

Getting HITRUST Ready
Scope, Timeline, Key Considerations

September 2026

Getting HITRUST Ready

Meet the Presenters



Will Koernig
Senior Manager, SOC & HITRUST

704.644.4838
will.koernig@us.forvismazars.com



Ryan Boggs
Principal, SOC & HITRUST

828.989.3176
ryan.boggs@us.forvismazars.com

Agenda

1. Market pressure and the 2026 HITRUST landscape
2. e1, i1, and r2 assessments compared
3. Scoping boundaries and common missteps
4. Practical timeline from gap analysis through certification
5. Control inheritance, evidence discipline, and next steps

Learning Objectives



1. Understand key considerations for defining HITRUST scope and boundaries.
2. Outline a practical timeline for the HITRUST journey from readiness through validation.
3. Recognize common considerations related to control inheritance and evidence gathering.

Market Pressures & Outlook



Market View



HITRUST Return on Investment (ROI)

Economic Overview

Growth

- **Enhances Security & Compliance:** Prioritizing HITRUST Certification can help organizations meet stringent security and compliance standards
- **Drives Business Efficiency:** HITRUST can help streamline vendor assessments, reduce audit redundancies, and accelerate procurement
- **Builds Trust & Competitive Advantage:** By adopting a standardized, independently validated framework, organizations can demonstrate a mature security posture

Risk Management

- **Establishes a Strong Security Foundation:** A consistent, well-defined approach like HITRUST can help organizations in regulated and/or high-risk industries identify security gaps, enforce controls, and stay aligned with evolving regulations
- **Supports Audit & Compliance Confidence:** HITRUST Certification can help support organizational readiness for audits, reduce the risk of compliance violations, and lower the likelihood of data breaches
- **Helps Protect Reputation & Continuity:** By reducing risk, HITRUST can help safeguard an organization's reputation and business continuity

Operations

- **Streamlines Multi-Framework Compliance:** HITRUST's structured documentation can be reused across standards like HIPAA, SOC 2, NIST, and ISO 27001, reducing redundant work
- **Can Help Reduce Audit Preparation Time:** HITRUST customers reported a 30% reduction in audit prep time, sometimes cutting cycles from 90 to 60 days
- **Boosts Operational Efficiency:** By reducing the need for some separate audit tasks, some organizations significantly increased efficiency related to audit and compliance activities

ROI Analysis

HITRUST Costs vs. ROI

The total investment in HITRUST Certification includes initial and ongoing costs such as certification and assessor fees, application processing, and internal labor for assessment preparation and documentation.

Reduce Insurance Costs

- **Cyber Insurance Savings:** Some HITRUST-certified organizations have received a 25% discount on cyber insurance premiums, translating to significant cost savings, e.g., \$16,250 off a \$65,000 premium.
- **Improved Underwriting & Renewals:** Certification can help streamline the underwriting process, simplify renewals, and provide access to enhanced policy terms, including higher coverage limits and simplified exclusions
- **Visible ROI & Efficiency:** These insurance-related benefits can contribute to the overall ROI by reducing annual costs and administrative effort in managing cyber insurance

Mitigate Risk

- **Can Help Reduce Breach & Regulatory Costs:** HITRUST Certification can help avert the financial impact of data breaches and regulatory penalties by demonstrating due diligence and aligning with compliance standards like HIPAA
- **Helps Reduce Downtime & Operational Disruption:** With enhanced security controls and incident response readiness, HITRUST can help the organization avert unplanned downtime
- **Strengthens Organizational Resilience:** By mitigating legal, reputational, and insurance-related risks, HITRUST can help enhance overall operational stability

Improve Revenue

- **Helps Support Revenue Enhancements:** HITRUST Certification can help an organization win new business, secure renewals, and qualify for RFPs where certification is a requirement
- **Advance Sales & Market Position:** HITRUST customers have reported faster sales cycles, improved competitive differentiation, and an increased ability to command premium pricing because of their certified security posture

Six Forces Pushing HITRUST Onto the Roadmap

1. Third-Party Risk Management

One report can answer common vendor security questionnaires.

2. Contractual Obligations

Now a contract term and a condition of renewal.

3. Cybersecurity Insurance Premiums

Underwriters price on demonstrated control maturity.

4. Framework Alignment (SOC 2, ISO, PCI, NIST)

One evidence set can serve several overlapping audits.

5. Regulatory Compliance

HIPAA and state privacy laws raise the evidence bar.

6. Maintaining Certification

Recertification makes this a program, not a project.



The 2026 HITRUST Landscape

Rising Fees Force an ROI Test

Subscription and report credit fees continue to climb under CSF v11.7, so HITRUST spend now competes head-on with SOC 2 and ISO 27001 budgets.

Cost of Certifying

- MyCSF report credits run roughly \$6K for an e1 to \$9K for an r2 submission
- All-in first certification commonly lands between \$50–200K, and higher for a large enterprise r2
- Internal effort adds 150–300 hours for an e1 and 600+ for an r2
- Credits, subscription, and assessor fees all reprice at renewal

How Alternatives Compare

- SOC 2 is an annual attestation; HITRUST issues a scored certification
- ISO 27001 certifies for three years with lighter annual surveillance audits
- SOC 2 alone rarely satisfies health plan and hospital vendor credentialing
- The CSF already maps to HIPAA, NIST, ISO, and SOC 2 criteria

Making the ROI Call

- Start with what's contractually required, not a framework preference
- Measure the potential revenue the certification protects or unlocks against the total cycle cost
- Right-size the tier; an e1 or i1 may satisfy the buyer asking for HITRUST
- Use inheritance and one evidence set to reduce duplicate audit spend

HITRUST Overview



HITRUST Overview

HITRUST Alliance, founded in 2007, is a not-for-profit organization that, in collaboration with other organizations within the healthcare and technology industries, developed a common security framework called the HITRUST CSF.

HITRUST CSF has been adopted by the healthcare industry as the compliance standard for demonstrating an organization's commitment to information security, regulatory compliance, and third-party risk management.

Three primary types of HITRUST engagements:

1. e1, Foundational Assessment
2. i1, Moderate-Level Assessment
3. r2, Risk-Based, Two-Year Validated Assessment



HITRUST Framework

What is the HITRUST framework?

The foundation of all HITRUST programs and services is the HITRUST CSF, a certifiable framework that provides organizations with an efficient approach to regulatory compliance and risk management.

The HITRUST CSF rationalizes relevant regulations and standards, such as ISO 27001, NIST 800-53, NIST 800-171, HIPAA, and GDPR, into a single overarching security and privacy framework.

Since the HITRUST CSF is both risk- and compliance-based, organizations of varying risk profiles can customize the security and privacy control baselines through various factors, including organization type, size, systems, and compliance requirements.



HITRUST Alliance's HITRUST Assessments

HITRUST Readiness Assessment

- A Readiness Assessment helps organizations prepare for HITRUST compliance
- Results of Readiness Assessments are intended for management only
- Readiness Assessments can be performed for e1, i1, and r2

HITRUST Essentials, 1-Year (e1) Assessment Essentials

- The e1 is an “entry level” assessment
- The e1 has only 43 requirement statements and is not tailorable
- The e1 is designed to provide entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place
- Results can be shared externally

HITRUST Implemented, 1-Year (i1) Validated Assessment

- The i1 is a “best practices” assessment recommended for situations that present moderate risk
- The i1 has 182 requirement statements and is not tailorable
- The i1 is designed to provide higher levels of transparency, integrity, and reliability over existing moderate assurance reports, with comparable levels of time, effort, and cost
- Results can be shared externally

HITRUST Risk-Based, 2-Year (r2) Validated Assessment

- Formerly named the HITRUST CSF Validated Assessment, the r2 remains the industry “gold standard” as a risk-based and tailorable assessment that continues to provide the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, and/or other risk factors
- This assessment averages 375 requirement statements but is tailorable
- HITRUST r2 Interim and Bridge Assessments are also available
- Results can be shared externally

HITRUST Framework Recap

What does MyCSF cover?

The current MyCSF version is 11.8, which is broken down into 19 domains as follows:

01 Information Protection Program

02 Endpoint Protection

03 Portable Media Security

04 Mobile Device Security

05 Wireless Security

06 Configuration Management

07 Vulnerability Management

08 Network Protection

09 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

Drawing the Scoping Boundary

Scope Drives Cost & Timeline

The assessment scope defines what your certification covers. Draw the boundary around the systems, data, and dependencies your customers care about, and document why everything else sits outside of it.

Systems in Scope	Data & Flows	Third Parties	People & Places
• Platforms delivering the service customers buy • Supporting infrastructure and admin tooling • Environments where production data is handled	• Where PHI and sensitive data enter, rest, and leave • Interfaces, integrations, and file transfers • Backups, archives, and downstream reporting	• Cloud and hosting providers carrying your workloads • Subservice organizations and subcontractors • Controls you can inherit rather than retest	• Teams that operate or support in-scope systems • Offices, data centers, and remote work settings • Business units named in customer contracts

Common Scoping Mistakes

Where Scope Decisions Can Go Wrong

Readiness activities can help organizations identify and address these common scoping challenges.

Scoping Too Broadly

Pulling in every system the company owns inflates requirement counts, evidence volume, and fees without providing value.

Scoping Too Narrowly

A certificate that excludes the platform your customer actually uses will not clear their review, and the gap will likely surface later.

Undocumented Data Flows

Shadow integrations, ad hoc file transfers, and test data copies routinely pull systems back into scope mid-assessment.

Overlooking Inheritance

Cloud and hosting providers may already carry controls you can inherit, reducing duplicate testing and evidence effort.

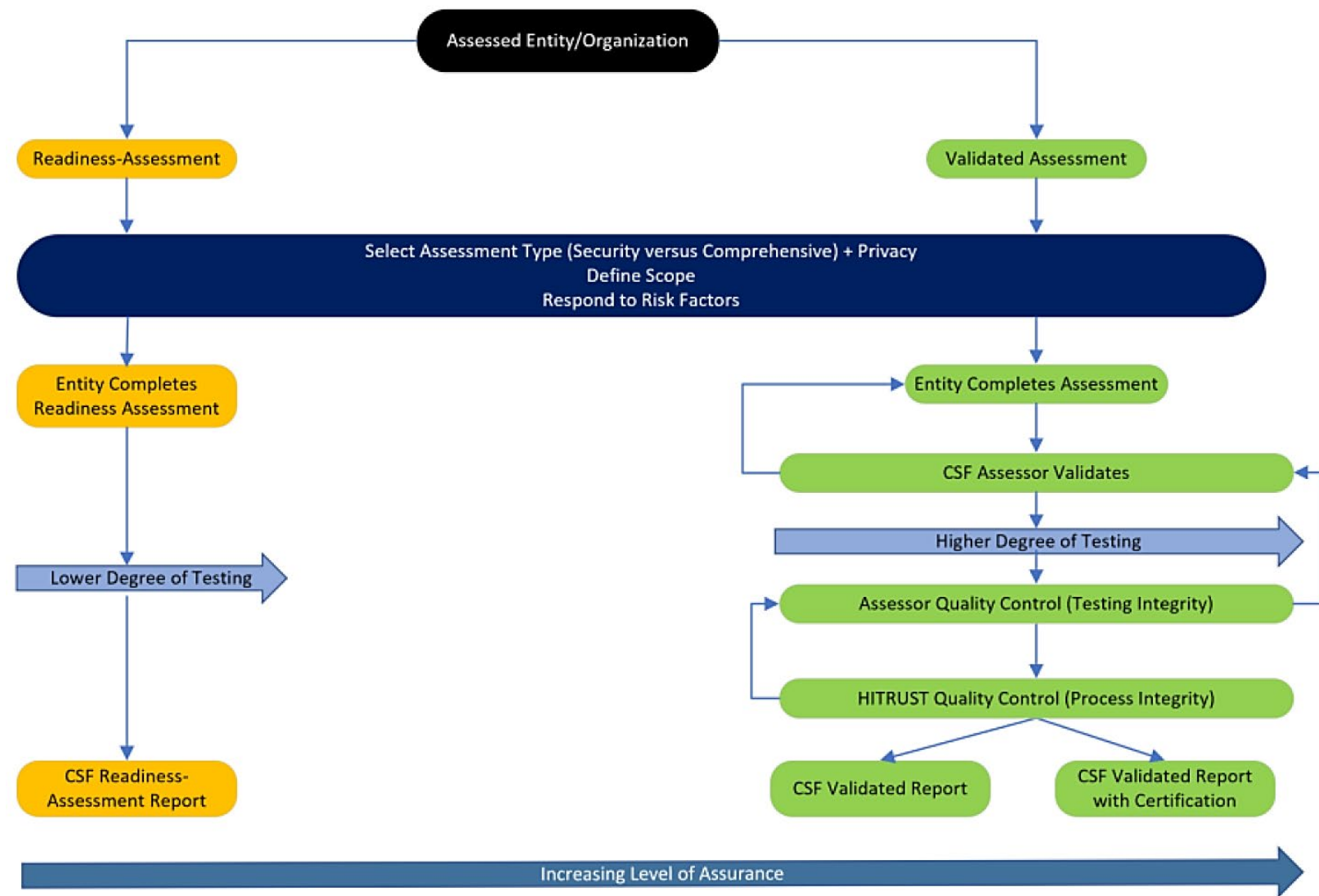
Late Scoping Factors

Changing record counts, geographies, or factor answers after work begins reopens requirements and resets the timeline.

Scoping Without Owners

Boundaries set by compliance alone may miss what engineering, sales, and legal know about how the service is really delivered.

HITRUST Engagement Process Overview



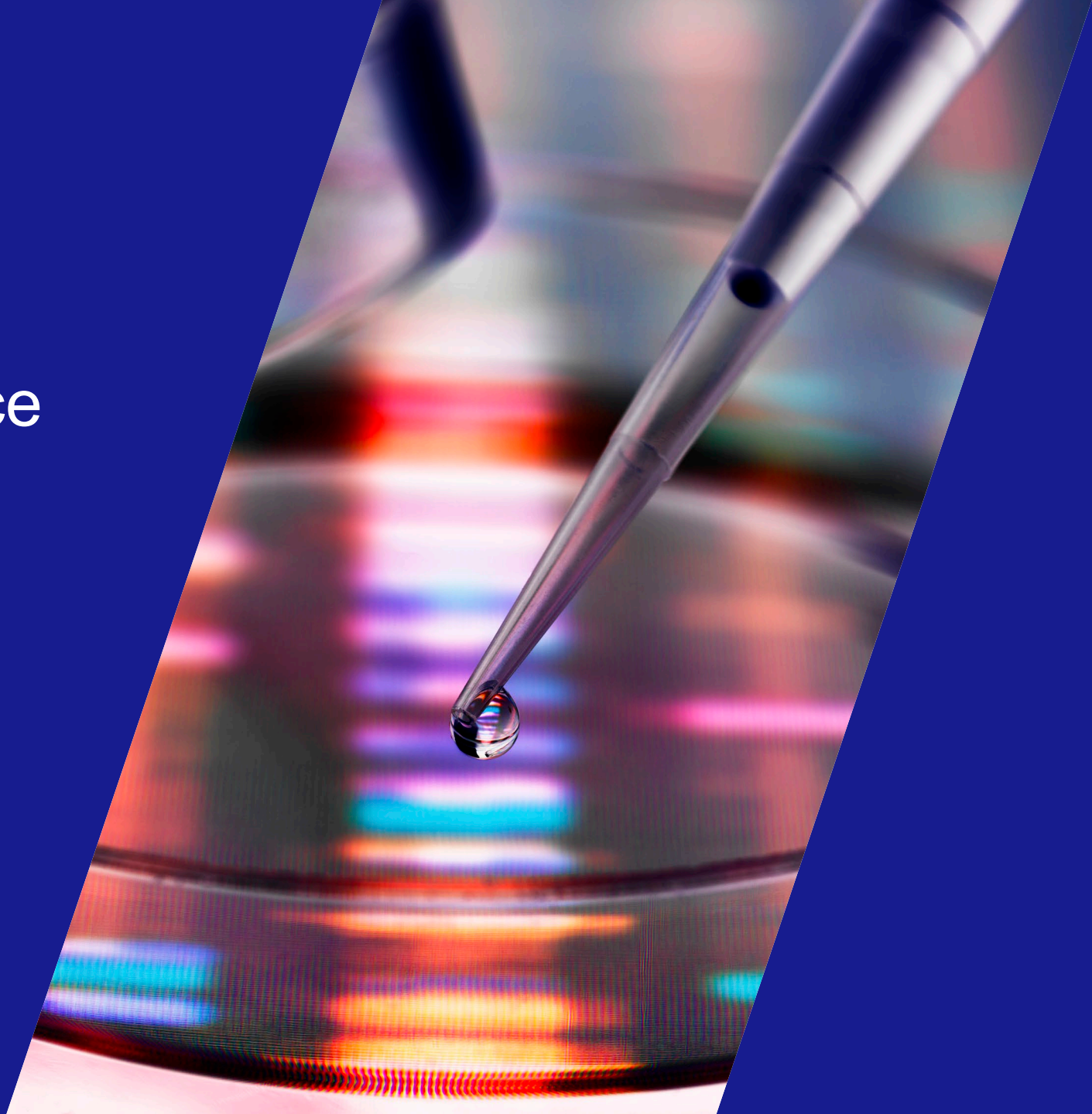
HITRUST Certification Timeline

Time to Certify Scales With Scope

Illustrative durations from kickoff through HITRUST QA and certification.



Testing Strategy & Evidence



HITRUST Documentation & Testing Basics



Engagement team members will be granted access to the client's MyCSF Tool.



Within the MyCSF Tool, HITRUST provides illustrative procedures to help Assessors evaluate each requirement statement.



Engagement team members review the documentation provided by the client and/or perform observations and draft responses for each of the maturity levels based on their interpretation of the requirement language in combination with the illustrative procedures.



These draft responses are recorded within the Assessor Comment(s) Column of the HITRUST Test Plan Workbook.



Generally, a draft response should incorporate the illustrative procedures along with additional details and results.

HITRUST Assessor Comment(s) Considerations

HITRUST reviews each validated assessment submission, so it's important to include sufficient details surrounding the procedures performed and results within the Assessor Comment(s).

For each result or conclusion drawn, there must be proper source documentation:

- **Inspections**

- Include the name of specific document(s) that was (were) inspected
- Include relevant page numbers and dates as appropriate

- **Observations/Walkthroughs**

- Include who the observation/walkthrough was performed with
- Include which system/location was specifically observed



HITRUST Engagement Best Practices

Ongoing Communication

- Provide weekly status updates
- Utilize secure portal for documentation transfers
- Ongoing assistance throughout the engagement

Our Approach

- Dedicated Team
 - Resources dedicated to the healthcare industry
 - Backgrounds in audit, compliance, and regulatory requirements
- Utilize work plan and project management to help provide timely completion



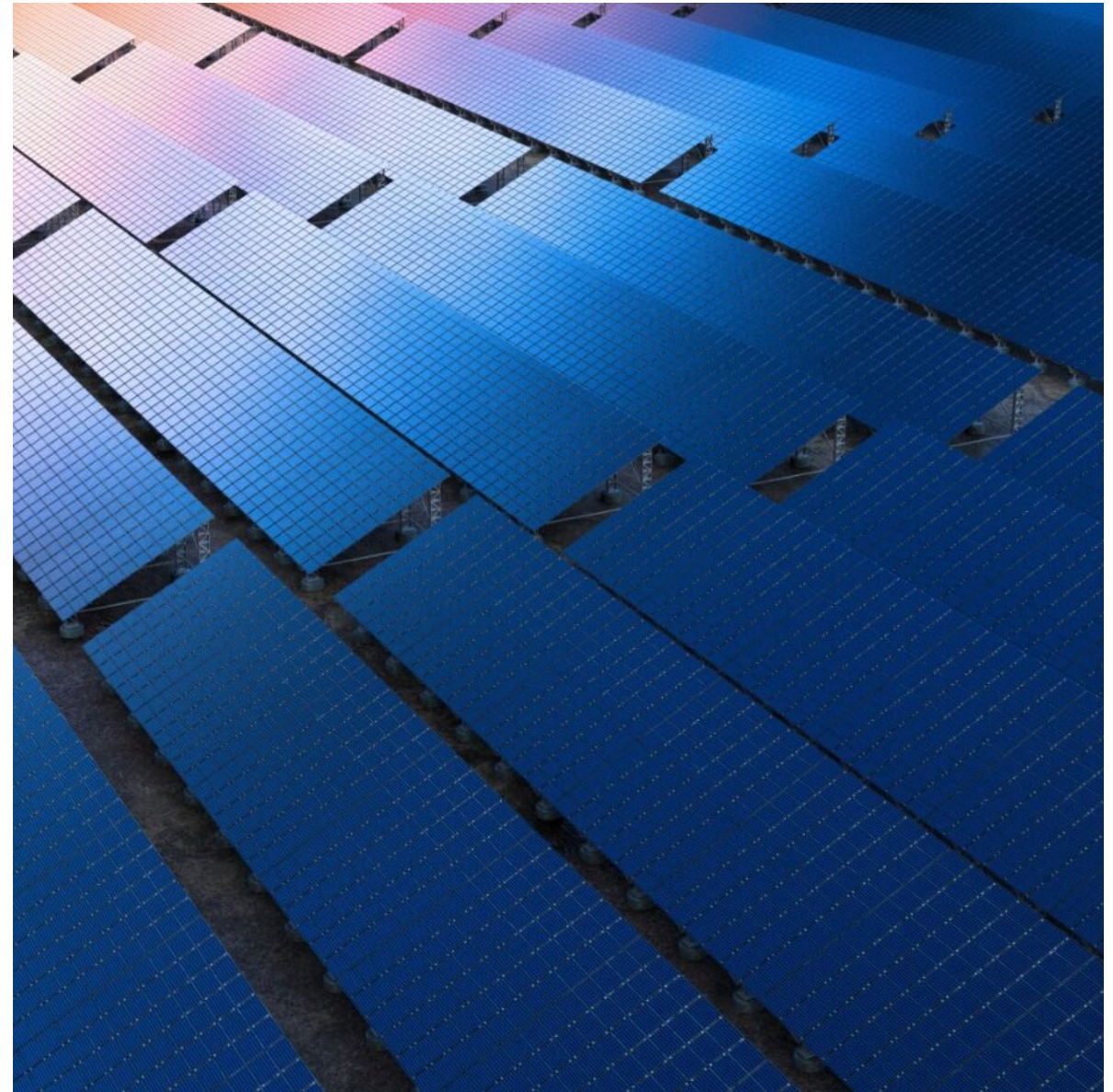
HITRUST CSF Maturity & Scoring Model

The HITRUST CSF Maturity & Scoring Model is used to evaluate each requirement statement.

Control Categories

1. Policy (15 points)
2. Procedures (20 points)
3. Implemented (40 points)
4. Measured (15 points)
5. Managed (10 points)

HITRUST has established a generic set of criteria to evaluate each requirement statement.



HITRUST Alliance Scoring Rubric

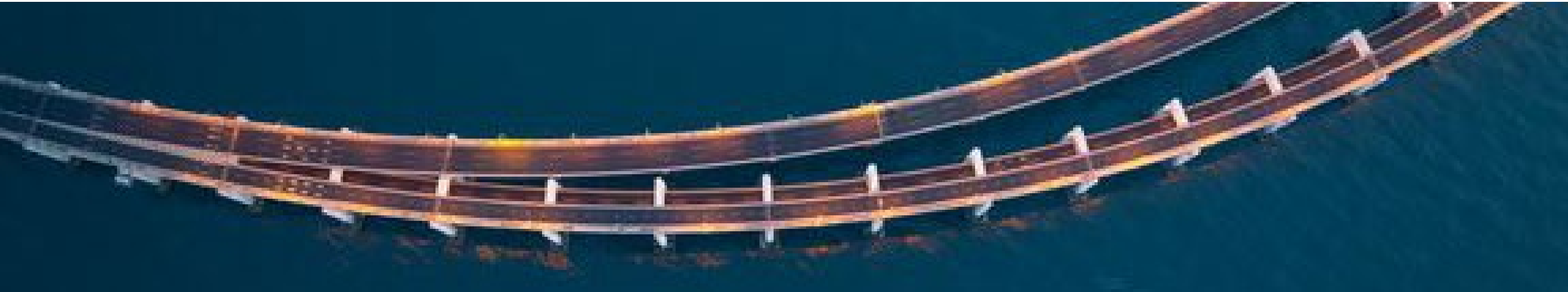
Rating (Score)	Policy	Procedure	Implemented	Measured	Managed
NC (0%)	None of the CSF requirements	None of the CSF requirements	None of the CSF requirements	No measure or metric in place	No management action taken
SC (25%)	Some CSF requirements AND ad hoc	Some CSF requirements are supported by ad hoc procedures	Some CSF requirements AND partial scope	Operational OR independent measure	Measure or metric AND management actions are sometimes taken on an ad hoc basis
PC (50%)	All CSF requirements AND ad hoc	All CSF requirements are supported by ad hoc procedures	Some CSF requirements AND full scope	Operational AND independent measure	Measure or metric AND management actions are sometimes taken AND a formal action management process exists
MC (75%)	Some CSF requirements are written/ signed AND the remainder ad hoc	Some CSF requirements are supported by written and/or automated procedures, AND the remaining CSF requirements are addressed by ad hoc procedures.	All CSF requirements and partial scope	Operational OR independent METRIC	Metric only AND corrective actions are always taken AND on an ad hoc basis
FC (100%)	All CSF requirements and written/signed	ALL CSF requirements are supported by written procedures and/or are automated	All CSF requirements AND full scope	Operational metric AND independent measure or metric	Metric only AND corrective actions always taken AND a formal remediation management process exists

Generic Evaluation Criteria

Policy

Level 1 – Policy Considerations Defined by HITRUST

- Do formal, up-to-date policies or standards exist that contain “shall” or “will” statements for each element of the requirement statement?
- Do the policies and standards that exist for each element of the requirement statement cover all major facilities and operations for the organizations and/or systems/assets in-scope for the assessment?
- Are the policies and standards that exist for each element of the requirement statement approved by management and communicated to the workforce?



Generic Evaluation Criteria Procedure



Level 2 – Procedure Considerations Defined by HITRUST

- Do formal, up-to-date, documented procedures exist for the implementation of each element of the requirement statement?
- Do the procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed?
- Do the procedures address each element of the requirement statement across all applicable facilities, operations and/or systems and assets in scope?
- Are procedures for the implementation of each element of the requirement statements communicated to the individuals who are required to follow them?

Generic Evaluation Criteria Implemented

Level 3 – Implemented Considerations Defined by HITRUST

- Is each element of the requirement statement implemented in a consistent manner everywhere that the policy and procedure applies?
- Are ad hoc approaches that tend to be applied on an individual or on a case-by-case basis discouraged?



Generic Evaluation Criteria Measured



Level 4 – Measured Defined by HITRUST

- Are self-assessments, audits, and/or tests routinely performed and/or metrics collected to evaluate the adequacy and effectiveness of the implementation of each element of the requirement statement?
- Are evaluation requirements, including requirements regarding the type and frequency of self-assessments, audits, tests, and/or metrics collection documented, approved, and effectively implemented?
- Does the frequency and rigor with which each element of the requirement statement is evaluated depend on the risks that will be posed if the implementation is not operating effectively?

Generic Evaluation Criteria

Managed

Level 5 – Managed Defined by HITRUST

- Are effective corrective actions taken to address identified weaknesses in the elements of the requirement statement, including those identified as a result of potential or actual information security incidents or through information security alerts?
- Do decisions around corrective actions consider cost, risk, and mission impact?
- Are threats impacting the requirements periodically re-evaluated and the requirements adapted as needed?



HITRUST Sampling Guidelines

Sampling Scenario	Minimum Number of Items to Test
Testing a manual control operating at a defined frequency	• Daily controls: 25 days • Weekly controls: 5 weeks • Monthly controls: 2 months • Quarterly controls: 2 quarters • Annual controls: 1 year (most recent control occurrence)
Testing a manual control operating at an undefined frequency (<i>i.e.</i> , “as needed”)	Sample size varies based on population size: • Pop. size ≥250: 25 items • Pop. size 50–249: 10% of the population, rounding up as needed • Pop. size <50: Sample size can range from a minimum of 3 items up to the entire population. Use professional judgment.
Testing an automated control (NOTE: If configured on or embedded within multiple systems/tools, each system/tool must be tested)	Can perform a test of 1 if the following are performed/met (otherwise, a full sample must be tested using the manual control sampling guidance provided above): • If configurable, the associated configuration(s) must be tested • To show that the system behaves as configured, the outcome/result of the configuration must be tested
Sampling from point-in-time populations (<i>e.g.</i> , endpoints, servers)	Observe the sampling guidance provided for the “Testing a manual control with an undefined frequency” scenario provided above.

Q&A



SOC &
HITRUST®
Solutions

Questions?

Contact

Forvis Mazars

Will Koernig

Senior Manager

704.644.4838

will.koernig@us.forvismazars.com

Ryan Boggs

Principal

828.989.3176

ryan.boggs@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.



Scan to learn more about our SOC & HITRUST® Services.