The CSF Provides Additional Value for Healthcare Organizations

HITRUST understands that healthcare organizations realize it is in their best interest to adopt an integrated information security framework rather than to develop and maintain a custom framework. There are several choices to be made, but unfortunately most of these are custom implementations. One exception—apart from the HITRUST CSF—is the Unified Compliance Framework (UCF) published by Network Frontiers LLC.

Similar to the CSF, the UCF is an open, prescriptive framework that integrates and harmonizes control requirements from multiple sources, e.g., general security and risk management frameworks, legislation and regulation. However, the UCF differs from the CSF in several important aspects such as industry specificity, the foundation upon which it's based, scaling and tailoring of the controls, assessment (maturity) approach, and suitability for organizational certification and third-party assurance.

The CSF – 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.

The CSF provides an integrated set of comprehensive security safeguards derived from multiple regulatory requirements applicable to U.S. healthcare, such as HIPAA and HITECH, as well as generally accepted information security standards and best practices, including ISO/IEC 27001 and NIST SP 80053. (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.)

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. The ongoing enhancements and maintenance to the CSF provide continuing value to healthcare organizations, sparing them from 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 large insurers having adopted the CSF.

Comparing the HITRUST and Network Frontiers Frameworks

As previously mentioned, both the UCF and CSF are open, integrated, prescriptive healthcare-specific control compliance frameworks harmonizing multiple international and domestic standards and best practices and various legislative and regulatory requirements.

However, while the CSF is built upon an international standard, the UCF is built on a proprietary set of controls and domains to which every other requirement is mapped and harmonized, including ISO/IEC 27001. And unlike the CSF, the UCF also considers authoritative sources that apply to a broad scope of environments and organizations, many of which do not apply or otherwise address the specific needs of the healthcare industry. And while it is understood that organizations may scope their authoritative sources to the same sources used by the CSF, the resulting control requirements may still reflect the influence of other non-healthcare sources incorporated into the UCF control language. The CSF control specifications are only determined by those sources considered relevant to healthcare, which is subsequently vetted with the healthcare industry through the HITRUST Alliance of organizations.
The CSF can also be scaled to specific sizes and types of healthcare organizations or systems. Organizational and system risk factors are identified and used to determine the controls considered “in scope” for an organization and 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 sizes and types of healthcare organizations. This is particularly relevant to evolving healthcare business models, such as accountable care organizations (ACOs), that will need to address sharing and protecting information amongst organizations with a wide range of sophistication and complexity. For example, the CSF is used by ACOs to determine practical controls for clinics versus large hospitals within the system. This type of cons as the framework allows each organization to select the authoritative sources and supporting controls with little or no oversight.

In addition, differences in how scaling is performed for the CSF and UCF are also reflected in how specific controls may be tailored by an organization. Not all healthcare organizations are capable of implementing a particular control, even if they are of the same type and size. Some organizations may choose to tailor their required controls by employing alternate controls to mitigate a specific risk or compensate for a system control failure. And as with scaling, the UCF does not provide a mechanism by which to do this in a controlled way. Only the CSF provides the opportunity for organizations to recommend and gain industry approval for alternate controls, as the framework specifically requires HITRUST 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.

The UCF and CSF frameworks are both compliance-based in that risk is determined via a gap analysis of the controls considered in scope for an organization or system. And both provide detailed assessment guidance at the control level. However, the CSF incorporates a multi-level maturity model to ensure all elements of a control requirement are considered during the assessment, including whether only some of the elements for a particular maturity level are in place. The UCF assessment guidance uses a simple binary approach for the control requirement; if applicable, it’s either in place or it’s not. Regardless, the use of a single framework like the CSF across the organization (e.g., audit, compliance, privacy, security, risk management, and information technology) will result in significant savings in compliance-related costs due to the elimination of redundant, stove-piped approaches to information protection.
In addition to providing assessment guidance for CSF controls, HITRUST also developed and manages the CSF Assurance Program. The program allows approved independent third party assessors to conduct assessments supporting a healthcare entity's organizational security certification in much the same way as organizations receive ISO 27001 and PCI-DSS certifications. However, unlike ISO and PCI, HITRUST also conducts a quality assurance review of independent assessor documentation to ensure the assessments are consistent and repeatable regardless of the assessor organization used.

The CSF Assurance Program also formally supports third party assurance through a control specification, assessment and reporting framework common to both business associates and the covered entities they support. And as previously stated, the CSF was based on the ISO/IEC 27001 control clauses by design to specifically address the implementation and assessment of information security and compliance risk for offshore business associates.

As a result, healthcare organizations and their business associates can be certified against the HITRUST CSF through independent assessment of their control environment and be assured their level of information security risk is comparable to other CSF certified organizations. Network Frontiers simply does not have an analogous program capable of certifying organizational compliance with the UCF or the ability of independent assessors to conduct the assessments.

Adopting the CSF

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 based on an organization’s particular needs. With a quick review of the most salient attributes of the UCF and CSF as presented here is arguably the de facto information security compliance and risk management framework in the healthcare industry.

For additional information, please visit https://hitrustalliance.net/hitrust-csf/.
Comparing the CSF and the Unified Compliance Framework

Footnotes

1. Factor Definitions:
   - Integrated Compliance Framework: Have multiple regulatory, standards, frameworks and best practices been incorporated into the framework?
   - Prescriptive: Are the framework control requirements sufficiently detailed to reduce ambiguity in implementation?
   - ISO 27001-based: Is the framework based on the international standard?
   - Healthcare Specific: Was the framework designed to accommodate the specific, unique needs of the healthcare industry?
   - Controlled Scaling: Can the framework be scaled to the needs of 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?
   - Audit/Assessment Guidance: Does the framework provide prescriptive guidance on how controls should be assessed through documentation review, observation, interview, or testing?
   - Maturity-based Assessment: Is the assessment of control effectiveness based on a multi-level maturity model that considers partial satisfaction of maturity requirements for each level?
   - 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?
   - Healthcare Standard: Does the framework have significant adoption within the industry?

2. UCF control content available online in separate, domain-specific HTML files
3. CSF control content available as a single PDF download
4. UCF is based on a proprietary set of domains and controls; ISO 27001 is integrated into the proprietary framework
5. UCF can be limited to healthcare-specific authoritative sources / requirements
6. Only HITRUST scales control requirements based on organizational and system risk in addition to regulatory factors
7. Only HITRUST provides a formal, central review and approval process for alternative controls
8. UCF assessment guidance takes a binary (Yes/No) approach if the control is applicable to an organization
9. Not supported by a formal assurance program for common control specification, assessment and reporting
10. HITRUST is rapidly becoming the de facto standard for the healthcare industry