HITRUST 101: An Introduction to HITRUST Assessments

McKonly & Asbury

Tax | Assurance | Consulting | Accounting

INTRODUCTION

Josh Bantz, CPA, CCSFP, CHQP

Principal

Josh joined McKonly & Asbury in 2006 and is currently a Principal with the firm. He is a key member of the firm's System and Organization Controls (SOC) & Technology, HITRUST and Consulting practice. Josh brings over 20 years of experience in performing pre-assessment services and attestation engagements over system and organization controls.

Chris Fieger, CPA, CISA, CCSFP

Supervisor

Chris joined McKonly & Asbury in 2019 and is currently a Supervisor with the firm. He is a member of the firm's System and Organization Controls (SOC) & Technology, HITRUST and Consulting practice performing SOC 1, SOC 2, and SOC 3 engagements, as well as HITRUST assessments.

FIRM OVERVIEW

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

We provide **Advisory & Business Consulting**, **Audit & Assurance**, **Entrepreneurial Support & Client Accounting**, **Internal Audit**, **Professional Placement**, **Tax**, and **Technology** services to a variety of industries including:

Affordable Housing

Construction

Employee Benefit Plans

Family-Owned Business

Healthcare

Manufacturing & Distribution

Nonprofits

AGENDA

- What is HITRUST? History and Background
- HITRUST Common Security Framework (CSF)
- Types of HITRUST Assessments
- HITRUST Assessment Timeline
- HITRUST Reporting
- Benefits of a HITRUST Assessment
- Questions

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

WHAT IS HITRUST? HISTORY AND BACKGROUND

BACKGROUND

- **Official Name:** Healthcare Information Trust Alliance (HITRUST)
- **Formation:** 2007
- **Mission:** Make information security a focus of the healthcare industry, effectively manage data, information risk and compliance.
- **Evolution:** Moved far beyond healthcare and is now a widely adopted framework across all industries.

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.

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

HITRUST COMMON SECURITY FRAMEWORK (CSF)

WHAT IS THE 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 evaluates compliance with security and privacy controls.
  - Supports the HITRUST CSF Assessment Certification process.
  - HITRUST has various tools to assist in the assessment process (myCSF, etc.)

HITRUST CSF DEFINITIONS

Tier	Definition	Areas
Category Control	High-level categories initially based on ISO27001 & 27002	14
Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures into a particular process	49
Control Reference	**The prescriptive statements in support of the establishment and maintenance of a control to meet the business, security and regulatory goals of the organization.**	**156**
Implementation Level	Derived from NIST 800-53, these are groupings of requirement statements that address increasing risk exposure in an organization	Level 1-3
Requirement Statement	**The individual requirements statements that support achievement of Control References**	**Max of 1,900**
Domain	**Developed by HITRUST to group requirements statements into "buckets" that align with the typical technology functions of an IT Organization**	**19**
Maturity Level	Level used to determine scoring for HITRUST assessment	5 - policy, process, implemented, measured and managed

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.
  - Scored by the client and evaluated by the external assessor during an assessment.

HITRUST CSF DESIGN

- **HITRUST Control References, Requirement Statements, and Elements**
  - Example:
    - **Domain:** 01 Information Protection Program
    - **Control Reference:** Management Commitment to Information Security
    - **Requirement Statement (4 elements):**
      - A senior-level information security official
        1. is appointed.
        2. The senior-level information security official is responsible for ensuring the organization's information security processes are in place,
        3. communicated to all stakeholders, and
        4. consider and address organizational requirements.

HITRUST ASSESSMENT DOMAINS

- **HITRUST Domains**

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

HITRUST ASSESSMENT OBJECT

- **HITRUST Assessment and Assessment Object**
  - Readiness assessment – define scope, identify gaps, and how to correct (corrective action plan – CAP).
  - Define Scope - defined and scoped by the client and include relevant locations, data, and operating systems to be included in the assessment object.
  - Based upon scope and risk factors, requirement statements are generated which define the assessment object for scoring.

  NOTE: HITRUST only certifies implemented systems and does not certify facilities, people, services, or products

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

TYPES OF HITRUST ASSESSMENTS

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)

HITRUST e1 ASSESSMENT

- **HITRUST Essentials (e1) validated assessment**
  - Lowest level of assurance
  - Valid for one (1) year
  - Based upon 44 foundational security controls
  - Only covers Implemented maturity level
  - Ideal for startups and companies with a low risk-profiles

HITRUST i1 ASSESSMENT

- **HITRUST Implemented (i1) validated assessment**
  - Moderate level of assurance
  - Valid for one (1) year [rapid recertification for 2nd year]
  - Based upon 182 requirement statements
  - Suitable for mid-level organizations with robust information security programs in place
  - Only covers Implemented maturity level

HITRUST r2 ASSESSMENT

- **HITRUST Risk based (r2) validated assessment**
  - Highest level of assurance
  - Valid for two (2) years
  - Uses a tailored approach based on risks
  - Can include HIPAA, NIST 800-53, FedRAMP, as well as dozens of other authoritative sources
  - Best suited for organizations that need to demonstrate a high level of regulatory compliance

McKONLY & ASBURY

TAX | ASSURANCE | CONSULTING | ACCOUNTING

HITRUST ASSESSMENT TIMELINE

HITRUST ASSESSMENT TIMELINE

- **Typical Timeline for a HITRUST Assessment**
  - Readiness Assessment (60-90 Days)
  - Remediation Period (60 Days)
  - Assessment Period (90 Days)*
  - Quality Assurance Review (60 Days)**
  - HITRUST Validated or Certified Report Issued (30-60 days)

*Controls must be tested by External Assessor during the 90-day window

** Quality review is performed by both External Assessor QA and HITRUST

McKONLY & ASBURY

TAX | ASSURANCE | CONSULTING | ACCOUNTING

HITRUST REPORTING

HITRUST REPORTING OVERVIEW

- **Report is issued by HITRUST**
- **Report includes remediation activities tracked via corrective action plans (CAPS)**
- **Reports are all validated.**
- **Report may be certified based upon scoring results e1, i1 and r2**
  - 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 SCORING REQUIRED FOR REPORT CERTIFICATION

Framework Level	r2 Score	e1, i1 Score	Result
Requirement Statement	Greater than 70	100	No Gap
	62-70	75	Risk Acceptance – no required CAP
	Less than 62	Less than 75	GAP
Control Reference	71 or higher	80 or higher	No required CAP
	Less than 71	Less than 80	Required CAP
Domain	Greater than 70	83 or higher	Certification Achieved
	62-70	83 or higher and controls reference less than 80	Certification Achieved with likely required CAPs
	Less than 62	Less than 83	Certification Not Achieved

HITRUST REPORTING PROCESS

- **HITRUST Process for Validated Reports**
  - Selects Type of Validated Assessment (e1, i1, r2)?
  - Defines the scope for the assessment object?
  - Completes the assessment generated from assessment object?
  - Reviews and validates the assessment to ensure testing and scoring integrity?
  - Completes first quality review to validate the integrity of the testing and scoring?
  - Performs quality assurance process on the assessment?
  - Issues validated report with or without certification?

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

BENEFITS OF HITRUST ASSESSMENTS

WHY HITRUST?

- **Benefits of HITRUST Assessments for Organizations:**
  - Validated or Certified report from HITRUST
  - Could reduce Cybersecurity insurance premiums
  - 3rd party vendor risk management tool
  - Streamlined report processing and additional compliance reports

WHY HITRUST?

- **Benefits of HITRUST Assessments for Organizations (cont'd):**
  - HITRUST Assessments are used, recommended and accepted by the following:
    - 81% of Hospitals and Health Systems
    - 83% of Health Plans
    - 75% of Fortune 20 companies
    - Top 3 Cloud Providers

McKONLY & ASBURY

TAX | ASSURANCE | CONSULTING | ACCOUNTING

QUESTIONS?

CONTACT INFORMATION

Josh Bantz, CPA, CCSFP, CHQP
Principal

jbantz@macpas.com

717-413-3932

Chris Fieger, CPA, CISA, CCSFP
Supervisor

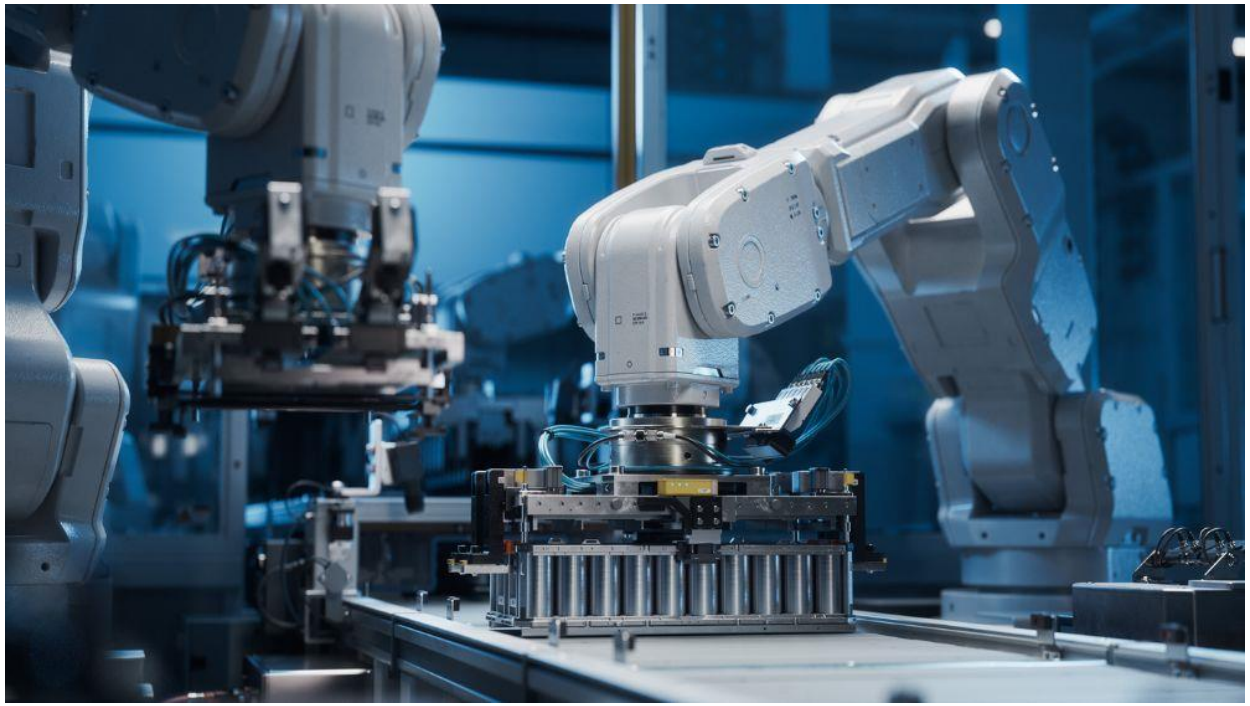
cfieger@macpas.com

717-735-3284

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

UPCOMING EVENTS

MAY 23 WEBINAR



Register Today!

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

Visit us online at **www.macpas.com** for more information.

COLLABORATE! 2024

Registration Ends April 26!

McKONLY & ASBURY
TAX | ASSURANCE | CONSULTING | ACCOUNTING

Visit us online at **www.macpas.com** for more information.