HITRUST
Health Information Trust Alliance

Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53

Why Choosing the CSF is the Best Choice

June 2014

Introduction

Many healthcare organizations realize it is in their best interest to adopt, and possibly tailor, an existing information security framework rather than to develop and maintain a custom framework. But that's only one decision that has to be made. The next one involves choosing from several comprehensive frameworks to best suit the needs of your organization. Choices include: ISO/IEC 27001/2, NIST SP 800-53, and the HITRUST CSF. But which one best suit the specific and unique needs of the healthcare industry?

All three of the frameworks referenced are fairly comprehensive and "open" frameworks, but they differ significantly in some very important aspects, including scope, level of integration, industry specificity and applicability, prescriptiveness, scaling, tailoring, compliance, certification, shared assurance, assessment guidance and tool support.

This document provides guidance on why choosing the HITRUST CSF is the best choice for healthcare organizations.

Built for Healthcare

When developing the CSF, HITRUST recognized the global nature of healthcare and the need to gain assurances around the protection of covered information from non-U.S. business associates, which led to ISO/IEC 27001 being used as the foundation upon which the CSF controls were built. ISO/IEC 27001 provides an international standard for the implementation and maintenance of an information security management system (ISMS) with high-level controls designed to suit almost any organization, in any industry, and in any country.

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 broad scope of environments and organizations. And while neither ISO nor NIST address the specific needs of any single industry, they do both 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. (Inclusion of NIST SP 800-53 allows the CSF to help demonstrate FISMA-compliance, which is often required when organizations receive healthcare grants or contracts from the U.S. government.) The CSF provides extensive guidance on the assessment of control maturity in the healthcare environment, as well as the evaluation of excessive residual risk to support remediation planning and risk reporting. Organizations can also leverage the HITRUST CSF for Statement on Standards for Attestation Engagements (SAE16) Service Organization Controls (SOC) 2 reporting of applicable American Institute of Certified Public Accountants (AICPA) Trust Services Principles.

Comparison of HITRUST, ISO & NIST

Factor[1]	ISO/IEC 27001	NIST SP 800-53	HITRUST CSF
ISO 27001-Based	✓	✗	✓
Integrated Compliance Framework	✗	✗	✓
Healthcare Specific	✗[2]	✗[2]	✓[3]
Healthcare Standard	✗	✗[4]	✓
Prescriptive	✗[5]	✓	✓
Controlled Scaling	✗	✗	✓[6]
Controlled Tailoring	✗	✓[7]	✓
Control Compliance-Based	✗[8]	✓	✓
Organizational Certification	✗	✓	✓
Supports Third-Party Assurance	✓	✗	✓
Assessment Guidance	✗[9]	✓	✓
Tool Support	✗	✓	✓

Table 1: Why the CSF is well accepted in the industry

Relevancy

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. As a result, the CSF has seen very broad adoption in the industry with more than 83 percent of hospitals and 82 percent of health plans having adopted the CSF.

Controlled Scaling

The CSF is an integrated, prescriptive healthcare specific framework based on international and domestic standards and best practices that can be scaled specifically for various sizes and types of organizations or systems. Organizational and system risk factors are identified and used to determine the controls considered "in scope" and there are up to three levels of implementation requirements for each of these controls. The result is a consistent level of protection and associated assurance for similar healthcare organizations. This is particularly relevant to evolving healthcare business models, such as accountable care organizations (ACOs), that will need, for example, the CSF is used by ACOs to determine practical controls for clinics versus large hospitals within the system.

This type of consistency can't be achieved with ISO, as the framework allows each organization to liberally select controls with little or no oversight. The NIST framework is on the other side of the spectrum in that the minimum control baseline is based on a "high water mark" determined by the highest impact rating assigned to information stored, processed or transmitted by the information system(s). There is no formal mechanism by which the controls can be scaled to the size or type of organization implementing the NIST framework.

Controlled Tailoring

Differences in how scaling is managed by these three frameworks are also reflected in how specific controls may be tailored by an organization. Not all organizations are capable of implementing a particular control, even if they are of the same type and size. Some organizations may tailor their required controls by employing alternate controls to mitigate a specific risk or compensate for a system control failure.

ISO/IEC 27001 provides high-level requirements that may be liberally tailored by the organization. NIST provides for more limited tailoring than ISO/IEC 27001 by allowing organizations to define certain control parameters. Organizations are also expected to add controls or enhancements based on additional risks not considered when NIST defined the baseline, e.g., the existence of insider threats or advanced persistent threats, and federal or state legislation or regulations pertaining to specific types of information. Organizations may also remove or relax control requirements based on a defensible rationale documented in a formal analysis and acceptance of risk by a designated approving authority. Exceptions apply only to that organization, although they would likely impact the risk shared by others (e.g., business partners and other third parties).

In many respects, HITRUST and contributing healthcare organizations created the CSF using a similar process by integrating NIST requirements into an ISO-based framework and subsequently tailoring control requirements for the healthcare industry as a whole. However, unlike NIST, the CSF specifically requires HITRUST's review and approval of any control specification that deviates from the standard control requirements. Like managed scaling, managed tailoring helps ensure consistent application of information security controls and interpretation of security and compliance risk across multiple organizations.

Compliance-Based

The NIST and HITRUST frameworks are both control compliance-based. Risk is determined via a gap analysis of the controls considered in scope for an organization or system. ISO is not control compliance-based, but is rather a management or process model for the ISMS that is typically assessed in much the same way as a quality program audit. This leads to an assurance gap, as it's possible to certify the ISMS without thoroughly vetting the efficacy of the controls the ISMS supports.

Certifiable Assurance

Both HITRUST and ISO take an organizational (top-down) approach to security, although the baseline controls were created with organizational considerations in mind, while NIST takes a system (bottoms-up) approach. Thus, it's possible for HITRUST and ISO to certify organizations, which generally is not done with NIST. And, by design, only HITRUST formally supports third-party assurance through a common control specification, assessment and reporting framework. And while NIST requirements are integrated into the CSF, 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.

Assessment Guidance

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.

Tool Support

ISO/IEC 27799 provides additional guidance on ISMS control requirements in a healthcare environment; however, there is very little in the way of tools—outside of proprietary ones provided by third party consultants—to support the standardized assessment, evaluation and reporting of risk using ISO/IEC 27001.

On the other hand, NIST provides a stand-alone HIPAA Security Rule (HSR) Toolkit that allows small and enterprise-level healthcare organizations to take a checklist approach to HIPAA compliance. Although there are some dependencies among the questions, a small organization starts out with well over 400 questions and an enterprise starts with just over 800. Each of these questions are mapped back to NIST controls and related documentation in the NIST RMF, which provides a starting point for the risk analysis required by HIPAA. Unrelated to the HSR Toolkit, organizations may also use the OCR Audit Protocol to determine those security and privacy requirements that are the current focus of the OCR audit program and conduct a self-assessment. However, the Protocol only provides high-level assessment guidance for HIPAA Security Rule implementation specifications and does not map back to NIST. It is not intended to support the implementation and management of a complete information protection program.

HITRUST CSF Assessor and subscribing organizations have access to MyCSF®, a Web-based governance, risk and compliance (GRC) solution that helps organizations with performing assessments, managing remediation activities, and reporting and tracking compliance. Assessments may be scoped and tailored to the organization based on multiple risk factors and conducted at various levels of granularity. Assessment guidance for requirements in every level of each

control in the CSF is detailed enough to provide a ready-made test plan, and the controls are evaluated based on a NIST maturity model that provides consistent and repeatable results regardless of the CSF Assessor used by the organization, internal or external. Non-contextual impact ratings for the CSF controls are also available to provide a starting point for an organization's risk analysis and support development and prioritization of remediation activities.

This allows for the meaningful sharing of risk scores by business partners, regulators and other third parties, as well as unmatched benchmarking by organizational size and healthcare industry segment.

The HITRUST CSF—The Right Choice

Selecting a framework is not an easy decision as each organization has its own unique needs that must be met. HITRUST believes the CSF is the only framework that can meet the varying needs of healthcare organizations and be easily adapted to an organization's particular needs. The HITRUST CSF and CSF Assurance Program, part of a broader healthcare risk management framework, also fully supports the President's Executive Order on Improving Critical Infrastructure Cybersecurity and is a model implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity for the healthcare industry. With a quick review of the most salient attributes of ISO, NIST and the CSF as presented here, it's easy to see why the CSF is arguably the de facto information security compliance and risk management framework in the healthcare industry.

For additional information, please visit http://hitrustalliance.net/hitrust-csf

---

[1] *Factor Definitions:*

- *ISO 27001-Based – Is the framework based on the international standard?*
- *Integrated Compliance Framework – Have multiple regulatory, standards, frameworks and best practices been incorporated into the framework?*
- *Healthcare Specific – Was the framework designed to accommodate the specific, unique needs of the healthcare industry?*
- *Healthcare Standard – Does the framework have significant adoption within the industry?*
- *Prescriptive – Are the framework control requirements sufficiently detailed to reduce ambiguity in implementation?*
- *Controlled Scaling – Can the framework be scaled to the specific needs of a healthcare organization in a centralized, pre–defined way?*
- *Controlled Tailoring – Does the framework allow the replacement of specified controls with alternate controls in a centralized, pre–defined way?*
- *Control Compliance-Based – Is risk determined through a gap–analysis of the control requirements and the maturity with which they're implemented?*
- *Organizational Certification – Does the framework provide for formal certification of the state of control compliance within an organization?*
- *Supports Third Party Assurance – Does the framework provide an adequate mechanism for the sharing of reasonably accurate and consistent risk information amongst organizations?*
- *Assessment Guidance – Does the framework provide prescriptive guidance on how controls should be assessed through documentation reviews, observation, interviews or testing?*
- *Tool Support – Availability of specific tools organizations may use to assess and manage controls and risks to the organization.*

[2] *Additional guidance for healthcare is provided separately (ISO/IEC 27799 & NIST SP 800-66)*

[3] *HITRUST is rapidly becoming the de facto standard for the healthcare industry*

[4] *NIST and OCR collaborate on specific tools like the HSR Toolkit but do not promulgate NIST SP800-66 as an industry standard for healthcare*

[5] *ISO 27001 provides relatively general requirements compared to NIST and HITRUST*

[6] *Only HITRUST scales control requirements based on organizational, system and regulatory risk factors7 ISO compliance*

[7] *Only HITRUST provides a formal, central review and approval process for alternative controls*

[8] *ISO compliance is based primarily on an evaluation of the ISMS rather than on a gap analysis of the controls and subsequent risk to the organization*

[9] *CSF Assessor organizations are not required to use the general guidance provided in ISO/IEC 27008*

HITRUST

Health Information Trust Alliance

855.HITRUST
(855.448.7878)
www.HITRUSTalliance.net