HITRUST

NIST Webinar Q&A

1. How were the non-contextual impact codes determined and are they valid (the same) for the NIST control that maps to the CSF control?

Answer: The non-contextual impact codes were derived from the DIACAP Severity Codes and are broadly applicable to the CSF control requirements based on their specification. The codes can subsequently be used for underlying requirements that map to NIST SP 800-53 controls. That said, these codes were originally developed almost 10 years ago and will likely be revisited by a HITRUST working group after the CSF v10 release.

2. Is there a crosswalk listing of HITRUST with the other frameworks such as HIPAA, FISMA, PCI, ISO, etc. that you can provide?

Answer: Mappings between the HITRUST CSF and its authoritative sources can be found in the HITRUST CSF Standards and Regulations Cross-reference spreadsheet, which is contained in the HITRUST CSF download package available by accepting the HITRUST license agreement at https://hitrustalliance.net/csf-license-agreement.

3. Does NIST recognize the NIST certification from HITRUST?

Answer: Yes. NIST does not offer their own certification but supports third-party assessment and certification programs for the NIST Cybersecurity Framework. But, while NIST recognizes these programs, they cannot formally endorse them.

4. Does the consulting industry recognize the HITRUST NIST certification?

Answer: Yes. HITRUST currently has 75+ consulting and professional services firms in the CSF Assessor Program, including "Big 4" firms.

5. The big problem in industry is audits for too many frameworks. This is requiring too much emphasis on compliance at the operational level. How can this help reduce the operational impact on IT teams?

Answer: HITRUST supports an "assess once, report many" approach to compliance and assurance. A single HITRUST CSF assessment can generate a scorecard against any of the CSF's authoritative sources, and the HITRUST CSF can even be used as the underlying basis for an AICPA SOC 2 engagement by a CPA firm. A HITRUST CSF assessment report will automatically provide the assessed entity with a HITRUST certification or validation letter and supporting scorecard for the organization's NIST Cybersecurity Framework implementation, which allows for the provision of assurances in a form that is suitable for consumption by any organization in any industry, domestically or internationally.

6. So why not work with the assessment consulting firms to leverage SOC2 against HITRUST controls and NIST controls? A SOC2 audit report can show requirements compliance against multiple framework controls?

Answer: True, but the Trust Services Criteria (TSC) used in a SOC 2 engagement perform the same function as the NIST Cybersecurity Framework Core Subcategories: (1) both provide high-level objectives or outcomes and (2) both must be supported by an underlying set of prescriptive controls to determine how well the organization is meeting those objectives/outcomes and satisfying their due diligence and due care obligations for information security and individual privacy. In fact, a SOC 2 + HITRUST engagement can provide both the SOC 2 and NIST Cybersecurity Framework certification with a single assessment against a common set of controls. Organizations are then free to communicate assurances about their information protection program using either the TSC, NIST Framework, or both depending on their business needs.

7. Is this assessment excel-based or there is some sort of platform where the assessment can be done and retained for future reference and to be shared with a client?

Answer: Yes. However, an organization would need to import the results of an assessment conducted outside of MyCSF into the tool before HITRUST can perform a quality assurance review and issue a HITRUST CSF assessment report.

8. Who is qualified to assess? How do they get qualified?

Answer: Criteria for HITRUST CSF assessors can be found in the HITRUST CSF Assessor Requirements brochure available for download from https://hitrustalliance.net/documents/assessor/CSFAssessorRequirements.pdf.

9. When will CSF BASICs go live?

Answer: Due to the development schedule for multiple new HITRUST tools, including MyCSF 2.0 and the HITRUST Assessment exchange, we anticipate an initial, limited roll-out of the HITRUST CSFBASICs program in Q4CY18 or Q1CY19.

10. I was under the impression that you couldn't get certified against NIST - but you can test compliance against the NIST requirements. Is what HITRUST is offering something different or is there now a NIST certification?

Answer: NIST does not offer its own assessment and/or certification against the NIST Cybersecurity Framework. And while NIST does not endorse any third-party assessment and/or certification program, NIST does recognize and actually encourage them. HITRUST assesses how well an organization is achieving the objectives or outcomes specified by the NIST Cybersecurity Framework Core Subcategories and certify the results. HITRUST can also certify the organization's Current and Target Profiles as determined by the HITRUST CSF control requirements placed in scope by its risk factors.

11. Going back to the NIST certification being a regulatory requirement, do you need to select NIST as the report type to get the NIST certification scorecard and letter? Or does that happen with any CSF assessment report?

Answer: A HITRUST NIST Cybersecurity Framework letter and scorecard is provided automatically with every new HITRUST CSF assessment report. One does not need to select a regulatory factor to receive it.

12. How can HITRUST state this is the official NIST Certification?

Answer: There's no such thing as an "official NIST certification" if we understand your intent correctly. This is because, while NIST will recognize 3rd party assessments and certifications, NIST will not endorse them. However, HITRUST worked with government and private sector organizations through the Critical Infrastructure Partnership Advisory Council's Joint Healthcare and Public Health (HPH) Cybersecurity Working Group (CWG) to produce the Healthcare Sector Cybersecurity Framework Implementation Guide, which features the HITRUST CSF as the underlying foundation for NIST Cybersecurity Framework implementation in the healthcare industry. A copy of the Guide can be downloaded from the US-CERT Cybersecurity Framework Website at https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance or directly from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf. A recent GAO report on NIST Cybersecurity Framework implementation also highlights use of the HITRUST CSF. "According to sector officials, the Healthcare and Public Health sector encourages the alignment of the NIST cybersecurity framework with existing cybersecurity guidelines currently in use within its respective sector. For example, the sector aligned the [HITRUST CSF] to the cybersecurity framework. This mapping fully incorporated the framework and provided for 135 individual security controls and 14 individual privacy controls that can be implemented by healthcare providers. Department officials stated that the alignment of the framework to the [HITRUST CSF] allows organizations to demonstrate compliance with NIST through their implementation of the pre-existing [HITRUST CSF]." The GAO report can be downloaded directly from https://www.gao.gov/assets/700/690112.pdf.

13. Could we get some links about "recognize without endorsement"?

Answer: "'Our stance has been all along, hey the private sector is going to do this when it's valuable for the private sector to do this, and we will gladly support any efforts,' Matthew Barrett said last week in explaining NIST's recently released update to the framework of cybersecurity standards. Certification has been a hot-button issue for industry officials who argue that use of third-party audits for comparative purposes could smack of a mandate, despite development of the framework with heavy business input as a strictly voluntary risk-management process. Barrett fell far short of offering a NIST endorsement of a certification program, but said the agency stands ready to support private-sector efforts to include framework use as part of any existing standards-based certification program." (https://insidecybersecurity.com/daily-news/nist-official-says-private-sector-will-drive-need-certification-cyber-framework-use)

14. Is NIST 800-30 and NIST 800-39 the best guides for creating doing the Risk Analysis/Risk Management requirements?

Answer: NIST 800-30 and -39 are excellent resources for a traditional or "text-book" risk analysis. However, NIST SP 800-53 is the best resource for organizations that wish to understand how to tailor a sector or industry-level overlay of one of the NIST SP 800-53 control baselines, which is the approach HITRUST takes to the HIPAA risk analysis requirement.

15. Where can I find more information about CSF Basics?

Answer: The CSFBASICs program is still under development but we anticipate providing more information on the program to the public in 4QCY2018.

16. What Special Publication (SP) does the NIST CSF Certification fall under?

Answer: There is no NIST SP that addresses third-party certification of the NIST Cybersecurity Framework or of the NIST SP 800-53 controls for that matter. (Note: NIST Special Publications, with rare exception, provide guidance and do not specify mandatory requirements, especially for private sector organizations. Mandatory requirements are generally promulgated in Federal Information Processing Standard (FIPS) documents.)

17. Can you be HITRUST Certified and not be NIST CSF Certified? i.e. pass the HITRUST cert but fail the NIST CSF Cert?

Answer: Yes, it's possible because the HITRUST CSF controls map differently to the HITRUST MyCSF reporting domains used for HITRUST CSF certification and the NIST Core Subcategories used for NIST Cybersecurity Framework certification.

18. In the medical field, nationwide, what is the spread of HITRUST vs ISO vs NIST percentage wise?

Answer: A 2018 HIMSS Cybersecurity survey indicates the HITRUST CSF is the most widely-used control framework in the healthcare industry. The NIST Cybersecurity Framework is used more broadly; however, a controls framework like the HITRUST CSF must be used to provide the underlying foundation for NIST Cybersecurity Framework implementation. For more information on why and how the HITRUST CSF is used to implement the NIST Framework, refer to the Healthcare Sector Cybersecurity Framework Implementation Guide available from the US-CERT Cybersecurity Framework Website at https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance.

19. If we want NIST certification, is that a regulatory check mark in the CSF assessment? (Risk Factor scope)

Answer: No need to select a risk factor. A certification or validation letter and scorecard for the NIST Cybersecurity Framework is issued with every new HITRUST CSF assessment report.

20. Can you please provide contact information on all speakers in the follow-up email? Thanks again.

Answer: Michael Parisi, VP Assurance Strategy and Community Development, michael.parisi@hitrustalliance.net, 469-269-1123; Dr. Bryan Cline, VP Standards & Analysis, bryan.cline@hitrustalliance.org, 469-269-1118.

21. Is there a version for small businesses?

Answer: CSFBASICs is the program designed to provide the flexibility of approach needed by small, low-risk organizations to adequately protect sensitive information.

22. What is the industry baseline does HITRUST certification use as it's reference to what is defined as acceptable risk based on industry?

Answer: HITRUST used a control-based approach to risk analysis to create an industry overlay of the NIST SP 800-53 moderate-impact baseline using the tailoring guidelines outlined in the SP. The approach is also explained in a Dec 2017 article in the ISSA Journal entitled, *Leveraging a Control-Based Framework to Simplify the Risk Analysis Process*.

23. Does HITRUST offer a set boilerplate/template policies for providers or business associates? If not, does HITRUST have a recommendation, either specifically or informally?

Answer: No, we do not currently provide nor recommend boilerplate/template policies. While this is something we have considered doing in the past (and are still considering), there are entire books written on the subject and it would be difficult for HITRUST to provide boilerplate for or a template of information security and privacy policies that could be broadly applicable to industry--at least not without writing another book. This is because information security and privacy policies must generally conform to the content, format and style guidelines that are often unique to any particular organization.

24. How quickly will the quantum resistant cryptography standards NIST is currently developing be integrated once released and what controls are already in place for blockchain uses?

Answer: HITRUST does not generally "require" the use of specific types of technologies, especially the use of emerging technologies like blockchain and quantum-resistant cryptograph standards, until (1) it is considered an industry "best practice" for information security or privacy or (2) mandated by one of the CSF's authoritative sources. The CSF does not currently require the use of blockchain technologies.

25. Is this certification implemented – meaning are organizations able to begin the process currently?

Answer: Yes, all new HITRUST CSF assessment reports will come with a certification or validation letter and NIST Cybersecurity Framework scorecard.

26. Are organizations free to share the HITRUST certified assessment report with their partners?

Answer: Yes, but they must provide the entire report. To facilitate the sharing of assurances based on the NIST Cybersecurity Framework, the certification or validation letter and scorecard for the NIST Framework is also provided separately.

27. What items make up the certified assessment report?

Answer: Although somewhat dated, the brochure entitled, *Leveraging HITRUST CSF Assessment Reports: A Guide for New Users*, provides a detailed explanation of its contents. New reports will also provide a certification or validation letter and scorecard for the NIST Cybersecurity Framework.

28. How do you determine if your organization should become HITRUST certified?

Answer: Business requirements such as contractual and other business relationships, regulatory requirements, and business/market advantage often drive an organization's decision to pursue HITRUST CSF certification.

29. Why would an organization not want to share their assessment?

Answer: Organizations withhold this level of detail for several reasons, not the least of which is it could potentially help an adversary develop a more effective course of attack against its information systems.

NIST Webinar Q&A

30. By completing HITRUST certification can we assume that we can get the DoD certification without any additional requirements?

Answer: No, the DoD (and the Federal and Intelligence communities) uses a different process that requires specific individuals to evaluate and authorize federal information systems. (In the past, these were referred to as certification and accreditation/authorizing authorities/officials.) While the DoD leverages the NIST SP 800-53 control baselines, it has developed its own overlays that could be substantially different from the HITRUST CSF overlay of the NIST SP 800-53 moderate-level baseline.

31. How is the CSF tool different from other GRC tools?

Answer: The HITRUST CSF is a risk-based security and privacy controls framework. MyCSF is an assessment and reporting tool that helps simplify the scoping and assessment process and provides the mechanism by which HITRUST performs a quality assurance review of the assessment results and issues a HITRUST CSF assessment report.

32. Would you say it's a gap analysis against NIST?

Answer: In a sense, yes. The HITRUST CSF control requirements that are scoped to an organization based on its risk factors provides the NIST Cybersecurity Framework Target Profile. A HITRUST CSF assessment against this Target Profile provides the organization's Current Profile. A gap analysis between the two profiles will identify any additional risk treatments the organization should implement, including any corrective actions needed to remediate specific gaps.

33. How do you determine how many and what type of files a small biz holds?

A: The most direct way of determining this would be through the Applicable Controls Report that can be found in Pre-Assessment. There are several other methods available in the Analytics and Searching, but none as simple as the Applicable Controls Report.

34. Are tools used or is it manual?

Answer: While assessments can be done "manually," the information must be uploaded in the HITRUST MyCSF assessment and reporting tool in order for HITRUST to perform a quality assurance review of the assessment and issue a HITRUST CSF assessment report.

35. Our current assessment option is comprehensive security and privacy. NIST is a separate assessment. We were told that our current assessment option would include NIST but I am understanding that it is separate?

Answer: The NIST Cybersecurity Framework is not a separate assessment as HITRUST's certification of its implementation is based on a standard HITRUST CSF security assessment. In fact, since you selected a comprehensive security and privacy assessment, you will actually have the most complete information for your Current Profile and Scorecard.

36. So, by completing a HITRUST CSF certification, NIST, ISO, etc. are automatically done or does something special need to be done when completing CSF for NIST vs ISO vs Etc.? I.e., scoping exercise is same for NIST vs ISO?

Answer: The HITRUST CSF incorporates ISO 27001, NIST SP 800-53, and the NIST Cybersecurity Framework. While ISO 27001 and the NIST Cybersecurity Framework are included automatically, one most select FISMA as a regulatory factor to ensure all NIST SP 800-53 moderate-level baseline controls are included within the scope of the assessment.

37. Since there is no NIST certificate per se that NIST requires, how is the NIST CSF Certificate issued from HITRUST different from the report provided by an independent organization? Basically, how is the certificate from HITRUST different from a regular report that is issued by a third-party doing a NIST CSF assessment?

Answer: Certification by HITRUST is different from the certification provided by other independent 3rd party organizations because, among other reasons, HITRUST certification is based on (1) an industry standard of due diligence and due care for the protection of sensitive information that (2) forms the basis of public-private partnership guidance for sector implementation of the NIST Cybersecurity Framework, is (3) issued by an industry standards development organization that was (4) recently recognized as such in a recent GAO report on NIST Cybersecurity Framework implementation. A copy of the *Healthcare Sector Cybersecurity Framework Implementation Guide* can be downloaded from the US-CERT Cybersecurity Framework Website at https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance. The GAO report can be downloaded directly from https://www.gao.gov/assets/700/690112.pdf.