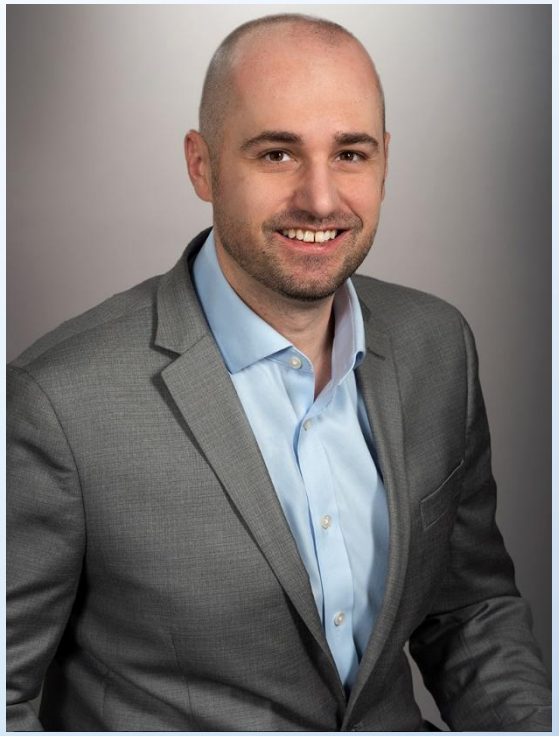
McKONLY & ASBURY

HITRUST Assessments: Understanding the Differences Between the e1, i1 and r2 Assessments

macpas.com

Introductions

David Hammarberg, CPA, CFE, CISSP, GSEC, MCSE, CISA, CCSFP, CHQP, CCA
Partner



Josh Bantz, CPA, CCSFP, CHQP, CISA, CCP
Director

Firm Overview

Helping You Thrive!

McKonly & Asbury

M&A is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, Bloomsburg, and Philadelphia.

accountingTODAY 2025 Best Firms to Work For

accountingTODAY 2025 Best Firms for Young Accountants

BEST PLACES to work in PA 2025

Services Provided

- Advisory & Business Consulting
- Audit & Assurance
- Tax
- Entrepreneurial Accounting Solutions
- SOC & Technology Consulting

Industries Served

- Affordable Housing
- Architecture, Engineering, and Construction (AEC)
- Entrepreneurial
- Family-owned Business
- Franchises
- Healthcare
- Manufacturing & Distribution
- Nonprofit
- Public Companies

Subscribe for M&A Insights

Pick your perfect thought leadership mix from 15 newsletters!

McKonly & Asbury

macpas.com

Agenda

- Introduction to HITRUST Assessments
- Differences and similarities between the HITRUST validated assessments (e1, i1 and r2)
- Evaluating the level of effort and requirements needed to complete the e1, i1 and r2 validated assessments
- Differences in the scoping, documentation and external assessment process for each type of assessment.
- Questions

McKONLY & ASBURY

Introduction and Background to HITRUST

What is HITRUST

- Official Definition: HITRUST is a comprehensive, flexible and efficient approach to compliance and risk management that has been adopted on a global scale.
- Plain English: HITRUST is a "framework of frameworks" that organizations who create, access, store or exchange sensitive information can use as roadmap to data security and compliance.
    - Based on ISO/IEC 27001 and 27002 + 40 other security and privacy-related regulations, standards, and frameworks.

HITRUST CSF

- The HITRUST CSF – “framework of frameworks”
  - Merges existing controls, standards, regulatory resources, business and third-party requirements into one framework. (ISO, NIST, etc.)
  - Compliance and risk management driven.
  - Quantitatively evaluate compliance and security risk driven.
  - Supports the HITRUST CSF Assessment Certification process.
  - HITRUST has various tools to assist in the assessment process (myCSF, etc.)

HITRUST CSF Design

- HITRUST Control References, Requirement Statements and Elements
  - Developed by HITRUST to provided detailed information to support the implementation of a control reference.
  - Control references may have multiple requirements statement.
  - Requirements statements are the specific statements that define the control activities that must be in place to meet the HITRUST CSF framework
    - Requirement Statements can have multiple evaluative elements that are required as part of HITRUST compliance
    - Requirements statements and evaluative elements are scored by the client and evaluated by an external assessor during an assessment

HITRUST Assessment Domains

- **HITRUST Domains**

1. Information Protection Program
2. Endpoint Protection
3. Portable Media Security
4. Mobile Device Security
5. Wireless Security
6. Configuration Management
7. Vulnerability Management
8. Network Protection
9. Transmission Protection
10. Password Management
11. Access Control
12. Audit Logging & Monitoring
13. Education, Training & Awareness
14. Third-Party Assurance
15. Incident Management
16. Business Continuity & Disaster Recovery
17. Risk Management
18. Physical & Environmental Security
19. Data Protection & Privacy

HITRUST Assessments

- Readiness vs. Validated/Certified
  - Readiness – can be completed by client
  - Validated/Certified – requires an external assessor
  - Varying levels of assurance

- HITRUST Assessments – 3 Types
  - Essentials (e1)
  - Implemented (i1)
  - Risk-based (r2)

McKONLY & ASBURY

Differences and Similarities Between the e1, i1 and r2 Validated Assessments

HITRUST Validated Assessments

- HITRUST Validated Assessments are assessments performed against the HITRUST CSF and validated by a HITRUST external assessor and the HITRUST assurance program
  - Validated Assessment Report and Certification Letter if (Scoring thresholds are met)
  - Report includes remediation activities tracked via corrective action plans (CAPS)
- Certification is based upon scoring results
  - Certification depends upon raw scores at the Domain level.
  - Gap and CAP are determined at the Requirement statement and Control Reference level.
  - All domains are required to meet the certification threshold as defined separately for e1, i1 and r2 assessments.

HITRUST Validated Assessment Types

- **HITRUST Essentials 1-Year (e1)**
  - **Foundational level assessment comprised of 43 HITRUST CSF Requirements Statements and only focused on the Implementation maturity level.**
- **HITRUST Implemented 1-Year (i1)**
  - **Moderate level assessment comprised of 182 HITRUST CSF Requirements Statements and focused on the Implementation maturity level.**
- **HITRUST Risk- Based 2-Year (r2)**
  - **Comprehensive risk driven assessment comprised of 200 – 1,900 HITRUST CSF Requirements Statements and focused on all 5 maturity levels. (Policy, Procedure, Implementation, Measured and Managed)**

HITRUST Assessment Similarities

- HITRUST CSF Provides Comprehensive Concentric Inclusion
  - Requirement Statements included in the e1 assessment (43) are also incorporated as part of the i1 assessment (182) and the i1 requirements are also incorporated into the r2 assessment requirements.
- Assessment Scope Consistency
  - Regardless of HITRUST Assessment the scope components and requirements are the same from assessment to assessment.
- Scoring and Sampling
  - Scoring methodology and sampling methodology for HITRUST assessments are consistent regardless of assessment level.

HITRUST Assessment Differences

- HITRUST e1, i1 and r2 Requirements Statements
  - The e1 and i1 assessments have consistent requirement statements (43 and 182 respectively)
  - The r2 assessment provides a risk-based approach that layer's requirement statements through a risk and compliance-based approach. (Range from 200-1,900 requirements)

- Maturity Level Applicability
  - The e1 and i1 focus only on the implementation maturity level, the r2 assessment focuses on a minimum of three (policy, procedure and implementation) and up to five (measured and managed)

- Scoring
  - Scoring is determined by domain score however threshold by domain for e1 and i1 is 83

McKonly & Asbury

Effort and Requirements Needed to Complete the e1, i1, and r2 Validated Assessments

HITRUST Assessment Level of Effort

- HITRUST e1 (Light – Moderate Level of Effort)
  - Organization being assessed needs to confirm implementation of all 43 requirements across all scope components
  - Documentation and evidence collection proving implementation of all requirement statements and evaluative elements within each requirement statement
  - Timeline for completion 4-6 months

- HITRUST i1 (Moderate to Substantial Level of Effort)
  - Organization being assessed needs to confirm implementation of all 182 requirements across all scope components
  - Documentation and evidence collection proving implementation of all requirement statements and evaluative elements within each requirement statement (600+ evaluative elements)
  - Timeline for completion 6-12 months

HITRUST Assessment Level of Effort

- HITRUST r2 Assessment (Substantial Level of Effort)
  - Organization being assessed needs to confirm policy, procedure and implementation of all requirements across all scope components (200-1,900).
  - Documentation and evidence collection proving documented policy and documented procedure for each requirement statement and all evaluative elements.
    - Policy must clearly state what must be done to meet the requirement statement and elements
    - Procedure must be substantively documented for the who, what when and how of the process/control for the requirement statement and all evaluative elements.
    - Implementation must have artifacts showing that implementation has occurred across the scope
    - Measured and Managed must show evidence of evaluation of performance for each requirements statement (measured) and focus toward improvement for gaps and CAPs (managed)
  - Timeline to completion (12-24 months)

McKONLY & ASBURY

The Scoping, Documentation, and External Assessment Process for Each Type of Assessment

HITRUST Scoping

- **SCOPING IS CRITICAL FOR ANY SUCCESSFUL HITRUST ASSESSMENT:**
  - **Determining the appropriate system or platform to include within the scope**
    - **Do clients rely on a system or platform?**
    - **Do clients or customer process, store or transmit information on the system or platform?**
    - **Is the system critical to your organizations operations or customer operations?**

- **NARROW THE SCOPE FOR SUCCESS (e1, i1, and r2):**
  - **HITRUST Scoping can follow any of the following methods**
    - **Enterprise**
    - **System/Platform**
    - **Enclave**
    - **Share IT Devices**

HITRUST Scoping

- Keys to Scoping any HITRUST Assessment:
  - HITRUST certifies Information Systems/Platforms not entire Organizations
    - Define the information system(s) in scope and define the primary scope components of each information system (Applications, Data/Databases, Operating Systems, Networks and Facilities)
    - The requirement statements must be assessed for all applicable scope components of each information system defined in the scope.
  - Focus on sensitive/confidential client information when determining information system to include.
    - Avoid utilities, auxiliary tools and applications as they can complicate the assessment process
    - Implications of third party managed components and systems.

HITRUST Scoping Components

- All applicable primary scope components must be assessed for all HITRUST CSF requirements statements.
  - Primary Scope Components Include
    - Applications
    - Facilities
    - Databases/Data
    - Operating systems
    - Networks
  - Secondary Scope Components must be assessed if they are part of or applicable to a primary scope component
    - SSO Tools
    - SIEM

Documenting HITRUST Compliance

- **DOCUMENTATION FOR EACH REQUIREMENT'S STATEMENT:**
  - **Evidence demonstrating compliance must be documented for each scope component for each maturity level.**
    - r2 Assessments require policies and procedures that specifically highlight where each requirement is met within the document
    - e1, i1 and r2 Assessments require implementation artifacts that include screenshots, checklists, system settings, etc., and must clearly show compliance with specific HITRUST requirement or evaluative element.
  - **Documentation and evidence supporting the score for each HITRUST requirement statement will be uploaded and validated by both the external assessor and HITRUST**

Documenting HITRUST Assessment

- **HITRUST MYCSF Application**
  - **All HITRUST assessments and documentation must scored and submitted in the HITRUST MyCSF application.**
  - **MyCSF provides a documentation repository for HITRUST assessments including scoring**
  - **External Assessors can access the HITRUST assessment, review the documentation and validate HITRUST scoring for the assessment and certification**
  - **HITRUST quality assurance personnel review documentation as part of the HITRUST Assurance Program**

NOTE: The OSA should create documentation including artifacts that allows the OSA personnel to present how they comply with each requirement and each evaluative element.

External Assessor Documentation Requirements

- **HITRUST ASSESSSMENT DOCUMENTATION FOR CERTIFICATION:**
  - **Required artifacts (policy, procedure, screenshot, checklist, ticket etc.) for all applicable scope components that clearly aligns to the HITRUST requirement statement and evaluative elements.**
  - **External Assessor must test artifacts within the 90-day period prior to the submission of the assessment to HITRUST**
  - **Sampling is required to evidence compliance with certain pre-defined requirements (security awareness training, change management etc.)**
  - **All testing and evidence must be provided and completed 90 days prior submission of the assessment to HITRUST.**

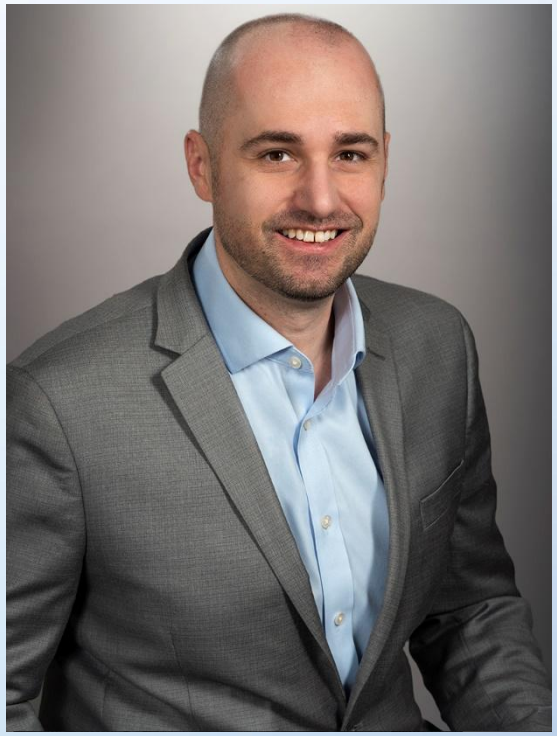
Questions?

Contact Information

David Hammarberg, CPA, CFE, CISSP, GSEC, MCSE, CISA, CCSFP, CHQP, CCA
Partner

dhammarberg@macpas.com

717-972-5723



Josh Bantz, CPA, CCSFP, CHQP, CISA, CCA
Director

jbantz@macpas.com

717-972-5714

McKONLY & ASBURY

Upcoming Events

July 30 Webinar

Year 15 for Low-Income Housing Tax Credit Partnerships

REGISTER NOW