Privacy and Security Town Hall

Maryland Health Care Commission

April 23, 2024

Agenda

- MHCC
  - Welcome and Introductory Remarks
  - Town Hall - Goals
  - MHCC's Privacy and Security Requirements
- HITRUST
  - Privacy and Security – Risk Management and Regulatory Compliance
  - HITRUST Certifiable Framework –Recent Changes
  - HITRUST Authorized External Assessor Program
    - Approach to Vetting
    - Requirements
- Q&A
- Closing Remarks

Town Hall Goals

- Provide a comprehensive overview of the recent changes to the framework and discuss potential implications on technology entities and other stakeholders
- Highlight key modifications, new guidelines, and enhanced security measures
- Build awareness and increase alignment of the latest framework requirements and best practices
- Foster dialogue among participants around navigating the complexities of achieving HITRUST Certification, and how to leverage learning lessons to strengthen cybersecurity posture

Maryland Regulatory Requirements

- COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information* – 14 registered health information exchanges (HIE) demonstrate compliance using:
  - SOC 2 – 71 percent
  - HITRUST – 36 percent
  - ISO – 29 percent
  - EHNAC – 14 percent
- COMAR 10.25.07, *Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses* – 32 certified electronic health networks (EHN)
  - EHNAC – 72 percent
  - HITRUST – 41 percent
- COMAR 10.25.19, *State Recognition of an Electronic Advance Directives Service*
  - One recognized electronic advance directives service demonstrates compliance using HITRUST

**Some organizations submit documentation from multiple third-party entities (e.g., HITRUST and EHNAC)*

Ryan Patrick
Vice President – Adoption
HITRUST Alliance

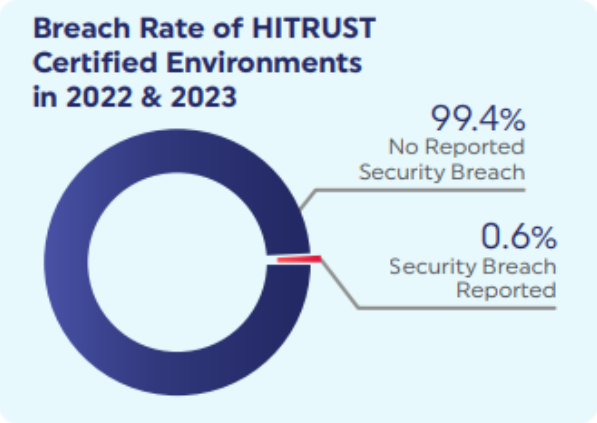
Ryan.Patrick@hitrustalliance.net

Evolving for Enhanced Cyber Resilience

- **Continuous Adaptation:**
  - HITRUST CSF updates respond to the evolving cyber threat landscape, ensuring relevance and timeliness in addressing new risks.
- **Quality Assurance:**
  - Inclusion of a robust Quality Assurance program for assessing the HITRUST certification process ensures integrity and accuracy.
- **Cyber Threat Adaptive:**
  - The CSF is dynamically updated with threat intelligence data, integrating insights from leading providers and mapping to the MITRE ATT&CK framework.
- **Reliable & Relevant Assurances:**
  - Establishing trust through transparency, scalability, consistency, integrity, and efficiency principles, HITRUST assessments offer assurances that are both dependable and pertinent to current threats.
- **Commitment to Security:**
  - Data indicates organizations with HITRUST certification have notably lower incidences of reported security breaches.
- **Continuous Improvement:**
  - Even post-certification, organizations are expected to remediate identified gaps and enhance their security posture.
- **Risk-Based Customization:**
  - Scalable r2 assessments through risk analysis specific to organizational needs.
  - Factors such as size, complexity, and regulatory requirements tailor the assessment.
- **Integration and Harmonization:**
  - Compliance factors from relevant standards and regulations are integrated into assessments.
  - Over 60% of organizations utilized compliance factors, with HIPAA as the leading selection.

97%

Of all threat indicators in MITRE ATT&CK are covered in CSF versions 11.2 & 11.3.0



By aligning with HITRUST, organizations demonstrate a proactive and committed approach to privacy and security.

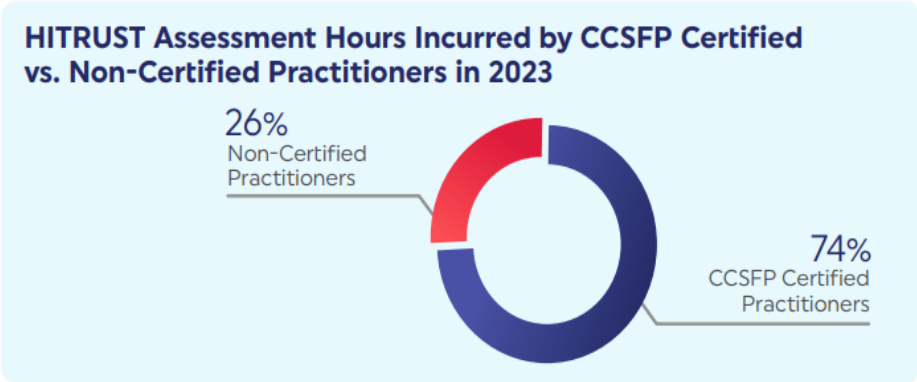
Question

Can you provide insight into common challenges or areas for improvement identified during recent HITRUST assessments?

HITRUST Assessor Program

- **Assessor Vetting:**
  - All organizations to engage with authorized External Assessors.
  - Vetting by HITRUST ensures quality and competency.
- **Certification Requirements:**
  - Assessors must hold Certified CSF Practitioner (CCSFP) or Certified HITRUST Quality Professional (CHQP) designations.
  - Annual refresher courses for certification maintenance.
  - Minimum of 140 hours of specific training for the firm.
- **Engagement Protocols:**
  - A minimum of 5 CCSFP and 2 CHQP designated practitioners per firm.
  - 50% of engagement hours by CCSFP practitioners.
  - Quality assurance reviewers to hold both CCSFP and CHQP without other assessment duties.
- **Quality Assurance Measures:**
  - Assurance Intelligence Engine with over 150 automated checks.
  - HITRUST Assurance department's Analysts perform QA reviews.
  - Ongoing training for QA Analysts to maintain expertise.
- **Impactful Results:**
  - Consistent, objective quality reviews.
  - Centralized Quality Assurance ensures consistency and high standards.

The HITRUST Assessor Program upholds the highest standards to ensure assessors are equipped to evaluate and certify with precision and expertise.



Questions

- What is the process for communicating HITRUST assessor concerns to HITRUST?
- Are there criteria that HITRUST can provide technology entities in matching with leading HITRUST consultants?

What's New in CSF v11.3.0

- Addition of FedRAMP, StateRAMP, and TX-RAMP authoritative sources, which provide a standardized approach to ensure that assessed entities doing business with the government comply with applicable information security requirements.
- Integration of NIST SP 800-172: Enhancing protections for Controlled Unclassified Information (CUI) and supporting organizations with high-risk profiles in their HITRUST r2 Assessment tailoring.
- Foundation for CMMC Level 3 Requirements: Preparing organizations for new compliance needs based on stringent NIST standards.
- Inclusion of MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (MITRE Atlas) Mitigations: Addressing security requirements crucial for safeguarding AI systems.
- **Streamlined Assessment Process: Reduced redundancy in requirement statements, significantly decreasing the average r2 assessment size without compromising control coverage.**

Questions

- How are updates or changes by HITRUST to the framework communicated?
- Are there any upcoming regulatory changes or emerging cybersecurity threats that HITRUST is actively monitoring, and how should we prepare?

Customer Benefits of v11.3.0

- **Staying Ahead of Regulations:**
  - By integrating and normalizing the latest industry standards and requirements, CSF v11.3.0 ensures organizations remain aligned with current and emerging regulations.
- **Comprehensive Cyber Threat Adaptation:**
  - The inclusion of cutting-edge authoritative sources like NIST SP 800-172 and MITRE ATLAS ensures the framework meets the challenges of today's dynamic threat landscape.
- **Enhanced Efficiency:**
  - Consolidation efforts have streamlined the assessment process, reducing effort and time investment for organizations pursuing HITRUST certification while meeting one or many regulatory compliance requirements.

With the launch of v11.3.0, new e1 and i1 assessments will be aligned with the updated framework, ensuring organizations benefit from the latest cybersecurity and compliance advancements. Existing assessments under v11.2.0 can still proceed, providing flexibility and continuity for ongoing certification efforts.

HITRUST

Questions

- How can HITRUST support us in maintaining compliance with evolving data privacy regulations and industry standards?
- What resources or tools does HITRUST offer to help technology entities enhance their cybersecurity posture and mitigate risks effectively?

Assurances

1

Start with a core of threat-adaptive controls

Supported by Cloud and AI Shared Responsibility Model

+

2

Optionally Include Other Authoritative Sources

- HIPAA Security Rule
- PHIPA
- GDPR
- NIST
- StateRAMP
- FedRAMP

=

3

HITRUST Issues Many Reports

HITRUST CSF Certification

r2 HITRUST CERTIFIED

Compliance Insights Report

HITRUST

Questions

- Is there any guidance you can provide in selecting an appropriate HITRUST assessment?
- What are the advantages to obtaining HITRUST Certification and SOC 2 examination?

Assurances Over AI through HITRUST

1

Start with a core of threat-adaptive controls

Supported by Cloud and AI Shared Responsibility Model

+

2

Optionally Include AI Authoritative Sources

AI / ML Security

ISO 23894

NIST AI RMF

AI Risk Mgmt.

=

3

HITRUST Issues Many Reports

HITRUST AI Security Certification

AI Risk Management Insights Report

HITRUST CSF Certification

r2 HITRUST CERTIFIED

HITRUST

Contact Information & Closing Remarks

For questions regarding registration/recognition:

- EHN.Certification@maryland.gov
- hie.registration@maryland.gov
- ad.staterecognition@maryland.gov

For any other questions, contact:

- Justine Springer, MHCC, justine.springer@maryland.gov
- Ryan Patrick, HITRUST, Ryan.Patrick@hitrustalliance.net

Thank you!

Appendix

HITRUST AI Assurance Program

- **Delivers practical and scalable assurance for AI risk and security management through AI certifications and assessment reports**
- **Helps organizations who use AI:**
  - Shape their AI risk management efforts
  - Understand best practices in the areas of AI security and AI governance
  - Evaluate their AI control environment through self and validated assessments
  - Achieve AI security certification that can be shared with internal and external stakeholders
- **Focuses on a few subsets of the larger concept of “Responsible AI”, namely risk management and security**

HITRUST

HITRUST Assessment Portfolio

Additional Resource

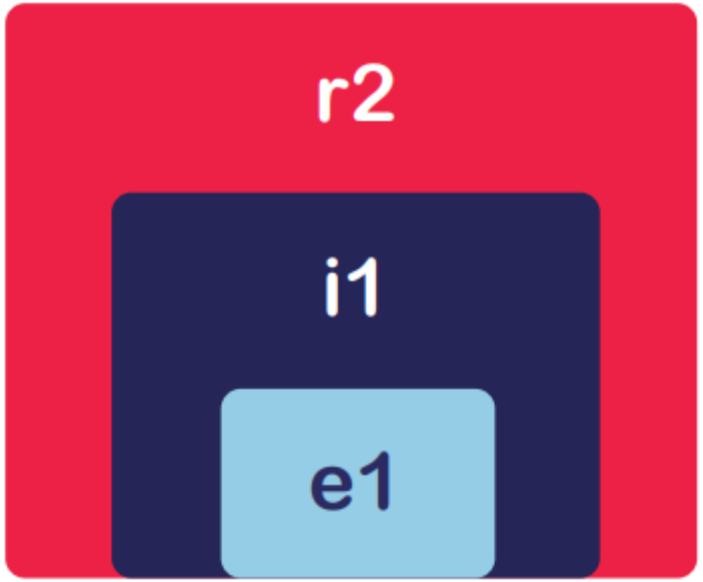
HITRUST Certification Options

HITRUST offers three certification options based on vendor needs, size, risk maturity, and business profile.

- The HITRUST Essentials (e1) Validated Assessment is ideal for low-risk vendors seeking to establish basic foundational cybersecurity or more complex organizations looking to start their certification journey with plans to move into a more comprehensive certification level.
- The HITRUST Implemented (i1) Validated Assessment offers more coverage than the e1. It is suited for third-party vendors demonstrating leading security practices.
- The HITRUST Risk-Based (r2) Validated Assessment is its most comprehensive assurance. It is considered the gold standard in the industry and is ideal for high-risk vendors.

Each level is built on a common framework. This means your third-party partner can begin with a lower-level assessment and move up to a higher level without losing the invested time, money, and effort.

Assessment Options



Considerations in Selecting an Assessor

Questions to ask yourself:

- What roles am I expecting the assessor to perform?
  - Initial scoring assistance
  - Remediation assistance
  - Validation of scores
- Do we have a staff capable of scoping and doing initial scoring and remediation?
- Do we have the technical expertise to get accurate results?
- Does our staff have sufficient bandwidth to perform the work?
- Do we have a wide geographic scope to evaluate?
- Do we have an existing relationship with a current external assessor?
- Do we have any special circumstances that would require a special skill set?
  - PCI, GDPR, CMMC, ISO 27001, HIPAA

Considerations in Selecting an Assessor

Questions to ask the assessor:

- What is your experience in conducting HITRUST assessments?
- What is your success rate in getting organizations certified?
- How often do you have assessments go into escalated QA?
- Can you explain your methodology in getting an organization certified?

Other considerations

- Personality match
- Relationship with HITRUST