-66
- **PCI:** Although intended for payment card information, the PCI DSS framework is comprehensive enough in scope to provide a reasonable baseline for the protection of any type of sensitive information

HCSC children's health

“Down-selecting” Candidate Frameworks

The following table provides an initial comparison of the six (6) candidate frameworks based on the specified requirements:

Requirement	CSF	COBIT	PCI DSS	ISO	NIST	HIPAA
Comprehensive coverage	Yes	Yes	Yes	Yes	Yes	Partial
Harmonizes relevant business and compliance requirements	Yes	No	No	No	No	No
Prescriptive controls	Yes	Yes	Yes	Partial	Yes	No
Practical and scalable controls	Yes	Yes	No	No	No	Yes
Risk-based rather than compliance-based	Yes	Yes	Partial	Yes	Yes	Partial
Supported and maintained by a third party	Yes	Yes	Yes	Yes	Yes	No
Vetted by healthcare and industry experts	Yes	No	No	Yes**	Yes**	No
Open and transparent update process	Yes	No	Yes	Yes	Yes	Yes
Detailed audit or assessment guidance	Yes	Yes	Yes	Yes	Yes	No
Consistency and accuracy in evaluation	Yes	Partial	Partial	Partial	Yes	No
Certifiable for implementing organizations	Yes	Yes	Yes	Yes	Partial*	No
Assess once and report many	Yes	No	No	Partial***	Partial***	No
Support for third-party assurance	Yes	Yes	Yes	Yes	Partial*	No

*NIST controls are typically certified by a specific information system or type of system rather than at the organizational-level

** ISO 27799 and NIST SP 800-66 both subject to comment period prior to release

*** ISO and NIST are considered “benchmark” frameworks by which many other frameworks are measured and often mapped

Based on the results outlined in the table, more detailed analysis can be limited to three candidate frameworks: CSF, ISO and NIST

HCSC children's health

Detailed Analysis of Candidate Risk Management Frameworks

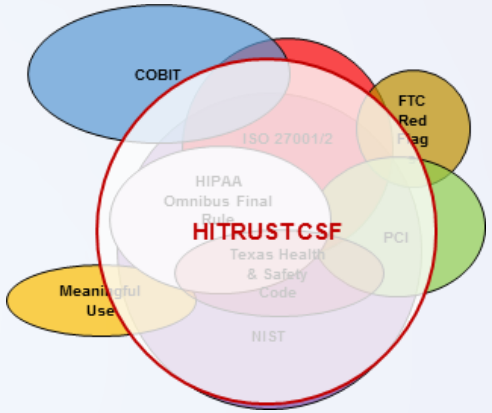
Comprehensive Coverage

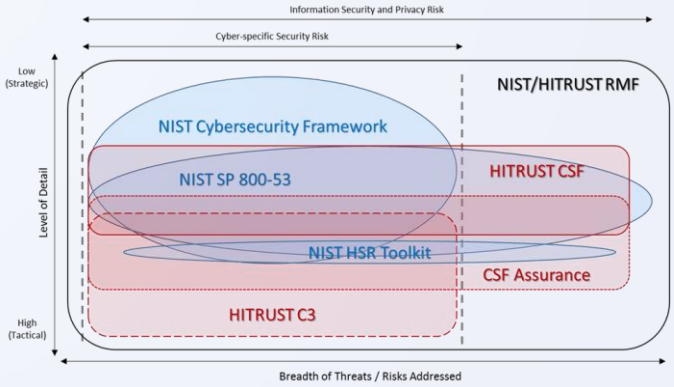
The framework should provide comprehensive coverage of general security requirements for the protection of ePHI specified in the HIPAA Security Rule under § 164.306(a) and § 164.308(a)(1)(ii), including best practices such as those specified in the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).

NIST SP 800-53 controls were designed specifically for U.S. government agencies, but NIST SP 800-53, as well as ISO/ IEC 27001, also provides information security standards that are applicable to a very broad scope of environments and organizations. And while neither ISO nor NIST address the specific needs of any single industry, they do discuss the application of their frameworks in a healthcare setting in separate documents: ISO/IEC 27799 and NIST SP 800-66.

The HITRUST CSF, on the other hand, provides an integrated set of comprehensive security safeguards derived from multiple regulatory requirements applicable to U.S. healthcare , such as the HIPAA Omnibus Security, Data Breach Notification and Privacy Rules, as well as generally accepted information security standards and best practices, including ISO/IEC 27001 and NIST SP 800-53.

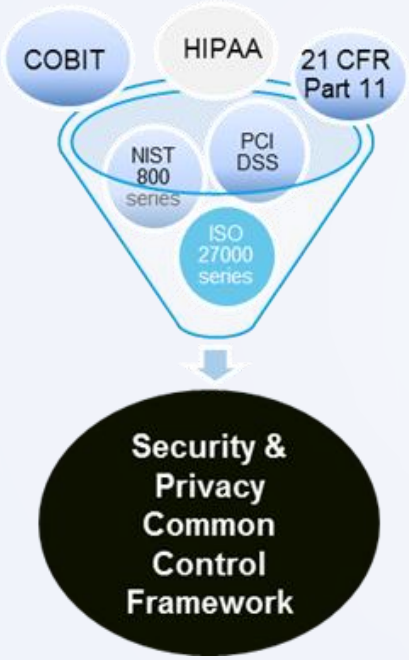
HITRUST provides a healthcare-specific implementation of the NIST Cybersecurity Framework and either meets or exceeds its guidelines for the NIST Framework Core, NIST Framework Profiles, and NIST Framework Implementation Tiers. The complete HITRUST risk management also addresses non-cyber threats to ePHI and incorporates a robust assurance program, also recommended by the NIST Cybersecurity Framework.





Harmonizes Relevant Requirements

The framework should address and harmonize relevant business and compliance requirements, e.g., from applicable federal and state statues and regulations, including the HIPAA Security Rule's standards and implementation specifications.



The HITRUST framework is based on the ISO/ IEC 27001 control clauses to support the implementation and assessment of information security and compliance risk for offshore business associates, and NIST requirements relevant to healthcare information protection are fully integrated into the CSF. Relevant requirements from other authoritative sources such as the HIPAA Security, Data Breach Notification and Privacy Rules, COBIT, NIST SP 800-63, NIST SP 800-66, ISO/IEC 27799 and PCI DSS are also fully integrated into the 3 implementation levels contained in the CSF.

Requirements that may be specific to an information type (e.g., payment card data or federal tax information) or to an organization type (e.g., a CMS contractor or Health Information Exchange) are segregated into "industry segments" and can be made available as needed. In this way healthcare organizations can use a single control framework, the CSF, as the basis for their entire information security program.

Prescriptive Controls

Since the HIPAA Security Rule's standards and implementation specifications are generally high-level, the framework should provide controls (safeguards) that are prescriptive, i.e., they should be detailed enough for a healthcare entity to understand what must be implemented in the intended environment to adequately address the threat(s).

HIPAA's Security Rule provides numerous standards implementation specifications that essentially require covered entities to implement reasonable and appropriate administrative, technical and physical safeguards for ePHI. Unfortunately, HIPAA lacks the level of prescriptiveness necessary to determine a standard of due care or diligence, i.e., what safeguards would be considered "reasonable and appropriate," or ensure the consistent application of these safeguards.

Although ISO controls are also relatively high-level and lack the prescription contained in the NIST framework, the HITRUST CSF integrates all relevant ISO and NIST controls along with additional requirements from relative authoritative sources like the NIST Cybersecurity Framework, CSA CCM, COBIT, PCI DSS, CMS IS ARS, MARS-E and IRS Pub 1075.

Practical and Scalable Controls

The framework's controls should be practical for a healthcare entity to implement and maintain and scalable based on the size and type of organization or information system being protected.

ISO/IEC 27001 provides high-level requirements that may be liberally tailored by an implementing organization. NIST provides more prescriptive controls and generally limits tailoring to the definition of certain control parameters. Although NIST encourages adding controls to address additional threats or mitigate more risk, NIST discourages removing or relaxing control requirements once a baseline has been selected. There is simply no formal mechanism by which the controls can be scaled to the size or type of organization implementing the NIST framework. Subsequently all the requirements contained in a specific NIST baseline may not always be appropriate to a non-governmental entity.

HITRUST addresses the practicality and scaling of CSF controls by tailoring the complete set of CSF control requirements to the healthcare industry and then creating overlays for specific classes of healthcare organizations based on organizational, system and regulatory risk factors.

Risk-based Rather than Compliance-based

The framework should allow for the flexibility of approach specified in the HIPAA Security Rule under § 164.306(b) and support a risk-based rather than a compliance-based selection of a reasonable and appropriate set of controls.

ISO allows organizations to select or modify the controls from its single baseline quite liberally but with no real oversight over the process. NIST provides for a specific methodology for tailoring its three baselines, including the development of industry/sector or organizational overlays. However NIST also does not provide any oversight over the process.

HITRUST adopts the NIST methodology and tailors the controls in the CSF based on healthcare industry requirements, essentially creating a healthcare-specific overlay of the integrated, harmonized requirements derived from its multiple authoritative sources. HITRUST then provides for the creation of additional overlays for specific classes of healthcare entities based on defined organizational, system and regulatory risk factors.

This provides healthcare organizations with an initial control baseline that better suits the healthcare industry as well as the specific needs of the organization.

It is only after the organization completes the tailoring process that HITRUST then requires a compliance-oriented approach to the implementation, maintenance and assessment of the assigned controls. Deficiencies then determine excessive residual risk to the organization's information assets and allows the development and prioritization of corrective actions.

Supported and Maintained by a Third Party

The framework should be fully supported and maintained by a third-party organization to ensure its continued relevance to the healthcare industry and the threat environment.

HITRUST maintains the relevancy of the CSF by regularly reviewing changes in source frameworks and best practices due to changes in the regulatory or threat environment. The CSF is updated no less than annually, whereas updates to ISO/IEC 27001 and NIST SP 800-53 are made much less frequently and may not necessarily reflect new federal or state legislation and regulations (e.g., recent omnibus HIPAA rulemaking or Texas House Bill 300). The ongoing enhancements and maintenance to the CSF provide continuing value to healthcare organizations, sparing them from much of the expense of integrating and tailoring these multiple requirements and best practices into a custom framework of their own.

Vetted by Healthcare and Industry Experts

The controls and implementation, assessment and reporting methodologies should be vetted by healthcare organizations and industry experts such as leading professional services firms.

Although NIST and ISO controls are not vetted specifically by healthcare and industry experts such as professional services firms, drafts are open for a public comment period in which anyone can provide input.

The HITRUST CSF on the other hand was created by healthcare and industry experts, content from new authoritative sources is typically developed by industry working groups or based on industry and CSF Advisory Committee input, and all content for each annual release is made available to healthcare and industry experts for comment.

Open and Transparent Update Process

The controls and implementation, assessment and reporting methodologies are subject to an open and transparent update process.

All three organizations—ISO, NIST and HITRUST—release updates to their frameworks for public comment. ISO and NIST may take years to update their standards but HITRUST updates the CSF no less than annually and each release is specifically made available to healthcare and industry experts, including professional services firms, for comment. Additional sources for integration into the CSF are based on industry and CSF Advisory Committee input.

ISO and NIST both provide summaries of changes, either in the document or separately, and NIST generally provides a redlined copy of the document. HITRUST releases a detailed summary of changes with each new release that clearly indicates each addition, deletion or modification to the CSF structure or content along with the relevant authoritative source and the reason the addition, deletion or modification was made.

Recent updates:

- Release v6.1 in Apr 2014 integrated the NIST Cybersecurity Framework
- Release v7 in Jan 2015 incorporated MARS-E and HIPAA-based privacy requirements for general use (previously only available for SecureTexas certification)

Detailed Audit or Assessment Guidance

The controls specified in the framework should be supported by detailed audit or assessment guidance that helps ensure the consistency and accuracy in evaluation and reporting regardless of the specific assessor used.

By its very nature, ISO's assessment methodology is very general in order to support global applicability in a wide variety of industry segments. ISO/IEC 27005 provides some guidance for risk assessment and analysis, but does not provide or recommend a specific methodology. The NIST Risk Management Framework (RMF), on the other hand, provides very specific guidance on a multitude of topics, including the implementation, maintenance, assessment and reporting of an information security risk management program. However, with the possible exception of NIST SP 800-66 r1, guidance is specific to the federal government and in many respects too complex and rigorous for the commercial sector. HITRUST leverages the NIST RMF guidance to provide a detailed information security control assessment methodology that is consistent with NIST guidance but tailored for the healthcare industry.

NIST and HITRUST provide detailed assessment guidance for each control in their respective frameworks; the ISO framework only provides assessment guidance for the ISMS in ISO/IEC 27008, which ISMS certification bodies are not required to use. Neither ISO/IEC 27001 nor 27002, which provides additional specificity around the controls, provides control-level assessment guidance.

Consistency and Accuracy in Evaluation

The assessment and scoring methodology should ensure consistency and accuracy in evaluation and reporting regardless of the specific assessor used.

ISO provides little guidance for the assessment of its information security controls as the framework's certification focuses primarily on an organization's information security risk management system. However, both NIST and HITRUST provide detailed assessment guidance for control evaluation.

However, HITRUST goes even further by leveraging a federal maturity model specific to the evaluation of information security controls, which look at policy, procedures, implementation and continuous monitoring relevant to each control requirement. HITRUST also provides detailed assessment guidance for each level in the model, specific guidance on how to evaluate the level of compliance at each level, and a scoring rubric for each maturity level.

Further, organizations are only allowed to engage HITRUST Certified CSF Assessor organizations if they wish to receive a HITRUST validated or certified assessment report, which can be used to provide high-levels of assurance to internal and external stakeholders.

The use of rigorous, detailed assessment and scoring methodologies along with qualified third-party assessors help ensure the highest levels of consistency and accuracy in the evaluation of an organization's information security program regardless of the organization assessed or the assessor organization used to conduct the assessment.

Certifiable for Implementing Organizations

The framework should employ an assessment approach and scoring methodology that makes the framework certifiable for implementing organizations, i.e., it supports the formal certification of an implementing healthcare entity against the framework's controls.

Both HITRUST and ISO take an organizational (top-down) approach to security but, although the baseline controls were created with organizational considerations in mind, NIST takes a system (bottoms-up) approach to evaluating overall security. Thus, it's possible for HITRUST and ISO to certify organizations, which generally is not done with NIST. Federal certification and authorization programs typically certify systems for compliance with NIST or other applicable security requirements. And, by design, only HITRUST formally supports third-party certification through a common control specification, assessment and reporting framework.

ISO does not require a standard baseline set of security controls for certification, and subsequently there's a limited ability to provide related assurances. But, although organizations can tailor the CSF controls in the baseline overlay specified by their organizational, system and regulatory risk factors, all the controls in the overlay required for certification must be assessed by all organizations. Because of the detailed assessment and scoring methodologies, use of certified assessor organizations, and the quality assurance reviews required for all third-party assessments, HITRUST CSF certification provides excellent validation of the controls implemented by a healthcare organization.

Assess Once and Report Many

The framework should allow an organization to assess once and report many, i.e., an assessment must address multiple compliance and best practice requirements (e.g., the HIPAA Security Rule and NIST) and support the reporting of assurances tailored to each requirement.

Although ISO and NIST are considered benchmarks by which other frameworks are measured and subsequent are mapped to many of them, neither formally support an "assess once, report many" approach. However, the CSF Assurance program:

- Streamlines the business associate assurance process
- Utilizes the tools and methodologies of the CSF Assurance Program
- Allows healthcare organizations to efficiently and effectively assess their business partners and manage risk
- Allows assessed organizations to undergo one assessment and report to multiple entities

Many healthcare entities accept a CSF validated and certified reports for evaluating **3rd party** information protection and some require them.

CSF assessment results can also be parsed along the mappings to its authoritative sources, such as NIST, CMS, and PCI to provide "scorecards" specific to those references. The CSF can also be used as the basis for the state-recognized **SecureTexas** certification or to support converged CSF-SOC2 reporting against the **AICPA Trust Principles**.

HCSC children's health

Support for Third-party Assurance

The framework should provide robust support for third party assurance using common, standardized assessment and reporting processes that can be tailored to the specific requirements of the requesting organization.

Organizations face multiple and varied assurance requirements from a variety of parties, including increased pressure and penalties associated with HHS enforcement efforts and an inordinate level of effort on negotiation of requirements, data collection, assessment and reporting. Although assessment guidelines exist for ISO assessments, there is little oversight of ISO assessors and ISO assessments and the assessments focus on the information security risk management system rather than how well a standard set of controls are implemented. And there is no third party assurance program for the NIST framework.

The HITRUST CSF Assurance Program ensures assessments are performed by qualified professional services firms and provides quality assurance reviews for validated and certified assessments, provides a risk-based approach for selecting a subset of CSF controls for assessment and formal certification while providing adequate assurances for the entire program. The program provides a common, standardized methodology to effectively and consistently measure compliance and risk through (1) simplified information collection and reporting, (2) consistent testing procedures and scoring, and demonstrable efficiencies and cost-containment.

Recommended Risk Management Framework for Healthcare

Recommended Framework for Healthcare Entities

The HITRUST CSF is *specific* to the healthcare industry, built and maintained by the healthcare industry, and simply better for the healthcare industry.

Requirement	CSF	COBIT	PCI DSS	ISO	NIST	HIPAA
Comprehensive coverage	Yes	Yes	Yes	Yes	Yes	Partial
Harmonizes relevant business and compliance requirements	Yes	No	No	No	No	No
Prescriptive controls	Yes	Yes	Yes	Partial	Yes	No
Practical and scalable controls	Yes	Yes	No	No	No	Yes
Risk-based rather than compliance-based	Yes	Yes	Partial	Yes	Yes	Partial
Supported and maintained by a third party	Yes	Yes	Yes	Yes	Yes	No
Vetted by healthcare and industry experts	Yes	No	No	Yes**	Yes**	No
Open and transparent update process	Yes	No	Yes	Yes	Yes	Yes
Detailed audit or assessment guidance	Yes	Yes	Yes	Yes	Yes	No
Consistency and accuracy in evaluation	Yes	Partial	Partial	Partial	Yes	No
Certifiable for implementing organizations	Yes	Yes	Yes	Yes	Partial*	No
Assess once and report many	Yes	No	No	Partial***	Partial***	No
Support for third-party assurance	Yes	Yes	Yes	Yes	Partial*	No

*NIST controls are typically certified by a specific information system or type of system rather than at the organizational-level

** ISO 27799 and NIST SP 800-66 both subject to comment period prior to release

*** ISO and NIST are considered “benchmark” frameworks by which many other frameworks are measured and often mapped

HCSC children's health

What Are Some Common Questions and Misconceptions?

Common Questions and Misconceptions

Should a healthcare entity choose the HITRUST CSF, NIST Cybersecurity Framework, or the NIST 800-53 or ISO 27002 control frameworks?

With adoption of the HITRUST CSF a healthcare organization can leverage and benefit from them all

The HITRUST RMF, which consists of the CSF, CSF Assurance Program and supporting tools, methods and services, is actually a model implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) for the healthcare industry.

The HITRUST RMF provides the necessary context for a healthcare-specific implementation of the NIST Cybersecurity Framework by integrating multiple healthcare-relevant legislative, regulatory and best practice guidelines and frameworks such as the HIPAA Security Rule and NIST SP 800-series and ISO 27000-series guidance.

These integrated controls are then tailored further by allowing organizations to select a reasonable and appropriate subset of these controls based on their specific organizational, system and regulatory risk factors.

Common Questions and Misconceptions

Is the HITRUST CSF a replacement standard for HIPAA or NIST 800-53?

No, the HITRUST CSF integrates NIST SP 800-53 and other relevant information protection standards to provide the prescription necessary to fully implement the requirements specified in the HIPAA Security Rule.

Why is the HITRUST CSF needed? Why can't we use HIPAA or NIST?

As risk analysis can be difficult for many healthcare organizations, HITRUST leverages frameworks like NIST to provide a common baseline of protection against reasonably anticipated threats to ePHI. HITRUST then tailors all the controls in the CSF to provide a healthcare-specific context and support the selection of multiple framework overlays—essentially new control baselines—for a common type or class of healthcare entity based on defined organizational, system and regulatory risk factors.

Although additional tailoring by an organization is necessary, this common set of baselines supplemented by a common assessment and certification methodology provides for the standardized reporting of risk and sharing of assurances with internal and external stakeholders (e.g., management, business partners and regulators) around the efficient and effective implementation of those standards by healthcare organizations.

About HITRUST

HITRUST in a Snapshot

Best known for:

- Developing HITRUST CSF—in 7th major release
- Annual health information breach and loss analysis report
- Cyber preparedness and response exercises—CyberRX

Adoption of CSF

- By 83% of hospitals[1] (most widely adopted)
- By 82% of health plans[2] (most widely adopted)

Adoption of CSF Assurance

- Over 23,000 CSF assessments in last three years (10,000 in 2014)
- Most widely utilized approach by healthcare organizations and 3rd party risk assessments
- Supports State of Texas Privacy and Security Certification – SecureTexas

Supporting Cyber Threat Intelligence Sharing and Incident Preparedness and Response

- Operates Cyber Threat XChange (CTX) as industry cyber threat early warning system and to automate indicator of compromise distribution
- Federally recognized Information Sharing and Analysis Organization (ISAO)
- Information sharing agreement with Department of Health and Human Services (HHS)
- Information sharing agreement with the Department of Homeland Security as part of critical infrastructure program
- Partnership with HHS for monthly industry cyber threat briefings
- Partnership with HHS for industry cyber threat preparedness and response exercises – CyberRX

Information Protection Education and Training

- Over 1500 professionals obtained Certified Common Security Framework Practitioner (CCSFP) designation—CSF specific
- Partnered with International Information System Security Certification Consortium, Inc., (ISC)² to develop broader healthcare certified information security professional credential—HealthCare Information Security and Privacy Practitioner (HCISPP)
- Annual conference: In 2012 HITRUST began holding health information protection professional annual conference

1 – Based on facilities in the 2011 AHA hospital and health system data as of Dec 2012 that have licensed the CSF
2 – Based on health plans with over 500,000 members as of Dec 2012 that have licensed the CSF

HCSC children's health

HITRUST

Health Information Trust Alliance

Visit www.HITRUSTAlliance.net for more information

To view their latest documents, visit the Content Spotlight