HITRUST THREAT CATALOGUE®

FAQs

FAQs are specific to this webinar. Visit our General FAQs here.

Q: Will this be importable into a GRC system such as Archer or ServiceNow or is it intended to be separate as a stand-alone threat assessment that proceeds control selection? Will this be sold as part of v10?

A: Yes, both the HITRUST CSF® and HITRUST Threat Catalogue® are governed under similar license agreements, which allow such use with express written permission of HITRUST. Subsequently, the MyCSF® subscription license will be modified to expressly allow such use by the time the Threat Catalogue is released, shortly after the CSF v10 release.

Q: Where can we download this?

A: You'll be able to download HITRUST CSF and Threat Catalogue content for incorporation into a GRC tool in MyCSF. You may also download the HITRUST Threat Catalogue on our website here.

Q: When will the Certified CSF Course begin to include the development of Threat Management Catalogues in its curriculum?

A: Yes, we anticipate incorporating content related to the HITRUST Threat Catalogue and its use into the CCSFP training course at the same time the course is updated for HITRUST CSF v10.

Q: What is the cost to access it? Is there a subscription required?

A: For MyCSF subscription costs, please contact sales@hitrustalliance.net. You may download the HITRUST Threat Catalogue free of charge here.

Q: What is the difference/advantage to this vs. NIST SP 800-30 appendices (Threat Sources, Events, etc.)?

A: The HITRUST Threat Catalogue provides a more comprehensive enumeration of "reasonably anticipated threats" than NIST SP 800-30, as can be seen in the last tab of the HITRUST Threat Catalogue spreadsheet. However, additional metadata, such as a list of threat actors and their relative capability and motivation, may not be available in the Threat Catalogue until the next release anticipated in late 2019 or early 2020.

Q: Can you help recap the primary use/benefit of the threat catalogue for 1) A company using the CSF and that has a HITRUST certification and 2) a company that is not working towards HITRUST certification?

A: The primary use case/benefit of the HITRUST Threat Catalogue for users of the HITRUST CSF is the ability to analyze the relationship between the controls they implement and the threats the controls are intended to address, and this information to meet regulatory requirements for a comprehensive risk analysis as well as supplemental and targeted risk analyses to support tailoring of the HITRUST CSF controls, analyses for compensating or alternative controls, and risk acceptance. Companies that aren't working toward CSF certification achieve the same benefits, even if they do not use the HITRUST CSF as their primary controls as they are currently mapped to other frameworks such as ISO 27001 and NIST SP 800-53.

Q: How is HITRUST CSF applicable to non-health industry organizations?

A: HITRUST CSF controls have always been applicable to all types of PII and other sensitive information, but the HITRUST CSF v9.2 release--available in mid-December 2019--pulls out healthcare and HIPAA-specific requirements into a separate industry segment, which makes the HITRUST CSF easily consumable by organizations regardless of their industry.

HITRUST THREAT CATALOGUE® FAQs

Q: When will the HITRUST Threat Catalogue be available in MyCSF?

A: The HITRUST Threat Catalogue will be available in MyCSF shortly after the HITRUST CSF v10 release, which is anticipated in Q2 2019.

Q: How about a vulnerability catalogue?

A: An enumeration of common asset types and related vulnerabilities is on the roadmap for the second major release of the HITRUST Threat Catalogue, anticipated in late 2019 or early 2020. Note the list will be enumerated at a level of granularity consistent with the threats list.

Q: How did you know the "appropriateness" of the threat and control mapping?

A: We used a risk statement to help ensure the appropriateness of the threat-to-control mappings: "A threat source produces a threat that exploits a vulnerability that has an impact on the organization, which subsequently requires a control."

Q: Will this be available to be mapped in the Unified Compliance Framework? If not, why not?

A: We do not plan to map the Threat Catalogue to the UCF as it is a compliance-only framework.

Q: How can this threat catalogue help in quantifying probability and impact?

A: The HITRUST Threat Catalogue provides basic information that will allow organizations to conduct risk analyses. Given the limited amount of 'actuarial' data that exists for many if not most security threats, we anticipate most analyses will be qualitative or quasi-quantitative.

Q: How will the threat catalogue impact SOC 2 + HITRUST reporting?

A: The HITRUST Threat Catalogue will impact the HITRUST CSF controls and even how the controls should be assessed; however, we do not believe it will impact AICPA SOC 2 + HITRUST CSF reporting per se. That said, it would be possible to include a dashboard or similar representation of the threats that are being addressed based on the implementation maturity and/or residual risk (if impact information is included).

Q: Why are some of the controls in the HITRUST CSF not mapped to a threat?

A: All HITRUST CSF controls should be mapped to one or more threats. Mappings to individual requirements within each control will become available shortly after the HITRUST CSF v10 release, anticipated in Q2 2019.

Q: Will the new HITRUST CSF be mapped to NIST CSF v1.1 or v1?

A: The HITRUST CSF v10 release will map to NIST Cybersecurity Framework v1.1 Subcategories.

Q: How is HITRUST risk and threat assessment different from SOX, SOC Attestation risk assessments?

A: The HITRUST CSF provides a controls framework-based approach to the comprehensive risk analysis, which makes it very easy for an organization to complete and produce an appropriate control specification than other methods. (For more information on the approach, see https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf). The controls gap assessments used to produce SOX or SOC 2 reports can vary by the organization conducting the assessment; however, the HITRUST CSF Assurance Program's assessment methodology ensures a transparent, comprehensive, consistent, precise and accurate assessment that is repeatable and produces a report that is very reliable, i.e., it provides a high degree of assurance for relying entities. (For more information on the HITRUST approach, see https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf).

HITRUST THREAT CATALOGUE® FAQs

Q: The slides referenced early release of the CSF v10 - where can we find that to begin looking at the future release?

A: The HITRUST CSF v10 release is currently scheduled for Q2 2019.

Q: Which NIST standard and threat catalogue did you recommend earlier in the presentation?

A: The NIST document referenced in the Webinar presentation was NIST SP 800-30.

Q: Please remind me how I can review the threat catalogue?

A: For information on how to review the HITRUST Threat Catalogue, refer to slide 17 in the Introduction PowerPoint: https://hitrustalliance.net/content/uploads/Introduction-to-the-HITRUST-Threat-Catalogue-v1.pdf.

Q: Can the HITRUST Threat Catalogue be integrated (loaded) into GRC tools such as RSAM?

A: Yes, MyCSF subscribers will be able to download the HITRUST Threat Catalogue in a format suitable for import into GRC tools such as RSAM.

Q: How heavy a lift will it be from CSF 9 to CSF 10, including the threat catalogue?

A: Considerations existing users of the HITRUST CSF should make include:

- Large entities may have a potential increase in the number of requirement statements due to assessing all CSF controls vs. 75 and mid-size entities will likely see an increase (note small, low-risk entities will see a decrease)
- Entities focused on the existing 75 controls required for certification may not be able to maintain certification due to the assessment of the entire breadth of the CSF as scoped to their organization, which should have been the focus
- Entities may need to leverage a control-by-control, if not a requirement-by-requirement, mapping to move the entity's information protection program to the new structure
- Entities should be aware that improved visibility across the breadth of an entity's information protection program in a HITRUST CSF assessment report may need to be socialized to internal & external stakeholders prior to the transition

The HITRUST Threat Catalogue will not impact an organization's transition from CSF v9.X to v10.