HITRUST WEBINAR:

Next Generation HITRUST Information Security Assessment Focuses on Continuous Cyber Relevance

February 3, 2022 | 11:00am-12:00pm CT

i1 IMPLEMENTED 1-YEAR HITRUST® CERTIFIED

HITRUST®

Presented By:

MICHAEL PARISI
Vice President of Adoption
HITRUST

JEREMY HUVAL
Chief Innovation Officer
HITRUST

ADAM SOLANDER
Partner
King & Spalding LLP

Agenda

- Why HITRUST developed a new information protection certification
  - Including: A problem with control frameworks relative to emerging threats
- The threat-adaptive and continuously relevant nature of the i1 assessment
- Characteristics of the i1 assessment and certification
- Where and why this matters
  - Interview with Adam Solander, Partner, King & Spalding LLP
- Audience Q&A

Business Needs Leading to a New HITRUST Certification

Current Assessment and Certification Portfolio

- Historically, the HITRUST assessment portfolio consisted of the following offerings:
  - **HITRUST CSF Rapid Assessment:** A self-assessed, security-only questionnaire facilitated through the HITRUST Assessment XChange (low level of assurance)
  - **HITRUST CSF Readiness Assessment:** Assessment performed in preparation for a validated assessment (low level of assurance)
  - **HITRUST CSF Validated Assessment:** Assessment leading to HITRUST CSF Certification, can optionally be tailored to include one or more authoritative sources (very high level of assurance)
- HITRUST offered entities only one certification (the *HITRUST CSF Validated Assessment Report with Certification*) at a very high level of assurance

A Need for a Broader Range of Assurances

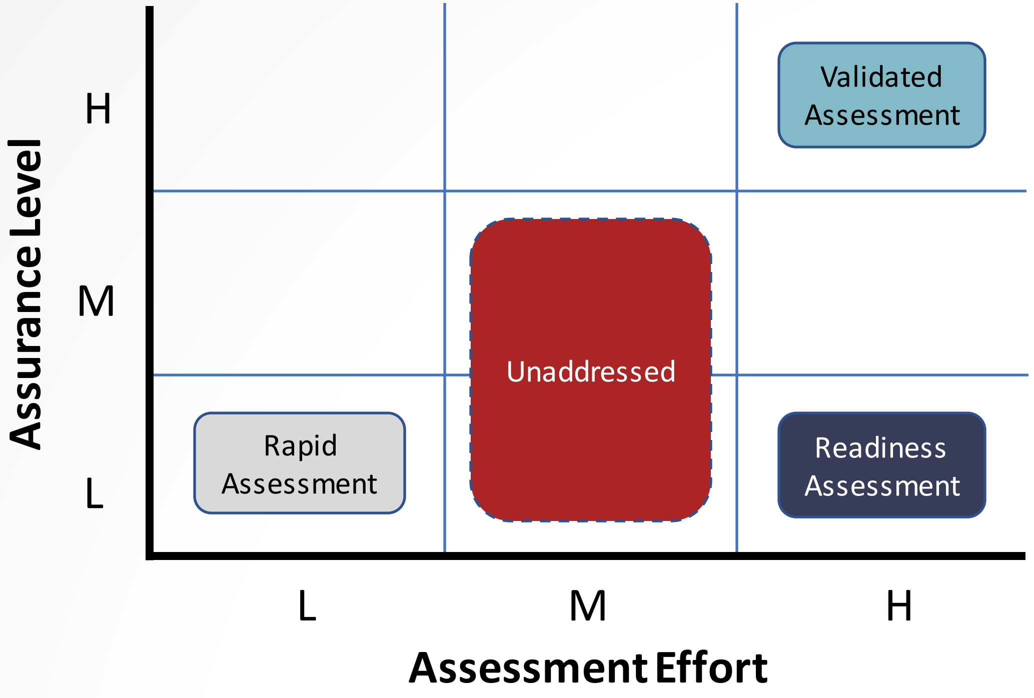
By design, the traditional HITRUST certification offered a gold-standard level of assurance due to the comprehensive control requirements and robust assurance program requirements.

- As a result: It is not appropriate for all assurance needs and requires a high level of effort to perform

To address varying assurance requirements, a broader range of assessment options was necessary.

Introducing new assessments and certification:

- Requiring **less effort** than today's validated assessment
- Suitable for situations requiring a **moderate strength of assurance** relative to that of the existing HITRUST certification
- While still living up to the **gold-standard level of quality and rely-ability** for which HITRUST certifications are known



A Need for a Very Rely-able™ Certification in the Moderate Assurance Space

Not all third-party assurance reports are created equal.

A table-stakes design goal for the i1: Live up to the gold-standard level of quality for which HITRUST certifications are known.

Some of the many issues with other third-party assurance reports in the moderate-assurance space:

Assurance program-level issues:

- Thousands of certification bodies, some unaccredited, each with their own way of doing things, resulting in extreme variations
- Lack of centralized oversight and quality management throughout

Control selection and design issues:

- Assessed entity-written controls
- Played-out controls which are disconnected from today's threat landscape (i.e., compliance-based instead of risk-based)
- Inconsistent and often lackluster coverage of important control areas

Issues with assessment procedures:

- Loosely defined assessment requirements such as assessors being able to pick own sample sizes with no minimum sample size
- Difficulty in including 3rd- and 4th-party performed controls makes the inclusive method exceedingly rare
- Wildly inconsistent quality of assessment performance, and wildly inconsistent quality in final deliverable

Issues in communicating assessment results:

- Binary assessment outcomes
- PDF distribution as the only way to communicate assessment results

A Need for a Different Approach to Control Selection and Rationalization

As we set out to create our moderate assessment, we found **gaps in the existing cybersecurity frameworks and standards**:

- **Required controls not always relevant:** Frameworks often contain controls designed to mitigate information risks which are no longer relevant, wasting time and effort while not delivering value.
- **Key cybersecurity risks not always addressed:** Frameworks fail to consistently mitigate real-world risks and cyber threats, such as ransomware.
- **Low frequency of updates:** While the threat landscape continually changes, many frameworks are updated only once every few years.
- **Lack of prescriptiveness:** Many frameworks are so high-level, or provide such significant latitude, it is difficult for relying parties to determine suitability or applicability.

> "**Control rationalization** is the effort to re-evaluate the existing control environment to remove duplicate, inefficient, unnecessary, or irrelevant controls from the testing population, and to re-assess the remaining controls for design efficiency to mitigate the respective risks."
>
> *Source: https://www.auditboard.com/*

A Need for a Widely Accepted Certification Focusing on Cybersecurity Good Hygiene and Leading Practices

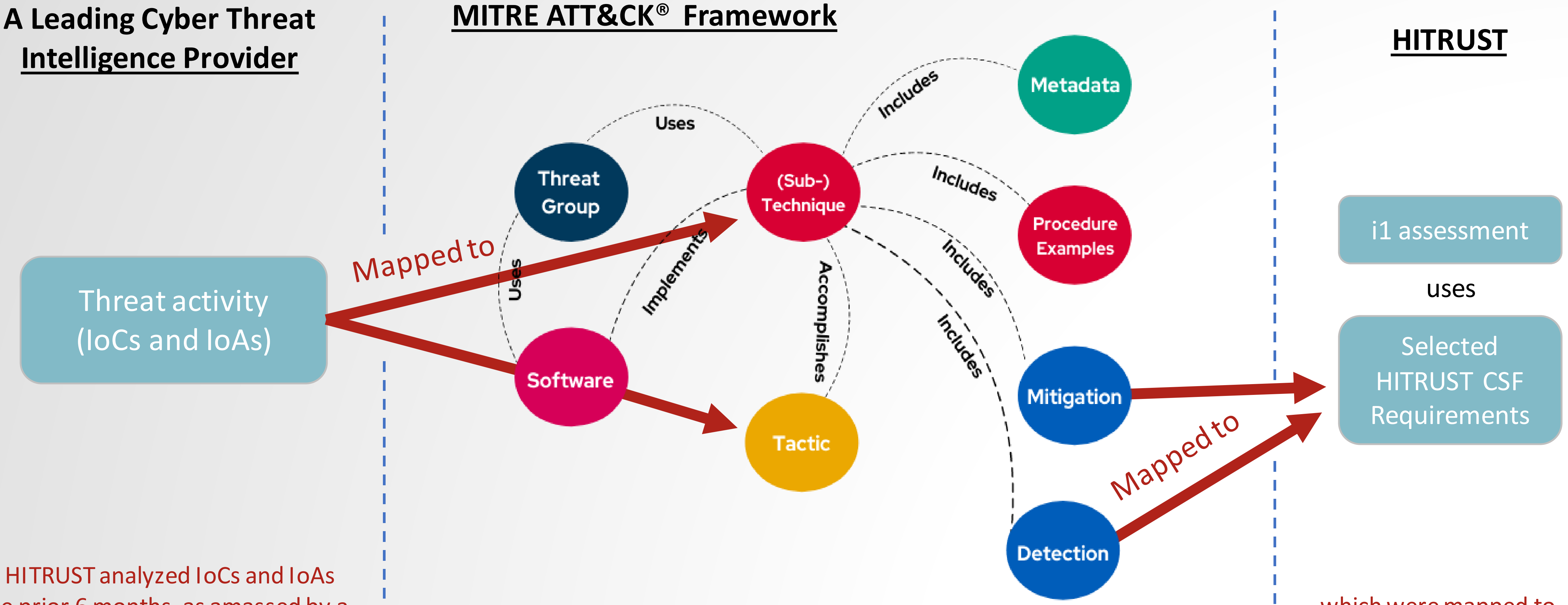
- The i1 is designed to be **industry agnostic** and **usable by a wide variety of organizations.**
  - Does not use any terminology that is specific to the federal government or specific legislation (e.g., Authority to Operation, covered entity)
  - Those seeking HITRUST assessments tailored to their industry can leverage the r2 assessment

- The i1 aims to focus on **good cybersecurity hygiene** and **leading cybersecurity practices.**
  - i1 control selection was guided by analyzing current and emerging cyber threats, and known relevant risks
  - Based on its design, it is not surprising that the i1 has a high degree of coverage with the following:
    - NIST 171
    - HIPAA Security Rule
    - GLBA Safeguards Rule (both current and 2021 proposed updated versions)
    - DOL EBSA Cybersecurity Program Best Practices
    - NAIC Data Security Law
    - NIST Interagency Report 7621, Small Business Information Security Fundamentals
    - Health Industry Cybersecurity Practices (HICP)

The Threat-adaptive Nature of the i1

The design and selection of the controls for the i1 place it in a new class of information security assessments that are threat-adaptive.

Using Threat Intelligence Data to make the i1 Control Selection Threat Adaptive



Initially HITRUST analyzed IoCs and IoAs from the prior 6 months, as amassed by a leading cyber threat intel provider. Going forward HITRUST will perform review quarterly.

This threat activity was mapped to TTPs (techniques, tactics, and procedures) within the MITRE ATT&CK Framework…

…which contain technical enterprise-level mitigations and detections (i.e., controls)....

…which were mapped to HITRUST CSF requirements, which were then included in the i1.

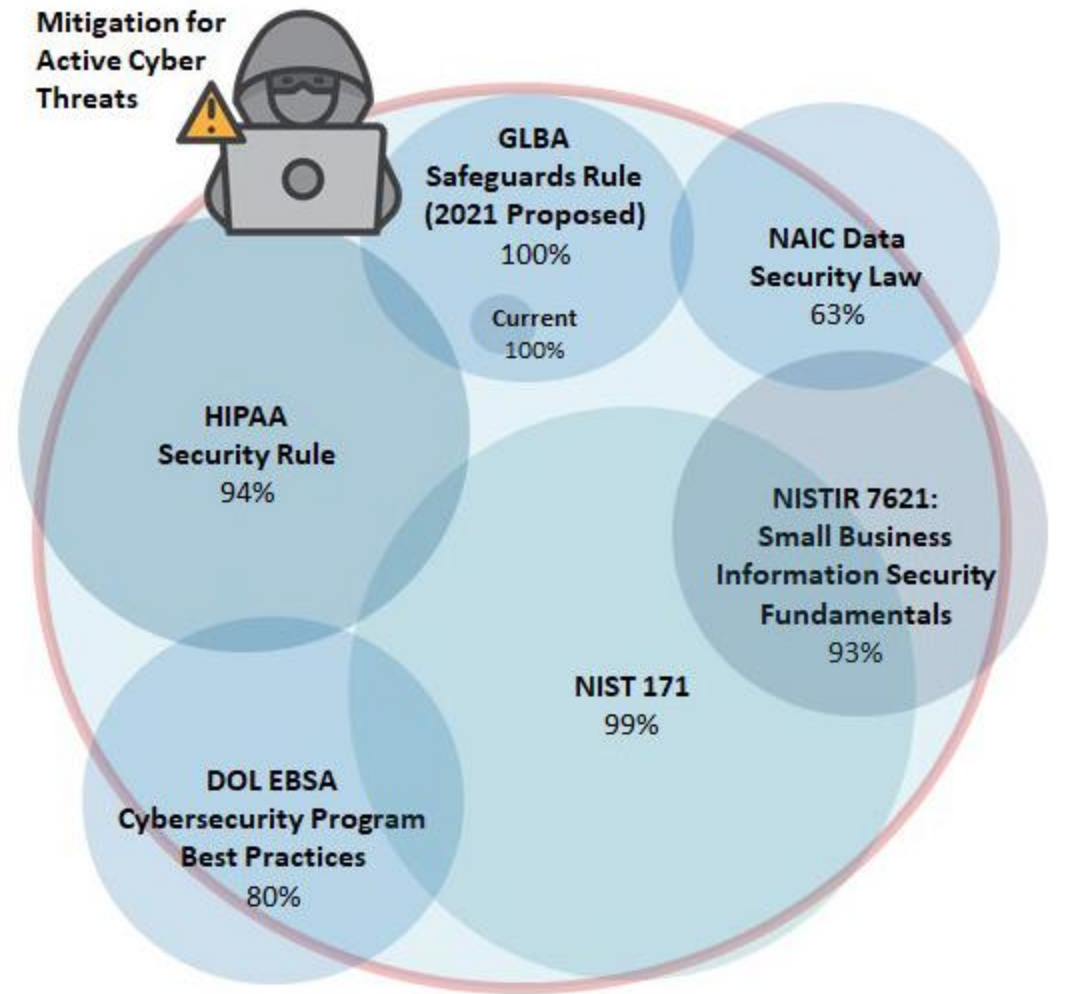
Continual Updates to the i1 Requirements

- HITRUST will reperform this threat intelligence analysis on a **quarterly** basis and update the i1 requirements as deemed necessary.
    - In addition to adding requirements in response to new and emerging cyber threats, **we will also sunset requirements** that are no longer justifiable (risk mitigation exceeds costs of incident), which reduces unnecessary assessment effort.
    - As a result of this design, all i1 assessments are required to use the then-current version of the HITRUST CSF (currently v9.6).
    - Those with i1 assessments underway (object created) and those with a valid i1 certification will not be affected by updates to the i1 control selection until their next HITRUST assessment effort.

Examples of HITRUST CSF Requirements Included Based on Threat Intel Analysis

From the MITRE ATT&CK® Framework				
Tactic	**Technique**	**Mitigation**	**Technique-specific mitigation guidance**	**Mapped HITRUST CSF Requirements included in the i1**
Privilege Escalation	T1543: Create or Modify System Process	M1018: User Account Management	Limit privileges of user accounts and groups so that only authorized administrators can interact with system-level process changes and service configurations.	**11182.01cCISSystem.8:** The organization uses automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges and validates that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
Initial Access	T1566: Phishing	M1054: Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.	**0231.09jCISOrganizational.7:** The organization has implemented the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers to lower the chance of spoofed email messages.
Initial Access	T1566: Phishing	M1021: Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.	**0957.09mCISOrganizational.15:** The organization maintains and enforces network-based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization specifically blocks access to known file transfer and email exfiltration websites. The organization subscribes to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites are blocked by default. This filtering is enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
Persistence	T1078: Valid Accounts	M1013: Application Developer Guidance	Ensure that applications do not store sensitive data or credentials insecurely. (e.g., plaintext credentials in code, published credentials in repositories, or credentials in public cloud storage).	**1315.02e2Organizational.67:** The organization provides specialized security and privacy education and training appropriate to the employee's roles/responsibilities, including organizational business unit security POCs and system/software developers.
Initial Access	T1190: Exploit Public-Facing Application	M1026: Privileged Account Management	Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.	**1146.01c2System.23:** The organization promotes the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.

The New HITRUST i1 Assessment


Mitigation for Active Cyber Threats
GLBA Safeguards Rule (2021 Proposed) 100%
Current 100%
NAIC Data Security Law 63%
HIPAA Security Rule 94%
NISTIR 7621: Small Business Information Security Fundamentals 93%
NIST 171 99%
DOL EBSA Cybersecurity Program Best Practices 80%

-year (i1) Validated Assessment

forward looking

HITRUST CSF requirements

litional HITRUST

nlike the r2, which

nanaged)

- Focuses on **cybersecurity leading practices** and **good cybersecurity hygiene**

- Backed by HITRUST's **best-in-class assurance program**
- Designed to ensure **continual relevance given its threat adaptive design**

HITRUST i1 Coverage

Note: Circle overlaps are not intended to convey overlap in authoritative source content

i1 and r2 Assessment Similarities

Both:

- Provide **a means to convey information protection** assurances over the assessed entity's scoped control environment
- Result in a **shareable, final report with certification** issued by HITRUST
- Can be shared with stakeholders using the HITRUST **Results Distribution System (RDS)** and the **HITRUST Assessment XChange**
- Use requirements resident in the **HITRUST CSF**
- Use HITRUST **MyCSF**
- Undergo 6 levels of independent and objective **quality assurance reviews** by HITRUST
- **Require an Authorized HITRUST External Assessor** to test control implementation
- Take advantage of HITRUST's patent-pending **Assurance Intelligence Engine (AIE)** to perform over 150 automated checks
- Feature **readiness** assessments **and validated** assessments

Interview with Adam Solander

Partner

King & Spalding LLP

HITRUST®

Audience Q&A

THANK YOU FOR ATTENDING

For additional HITRUST resources, please visit:

HITRUSTAlliance.net or our Download Center