The HITRUST Assessment Handbook

Comprehensive guide on performing a HITRUST assessment

HITRUST®

Version 1.2

Table of Contents

1. Introduction

The purpose of this Assessment Handbook is to define the requirements for those organizations assessing their information protection programs against the HITRUST CSF utilizing a readiness or validated assessment. The Assessment Handbook is intended to provide guidance and expectations to Assessed Entities[1] and HITRUST External Assessors on the HITRUST assessment and certification processes. HITRUST External Assessors are expected to maintain an understanding of the requirements and Assurance Program processes defined in this Assessment Handbook. For additional details around the development of the HITRUST CSF and the HITRUST approach to risk management, please see the HITRUST Risk Management Handbook.

The Assessment Handbook assumes a baseline understanding of HITRUST, the HITRUST CSF Framework and the HITRUST Assurance Program. The following resources provide additional information about HITRUST:

- HITRUST CSF Framework
- MyCSF Help
- HITRUST Assurance Program
- Assessed Entity Resources
- External Assessor Resources
- HITRUST Academy Information

Any updates to the Assurance Program will be communicated via Advisories published at: https://hitrustalliance.net/advisories. HITRUST will provide notice of any changes to requirements in the Assessment Handbook using those Advisories. In addition, HITRUST will provide a comparison log detailing the changes outlined within those Advisories. HITRUST will provide a notice period for any changes to requirements in this Assessment Handbook to allow sufficient time for Assessed Entities and External Assessors to prepare for the change. HITRUST may include additional FAQs or Examples within the Assessment Handbook at any time to provide Assessed Entities and External Assessors with additional clarification or guidance on the requirements herein.

Terminology used within the Assessment Handbook follows the definitions in the *HITRUST Glossary of Terms and Acronyms* (accessible within MyCSF in the “References” tab and MyCSF Help), unless otherwise defined herein.

HITRUST expects all Assessed Entities and External Assessors to maintain awareness of the current Assurance Program requirements and updated requirements through this Assessment Handbook and corresponding Advisories.

[1] An “Assessed Entity” is any organization which undergoes a HITRUST assessment.

2. Background

The HITRUST CSF is an overarching security and privacy framework that incorporates and harmonizes information protection requirements, including federal, state, and international legislation; regulatory agency rules and guidance; and industry frameworks. The HITRUST Assurance Program utilizes the HITRUST CSF to include a common set of information protection requirements with standardized assessment and reporting processes which are expected to be adopted by Assessed Entities and accepted by their relying parties.

The MyCSF assessment platform incorporates the HITRUST CSF in a single tool so organizations can manage information risk and their compliance needs. The MyCSF assessment platform provides organizations of all sizes with a purposefully designed and engineered Software as a Service (SaaS) solution for performing assessments and corrective action plan management, including enhanced benchmarking and dashboards.

Organizations that would like to become HITRUST certified are expected to adopt all requirements and evaluative elements in scope for them based on the various factors defined in their assessment. Due to the granularity of the requirements within the HITRUST CSF, it is recommended that organizations perform a readiness assessment to identify their current maturity level prior to pursuing HITRUST certification.

The standard requirements, methodology, and tools developed and maintained by HITRUST in collaboration with information security and privacy professionals, enable both relying parties[2] and Assessed Entities to implement a consistent approach to third-party compliance management.

The HITRUST Assurance Program provides a practical mechanism for validating an organization's compliance with the HITRUST CSF. Utilizing the HITRUST Assurance Program, organizations can perform an assessment against the requirements contained within the HITRUST CSF. This single assessment can provide an organization insight into its maturity against the various requirements in the HITRUST CSF, legal and regulatory compliance standards, and can be used in lieu of proprietary requirements and processes to provide assurances to third parties.

The HITRUST Assurance Program allows for an organization to receive immediate and incremental value from the HITRUST CSF as it follows a logical path to certification. This Assessment Handbook includes the workflow and HITRUST expectations as an Assessed Entity and its External Assessor follow that certification path.

[2] A "relying party" is any party that accepts a HITRUST assessment report, certification letter, and/or assessment results as an attestation of an Assessed Entity's information security posture.

3. Roles & Responsibilities

The following sections describe the roles and responsibilities of HITRUST Assessed Entities and Authorized HITRUST External Assessors. Each organization has specific roles with accompanying responsibilities that must be executed for an assessment to be validated or certified by HITRUST.

3.1 Assessed Entity

Organizations that would like to become HITRUST certified are expected to meet the HITRUST CSF requirements within their information protection framework. An organization becomes an Assessed Entity once they have started the assessment process (regardless of assessment type). Under the HITRUST Assurance Program, an Assessed Entity's responsibilities include:

3.1.1 Implementing the information protection controls as required in the HITRUST CSF.

3.1.2 Maintaining the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.

3.1.3 Responding honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.

3.1.4 Providing the HITRUST External Assessor with accurate and complete records and necessary documentation related to the information protection controls included within the scope of its assessment.

3.1.5 Disclosing all design and operating deficiencies in its information protection controls of which it is aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.

3.1.6 Performing the necessary readiness and/or validated assessments to determine they are sufficiently meeting the HITRUST CSF requirements.

3.1.7 Accurately defining and communicating the scope of readiness and/or validated assessments to both its External Assessor and HITRUST.

3.1.8 Coordinating and supporting the performance of assessments and implementing corrective actions and organizational transformations, as necessary. This includes collecting evidence, personnel availability, timely and truthful communication, and overseeing the assessment timeline.

3.1.9 Funding its HITRUST assessment effort, including assessments for readiness, validation and/or certification, internal and/or external resources, and completing any corrective actions.

3.1.10 Communicating significant changes to its certified environment to HITRUST on a timely basis (For additional details on what constitutes a significant change, see Chapter 15.6 Significant Changes).

3.1.11 Communicating actual or suspected security events involving the certified environment to HITRUST and its External Assessor (see Chapter 15.3 Security Events & Fraud).

3.1.12 Performing its own due diligence prior to engaging with an External Assessor to perform its HITRUST assessment. **Although HITRUST employs processes to confirm External Assessors continue to meet HITRUST standards, HITRUST cannot guarantee that any External Assessor will**

be successful in its role on any specific engagement.

3.2 Assessors

HITRUST requires professional services firms and the individuals within those firms to meet certain requirements before receiving HITRUST's approval to perform HITRUST CSF related engagements as an Assessor. There are two types of Assessors: External and Internal. Obtaining an External or Internal Assessor status indicates the Assessor has met the requirements to perform HITRUST assessments. Each HITRUST Assessor must undergo a vetting process and demonstrate the capability to perform HITRUST assessments. The vetting process includes reviewing the Assessor's policies and procedures and the professional backgrounds of the individuals who will be performing assessments. In addition, there are two HITRUST certifications that individuals within an External or Internal Assessor firm may receive, Certified CSF Practitioner (CCSFP) and/or Certified HITRUST Quality Professional (CHQP). HITRUST has specified requirements in this Chapter on an External or Internal Assessor's utilization of individuals based on the certification type and individual's role on a validated assessment.

- CCSFP is a designation reserved for individuals who have completed the CCSFP training course, passed the certification exam, and have met the required background and experience requirements necessary to effectively use the HITRUST CSF. Such individuals typically work for a HITRUST External Assessor, an Assessed Entity, or a HITRUST licensed firm/practice that provides HITRUST consulting services.

- CHQP is a designation reserved for Certified CSF Practitioners who act in a quality assurance role on HITRUST assessment engagements, have completed the CHQP training course, and passed the CHQP certification exam. Such individuals typically work for a HITRUST External Assessor.

3.2.1 All External and Internal Assessors are required to maintain their knowledge of the HITRUST assurance process, CSF methodology and framework by having a comprehensive understanding of this Assessment Handbook and corresponding Advisories.

External Assessors

External Assessors are organizations that have been approved by HITRUST for performing assessment and services associated with the HITRUST Assurance Program and the HITRUST CSF.

3.2.2 All External Assessors must be approved by HITRUST via an application process. See External Assessors for more information on External Assessor requirements.

3.2.3 All External Assessors must employ at least 5 CCSFPs and 2 CHQPs within their organization at all times to maintain its license. HITRUST requires that the following engagement team members on a validated assessment hold the CCSFP designation:

- On-site team lead / manager responsible for assessment fieldwork
- Engagement executive
- Engagement quality assurance reviewer

3.2.4 The External Assessor Quality Assurance review for a validated assessment must be performed by the engagement team's Quality Assurance Reviewer. This individual is required to hold both a CCSFP and CHQP designation.

3.2.5 The individual acting as a validated assessment's CHQP may not perform any other duty on that assessment, such as client-facing engagement executive, fieldwork lead, etc. This requirement helps ensure that the External Assessor's pre-submission quality review is performed with objectivity.

3.2.6 To ensure the team has an appropriate understanding of the HITRUST CSF and HITRUST Assurance Program methodologies and tools, at least 50% of all validated assessment engagement hours must be performed by CCSFPs.

3.2.7 Both the engagement executive and QA reviewer must sign off on the QA checklist upon completion of their corresponding review activities.

3.2.8 Professional services firms that will only work on readiness assessments and are not External Assessors will need to obtain a readiness license.

3.2.9 Professional services firms that have a readiness license must have two individuals hold the CCSFP designation at all times to maintain its license.

There are three defined roles within an External Assessor's team that must be reported to HITRUST as part of a validated assessment, all of which must be subject matter experts in the field of information security and/or privacy and holders of HITRUST-issued certifications:

3.2.10 The Engagement Executive is the CCSFP who owns the relationship between the External Assessor firm and the Assessed Entity. This individual is expected to review and approve the engagement scope, the Test Plan, testing results, and testing documentation.

3.2.11 The Engagement Lead is the CCSFP responsible for the creation and execution of the Test Plan, performing/overseeing sampling, analyzing test results, leading walkthroughs and interviews, and coordinating the validated assessment's day-to-day fieldwork.

3.2.12 The Quality Assurance Reviewer must be a CHQP who ensures that engagement execution meets internally defined and HITRUST-defined quality assurance requirements within this Assessment Handbook, including adequacy and completeness of the working papers, appropriate treatment of exceptions, and proper definition and application of scoping decisions.

HITRUST expects that External and Internal Assessors will appropriately staff each assessment with individuals who maintain the necessary audit and technical background to appropriately perform the expected validation procedures for a HITRUST assessment. Depending on the type of assessment, different technical backgrounds may be necessary. For HITRUST assessments containing requirements specific to Artificial Intelligence (AI), External and Internal Assessors should follow the guidelines in Appendix A-17: Expected AI Expertise.

Internal Assessors

Internal Assessors are those departments or business units who facilitate the HITRUST assessment process by performing readiness / self-assessment efforts or performing testing on behalf of management of the Assessed Entity in advance of an External Assessor's validated assessment fieldwork. Internal Assessor practitioners are in-house or outsourced CCSFPs who are typically positioned within, or engaged by, an Assessed Entity's Internal Audit Department, but also may be positioned within or engaged by any department meeting specific objectivity requirements (see Chapter 3.3 Independence Requirements), resource qualification requirements, and approval by HITRUST (via the defined application process).

3.2.13 All Internal Assessors must be approved by HITRUST via an application process prior to External Assessors being able to rely on their work for a validated assessment. See Internal Assessors for more information.

3.2.14 The Internal Assessor must be competent with respect to the HITRUST CSF, the HITRUST Assurance Program requirements, and the overall HITRUST validated assessment process.

3.2.15 Internal Assessor functions must consist of at least two individuals who maintain the CCSFP designation at all times.

As mentioned above, in advance of a validated assessment, an Assessed Entity may perform assessment procedures against the HITRUST CSF internally using an Internal Assessor. The results of recently completed testing performed by Internal Assessors can — at the External Assessor's discretion — be relied upon by the External Assessor to reduce the extent of the External Assessor's direct testing. For further details around relying on Internal Assessor testing, see Chapter 12.4 Reliance on testing performed by the Assessed Entity.

3.3 Independence Requirements

Objectivity is essential for both External and Internal Assessors. However, there may be a level of complexity when an External or Internal Assessor attempts to determine their independence and objectivity during a HITRUST assessment as it involves both the fact and appearance of the specific circumstances. HITRUST has defined the following independence guidance for External and Internal Assessors during performance of a validated assessment. However, these requirements may not consider all potential situations so HITRUST encourages External and Internal Assessors to consult with HITRUST as necessary prior to performing ancillary services for an Assessed Entity:

3.3.1 The External Assessor firm used for a validated assessment must be a separate legal entity from the Assessed Entity.

3.3.2 The External or Internal Assessor function must be independent of the business functions being assessed. Independence requires there be no overlap in responsibilities, staffing, ownership of the controls, or reporting between the business functions being assessed and the External or Internal Assessor function.

3.3.3 Ownership of the policies and procedures being assessed must be independent from the External or Internal Assessor function.

3.3.4 Management of the Assessed Entity must not be able to restrict the nature, scope, and extent of testing determined to be required by the External or Internal Assessor.

3.3.5 External or Internal Assessor personnel involved (in the prior 12 months) in the implementation or operation of Assessed Entity controls evaluated within a HITRUST validated assessment may not work on the validated assessment for that Assessed Entity. A separate team (including a separate engagement executive / partner) must be brought in for the validated assessment effort.

3.3.6 External or Internal Assessor personnel involved in a HITRUST validated assessment may perform consulting or evaluation services for the Assessed Entity, such as the following:

- HITRUST policy and/or procedure consulting assessments (excluding remediation activities, such as writing an Assessed Entity’s policies and/or procedures)
- Penetration testing (excluding remediation activities that involve implementation or operation of a control)
- Vulnerability scanning (excluding remediation activities that involve implementation or operation of a control)
- HITRUST readiness / gap assessments (excluding remediation activities that involve implementation or operation of a control)

4. Assessment Types

HITRUST has multiple assessment types that an organization may pursue to determine its maturity level, including the r2, i1, e1, and targeted assessments.

- HITRUST Risk-based, 2-year (r2) Assessment: A risk-based and tailorable assessment that provides the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. The r2 provides a high level of assurance that focuses on a comprehensive risk-based specification of controls with an expanded approach to risk management and compliance evaluation.

- HITRUST Implemented, 1-year (i1) Assessment: A cybersecurity assessment inclusive of Information Technology controls generally recognized as leading cybersecurity practices that allows for the optional addition of other authoritative sources available through the HITRUST CSF. The i1 provides a moderate level of assurance that addresses cybersecurity leading practices and a broader range of active cyber threats than the e1 assessment.

- HITRUST Essentials, 1-year (e1) Assessment: A cybersecurity assessment that focuses on a curated set of cybersecurity controls encompassing fundamental cybersecurity practices, or “good cybersecurity hygiene” that allows for the optional addition of other authoritative sources available through the HITRUST CSF. The e1 provides entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place.

- Targeted assessment: A non-certifiable self-assessment which consists only of HITRUST requirement statements that map to one or more authoritative sources (e.g., NIST 171, FedRAMP, HIPAA). The authoritative source(s) for this assessment is selected by the Assessed Entity.

HITRUST refers to the r2, i1, and e1 as a traversable portfolio, meaning the portfolio builds on the baseline requirement statements within each assessment type starting with the e1. All requirements within the e1 assessment are included within the i1, and all requirements within the i1 are included within the baseline requirements of the r2 assessment.

HITRUST also offers Insights Reports (e.g., HIPAA, AI Risk Management) or additional certifications (e.g., NIST CSF, ai1, ai2) when assessing requirement statements where the authoritative source has been selected as a Compliance Factor within the r2, i1 or e1 assessment and the source is available for an Insights Report or certification. For additional information on these report types, see Chapter 15.1 HITRUST Reporting.

The following table further details the characteristics and differences between the r2, i1, and e1 assessments.

Characteristic	e1	i1	r2
Deliverables			

Can result in a HITRUST-issued certification (i.e., HITRUST certifiable)	Yes	Yes	Yes
Length of certification	1 year	1 year	2 years
Final reports resulting from the assessment can be shared through the HITRUST Assessment XChange and assessment results can be shared through the HITRUST Results Distribution System	Yes	Yes	Yes
Can result in a HITRUST-issued certification over the NIST Cybersecurity Framework	No	No	Yes
Can result in a HITRUST-issued certification over Artificial Intelligence (AI)	Yes	Yes	Yes
Can result in Insights Reports over select authoritative sources	Yes	Yes	Yes
Assessments			
Readiness assessments and validated assessments can be performed	Yes	Yes	Yes
Requires an Authorized HITRUST External Assessor to inspect documented evidence to validate control implementation	Yes	Yes	Yes
Leverages the HITRUST Control Maturity Scoring Rubric	Yes	Yes	Yes
Assessor's validated assessment fieldwork window (maximum)	90 days	90 days	90 days
HITRUST CSF requirements performed by the assessed entity's service providers (such as cloud service providers) on behalf of the organization can be carved out / excluded from consideration	Yes	Yes	No
Personnel from either Assessed Entity or their External Assessors are allowed to enter control maturity scoring and assessment scoping information	Yes	Yes	No
Requires an interim assessment	No	No	Yes
Can be bridged through a HITRUST bridge certificate	No	No	Yes
Must use the most current version of the CSF available at time of assessment creation	Yes	Yes	No
CSF Report Subject Matter			
Threat-adaptive assessment	Yes	Yes	Yes*
Includes HITRUST CSF requirements specifically tailored to the assessment scope	No	No	Yes
Can be tailored to optionally convey assurances over dozens of information protection regulations and standards (e.g., HIPAA, PHIPA, NIST AI RMF & ISO/IEC 23894).	Yes**	Yes**	Yes
Can be tailored to include privacy	No	No	Yes
**For HITRUST CSF v11 and later*			
*** The e1 and i1 can include certain regulations and standards when performing a combined assessment for*			

the available authoritative sources.

This Assessment Handbook defines the Assessed Entity and External Assessor responsibilities and HITRUST requirements for readiness, validated, bridge, rapid assessment, and interim assessments related to the r2, i1, and e1 assessment types.

4.1 Readiness Assessments

For r2, i1, or e1 assessments, organizations may choose to perform a readiness assessment using the standard methodology, requirements, and tools provided under the HITRUST Assurance Program.

HITRUST does not perform a quality assurance review of the results of the readiness assessment. A readiness assessment is useful for Assessed Entities to identify and remediate gaps prior to performance of a validated assessment and demonstrate progress toward assessment milestones.

For r2 readiness assessments, the Assessed Entity first completes a risk-based scoping questionnaire within MyCSF that drives control selection and assessment scope based on General, Organizational, Geographical, Systematic, and optional Compliance factors. Upon completion of the scoping questionnaire, a customized set of HITRUST CSF control references and requirement statements are automatically generated.

For an i1 or e1 readiness assessment, the i1 and e1 requirement statements are pre-defined and the organization may optionally add authoritative sources which will add additional requirement statements.

The Assessed Entity, or its designee, enters responses for each requirement statement and determines the level of compliance for each of the five control maturity levels for the r2 and the *Implemented* maturity level for the i1 or e1 (see Chapter 9 Control Maturity Levels for additional information on the control maturity levels). The Assessed Entity, or its designee, also may generate and/or respond to corresponding Corrective Action Plans (CAPs)/Gaps within the assessment.

Once the Assessed Entity, or its designee, has determined and entered compliance scores for the corresponding control maturity level across all requirement statements, the Assessed Entity may submit the populated MyCSF object to HITRUST for report generation. This is an optional step, as Assessed Entities may choose to perform the readiness work to identify their gaps and may not require the final report. Please note that readiness assessments do not undergo HITRUST Quality Assurance review so they will have a lower level of reliability. For additional information on utilizing HITRUST reports to manage vendor risk, see additional information within the HITRUST Third-Party Risk Management Program.

4.2 Validated Assessments

Organizations are required to perform a r2, i1, or e1 validated assessment to obtain a HITRUST certification. HITRUST validated assessments can be leveraged by organizations of any size or complexity and include testing performed by an authorized HITRUST External Assessor.

For a r2 validated assessment, the Assessed Entity begins by completing the risk-based scoping questionnaire in the MyCSF tool. Upon completion of the scoping questionnaire, a customized set of HITRUST CSF control references and requirement statements will be generated.

For an i1 or e1 validated assessment, the i1 and e1 requirement statements are pre-defined and the organization may optionally add authoritative sources to perform a combined assessment of the authoritative source alongside the i1 or e1 requirement statements. In an i1 or e1 validated assessment, the requirement statement scores for any added authoritative sources do not impact scoring towards achievement of the underlying i1 or e1 certification.

For the r2, i1, and e1 validated assessments, the Assessed Entity, or its designee, responds to the requirement statements and determines the level of compliance for each of the five control maturity levels for the r2 and the *Implemented* maturity level for the i1 or e1 (see Chapter 9 Control Maturity Levels for additional information). Once the Assessed Entity, or its designee, has determined and entered compliance scores for each control maturity level across all requirement statements, it submits the populated MyCSF object to its External Assessor for validation.

The External Assessor will validate the scores using its testing procedures, which it documents within MyCSF (see Chapter 11 Testing and Evidence Requirements for additional details). Upon completion of the External Assessor validation procedures and any necessary score adjustments, the Assessed Entity will sign the Management Representation Letter and Validated Report Agreement, and provide any necessary Corrective Action Plans (CAPs). The External Assessor will validate the CAPs (see criteria 13.9.7 in Chapter 13.9 CAPS and Gaps) and submit the assessment to HITRUST.

After submitting the validated assessment, HITRUST will perform Quality Assurance (QA) procedures (during the Assessed Entity's reservation block) to validate the submission. If there are questions during QA, HITRUST will coordinate directly with the Assessed Entity and/or External Assessor to address them. After successful completion of QA, the Assessed Entity will receive draft reports for their review (see Chapter 14 Undergoing Quality Assurance for additional details).

Upon successful completion of the validated assessment and meeting the scoring threshold for certification, Assessed Entities will receive their HITRUST certification reports along with any add-on certification reports. Additionally, after all other reports are finalized, if any Compliance Factors eligible for an Insights Report were included within an r2 assessment, the Assessed Entity may optionally request an Insights Report which details the organization's coverage and conformity with the associated authoritative source. For the i1 and e1, if a combined assessment was performed, the Assessed Entity will receive Insights Report(s) corresponding to each authoritative source which was assessed.

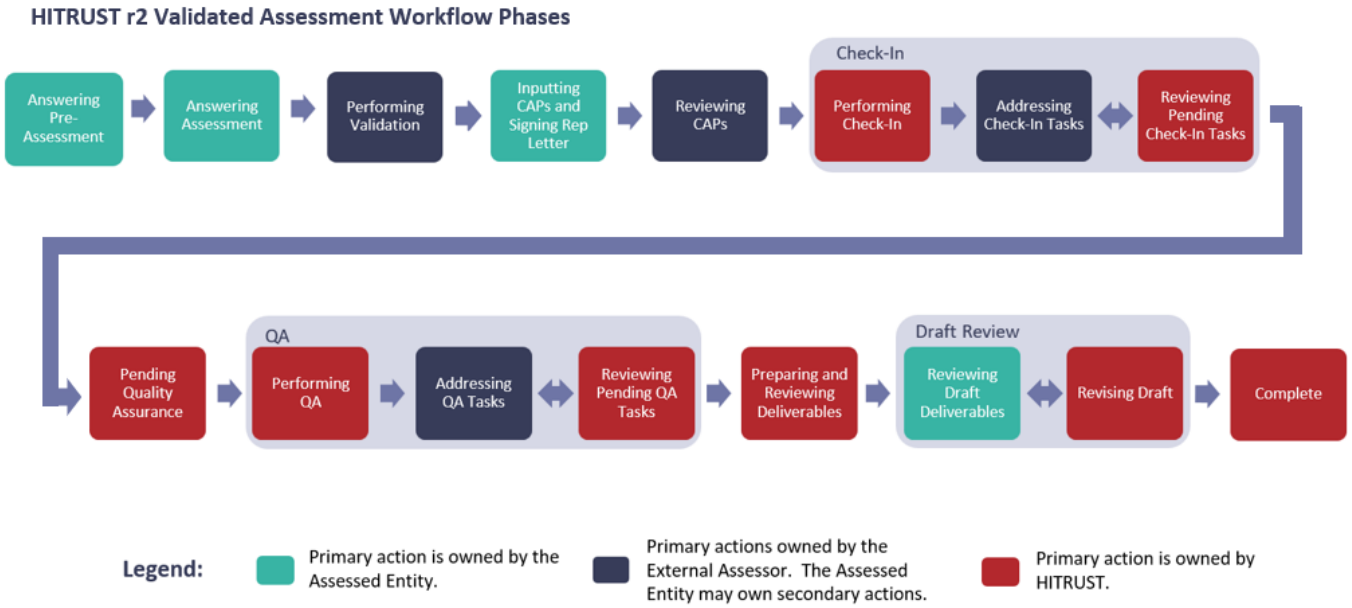
For the any validated assessment, if the scoring thresholds for certification were not , the Assessed Entity will receive a ‘validated-only’ report, which does not include a certification letter. For additional information on the HITRUST reports issued for each assessment type, see Chapter 15.1 HITRUST Reporting.

5. HITRUST Assessment Workflow

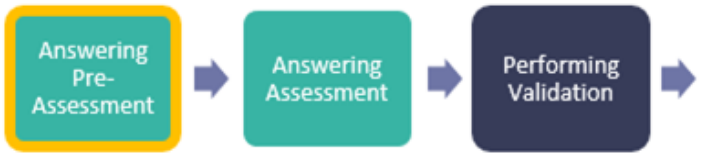
The following chapters outline the assessment workflows for validated, readiness, interim, and bridge assessments, along with the dashboards and notifications available to facilitate the tracking of assessment progress via the workflows.

5.1 r2 Validated Assessment Workflow

The assessment workflow for HITRUST r2 validated assessments is comprised of 16 workflow phases. The following diagram displays the workflow phases, including the primary owner of each phase. All phases are performed sequentially, and each phase owner should allot the necessary time to perform the corresponding responsibilities in each phase to complete their assessment in a timely manner. A brief description and summary of each phase is included below, but note that many of the phases are described in more detail with the necessary requirements in corresponding sections of this Handbook.



Answering Pre-Assessment



When an Assessed Entity creates a new assessment object, it begins the assessment process by entering key preliminary information. After completing these fields, MyCSF will be able to generate its assessment.

The Assessed Entity must complete each of the following pre-assessment webforms within MyCSF:

- Name & Security
- Organization Information

- Assessment Options
- Scope of the Assessment
- Default Scoring Profile
- Factors

For additional information on the pre-assessment, see Chapter 6 Pre-Assessment.

Answering Assessment

The Assessed Entity, or its designee, must accurately respond to each requirement statement in the assessment based upon the HITRUST control maturity model. For additional information on the control maturity levels, see Chapter 9 Control Maturity Levels.

The Assessed Entity will use the HITRUST Control Maturity Scoring Rubric to determine scores for each control maturity level across the assessment. When a requirement statement is marked “not applicable”, the Assessed Entity includes commentary within the ‘Subscriber Comment’ field in MyCSF explaining why the requirement statement is not applicable to the scope of the assessment. This commentary will appear in the assessment report. For additional information on requirement statements and scoring, see Chapter 8 Requirement Statements and Chapter 10 HITRUST Scoring Rubric.

The Assessed Entity will resolve all triggered potential quality issues (PQIs) by either following the recommendations to address the issue or by choosing to override the issue (with explanation). All overridden PQIs are subject to HITRUST QA review (see Chapter 13.4 Automated Quality Checks for additional information on PQIs). During this phase, the Assessed Entity is advised, but not required, to book its QA Reservation and begin the process of completing the Validated Report Agreement webform.

Performing Validation

In this phase, the External Assessor will validate the information input by the Assessed Entity. First, the External Assessor must review and approve the content of each pre-assessment section before being allowed to link documentation or agree to requirement statement scoring within the assessment. The

External Assessor must review requirement statements scoring, link relevant documentation, and address any PQIs that have been triggered. The External Assessor is required to complete the Test Plan, Audits and Assessments Utilized page, External Assessor Time Sheet, and the QA Checklist. The QA Checklist should be utilized throughout this process to ensure all the necessary activities are being properly completed. The External Assessor should remind the Assessed Entity to complete the Validated Report Agreement and Management Representation letter ("Rep Letter") during the upcoming phases.

For additional details and guidance on External Assessor expectations see Chapter 13 Assessment Submission Process.

Inputting CAPs and Signing Rep Letter

In this phase, the Assessed Entity must complete the Validated Report Agreement (VRA) and Rep Letter. For additional information on the VRA and Rep Letter, see Chapter 13.3 Validated Report Agreement and Chapter 13.8 Management Representation Letter. Any requirement statements requiring CAPs will be identified in MyCSF, and the Assessed Entity must enter the required CAPs. For additional information on CAPs, see Chapter 13.9 CAPs and Gaps.

Reviewing CAPs

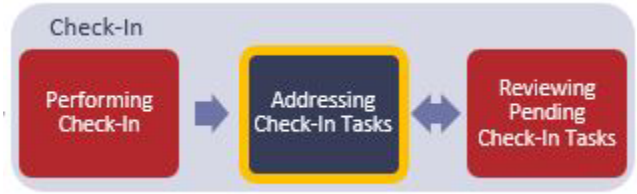
In this phase, the External Assessor must review the linked CAPs. The Assessed Entity can also demonstrate progress against the CAPs. All CAPs must include the information defined in criteria 13.9.4 (see Chapter 13.9 CAPs and Gaps) for the External Assessor to document its approval using the "thumbs up" button in MyCSF. Clicking the "thumbs up" button will change the requirement statement-level response status to "CAP Review Completed." For CAPs that do not meet the review criteria, the External Assessor will disapprove, using the "thumbs down" button, which reverts the requirement statement back to the Assessed Entity. Once the External Assessor agrees with all the CAPs, they will submit the assessment to HITRUST. For additional information on CAPs, see Chapter 13.9 CAPs and Gaps.

Performing Check-In

During this phase, HITRUST performs automated Quality Assurance (QA) checks and a high-level review of the assessment, accompanying required documents, and webforms (Organization Information, Scope of the Assessment, Factors, Validated Report Agreement, Rep Letter, Test Plans, External Assessor Time Sheet, QA Checklist, and Audits and Assessments Utilized) to determine if the assessment is ready for a HITRUST QA Analyst to review.

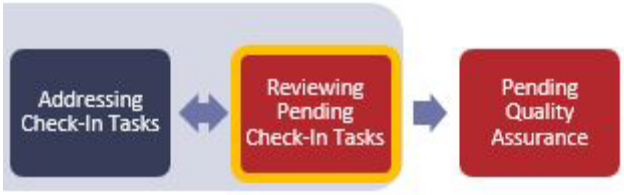
For additional information on the check-in process and potential scenarios, see Chapter 13.10 Check-in Process.

Addressing Check-In Tasks



During this phase, the Assessed Entity and/or External Assessor must address and send back all the tasks to HITRUST if any were identified during the *Performing Check-In* phase.

Reviewing Pending Check-In Tasks



In this phase, HITRUST reviews all tasks addressed by the Assessed Entity and External Assessor. HITRUST will close the tasks that have been resolved and, if all tasks have been resolved, accept the assessment after which the assessment moves into the *Pending Quality Assurance* phase. HITRUST will send any tasks requiring additional attention back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing Check-In Tasks* phase. All check-in items must be resolved by the beginning of the reserved QA block or the assessment's QA reservation will be canceled

and the Assessed Entity will be required to make a new QA reservation.

For additional information on check-in tasks, see Chapter 13.11 Addressing Check-in Tasks.

Pending Quality Assurance

In this phase, HITRUST assigns the assessment to a HITRUST QA Analyst. The HITRUST QA Analyst will begin QA during the week of the reserved QA Block.

Performing QA

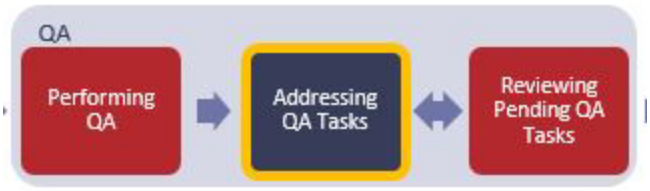
In this phase, the HITRUST QA Analyst will begin QA and review the following:

- The Pre-Assessment
- Required Documents and Webforms
- Risk-based sample of scored requirement statements
- All requirement statements marked as Not Applicable (N/A)
- Requirement statements with *Measured* and *Managed* scores
- Overridden PQIs
- CAP Responses

The HITRUST QA Analyst creates and enters all tasks from their review in MyCSF and the assessment moves to the *Addressing QA Tasks* phase.

If the QA review identifies higher volume and/or severity of concerns in an assessment than is typically expected, HITRUST will notify the External Assessor and Assessed Entity that the assessment will require further internal management review within HITRUST. After the internal management review has been completed, the assessment will either continue the normal QA process or move to Escalated QA. For further details on the QA process, see Chapter 14 Undergoing QA.

Addressing QA Tasks



In this phase, the Assessed Entity and External Assessor address the tasks opened by HITRUST. If the action taken to address a task adds new required CAPs to the assessment, those CAPs must be entered by the Assessed Entity and reviewed by the External Assessor. Similarly, if an action taken to resolve a task adds additional requirement statements those must be scored by the Assessed Entity and validated by the External Assessor. When all tasks have been returned to HITRUST and all new requirement statements and / or CAPs have been reviewed by the External Assessor, the assessment automatically enters the *Reviewing Pending QA Tasks* phase. For further details on the QA process, see Chapter 14 Undergoing QA.

Reviewing Pending QA Tasks

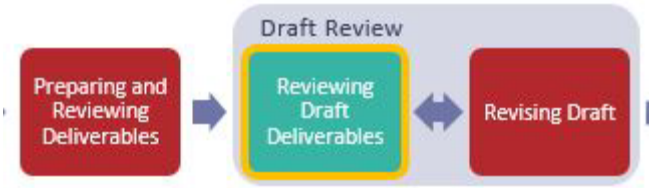
During this phase, the HITRUST QA Analyst will review the QA Tasks addressed by the Assessed Entity and External Assessor. HITRUST will send any tasks that still require attention back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing QA Tasks* phase. HITRUST will close all tasks that have been resolved. After all QA Tasks have been resolved by the Assessed Entity and /or External Assessor and closed by HITRUST, the assessment will move to the *Preparing and Reviewing Deliverables* phase. For further details on the QA process, see Chapter 14 Undergoing QA.

Preparing and Reviewing Deliverables

In this phase, HITRUST will prepare and review the draft reports. If any questions arise during this phase, the HITRUST QA Analyst creates additional tasks and the assessment returns to the Addressing QA Tasks phase. The HITRUST QA Analyst will upload the draft report(s) to MyCSF once the draft reports are

internally reviewed by HITRUST and all follow-up questions are resolved. The assessment will then enter the *Reviewing Draft Deliverables* phase. For additional information on reporting, see Chapter 15 Reporting & Maintaining a HITRUST Certification.

Reviewing Draft Deliverables



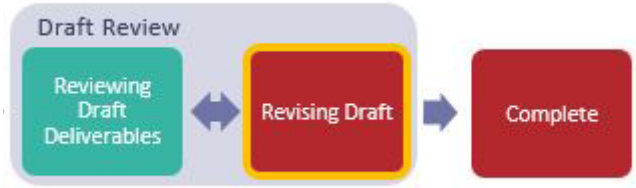
In this phase, the Assessed Entity has up to 30 days to review the draft reports. After the Assessed Entity has reviewed the draft reports, it may either:

- Approve the draft reports by clicking the “Approve HITRUST CSF Draft Report” button within the HITRUST CSF Reports section of the assessment.
- Or Request Revisions in MyCSF (see Chapter 15.1 HITRUST Reporting for additional details on the revision process).

If the Assessed Entity does not approve the draft reports or request revisions within 30 days, the draft reports are automatically approved by MyCSF, and the assessment enters the *Revising Draft* phase.

For additional information on reporting, see Chapter 15 Reporting & Maintaining a HITRUST Certification.

Revising Draft



In this phase, the HITRUST QA Analyst reviews any requested revisions and updates the status of each request to Completed, or Not Accepted by HITRUST. After processing any revision requests, HITRUST will return the assessment to the *Reviewing Draft Deliverables* phase for the Assessed Entity to either approve the revised draft reports or request additional revisions.

The HITRUST QA Analyst will also provide an explanation within the “Rationale” section if any revision request is Not Accepted.

When the assessment enters the *Revising Draft* phase due to the Assessed Entity approving the draft

reports, the HITRUST QA Analyst builds the final reports and uploads them into MyCSF. For additional information on reporting, see Chapter 15 Reporting & Maintaining a HITRUST Certification.

Complete

When the final HITRUST CSF reports are uploaded, the assessment enters the *Complete* phase.

In the Complete phase, if any Compliance factors eligible for an Insights Report were included within the assessment, the Assessed Entity may optionally request the associated Insights Reports. This is done by selecting the desired authoritative sources on the Insights Reports page within the assessment. Each Insights Report will require an Insights Report Credit to request. The Assessed Entity may contact their HITRUST Customer Success Manager (CSM) to acquire any necessary credits.

After the necessary credits have been acquired and the Insights Reports have been requested, the Assessed Entity will have the opportunity to review the draft Insights Reports and request revisions or approve the reports. Once approved, the final Insights Reports will be available within MyCSF.

Press Kit Distribution

When an Assessed Entity receives its first certification (and upon request for additional certifications), the HITRUST Marketing team will distribute a HITRUST certification press kit within 10 business days that includes:

- HITRUST Certification Announcement Guidelines comprised of instructions for a customized press release, logo usage, and additional media support information.
- HITRUST Certification Press Release Template containing approved content and pre-approved quotes from a HITRUST executive. NOTE: The scope of the Assessed Entity's HITRUST certification is required to be included in the press release.
- Certification Logo

The HITRUST certification press release requires a final approval from HITRUST prior to publishing. The Assessed Entity must send the press release draft to PR@hitrustalliance.net for final review.

Assessment Object Archiving

The MyCSF archive process for assessment objects is initiated only if the Assessed Entity's account has expired for 60 days OR a user attempts to delete an object that is certified. After the archive process is

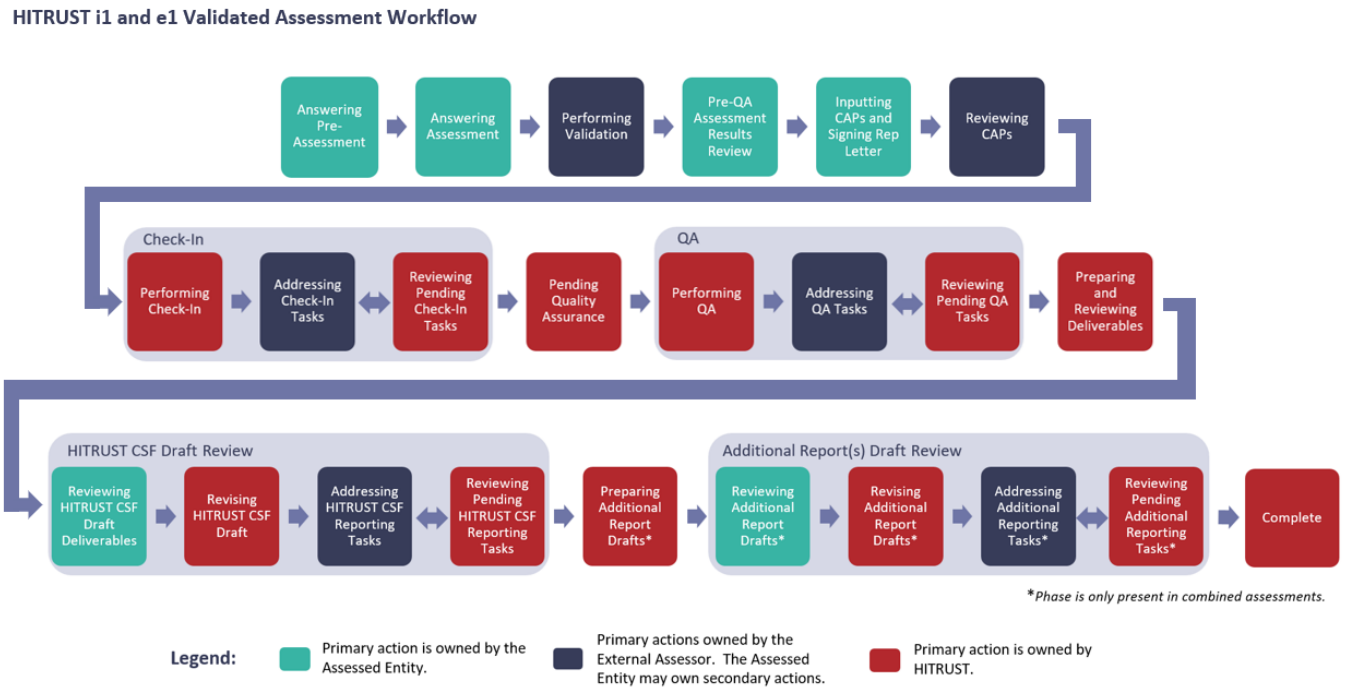
initiated:

- For all certified assessment objects, the deletion date is set to 2 years + 6 months after the final report date.

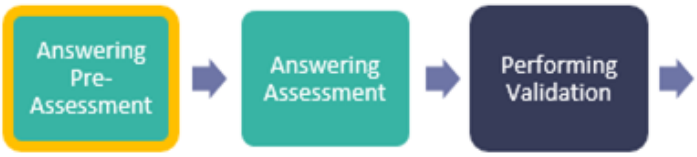
- For all other assessment objects (e.g., readiness assessments, validated-only (i.e., non-certified) assessments, or assessments in progress) the deletion date is set to 6 months after the current date. NOTE: For non-certified assessments, the user may mark the object for deletion on the current day.

5.2 i1 and e1 Validated Assessment Workflow

The assessment workflow for HITRUST e1 and i1 validated assessments is comprised of 24 workflow phases. The following diagram displays the workflow phases, including the primary owner of each phase. All phases are performed sequentially. Each phase owner should allot enough time to perform the corresponding responsibilities specified in each phase to complete the assessment in a timely manner. A brief description and summary of each phase is included below.



Answering Pre-Assessment



When an Assessed Entity creates a new assessment object, it begins the assessment process by entering key preliminary information. After completing these fields, MyCSF will be able to generate its assessment.

The Assessed Entity or the External Assessor must complete each of the following pre-assessment webforms within MyCSF:

- Name & Security
- Organization Information
- Assessment Options

- Scope of the Assessment
- Default Scoring Profile
- Factors

If the Assessed Entity would like to perform a combined assessment of an authoritative source within an i1 or e1, the Compliance factor for the authoritative source must be selected on the Factors page.

For additional information on the pre-assessment, see Chapter 6 Pre-Assessment.

Answering Assessment

The Assessed Entity or External Assessor must accurately respond to each requirement statement in the assessment based upon the *Implemented* control maturity model. For additional information on the control maturity levels, see Chapter 9 Control Maturity Levels.

The Assessed Entity and External Assessor will use the HITRUST Control Maturity Scoring Rubric to determine scores for each control maturity level across the assessment. When a requirement statement is marked “not applicable”, the Assessed Entity includes commentary within the ‘Subscriber Comment’ field in MyCSF explaining why the requirement statement is not applicable to the scope of the assessment. This commentary will appear in the assessment report. For additional information on requirement statements and scoring, see Chapter 8 Requirement Statements and Chapter 10 HITRUST Scoring Rubric.

The Assessed Entity will resolve all triggered potential quality issues (PQIs) by either following the recommendations to address the issue or by choosing to override / accept the issue (with explanation). All overridden / accepted PQIs are subject to HITRUST QA review (see Chapter 13.4 Automated Quality Checks for additional information on PQIs). During this phase, the Assessed Entity is advised, but not required, to book its QA Reservation and begin the process of completing the Validated Report Agreement webform.

Performing Validation

In this phase, the External Assessor will validate the information input during the *Answering Assessment*

phase. First, the External Assessor must review and approve the content of each pre-assessment section before being allowed to link documentation or agree to requirement statement scoring within the assessment. The External Assessor must review requirement statements scoring, link relevant documentation, and address any PQIs that have been triggered. The External Assessor is required to complete the Test Plan, Audits and Assessments Utilized page, External Assessor Time Sheet, and the QA Checklist. The QA Checklist should be utilized throughout this process to ensure all the necessary activities are being properly completed. The External Assessor should remind the Assessed Entity to complete the Validated Report Agreement and Management Representation Letter ("Rep Letter") during the upcoming phases.

For details on the guidance on External Assessor expectations see Chapter 13 Assessment Submission Process.

Pre-QA Assessment Results Review

In this phase, the Assessed Entity and External Assessor review and approve the pre-QA assessment results page. The pre-QA assessment results are an indication of the point-in-time results of the assessment and are subject to change based on the HITRUST QA review of the assessment. Additionally, the pre-QA assessment results do not guarantee that the assessment will successfully pass QA and result in report issuance (see Chapter 14.4 Escalated QA).

The Pre-QA Assessment Results page includes:

- For the i1 or e1 core requirement statements:
  - The average score for each Assessment Domain (considering only the i1 or e1 core requirement statements) and an indication of whether CSF certification can be achieved based on the domain scores.
  - Listing of Requirement Statements that will be identified as CAPs and gaps in the i1 or e1 HITRUST CSF Report.

- In combined i1 or e1 assessments, for each Compliance factor:
  - Listing of Requirement Statements that will be identified as control observations in the associated Insights Report.

The Assessed Entity and External Assessor must both review and approve or reject the pre-QA assessment results. If either party rejects the results, the assessment will automatically return to the Performing Validation phase. If both parties approve the results, the assessment will automatically move to the Inputting CAPs and Signing Rep Letter phase.

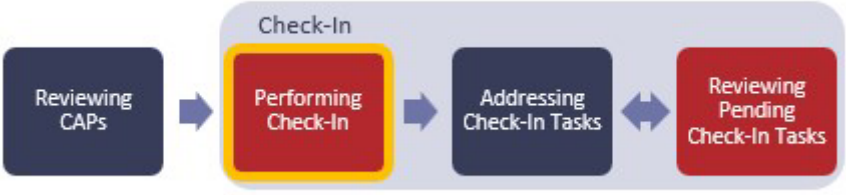
Inputting CAPs and Signing Rep Letter

In this phase, the Assessed Entity must complete the Validated Report Agreement and Rep Letter. Any requirement statements requiring CAPs will be identified in MyCSF, and the Assessed Entity must enter the required CAPs. For additional information on CAPs, see Chapter 13.9 CAPs and Gaps.

Reviewing CAPs

In this phase, the External Assessor must review the linked CAPs. The Assessed Entity can also demonstrate progress against the CAPs. All CAPs must include the information defined in criteria 13.9.4 (see Chapter 13.9 CAPs and Gaps) for the External Assessor to document its approval using the “thumbs up” button in MyCSF. Clicking the “thumbs up” button will change the requirement statement-level response status to “CAP Review Completed.” For CAPs that do not meet the review criteria, the External Assessor will disapprove, using the “thumbs down” button, which reverts the requirement statement back to the Assessed Entity. Once the External Assessor agrees with all the CAPs, they will submit the assessment to HITRUST. For additional information on CAPs, see Chapter 13.9 CAPs and Gaps.

Performing Check-In



During this phase, HITRUST performs automated Quality Assurance (QA) checks and a high-level review of the assessment, accompanying required documents, and webforms (Organization Information, Scope of the Assessment, Factors, Validated Report Agreement, Rep Letter, Test Plans, External Assessor Time Sheet, QA Checklist, and Audits and Assessments Utilized) to determine if the assessment is ready for a HITRUST

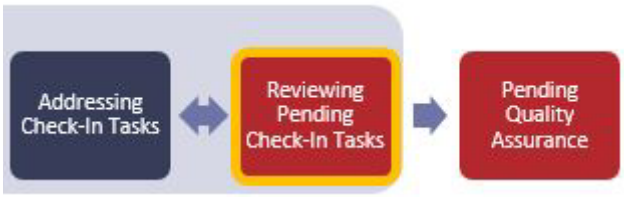
QA Analyst to review.

For additional information on the check-in process and potential scenarios, see Chapter 13.10 Check-in Process.

Addressing Check-In Tasks

During this phase, the Assessed Entity and/or External Assessor must address and send back all the tasks to HITRUST if any were identified during the *Performing Check-In* phase.

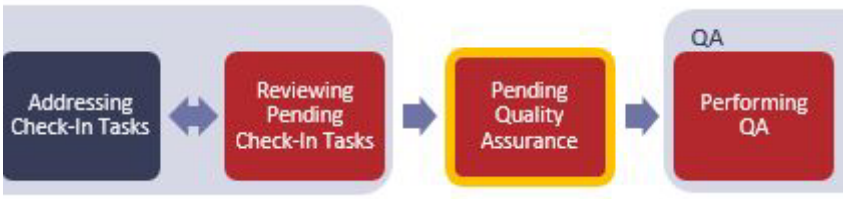
Reviewing Pending Check-In Tasks



In this phase, HITRUST reviews all tasks addressed by the Assessed Entity and External Assessor. HITRUST will close the tasks that have been resolved and, if all tasks have been resolved, accept the assessment after which the assessment moves into the *Pending Quality Assurance* phase. HITRUST will send any tasks requiring additional attention back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing Check-In Tasks* phase. All check-in items must be resolved by the beginning of the reserved QA block or the assessment's QA reservation will be canceled and the Assessed Entity will be required to make a new QA reservation.

For additional information on check-in tasks, see Chapter 13.11 Addressing Check-in Tasks.

Pending Quality Assurance



In this phase, HITRUST assigns the assessment to a HITRUST QA Analyst. The HITRUST QA Analyst will begin QA during the week of the reserved QA Block.

Performing QA

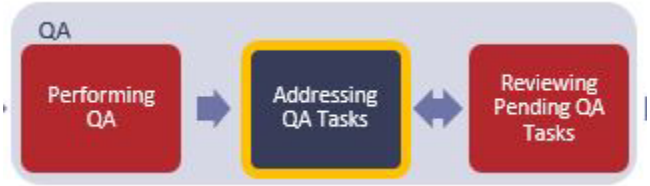
In this phase, the HITRUST QA Analyst will begin QA and review the following:

- The Pre-Assessment
- Required Documents and Webforms
- Risk-based samples of scored requirement statements selected from the i1 or e1 core requirement statements and each Compliance factor, if a combined assessment was performed
- All requirement statements marked as Not Applicable (N/A)
- Overridden PQIs
- CAP Responses

The HITRUST QA Analyst creates and enters all tasks from their review in MyCSF and the assessment moves to the *Addressing QA Tasks* phase.

If the QA review identifies higher volume and/or severity of concerns in an assessment than is typically expected, HITRUST will notify the External Assessor and Assessed Entity that the assessment will require further internal management review within HITRUST. After the internal management review has been completed, the assessment will either continue the normal QA process or move to Escalated QA. For further details on the QA process, see Chapter 14 Undergoing QA.

Addressing QA Tasks



In this phase, the Assessed Entity and External Assessor address the tasks opened by HITRUST. If the action taken to address a task adds new required CAPs to the assessment, those CAPs must be entered by the Assessed Entity and reviewed by the External Assessor. Similarly, if an action taken to resolve a task adds additional requirement statements those must be scored by the Assessed Entity and validated by the External Assessor. When all tasks have been returned to HITRUST and all new requirement statements and

/ or CAPs have been reviewed by the External Assessor, the assessment automatically enters the *Reviewing Pending QA Tasks* phase. For further details on the QA process, see Chapter 14 Undergoing QA.

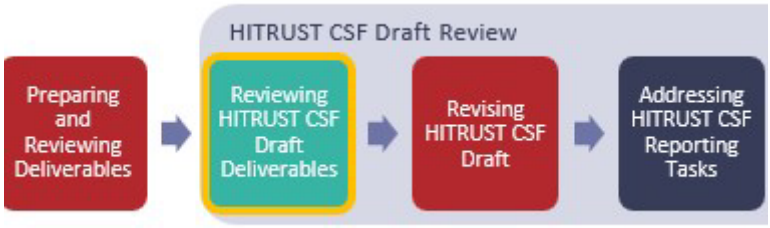
Reviewing Pending QA Tasks

During this phase, the HITRUST QA Analyst will review the QA Tasks addressed by the Assessed Entity and External Assessor. HITRUST will send any tasks that still require attention back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing QA Tasks* phase. HITRUST will close all tasks that have been resolved. After all QA Tasks have been resolved by the Assessed Entity and /or External Assessor and closed by HITRUST, the assessment will move to the *Preparing and Reviewing Deliverables* phase. For further details on the QA process, see Chapter 14 Undergoing QA.

Preparing and Reviewing Deliverables

In this phase, HITRUST will prepare and review the HITRUST CSF i1 or e1 draft reports. If any questions arise during this phase, the HITRUST QA Analyst creates additional tasks and the assessment returns to the Addressing QA Tasks phase. The HITRUST QA Analyst will upload the draft report(s) to MyCSF once the draft reports are internally reviewed by HITRUST and all follow-up questions are resolved. The assessment will then enter the *Reviewing HITRUST CSF Draft Deliverables* phase. For additional information on reporting, see Chapter 15 Reporting & Maintaining a HITRUST Certification.

Reviewing HITRUST CSF Draft Deliverables



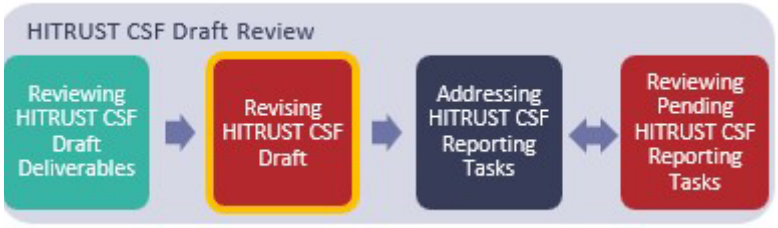
In this phase, the Assessed Entity has up to 30 days to review the HITRUST CSF i1 or e1 draft reports. After the Assessed Entity has reviewed the draft reports, it may either:

- Approve the draft reports by clicking the “Approve HITRUST CSF Draft Report” button within the HITRUST CSF Reports section of the assessment.
- Or Request Revisions in MyCSF (see Chapter 15.1 HITRUST Reporting for additional details on the revision process).

If the Assessed Entity does not approve the draft reports or request revisions within 30 days, the draft reports are automatically approved by MyCSF, and the assessment enters the *Revising HITRUST CSF Draft* phase.

For additional information on reporting, see Chapter 15 Reporting & Maintaining a HITRUST Certification.

Revising HITRUST CSF Draft



In this phase, the HITRUST QA Analyst reviews any requested revisions. If updates within MyCSF are needed to address a revision request, the HITRUST QA Analyst will open a task and the assessment will enter the *Addressing HITRUST CSF Report Tasks* phase. If updates are not needed within MyCSF, the HITRUST QA Analyst updates the status of each request to Completed, or Not Accepted by HITRUST. After processing any revision requests and issuing revised draft reports, HITRUST will return the assessment to the *Reviewing Draft Deliverables* phase for the Assessed Entity to either approve the revised draft reports or request additional revisions.

The HITRUST QA Analyst will also provide an explanation within the “Rationale” section if any revision request is Not Accepted.

When the assessment enters the Revising Draft phase due to the Assessed Entity approving the HITRUST CSF draft reports, the HITRUST QA Analyst builds the final HITRUST CSF reports and uploads them into MyCSF. If no Compliance factors have been included within the assessment, the assessment then enters the Complete phase. If a combined assessment with included Compliance factors was performed, the assessment enters the *Preparing Additional Report Draft(s)* phase

For additional information on reporting, see Chapter 15 Reporting & Maintaining a HITRUST Certification.

Addressing HITRUST CSF Reporting Tasks

In this phase, the Assessed Entity and External Assessor address the tasks opened by HITRUST. When all tasks have been returned to HITRUST, the assessment automatically enters the *Reviewing Pending HITRUST CSF Reporting Tasks* phase.

Reviewing Pending HITRUST CSF Reporting Tasks

During this phase, the HITRUST QA Analyst will review the HITRUST CSF Reporting Tasks addressed by the Assessed Entity and External Assessor. HITRUST will send any tasks that still require attention back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing HITRUST CSF Reporting Tasks* phase. HITRUST will close all tasks that have been resolved.

After all Tasks have been resolved by the Assessed Entity and/or External Assessor and closed by HITRUST, the QA Analyst updates the status of each request to Not Started, Completed, or Not Accepted by HITRUST. After processing any revision requests and issuing revised draft reports, HITRUST will return the assessment to the *Reviewing Draft Deliverables* phase for the Assessed Entity to either approve the revised draft reports or request additional revisions.

Preparing Additional Report Drafts

In this phase, HITRUST will prepare the Insights Report(s) drafts. When the Insights Reports drafts are uploaded to MyCSF, the assessment will enter the *Reviewing Additional Report Drafts* phase.

Reviewing Additional Report Drafts

In this phase, the Assessed Entity has up to 30 days to review the Insights Report drafts. After the Assessed Entity has reviewed the draft reports, it may either:

- Approve the draft reports by clicking the “Approve Draft Report” button within the HITRUST CSF Reports section of the assessment.
- Or Request Revisions in MyCSF (see Chapter 15.1 HITRUST Reporting for additional details on the revision process).

If the Assessed Entity does not approve the draft reports or request revisions within 30 days, the draft reports are automatically approved by MyCSF, and the assessment enters the *Revising Additional Report Drafts* phase.

Revising Additional Report Drafts

In this phase, the HITRUST QA Analyst reviews any requested revisions. If updates within MyCSF are needed to address a revision request, the HITRUST QA Analyst will open a task and the assessment will enter the *Addressing Additional Reporting Tasks* phase. If updates are not needed within MyCSF, the HITRUST QA Analyst updates the status of each request to Completed, or Not Accepted by HITRUST. After processing any revision requests and issuing revised draft reports, HITRUST will return the assessment to the *Reviewing Additional Report Drafts* phase for the Assessed Entity to either approve the revised draft reports or request additional revisions.

The HITRUST QA Analyst will also provide an explanation within the “Rationale” section if any revision request is Not Accepted.

When the assessment enters the Revising Additional Report Drafts phase due to the Assessed Entity approving the draft reports, the final Insights Reports are automatically uploaded into MyCSF and the assessment enters the *Complete* phase.

Addressing Additional Reporting Tasks

In this phase, the Assessed Entity and External Assessor address the tasks opened by HITRUST. When all tasks have been returned to HITRUST, the assessment automatically enters the *Reviewing Additional Reporting Tasks* phase.

Reviewing Pending Additional Reporting Tasks

During this phase, the HITRUST QA Analyst will review the Additional Reporting Tasks addressed by the Assessed Entity and External Assessor. HITRUST will send any tasks that still require attention back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing Additional Reporting Tasks* phase. HITRUST will close all tasks that have been resolved.

After all Tasks have been resolved by the Assessed Entity and/or External Assessor and closed by

HITRUST, the QA Analyst updates the status of each request to Completed, or Not Accepted by HITRUST. After processing any revision requests and issuing revised draft reports, HITRUST will return the assessment to the *Reviewing Additional Report Drafts* phase for the Assessed Entity to either approve the revised draft reports or request additional revisions.

Complete

When all final reports are uploaded, the assessment enters the *Complete* phase.

Press Kit Distribution

When an Assessed Entity receives its first certification (and upon request for additional certifications), the HITRUST Marketing team will distribute a HITRUST certification press kit within 10 business days that includes:

- HITRUST Certification Announcement Guidelines comprised of instructions for a customized press release, logo usage, and additional media support information.
- HITRUST Certification Press Release Template containing approved content and pre-approved quotes from a HITRUST executive. NOTE: The scope of the Assessed Entity's HITRUST certification is required to be included in the press release.
- Certification Logo

The HITRUST certification press release requires a final approval from HITRUST prior to publishing. The Assessed Entity must send the press release draft to PR@hitrustalliance.net for final review.

Assessment Object Archiving

The MyCSF archive process for assessment objects is initiated only if the Assessed Entity's account has expired for 60 days OR a user attempts to delete an object that is certified. After the archive process is initiated:

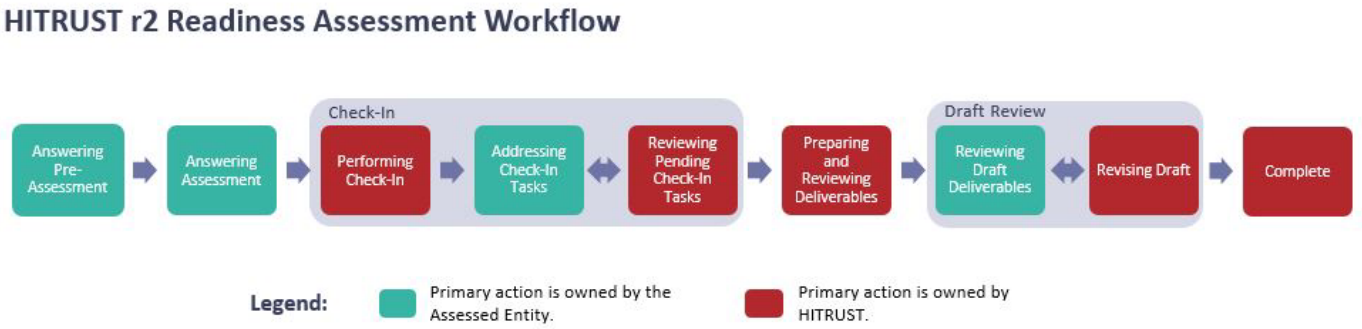
- For all certified assessment objects, the deletion date is set to 2 years + 6 months after the final report date.
- For all other assessment objects (e.g., readiness assessments, validated-only (i.e., non-certified) assessments, or assessments in progress) the deletion date is set to 6 months after the current date.

NOTE: For non-certified assessments, the user may mark the object for deletion on the current day.

5.3 r2 Readiness Assessment Workflow

The assessment workflow for HITRUST r2 readiness assessments submitted to HITRUST for report processing features a subset of the phases present in the workflow outlined above for HITRUST r2 validated assessments.

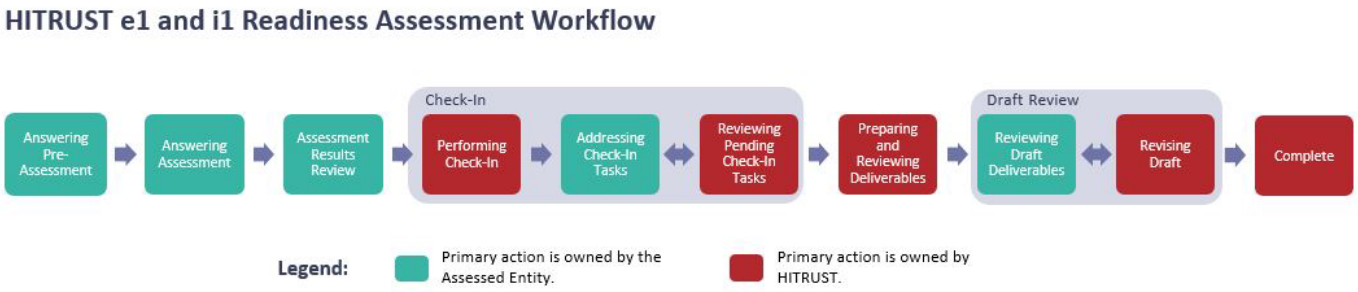
The diagram below displays the workflow for r2 readiness assessments, including the primary owner of each phase. The descriptions of each phase, including requirements and responsibilities, are identical to those applicable phases described in Chapter 5.1 r2 Validated Assessment Workflow.



5.4 i1 & e1 Readiness Assessment Workflow

The assessment workflow for HITRUST e1 and i1 readiness assessments submitted to HITRUST for report processing features a subset of the phases present in the workflow outlined above for HITRUST i1 and e1 validated assessments.

The diagram below displays the workflow for i1 and e1 readiness assessments, including the primary owner of each phase. The descriptions of each phase, including requirements and responsibilities, are identical to those applicable phases described in Chapter 5.2 i1 and e1 Validated Assessment Workflow.



5.5 Interim and Bridge Assessment Workflow

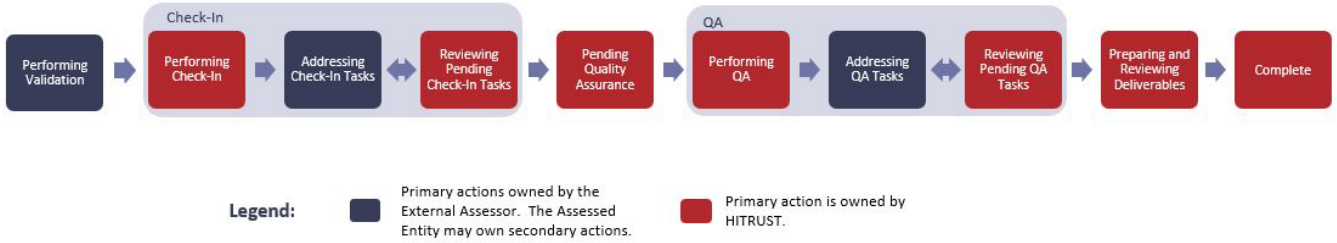
For an entity to retain its r2 certification for a two-year period, an interim assessment must be completed and submitted to HITRUST in the 90-day window leading up to the one-year anniversary of the certification issuance date.

A HITRUST bridge assessment allows an organization to maintain a form of HITRUST r2 certification status for an additional 90 days even if its r2 validated assessment recertification date has passed.

The assessment workflow for both HITRUST interim and bridge assessments (only applicable for r2 validated assessments) features a subset of the phases present in the workflow outlined above for HITRUST validated assessments.

The diagram below displays the workflow for interim and bridge assessments after each assessment has been submitted in MyCSF, including the primary owner of each phase. The descriptions of each phase, including requirements and responsibilities, are identical to those applicable phases described in Chapter 5.1 r2 Validated Assessment Workflow.

HITRUST r2 Interim and Bridge Assessment Workflow



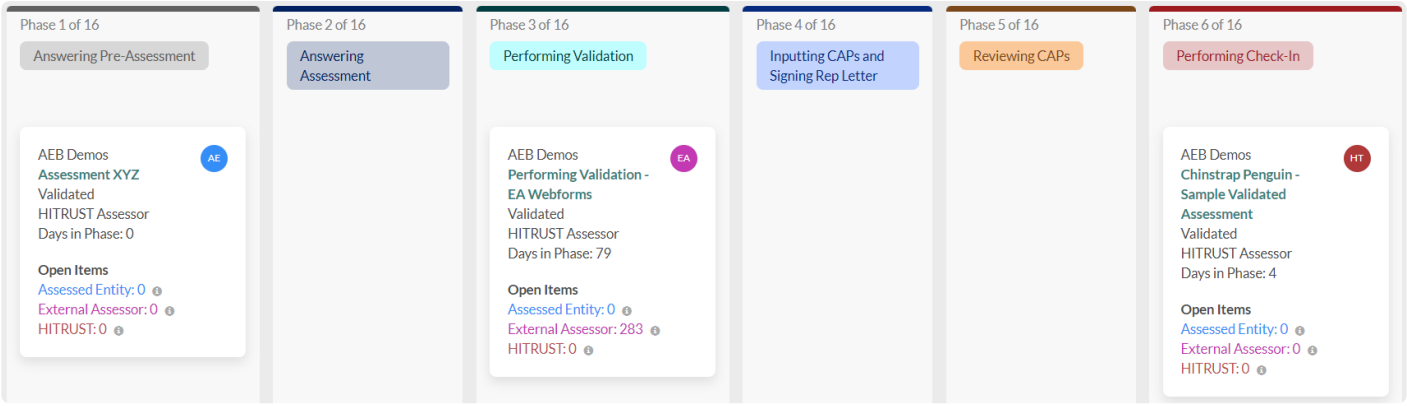
For more information on interim and bridge assessment requirements, see Chapter 15.4 Interim Assessments and Chapter 15.8 Bridge Assessments.

5.6 Assessment Status Dashboards

Several status dashboards exist in MyCSF to provide transparency regarding assessment status, open action items and their ownership, and next steps in the assessment workflow.

These dashboards include:

Kanban View



A Kanban-style board that displays HITRUST validated assessments as they traverse each phase of the validated assessment workflow. The board includes key details of each validated assessment, including:

- Colored, circle badges depicting responsible parties for action items
- Summary of open items for the organization
- Time elapsed in current phase
- HITRUST-assigned point of contact

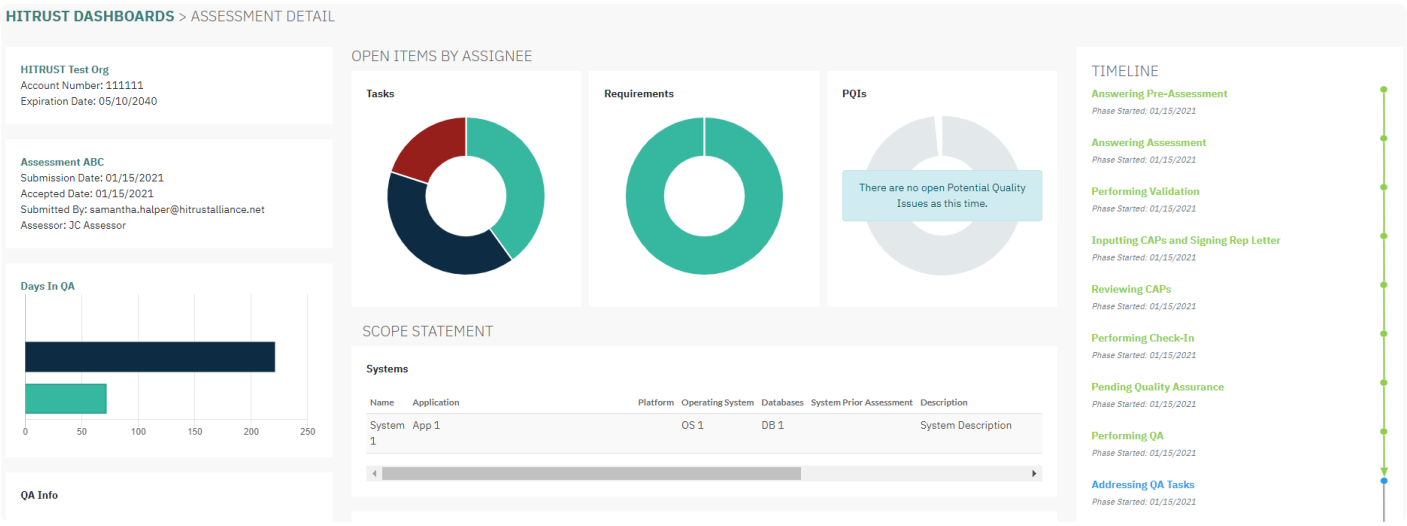
The Assessed Entities and External Assessors may customize the Kanban View by configuring the data points and icons shown on their assessment's cards.

Matrix View

Id	Name	Type	Subscriber	Account Number	Expiration Date	Answering Pre-Assessment	Answering Pre-Assessment (Days)	Answering Assessment	Answering Assessment (Days)	Performing Validation	Performing Validation (Days)
1687	**Chinstrap Penguin - Sample Validated Assessment**	Validated	**AEB Demos**	HT-00009999911111	08/01/2022	09/08/2021	7	09/15/2021	1	09/16/2021	1
1708	**Assessment XYZ**	Validated	**AEB Demos**	HT-00009999911111	08/01/2022	11/03/2021	0				

A spreadsheet-style view that displays the date that HITRUST validated assessments enter each phase of the validated assessment workflow, as well as the number of days that the assessments have been in each phase.

Assessment Details Page



A dashboard of assessment metadata and status information, including:

- Key dates along the assessment timeline
- Open items assigned to the Assessed Entity, External Assessor, and HITRUST
- Assessment scope

5.7 MyCSF Assessment Status Notifications

As each HITRUST assessment traverses the assessment workflow, the Assessed Entity and External Assessor are notified of the status of the assessment via notifications on the homepage of MyCSF and email. There are two types of assessment status notifications: workflow phase notifications and summary email notifications.

Workflow Phase Notifications

Workflow phase notifications are sent to the Assessed Entity and External Assessor as the assessment enters each phase of the assessment workflow. These notifications appear in the notification panel on the homepage of MyCSF and are also sent via email. The email notifications will contain more detailed information and instructions than the notification that appears in MyCSF.

Summary Email Notifications

Assessed Entities and External Assessors have the option to receive several summary email notifications in addition to the workflow phase notifications.

6. Pre-Assessment

The following section outlines the six webforms that comprise the pre-assessment and must be completed to create a HITRUST validated assessment or readiness assessment.

6.1 Pre-Assessment Webforms

The Pre-Assessment is a collection of six webforms that must be completed to create a HITRUST validated assessment or readiness assessment. The Pre-Assessment is initially completed during the *Answering Pre-Assessment* phase, which is the first phase of the validated assessment and readiness assessment workflows. The key requirements in this phase include the following:

6.1.1 The Pre-Assessment webforms must be completed by the Assessed Entity or its designee.

6.1.2 When completing a readiness assessment, the Pre-Assessment webforms can be edited until the assessment is submitted to HITRUST and it enters the *Performing Check-in* phase.

6.1.3 When completing a validated assessment, the Pre-Assessment webforms can be edited until an assessment domain is submitted to the External Assessor for review.

6.1.4 The External Assessor must review and approve the contents of each Pre-Assessment webform that was completed by the Assessed Entity for a validated assessment.

6.1.5 Any Pre-Assessment webforms completed by the External Assessor (only allowable for i1 and e1 assessments) will be approved automatically.

6.1.6 If any Pre-Assessment webforms are not approved by the External Assessor, the External Assessor is prompted to send them back for the Assessed Entity to update.

The Pre-Assessment consists of the following webforms within MyCSF:

- Name & Security
- Assessment Options
- Organization Information
- Scope of the Assessment
- Default Scoring Profile
- Factors

6.2 Name & Security

6.2.1 The Assessed Entity must complete the Name & Security webform in MyCSF, including entering the assessment name and, for validated assessments, selecting the External Assessor Organization that will perform validation procedures.

6.2.2 The Assessed Entity must also set the access permissions for the Assessed Entity and, for validated assessments, External Assessor users in the webform.

6.2.3 The Subscriber name on the webform is automatically completed and locked with the name on the Assessed Entity's subscription. This name will appear as the Assessed Entity in any subsequently issued HITRUST reports.
NOTE: Only one organization name may be included as the Assessed Entity in a HITRUST assessment report.

6.3 Assessment Options

6.3.1 For r2 assessments, the Assessment Options webform in MyCSF must be completed by the Assessed Entity. For i1 or e1 assessments, the Assessment Options page in MyCSF can be completed by either the Assessed Entity or External Assessor.

6.3.2 The Assessed Entity may select the assessment type preset to indicate the type of assessment that will be performed. Alternatively, the Assessed Entity may answer the questions listed in the MyCSF Assessment Options webform to determine the assessment type.

6.3.3 The Assessed Entity must select the CSF version to be used during the assessment (when there is more than one version available for creation). For additional information on the current version of the CSF, see HITRUST CSF Framework.

6.3.4 For r2 assessments, the Assessed Entity must select whether the *Measured* and *Managed* control maturity levels will be scored in the assessment. Assessed Entities can achieve certification without scoring the *Measured* and *Managed* maturity levels. For additional information on these maturity levels, see Chapters 9.4 Measured Maturity Level and 9.5 Managed Maturity Level.

6.3.5 For r2 assessments, the Assessed Entity must select whether they will be including all CSF security controls in the assessment or only those required for certification, and whether Privacy controls should be included in the assessment.

6.4 Organization Information

6.4.1 For r2 assessments, the Organization Information webform in MyCSF must be completed by the Assessed Entity. For i1 or e1 assessments, the Organization Information page in MyCSF can be completed by either the Assessed Entity or External Assessor.

The following information is entered on the Organization Information webform:

Organization/Company Background

6.4.2 The Company Background section should be a one to two paragraph overview of the Assessed Entity which will appear in the final assessment report. Content may include the assessed organization's mission statement, values, or primary business lines. This information may be similar to the "About us" section of the Assessed Entity's website.

6.4.3 The organization/company background may NOT:

- Include information related to number of employees, geographic areas served, compliance requirements, or systems in scope. This information is presented elsewhere in the report.
- Use industry-specific terms or acronyms that are not defined.
- Discuss scope of the assessment.
- Include marketing language such as "We are the best service provider…".

Overview of the Security Organization

6.4.4 The Overview of the Security Organization section should include information about the structure and operation of the information security program at the Assessed Entity and will appear in the final assessment report. It is recommended that this is limited to no more than three paragraphs. Topics may include:

- Organization's information security framework
- Description of the information security organization
- Scope and responsibilities of different information security teams within the organization
- Management and monitoring of the information security program
- Objectives, approach, scope, and goals of the information security program
- Risk assessment process and risk management program

6.4.5 The overview of the security organization may NOT:

- Mention specific tools
- Include information about the scope of the assessment
- Include confidential information

Contact Information

6.4.6 The Contact Information should include the name, job title, email, and phone number of the primary point of contact from the Assessed Entity.

Primary Mailing Address

The Primary Mailing Address will appear in the final assessment reports.

6.5 Scope of the Assessment

6.5.1 For r2 assessments, the Scope of the Assessment webform in MyCSF must be completed by the Assessed Entity. For i1 or e1 assessments, the Scope of the Assessment webform in MyCSF can be completed by either the Assessed Entity or External Assessor.

6.5.2 HITRUST uses information entered into the Scope of the Assessment webform when reporting the assessment scope within the HITRUST certification letter. Information not entered into this webform will not be able to be included in the final HITRUST certification letter.

6.5.3 The following information is entered on the Scope of the Assessment webform:

a) Platforms/Systems: The Platforms/Systems table should contain all platforms/systems contained in the scope of the assessment. The description of the platform must include the following:

- The business function of the platform (service offering)
- Relevant technical details around the platform (describing any exclusions)
- A description of any supporting infrastructure
- How the platform is accessed by the Assessed Entity, the Assessed Entity's customers, and third parties (if applicable)
- Whether the platform/system incorporates an AI model

b) Facilities: The Facilities table should contain all facilities included in the scope of the assessment. All fields in the Facility table must be completed.

c) Services Outsourced for In-Scope Platforms and Facilities: The Services Outsourced table should contain all organizations that provide services which impact the controls for the in-scope platforms and facilities.

For further details around assessment scoping, see Chapter 7 Scoping the Assessment.

6.6 Default Scoring Profile

The Default Scoring Profile webform in MyCSF is available to organizations with certain subscription levels. This page allows the user to pre-score the assessment with default scores.

6.6.1 For r2 assessments, the Default Scoring Profile webform in MyCSF must be completed by the Assessed Entity. For i1 or e1 assessments, the Default Scoring Profile webform in MyCSF may be completed by either the Assessed Entity or External Assessor.

6.7 Factors

The Factors webform allows the Assessed Entity to tailor the requirement statements included in the r2 assessment based on the assessed organization's inherent risk. The r2 assessment factor questions are organized in the following categories:

- General Factors: General information about the Assessed Entity.
- Organizational Factors: Information around the data held and processed in the in-scope environment.
- Geographic Factors: Geographic reach of the in-scope system(s) and facility(s).
- Technical Factors: IT information around the in-scope systems and facility(s).
- Compliance Factors: Regulatory or Compliance frameworks that the Assessed Entity may optionally include in their assessment.

6.7.1 For r2 assessments, the Factors webform in MyCSF must be completed by the Assessed Entity.

6.7.2 All factor questions in the General, Organizational, Geographic, and Technical categories must be completed. Compliance factors are optionally selected for inclusion within an assessment.

6.7.3 When a factor question is answered "No", the rationale for answering "No" must be provided. The rationale should directly answer the factor question and be clear, concise, and free of spelling and grammatical errors.

HITRUST i1 and e1 assessments allow the Assessed Entity to optionally select Compliance factors in order to perform a combined assessment of an authoritative source alongside the i1 or e1 requirement statements. A combined assessment results in an Insights Report for each included authoritative source in addition to the i1 or e1 HITRUST CSF reports. Note that the authoritative sources eligible for inclusion within e1 and i1 combined assessments vary based on the CSF version.

6.7.4 For i1 and e1 assessments, the Factors webform in MyCSF may be completed by the Assessed Entity or External Assessor.

6.7.5 In an i1 or e1 validated assessment, only the scores for the core i1 or e1 requirement statements are considered when determining achievement of the i1 or e1 certification (authoritative sources included as part of a combined assessment do not impact achievement of the underlying i1 or e1 certification).

6.7.6 For i1 and e1 assessments, the HITRUST CSF i1 and e1 Validated Assessment Reports include only the core i1 or e1 requirement statements (even when a combined assessment with included Compliance factors is performed).

6.7.7 For combined i1 and e1 assessments, each Compliance factor selected requires an Insights Report

Credit to be obtained prior to submission of the assessment to HITRUST.

For a list of all factor questions and guidance for responding to factors see MyCSF Help.

7. Scoping the Assessment

The following sections outline the assessment scoping process including the requirements and criteria for identifying the in-scope components for an assessment.

7.1 Assessment Scoping

Assessment scoping is the process of identifying the specific organizational business units, physical locations, systems, and other components to be considered in a HITRUST assessment. The scoping process is designed to be flexible and adaptive so that it can be tailored to fit the unique environment of an Assessed Entity. The scope of an assessment determines the boundary of what will be subject to assessment procedures in a HITRUST assessment. The scope defined by the Assessed Entity depends on several considerations, which may include:

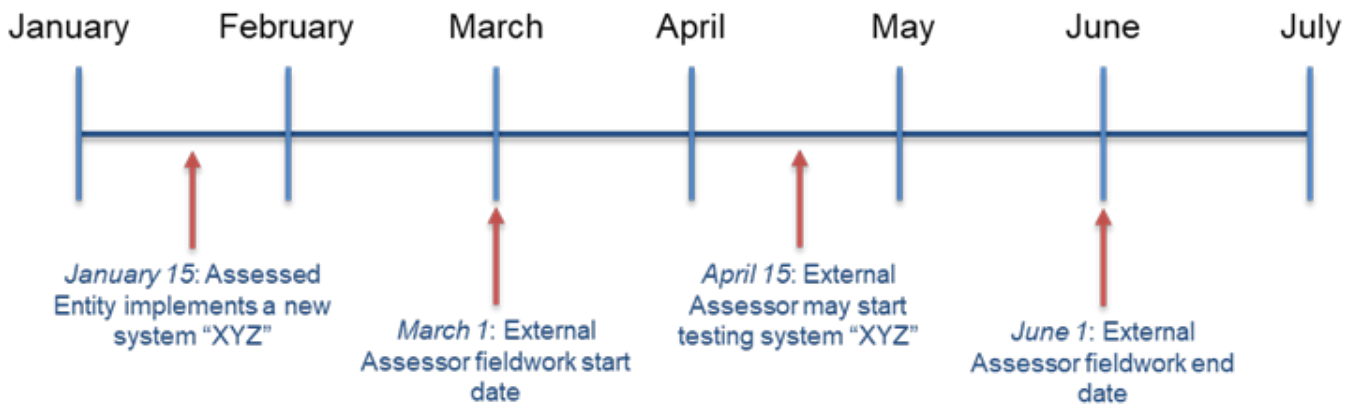
- Expectations of the Assessed Entity's security program by the Assessed Entity, stakeholders relying on the Assessed Entity, and the general public
- Needs of the Assessed Entity's relying parties
- Assessed Entity's available personnel and/or resources to support the assessment
- Security and privacy program maturity of the Assessed Entity
- Use and flow of covered and/or confidential data
- Potential short-term significant changes in the IT environment

For additional examples of how an Assessed Entity may decide to approach its scoping process, see Appendix A-14 Scoping Approaches.

HITRUST has defined specific criteria to assist Assessed Entities with determining the scope of their assessments:

7.1.1 HITRUST only certifies implemented systems under control of the Assessed Entity. An implemented system is a system that has been installed and configured within the assessed control environment for at least 90 days. The installation and configuration must include all primary scope components (see Chapter 7.2 Required Scope Components) of the system (e.g., operating system, database, etc.) for the entire 90-day period. There is no requirement for the system to be storing or processing data during the 90-day period, but it must be operating in the production environment.[3]

NOTE: The 90-day implementation period may overlap with the fieldwork period if testing on the implemented system is performed after the 90-day implementation period has been achieved. The following example timeline demonstrates how a system's implementation period may overlap the fieldwork period.



7.1.2 HITRUST utilizes the NIST definition of a "system" which is *a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*[4]

NOTE: HITRUST uses the terms "system", "information system", and "platform" interchangeably.

7.1.3 HITRUST cannot certify application(s) where the application instance(s) is not under the control of the Assessed Entity (e.g., HITRUST cannot certify mobile applications). However, the back-end infrastructure supporting that application can be certified. For example, a cloud service provider (CSP) can certify the system(s) it provides to customers, but the customer is responsible for certifying the specific platform it will be customizing and operating utilizing the CSP's infrastructure.

7.1.4 HITRUST incorporates the facility(s) included in the scope of an assessment within the certification letter to provide the Assessed Entity and its relying parties context around the location of in-scope platform(s).

The Assessed Entity's scope definition helps direct its control implementation and remediation efforts as they relate to the HITRUST CSF. A properly defined scope for the HITRUST assessment is necessary to create a targeted environment for the assessment. Scope components that influence the in-scope technical environment should be clearly understood to determine the extent of testing necessary within each HITRUST requirement statement.

---

[3] In this instance, HITRUST considers the following NIST definition of 'production environment': An environment where functionality and availability must be ensured for the completion of day-to-day activities.

[4] NIST Special Publication 800-171 Revision 2

7.2 Required Scope Components

During assessment planning, Assessed Entities and/or External Assessors will identify the components in scope following the below scoping criteria. The scope of an assessment includes two distinct categories:

1. **Primary scope components:** The main platform(s) being assessed. These include the components defined by the Assessed Entity to be in-scope of the assessment. Primary scope typically consists of the following component types*:
    - Application(s)
    - Operating System(s)
    - Database(s)
    - Network(s)
    - Facility(s)

    *The above list includes typical components that comprise a platform. There may be other information technology asset types (e.g., hardware, software, or firmware) that an Assessed Entity can include in the primary scope of its assessment.

2. **Secondary scope components:** Components included within an assessment based on the defined primary scope (e.g., supporting infrastructure, systems, and/or tools). Secondary scope components may consist of the following component types:
    - Wireless Networks & Network Infrastructure
    - Endpoints
    - Portable Media
    - Mobile Devices
    - Authentication, Authorization, Accounting (AAA) Platforms
    - Data Transmissions
    - Reporting Services
    - Data Storage Tools
    - Hypervisors
    - Other Supporting Tools

The key characteristics differentiating primary scope components and secondary scope components include**:

7.2.1 Primary scope components are defined and driven by the Assessed Entity. The Assessed Entity may include in scope of its assessment any component that is considered one of the primary scope component types.

7.2.2 Secondary scope components are determined by the primary scope components. The Assessed Entity must only include secondary scope components that meet the HITRUST criteria.

For example: For any requirement statements that include the assessment of wireless networks, the Assessed Entity must include all wireless networks that connect to the primary scope network(s) when

testing wireless networks in the assessment. In addition, the Assessed Entity may not assess a wireless network not connected to a primary in-scope network (without adding that entire network as a primary scope component).

7.2.3 All primary scope components must be considered for each HITRUST requirement statement in an assessment. The primary scope component(s) may only be excluded from testing if the requirement statement is not relevant for the component type or the requirement statement specifically restricts the scope (e.g., in-scope facilities only can be tested for physical security/environmental requirements). If the component(s) is managed by a service provider, see *Other Scoping Topics* below for additional information.

7.2.4 Secondary scope components must be considered for testing when the HITRUST requirement statement specifically refers or applies to the secondary scope component.

For example: If a requirement statement states, “The organization’s security gateways (e.g., firewalls) (i) enforce security policies; (ii) are configured to filter traffic between domains; …”, then all security gateways identified as a secondary scope component must be included when testing the requirement statement.

**NOTE: It is possible for a scope component to be both a primary and secondary scope component. For example, an Assessed Entity might include its “Active Directory” server as a primary in-scope system. In this instance, it will be part of the primary scope testing, but also included as a secondary scope component when validating requirement statements related to authentication, authorization, and accounting for the other primary scope component(s).

Primary scope components: Scoping considerations

The following must be considered when determining the primary scope component(s) during an assessment:

7.2.5 Any implemented in-scope component that is part of the technology stack for the in-scope platform(s)/system(s) must be included as a primary scope component (i.e., corresponding applications, operating systems, and databases).

7.2.6 Facility(s) hosting any component of technology stack for the in-scope platform(s)/system(s) must be included as a primary scope component.

7.2.7 Additional facility(s) not hosting the in-scope platform(s)/system(s) also may be included as a primary scope component if the facility(s) includes risks to the in-scope platform(s) / system(s) (e.g., employees directly accessing the in-scope platform from the location).

7.2.8 The in-scope facility(s) of an assessment may not include physical locations not controlled by the organization and/or not managed by a service provider of the Assessed Entity (e.g., employee homes, “WeWork” offices). NOTE: An Assessed Entity is not required to include their corporate office(s) in scope of a validated assessment if none of the primary scope components reside at that facility.

7.2.9 Private network(s) connected to the technology stack for the in-scope platform(s)/system(s) must be included as a primary scope component. Private network(s) with infrastructure that allows a direct connection and/or trust relationship with a primary in-scope network also must be included as a primary scope component.

NOTE: The HITRUST glossary defines “Private Network” as: *A telecommunications network designed and operated to convey traffic between systems and users who share a common purpose (e.g., branches of a company or individual school campuses).*

7.2.10 For a network to be considered segmented from another network, it must apply isolation techniques as described from NIST[5]: *Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both.*

7.2.11 Additional network(s) not connecting to the in-scope platform(s) / system(s) may be included as a primary scope component.

7.2.12 The scope of an assessment may include user workstations as primary scope components. However, if workstations are included in-scope, the Operating System for the workstations also must be included as a primary scope component. If those workstations reside permanently at a facility owned by the Assessed Entity (e.g., desktop computers) with a dedicated connection to the network(s) at that facility, the corresponding facility and network(s) also must be included as primary scope components.

Secondary scope components: Scoping considerations

The following must be considered when determining the secondary scope component(s) for an assessment:

7.2.13 Requirement statement language takes precedence when determining the components that require testing within an assessment.

For example: The requirement statement “The organization ensures that mobile devices connecting to corporate networks, or storing and accessing company information, allow for remote wipe” may include a broader population of mobile devices for testing than criteria 7.2.17 since this requirement includes mobile devices beyond just those that can access the primary scope of the assessment. In this instance, the population requested by the requirement statement takes precedence as it is considering the performance of the requirement at an entity level, rather than primary scope level.

7.2.14 Wireless Networks & Network Infrastructure: HITRUST assessments include specific domains for Wireless Security and Network Protection. Wireless networks and network infrastructure (e.g., security gateways, routers, firewalls, etc.) used on the primary in-scope network(s) must be tested for corresponding requirement statements referencing the wireless network and/or network infrastructure. No additional wireless networks or network infrastructure may be included when testing those requirement statements without including that network segment as a primary scope component.

7.2.15 Endpoints: HITRUST assessments include a specific domain for Endpoint Protection. The scope of endpoint testing must include both server endpoints (physical or virtual) and user endpoints (e.g., phones, tablets, desktops, laptops, or virtual desktops). The scope must include any server or user endpoint that is used or can be used to directly access or connect to a primary scope component, *without using a bastion host, jump server, or virtual desktop infrastructure (VDI).* All primary scope components also must be in the scope of endpoint testing. If the environment utilizes a bastion host, jump server, or VDI:

- In order to exclude the server or user endpoint(s) from testing, the bastion host, jump server, or VDI must appropriately compartmentalize the environment (i.e., restrict data from leaving the environment to the connected server or user endpoint(s)).
- The bastion host, jump server, or VDI must be included in the scope of the endpoint testing.
- Those endpoints that are using a bastion host, jump server, or VDI may be included as a secondary scope component.

When web applications that can be accessed from any endpoint are a primary scope component, the public endpoints are not considered as secondary scope components.

NOTE: HITRUST uses the following definitions for bastion host, jump server, and VDI:

- Bastion host: A special purpose computer on a network specifically designed and configured to withstand attacks.[6] The computer is used by endpoints to access other servers or devices on an organization's private network.
- Jump server: A hardened system across two or more networks used to manage access between the networks.
- VDI: A centralized server that provides virtual desktops to endpoints upon request. The computing occurs on the VDI environment rather than the endpoint.

7.2.16 Portable Media: HITRUST assessments include a specific domain for Portable Media Security. Portable media includes mobile storage such as memory cards, portable hard drives, USB drives, CDs, DVDs and/or backup tapes. The portable media must include any portable media (organization owned or personally owned) that can be used within the in-scope environment. The in-scope environment used to identify all corresponding portable media includes all endpoints identified as primary or secondary scope component(s). For example, if the primary or secondary in-scope server or user endpoints have functioning USB ports or CD/DVD burners, the corresponding storage technology must be considered as in-scope portable media.

NOTE: For purposes of a HITRUST assessment, laptops are not classified as portable media. However, the technology they enable (e.g., USB devices, CD/DVD burners) should be considered when evaluating requirements within this domain.

7.2.17 Mobile Devices: HITRUST assessments include a specific domain for Mobile Device Security. Mobile devices include devices such as notebook/laptop computers, personal digital assistants, smart phones, tablets, digital cameras, and any other portable device which can be used to directly access a

primary scope component, *without using a bastion host, jump server, or virtual desktop infrastructure (VDI).* Those mobile devices that are using a bastion host, jump server, or VDI may optionally be included as a secondary scoping component.

7.2.18 Authentication, Authorization, Accounting (AAA) Platforms: HITRUST assessments include specific domains for Password Management, Access Control, and Audit Logging & Monitoring. AAA platforms typically operate to support requirement statements in those domains. The AAA platforms include system(s) or service(s) utilized by an end user to authenticate with and/or access a primary scope component. These must be included as a secondary scope component(s) when testing corresponding requirement statements related to authentication, authorization, and accounting for the primary scope component(s).

7.2.19 Data Transmissions: HITRUST assessments include a specific domain for Transmission Protection. Transmissions of sensitive information to/from the primary scope components must be included when testing corresponding requirement statements related to the transmission of sensitive electronic information.

7.2.20 Reporting Services, Data Storage Tools, and Hypervisors: HITRUST assessments include a specific domain for Data Protection & Privacy. When sensitive information from the primary scope components is stored and/or processed via a transmission from the primary scope components to these tools or systems, the systems and/or tools must be included when testing the corresponding requirement statements related to the storage and/or processing of sensitive electronic information.

7.2.21 Other Supporting Tools: Other supporting tools not addressed above must be tested as needed to satisfy specific requirements that include functionality and/or controls supporting the primary scope components. Other supporting tools utilized in the performance or operation of HITRUST requirements within an assessment may include:

- Disaster Recovery Facilities
- Remote Access Solutions (i.e., VPN, SSH, etc.)
- Back-up tools/media
- Anti-virus software
- Vulnerability Scanners
- Mobile Device Management (MDM) solutions
- Security Information and Event Management (SIEM) solutions
- Configuration Management Databases
- Source Code repositories
- Change Management tools
- Change and/or Incident Management ticketing systems
- Password vaults
- Encryption software
- Data Loss Prevention (DLP) software

HITRUST AI Security Assessment (ai1 and ai2): Scoping considerations

HITRUST offers an ai1 (when combined with an e1 or i1 assessment) or ai2 (when combined with an r2 assessment) certification for Assessed Entities with deployed AI systems (see Chapter 15.1 HITRUST Reporting for additional information). There are key scoping considerations that must be followed when undergoing an ai1 or ai2 assessment:

7.2.22 Within MyCSF, the Assessed Entity must disclose which in-scope platforms leverage the in-scope AI model(s). The underlying IT platform that comprises the IT system with the AI model must be included in the scope of the corresponding e1, i1 or r2 validated assessment.

7.2.23 For the AI model, the Assessed Entity must, at a minimum, describe the AI model type (e.g., generative or predictive), model name (e.g., ChatGPT) and version number.

7.2.24 The AI model must follow the 90-day implementation period described in criteria 7.1.1.

7.2.25 HITRUST can only certify AI models under control of the Assessed Entity. For cloud-based AI deployments, this would typically mean:

- Infrastructure-as-a-Service (IaaS) (i.e., bring-your-own-model): The AI application provider can achieve this HITRUST certification over the AI application, and the IaaS provider is responsible for controls at the IT infrastructure and AI compute infrastructure level.
- Platform-as-a-Service (PaaS): The AI application provider can achieve this HITRUST certification over the AI application, and the PaaS provider is responsible for controls at the IT infrastructure, AI compute infrastructure, and AI platform level.
- Software-as-a-Service (SaaS): An organization using an AI-enabled SaaS platform cannot achieve the ai1 or ai2 certification over the SaaS product. However, the deployer of the SaaS platform may perform an ai1 or ai2 assessment.

For additional details on certification eligibility, see A-19: AI Security Certification Eligibility.

7.2.26 HITRUST requirements within the ai1 or ai2 assessment will specify which scope components must be tested for that particular requirement. Examples of AI scope components within the ai1 or ai2 assessment include:

- AI model
- AI engineering environment(s)
- AI platforms used to serve the AI model
- AI language model tools (such as agents and plugins)
- Datasets used to train, test, validate and tune an AI model
- Information made available to the AI model through retrieval augmented generation
- Stored embeddings used by the AI system (AI-specific)

7.2.27 HITRUST will not award the ai1 or ai2 certification to any AI deployments categorized as unacceptable or otherwise banned by applicable AI regulation in the jurisdiction of the Assessed Entity.

Other Scoping Topics

7.2.28 Service providers are not considered a scope component because they are responsible for providing support or services for a primary or secondary scope component. All service providers (unless carved-out in an i1 or e1, see Chapter 7.3 Carve-outs) must be tested following HITRUST's third-party testing approach (see Chapter 12 Reliance & Third-party Coverage) when utilized by an Assessed Entity as a service provider supporting a primary or secondary scope component.

7.2.29 Certain requirement statements refer to distinct types of people within an Assessed Entity (e.g., contractors, employees, workforce, non-employees, etc.). The *HITRUST Glossary of Terms and Acronyms* (accessible within MyCSF in the "References" tab and MyCSF Help) should be used to determine the scope of people that should be included when testing those requirements.

7.2.30 Sampling is allowed when there is uniformity in the management and operation of controls across a group of scope components. The External Assessor must document its approach and rationale for testing controls across a group of scope components.

For example: The Assessed Entity may have Enterprise policies and procedures for managing physical security across its data centers. The External Assessor validates how those policies and procedures are being uniformly managed and communicated to utilize them across all Assessed Entity's data centers in scope of the assessment.

7.2.31 The External Assessor may change how scope components are grouped depending on the HITRUST requirement statement.

For example: When testing configuration management, the Assessed Entity may have a centralized configuration management system for Linux that allows all primary in-scope Linux Operating Systems to be in a group for testing. The grouping may be different when testing other requirement statements if there are additional scope components uniformly managed and operated for those controls.

7.2.32 When sampling scope components, the External Assessor must follow the sampling guidance in the HITRUST Control Maturity Scoring Rubric.

---

[5] NIST Special Publication 800-171 Revision 2

[6] Committee on National Security Systems CNSSI 4009-2015

7.3 Carve-outs

In a HITRUST assessment, carve-out means that a third-party responsible for managing a portion of the Assessed Entity's control environment is excluded from assessment scoring.

7.3.1 For r2 assessments, HITRUST does not accept any carve-outs of third-parties. As a result, if a third-party manages any of the scope components, as defined in Chapter 7.2 Required Scope Components, they must be included as part of the assessment. For further information on potential testing approaches for third-parties, see Chapter 12 Reliance & Third-Party Coverage.

NOTE: Assessed entities may contact HITRUST (support@hitrustalliance.net) for guidance in situations where reliance or inheritance may not be possible within an r2 assessment. Assessed Entities who perform r2 assessments may be able to carve-out a service provider within an add-on certification such as the HITRUST AI Security Assessment (see A-18: Example Add-on Certification Approach for Existing HITRUST Certifications).

For i1 and e1 assessments, third-parties relevant to the in-scope environment may be excluded from testing (i.e., carved-out). In order to exclude the third-party:

7.3.2 The Assessed Entity must clearly document in the Scope of the Assessment webform the responsibilities of the third-party which it excluded from testing.

7.3.3 The third-party being excluded from scope must be completely removed from scoring throughout the assessment. They cannot be addressed partially during the assessment.

7.3.4 Within the assessment, requirements that are completely the responsibility of the third-party should be documented as Not Applicable (N/A) and include the corresponding rationale.

7.3.5 If any elements in a requirement statement are the responsibility of the Assessed Entity and/or another included third-party, that part must be scored.

For additional information on carve-out scoring, see A-1: Carve-out Scoring Details.

8. Requirement Statements

The following sections describe the HITRUST requirement statements and their evaluative elements and include requirements for determining and documenting the non-applicability of a requirement statement.

8.1 Requirement Statement Background

Requirement statements form the basis of a HITRUST assessment. The assessment's requirement statements are the information protection requirements expected of each Assessed Entity.

Each requirement statement in an assessment includes specific illustrative procedures. The illustrative procedures provide additional context for evaluating the requirement statement at each maturity level (see Chapter 9 Control Maturity Levels). The illustrative procedures should be leveraged by External Assessors to establish consistency and repeatability of its assessment procedures.

8.1.1 External Assessors must use the illustrative procedures as the basis for their more detailed assessment Test Plans (see Chapter 13.5 Test Plan) to evaluate the Assessed Entity's compliance at each maturity level.

NOTE: Regardless of the illustrative procedure wording, the External Assessor must ensure testing coverage of the entire requirement statement.

Requirement statements included in an assessment will vary based on the assessment type and/or responses to the factor questions. When an Assessed Entity responds to the factor questions within a r2 readiness or validated assessment, MyCSF either will add or remove requirement statements from that assessment based upon the corresponding inherent risk. Including optional Compliance factor(s) in an i1 or e1 combined assessment or r2 assessment (readiness or validated) will add additional requirement statements based upon mappings to the selected authoritative source (e.g., HIPAA, NIST 800-53, FedRAMP, etc.). After the factors have been entered into and an assessment is built, the Assessed Entity will have an assessment that contains its own set of unique requirement statements to be scored and tested in order to complete the assessment.

Each requirement statement in an r2, i1, or e1 assessment contains one or more elements expected to be addressed during scoring and External Assessor testing. Depending on the type and version of the assessment, the location and enumeration of the elements may differ.

For r2 assessment types:

- CSF versions prior to 11.0: The evaluative elements are contained in the illustrative procedures for the *Policy* maturity level (these may not be enumerated in certain versions).
- CSF version 11.0 and later: The evaluative elements are contained and enumerated in each requirement statement.

For all i1 and e1 assessment types, the evaluative elements are contained and enumerated in each requirement statement.

8.1.2 Regardless of the assessment type or CSF version, **ALL** evaluative elements in each requirement statement in an assessment must be addressed.

8.2 Alternate Controls

HITRUST built the CSF to address a comprehensive series of threats resulting in a common set of information protection requirements for Assessed Entities. For r2 assessments, HITRUST addresses differences in organizations by tailoring the requirement statements in an Assessed Entity's assessment based on a set of organizational, system, and regulatory risk factors (see Chapter 6 Pre-Assessment). HITRUST expects each Assessed Entity to implement the corresponding requirement statements in its organization to address each of the HITRUST-identified threats. If an Assessed Entity cannot implement a specified requirement statement but believes it is addressing the risk(s) through an alternate process, it may provide HITRUST with the implemented control(s) which address the risk(s) posed by the threats(s) the originally-specified HITRUST requirement statement was meant to address. HITRUST refers to these controls submitted to and approved by a HITRUST Alternate Controls Committee as 'alternate controls.'

8.2.1. For those Assessed Entities that would like HITRUST to consider a separate control to be performed in lieu of a requirement statement, the Assessed Entity must first submit the requirement statement(s) and corresponding alternate control(s) to HITRUST Support (support@hitrustalliance.net). For consideration within a validated assessment, the alternate control(s) and all supporting documentation must be submitted at least 30 days prior to the start of fieldwork for the corresponding HITRUST validated assessment.

8.2.2. The submission must include a corresponding risk analysis, which will be used to justify an exception to one or more requirement statements applicable to the Assessed Entity. The Assessed Entity must demonstrate the validity of an alternative control by producing a risk analysis that shows the compensating control addresses a similar type and level of risk as the original requirement statement. For additional details on the necessary components of the risk analysis, see HITRUST Risk Management Handbook Appendix, A-1 Alternate Controls.

8.2.3. In addition, the alternate control(s) must be something other than what may be required by other, existing requirement statements within the HITRUST assessment because all requirement statements specified in an assessment must be implemented to provide a minimally acceptable level of residual risk.

8.2.4. HITRUST will convene an Alternate Controls Committee who will review the content submitted and determine whether to accept the compensating control(s) as an alternate control(s). If approved, HITRUST will provide the process for documenting, scoring, and validating the alternate control(s) in the validated assessment. The HITRUST Alternate Controls Committee consists of members of HITRUST leadership and any Subject Matter Experts (SMEs) for the particular controls and/or technologies relevant for the request.

8.3 Not Applicable (N/A) Requirement Statements

In certain cases, an Assessed Entity may determine that a requirement statement is not applicable. The following steps must be followed to determine and document the non-applicability:

8.3.1 In situations where an Assessed Entity determines a requirement statement is not applicable, the Assessed Entity must document the corresponding rationale within the assessment in the 'Subscriber Comments' and select the 'N/A?' checkbox. The rationale must specify what causes the requirement statement to be not applicable for the in-scope environment.

8.3.2 The rationale for the "N/A" must be consistent across the assessment. If a requirement statement is marked "N/A" because the Assessed Entity does not perform that service, but that service is part of a scored requirement in another part of the assessment, HITRUST will identify a concern related to 'mixed applicability' for the Assessed Entity and/or Assessor to clarify. For more information on the Quality checks performed by HITRUST during submission, see Chapter 13.4 Automated Quality Checks. For more information on 'mixed applicability,' see Appendix A-2: Mixed Applicability Errors.

8.3.3 The "N/A" rationale must fully address all aspects of the assessment scope, including systems, facilities, and third parties.

8.3.4 A requirement statement being performed by a third-party is not appropriate rationale for a "N/A", unless the assessment type is an i1 or e1 and there is a documented carve-out for the third party (See Chapter 7.3 Carve-outs).

8.3.5 Non-occurrence of a requirement statement cannot be used as rationale to mark the requirement as "N/A." For additional information on the correct testing approach when there has been no occurrence of a requirement statement, see Chapter 11 Testing & Evidence Requirements.

8.3.6 The "N/A" rationale should relate to the requirement statement where the rationale is documented, and it should address all evaluative elements for the requirement.

8.3.7 The "N/A" rationale should not include descriptions of test procedures or test results, or include references to supporting evidence.

8.3.8 The "N/A" rationale must be clear, concise, and free of spelling and grammatical errors.

8.3.9 It is possible that only certain elements in a requirement statement are considered "N/A." In those cases, the elements considered as "N/A" should be documented in the corresponding testing with the rationale and the scoring determined based on testing of the remaining evaluative elements (excluding the non-applicable elements from any scoring calculation).

There are certain requirement statements that typically cannot be marked "N/A." For guidance on the core

requirements that should never be marked “N/A”, see Appendix A-20: Never N/A Registry. Please note this list is not exhaustive, and there may be other HITRUST requirements that should not typically be considered N/A.

Assessed Entities and External Assessors must always have an appropriate rationale for considering a HITRUST requirement statement as not applicable in its HITRUST assessment. HITRUST Quality Assurance will notify the Assessed Entity and External Assessor through a QA task if they are unable to “N/A” a particular requirement.

For “N/A” wording examples, additional N/A guidance, and a decision tree that follows the above guidance, see Appendix A-3: Not Applicable (N/A) Examples, Appendix A-4: Never N/A Examples, and Appendix A-5: N/A Decision Tree.

9. Control Maturity Levels

For all assessment types, Assessed Entities and/or External Assessors will document scores (see Chapter 10 HITRUST Scoring Rubric for detailed scoring information) for each requirement statement by control maturity level. These maturity levels are based upon HITRUST's version of the PRISMA maturity model (see HITRUST CSF Control Maturity Model in the HITRUST Risk Management Handbook for additional background). The HITRUST control maturity model includes five levels for the r2: *Policy*, *Procedure*, *Implemented*, *Measured* and *Managed* (for the i1 and e1, only the *Implemented* maturity level is scored):

- *Policy*: The *Policy* maturity level considers the existence of current, documented information security policies or standards in the Assessed Entity's information security program and whether they include language that formally requires implementation of the evaluative elements within the HITRUST requirements. A policy is the overall intention and direction as formally expressed by management, most often articulated in documents that record high-level principles or courses of action that have been decided. Policies may provide guidance on specific issues or systems but should not be confused with procedures.

- *Procedure*: The *Procedure* maturity level considers the existence of documented procedures or processes developed from the policies and whether they reasonably apply to the Assessed Entity's systems within scope of the assessment. A procedure is a description of the steps necessary to perform specific operations in conformance with applicable policies.

- *Implemented*: The *Implemented* maturity level considers the actual implementation of the policies and whether the Assessed Entity's control implementation specifications have been applied to all the Assessed Entity's systems within scope of the assessment.

- *Measured*: The *Measured* maturity level considers separate monitoring activities that involve the testing or measurement (metrics) of the control's implementation and whether they continue to remain effective.

- *Managed*: The *Managed* maturity level considers whether corrective action or enhancements are necessary, based on the measurement results.

Please note that within HITRUST r2 assessments, scoring of the *Measured* and *Managed* maturity levels is optional. When configuring an assessment, the Assessed Entity will select whether *Measured* and *Managed* maturity levels will be evaluated during the assessment.

9.1 Policy Maturity Level

The *Policy* maturity level requires examination of current, documented information security policies or standards within the Assessed Entity's information security program to determine if they fully address the elements within the requirement statements for the scope of the assessment. Scoring is based upon whether the Assessed Entity's policies are not defined, undocumented, or documented for each of the corresponding requirement statement evaluative elements.

9.1.1. A documented, up-to-date (see Chapter 11.3 Working Papers & Evidence for evidence timeliness requirements) policy must specify the mandatory nature of the requirement statement's elements in a written format. This information may reside in a document identified as a policy, standard, directive, handbook, etc.

9.1.2. The identified policy(s) must cover all facilities and operations and/or systems within scope of the assessment.

9.1.3. Undocumented policies are those that are:

(i) Well-understood by those required to implement them and / or adhere to them,
(ii) Consistently observed*, and
(iii) Unwritten.

(*Consistently observed can be interpreted to indicate that it was visually seen by the External Assessor during fieldwork and/or evidence was inspected during implementation testing.)

For additional information on assessing the appropriateness of policies, see Appendix A-10: Policies & Procedures FAQs & Examples.

9.2 Procedure Maturity Level

The second maturity level, *Procedure*, reviews the existence of documented procedures or processes developed from the policies or standards to determine if they specify the procedures for applying the requirement statement evaluative elements to the scope of the assessment. Scoring is based upon whether the Assessed Entity's procedures are not defined, undocumented, or documented for each of the corresponding requirement statement elements.

9.2.1 A formal, up to date (see Chapter 11.3 Working Papers & Evidence for evidence timeliness requirements), documented procedure will state how to implement the security controls identified by the defined policies.

9.2.2 A documented procedure must address the operational aspects of how to perform all evaluative elements in the requirement statement. The procedure should be at a sufficient level of detail to enable a knowledgeable and qualified individual to perform the requirement.

9.2.3 Procedures document the implementation of and the rigor in which the elements of the requirement are applied.

9.2.4 The identified procedure(s) must cover all facilities and operations and/or systems within scope of the assessment.

9.2.5 Undocumented procedures are those that are:

(i) Well-understood by those required to implement them and/ or adhere to them,
(ii) Consistently observed, and
(iii) Unwritten.

For additional information on assessing the appropriateness of procedures, see Appendix A-10: Policies & Procedures FAQs & Examples.

9.3 Implemented Maturity Level

The third maturity level, *Implemented*, reviews the implementation of the policies and procedures to ensure the control has been correctly applied to all the organizational units and systems within scope of the assessment.

9.3.1 Testing must be performed at the *Implemented* maturity level for all evaluative elements in a requirement statement to determine whether they have been implemented in a consistent manner and controls are operating as intended. For additional details on acceptable testing approaches, see Chapter 11 Testing & Evidence Requirements.

9.3.2 The illustrative procedures for the *Implemented* maturity level will typically indicate whether a sample-based test is expected for a requirement statement. However, the External Assessor may determine that a sample-based test is necessary to validate the scoring even if HITRUST has not specified a sample-based test is expected. Alternatively, an External Assessor may determine that a sample-based test is not necessary even when HITRUST has indicated that a sample-based test is expected. In these instances, the External Assessor should document its rationale and alternative testing approach. This rationale will be subject to QA review so the External Assessor must ensure the nature, timing, and extent of testing is sufficient to support the scoring.

9.3.3 Testing must cover all facilities, systems and supporting infrastructure within scope of the assessment.

9.3.4 Testing must adhere to the HITRUST population and sampling methodology as defined in the HITRUST Scoring Rubric and Chapter 11 Testing & Evidence Requirements.

9.4 Measured Maturity Level

The fourth maturity level, *Measured*, reviews whether separate or ongoing monitoring activities are performed to measure the implementation and effectiveness of the control's implementation. Scoring of this level is based on whether there is a Measure or Metric in place and whether review of the Measure or Metric is performed by an Operational or Independent party (see criteria 9.4.3 and 9.4.4).

9.4.1 To be classified as a measure for HITRUST assessment purposes, supporting evidence must:

i. address the control's operation / performance: the measure must include a description of the control that is being measured by the Assessed Entity and/or third party;

ii. specify an appropriate frequency: the measure must document how often the control is performed by the Assessed Entity and/or third party;

iii. define what is measured: the measure must document the data used to determine whether the control is being performed effectively;

iv. identify who is responsible for gathering the data: the measure must document the individual that obtained the supporting documentation on the performance of the control.

v. describe how the data is recorded: the measure must include the supporting data that was obtained and how it was obtained to support the performance of the control;

vi. describe how the measurement is performed/calculated: the measure must include how control effectiveness was determined; and

vii. specify how often the measure is reviewed and by whom: the measure must document the individual that reviewed the performance of the control and frequency of the review. To be considered a measure, the frequency of the review must be at least once every 12 months.

9.4.2 To be classified as metric for HITRUST assessment purposes, the measurement must meet ALL requirements for a measure (listed above) AND:

i. be tracked over time. This can include documenting the results collected for the measure in a spreadsheet and/or chart to be able to determine whether the control effectiveness is increasing or decreasing; and

ii. have explicitly stated (not implied), established thresholds (i.e., upper and/or lower bounds on a value) or targets (i.e., targeted goals, what the organization is trying to achieve). The threshold or target should be a data point that corresponds to the results being captured in the measure. It may be documented within the same spreadsheet or chart as those results to determine whether the threshold or target has been achieved.

9.4.3 Operational measures and metrics are prepared and/or reviewed by a person or group responsible for the control / requirement being measured (e.g., the control owner) or by a person or group influenced by the control owner (a subordinate, a peer reporting to the same department head, etc.).

9.4.4 Independent measures and metrics are prepared and reviewed by a person or group (e.g., auditors, analysts) who are not influenced by the person or group responsible for the operation of the requirement / control being measured (e.g., the control owner).

For additional information and examples of *Measured* scoring, see Appendix A-7: Rubric Scoring – Measured & Managed.

9.5 Managed Maturity Level

The fifth maturity level, *Managed*, reviews the organization's management of its control implementations based on its identified measurements. The organization should be able to demonstrate that it has a management process for the measurement/metric and when variations occur, it has performed a root cause analysis and taken corrective actions using its risk treatment process. Scoring is based on whether there is a documented risk treatment plan in place and the number of criteria addressed within that documented risk treatment process ("strength") and the percent of issues included in the risk treatment process for the corresponding evaluative elements ("coverage").

9.5.1 To be classified as a risk treatment process for HITRUST assessment purposes, one or more of the following criteria must be documented. The number of documented criteria determines the "strength" of the risk treatment process:

i. initial involvement of an appropriate level of management or a defined escalation or review process to be observed if / when the appropriate level of management is not initially involved,

ii. a defined mechanism to track issues, risks, and risk treatment decisions, and

iii. cost, level of risk, and mission impact considered in risk treatment decisions.

9.5.2 If none of the criteria in 9.5.1 were documented but a risk treatment process was observed to be in place the risk treatment process may be considered as "undocumented".

9.5.3 In order to determine "coverage", the total issues identified from the corresponding measure of the requirement statement's evaluative elements should be identified. The percent of those issues that were included in the risk treatment plan will determine the "coverage" component of the maturity score. NOTE: If no issues were identified in the corresponding measure, "coverage" is considered to be Very High.

9.5.4 Since measures and/or metrics are required as input into the *Managed* scoring, the *Managed* score cannot exceed that of *Measured* "coverage." However, the overall *Managed* score can be higher than the overall *Measured* score. If the final *Managed* score is higher than *Measured* coverage, the *Managed* score must be lowered to equal the *Measured* "coverage" score. For examples of *Measured* and *Managed* score calculations, see Appendix A-7: Rubric Scoring – Measured & Managed.

10. HITRUST Scoring Rubric

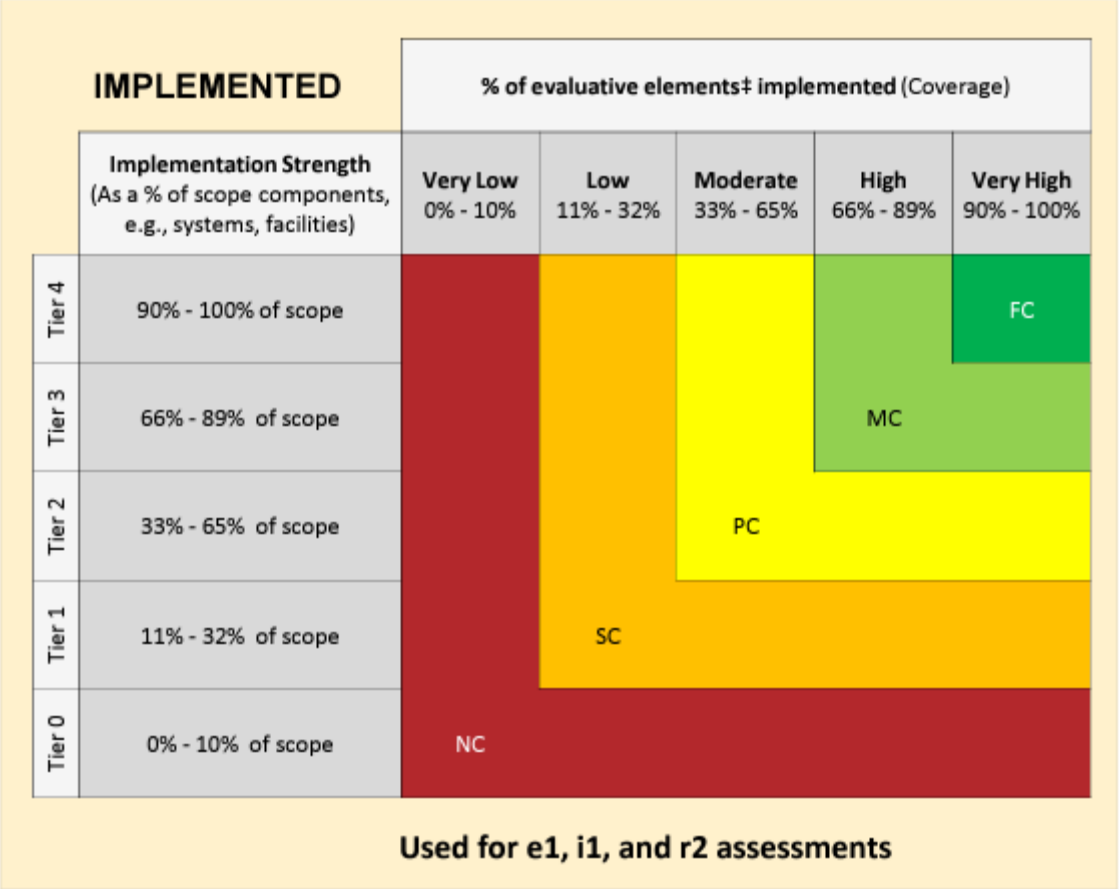
This page is intentionally left blank.

10.1 HITRUST Scoring

HITRUST has developed the Control Maturity Scoring Rubric ("Rubric") to assist Assessed Entities and Assessors with scoring control maturity for each requirement statement in an assessment in a consistent and repeatable way. The Rubric provides guidance on how to score a requirement statement based on an evaluation of strength and coverage for each maturity level. Strength and coverage are defined separately for each of the control maturity levels, but they generally refer to:

- Strength: The rigor with which the Assessed Entity has implemented the requirement within its organization.
- Coverage: Percentage of evaluative elements where the Assessed Entity is compliant.

The Rubric addresses each of the five maturity levels in separate tables, each similar to the following structure:



The rows in the table, Tiers 0 through 4, represent increasing strength in the maturity criteria. The columns, from very low to very high, represent the level of coverage with respect to the evaluative elements specified for each requirement statement. The *Implemented*, *Measured* and *Managed* maturity levels all contain five tiers for strength.

For the *Policy* and *Procedure* level rubrics, there are only three rows in the table representing strength since

the organization will either have: no policy/procedure, an undocumented policy/procedure, or a fully documented policy/procedure. For additional discussion on what constitutes a documented policy/procedure, see Chapter 9 Control Maturity Levels.

POLICY†		% of evaluative elements‡ addressed by the organization's policy (Coverage)				
	Policy Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
Tier 2	Documented policy	NC	SC	PC	MC	FC
Tier 1	Undocumented policy					
Tier 0	No policy					

For all five maturity levels, the intersection of the level-specific strength and coverage results in one of five maturity ratings: Non-Compliant, Somewhat Compliant, Partially Compliant, Mostly Compliant, or Fully Compliant (NC, SC, PC, MC, or FC) from which the requirement statement's final maturity score is computed. The following table from the Rubric indicates the corresponding maturity scores for each rating.

Rating	Range	Points Awarded
Non-Compliant	0% - 10%	0% of points awarded
Somewhat Compliant	11% - 32%	25% of points awarded
Partially Compliant	33% - 65%	50% of points awarded
Mostly Compliant	66% - 89%	75% of points awarded
Fully Compliant	90% - 100%	100% of points awarded

For variances in scope, the scores for each scope item may be calculated separately and the overall maturity level score for a requirement statement determined based on the average of those scores. Suppose an organization has specified all the evaluative elements of a requirement statement in policy, but the policy only applies to three of the four business units within scope of the assessment. The organization will score FC (100%) for those three business units, but NC (0%) for the fourth business unit, resulting in an overall score of 75% ((100+100+100+0)/ 4).

The scores for each scope item also may be weighted separately if there is a corresponding rationale for the

varied weighting. For example, if there are two Data Centers in-scope of the assessment and 10 of the in-scope applications are located at one Data Center and two in-scope applications are located at the second Data Center, the scores may be calculated with corresponding weights using that rationale. Similarly, weighting may be calculated based on the number of transactions processed by each in-scope system or location.

10.1.1 If the Assessed Entity determines there should be a difference in weighting of the scope components for a corresponding HITRUST requirement statement, the Assessed Entity and/or External Assessor must apply a rationale to justify the corresponding weight percentages.

NOTE: There is no requirement to use varying weights for scope components. A rationale is not required if the Assessed Entity takes all scope components into account equally.

10.1.2 The Assessed Entity and/or External Assessor must document the rationale used for any varying weight percentages between scope components within the validated assessment.

10.1.3 If HITRUST determines the weight rationale is not justified, it may request additional support and/or request modifications in the requirement statement scores.

For additional details and examples of rubric scoring, see Appendix A-6: Rubric Scoring – Policy, Procedure, and Implemented and Appendix A-7: Rubric Scoring – Measured & Managed.

For information on current scoring thresholds for each certification type, see Chapter 15.1 HITRUST Reporting.

11. Testing & Evidence Requirements

The following sections detail the External Assessor requirements for performing and documenting testing.

11.1 Testing Approach

HITRUST expects the External Assessor will perform a sufficient level of testing to support the scores in any HITRUST validated assessment. The integrity of the certification is maintained via HITRUST's testing requirements and HITRUST's enforcement of these requirements utilizing the quality assurance review process. This section includes the expectations and guidelines for External Assessor testing within any HITRUST validated assessment. For further information on the Quality Assurance review process performed by HITRUST, see Chapter 14 Undergoing Quality Assurance.

11.1.1 HITRUST External Assessors must ensure the testing approach and evidence requirements meet all guidance outlined in this chapter (including any supplemental guidance such as the HITRUST Scoring Rubric). Deviations from these requirements may lead to delays or the inability of an Assessed Entity to obtain certification.

11.1.2 External Assessors must perform a sufficient level of walkthroughs and testing procedures, which includes producing sufficient documentation, to:

i. Confirm and/or validate the Assessed Entity's self-identified scoring levels/responses, and

ii. to ensure that compliance gaps have been identified.

11.1.3 All requirement statements within a validated assessment must be validated by an External Assessor. Validation procedures are performed using a variety of testing strategies in order to provide assurances to relying parties that the control achieves the documented maturity score(s).

11.1.4 Procedures performed by External Assessors during validated assessment fieldwork must include one or more of the following types of audit procedures:

- Walkthroughs and interviews of personnel to verify that policies and procedures are documented and implemented. *
- Inspection of written policies and procedures to ensure sufficient coverage of each requirement statement's evaluative elements.
- Observation of the performance or existence of relevant controls and control processes.
- Inspection of documentation evidencing the existence/performance of relevant controls, including inspection of documentation associated with samples.
- Performance of technical testing to validate the implementation or operation of relevant controls.
- Reliance on testing performed by other Assessors and/or auditors. For detailed requirements, see Chapter 12 Reliance & Third-Party Coverage.

- Inspection of operational or independent measures or metrics used by the Assessed Entity.
- Inspection of evidence generated by mechanisms used by the Assessed Entity to manage relevant controls.
- Analytical procedures to identify relationships, trends, and/or anomalies in a set of data.
- Recalculation of information generated by an automated or semi-automated process to validate proper functionality (e.g., population completeness).

*NOTE: A walkthrough involves reviewing each requirement statement's evaluative elements with the individuals responsible for performing/operating the control to gain an understanding of what procedures are being performed at the Assessed Entity. The intention of a walkthrough is for the External Assessor to gain a sufficient understanding of the process to initially identify missing elements in the design and/or operation of the control. Walkthrough procedures may include a combination of inquiry, observation, inspection of relevant documentation, recalculation, and control re-performance. A walkthrough alone is typically insufficient to meet the expected nature and extent of testing to support scoring of a requirement statement. The External Assessor must determine, based on the HITRUST testing requirements within this Assessment Handbook, the testing necessary to validate scores within each HITRUST requirement statement.

11.1.5 If only inquiry was used during an External Assessor's walkthroughs and/or interviews, additional supporting evidence must be reviewed and documented within MyCSF to corroborate scoring within a validated assessment. For examples of insufficient evidence to address HITRUST requirement statements, see Appendix A-8: Testing and Evidence FAQs & Examples.

11.1.6 On-site observations (e.g., data center visits) must include additional documentation within MyCSF to corroborate the observations (e.g., pictures, maintenance records, installation documentation, facility diagrams, etc.). The assessment documentation must also include sufficient evidence to demonstrate the timing of the observations.

11.1.7 External Assessors are not required to be on-site to perform any of the listed audit procedures. The Assessed Entity and External Assessor should determine the most effective and efficient approach for each assessment.

11.1.8 In situations where External Assessors choose to leverage alternative approaches to on-site testing, such as video conferencing, to perform necessary walkthroughs and observations, assessment documentation must clearly reflect the nature, timing, and extent of the alternative approaches used. The External Assessor must still utilize sufficient evidence to demonstrate the Assessed Entity has met the requirement statement's elements, potentially using less traditional supporting artifacts—such as maintenance records, installation documentation, facility diagrams, etc.—which collectively evidence both the implementation and ongoing operation of the corresponding HITRUST requirement statements. For additional information on remote testing approaches, see Appendix A-9: Off-site Validation Procedures.

11.2 Testing Requirements

During the planning phase of a validated assessment effort, the HITRUST External Assessor must prepare a Test Plan that outlines the anticipated testing approach of all applicable/in-scope requirement statements; it serves as the blueprint for the performance of the validated assessment.

11.2.1 The testing approach documented in the Test Plan must be based on each requirement statement's evaluative elements.

11.2.2 The Test Plan must document the testing approach, including the nature, timing, and extent of testing, which will be taken for each of the requirement statement's evaluative elements across the scope of the assessment (including all systems, locations, and business units).

11.2.3 If third parties are used to manage aspects of the in-scope environment and not carved out in an i1 or e1 (see Chapter 7.3 Carve-outs), the Assessed Entity and External Assessor must determine how they will perform the necessary testing of those third parties for each applicable requirement statement across the assessment. For guidance on the authorized HITRUST approaches for addressing third parties, see Chapter 12 Reliance & Third-Party Coverage.

11.2.4 The Test Plan should document the populations necessary for sample-based testing and how those will be obtained for each requirement statement. For details around population requirements, see Chapter 11.4 Population & Sampling.

11.2.5 All testing performed by the External Assessor in support of the validated assessment must be conducted in a 90-day period concluding with the Assessed Entity signing the Management Representation Letter (see Chapter 13.8 Management Representation Letter for more details).

11.2.6 External Assessors may conduct fieldwork planning activities, such as scoping, building Test Plans, and preparing/sending documentation request lists, prior to the start of fieldwork. For guidance on evidence utilization during and prior to the fieldwork period, see Chapter 11.3 Working Papers and Evidence.

11.2.7 Prior to the Assessed Entity signing the Management Representation Letter, the External Assessor must agree to all requirement statement scoring within the assessment.

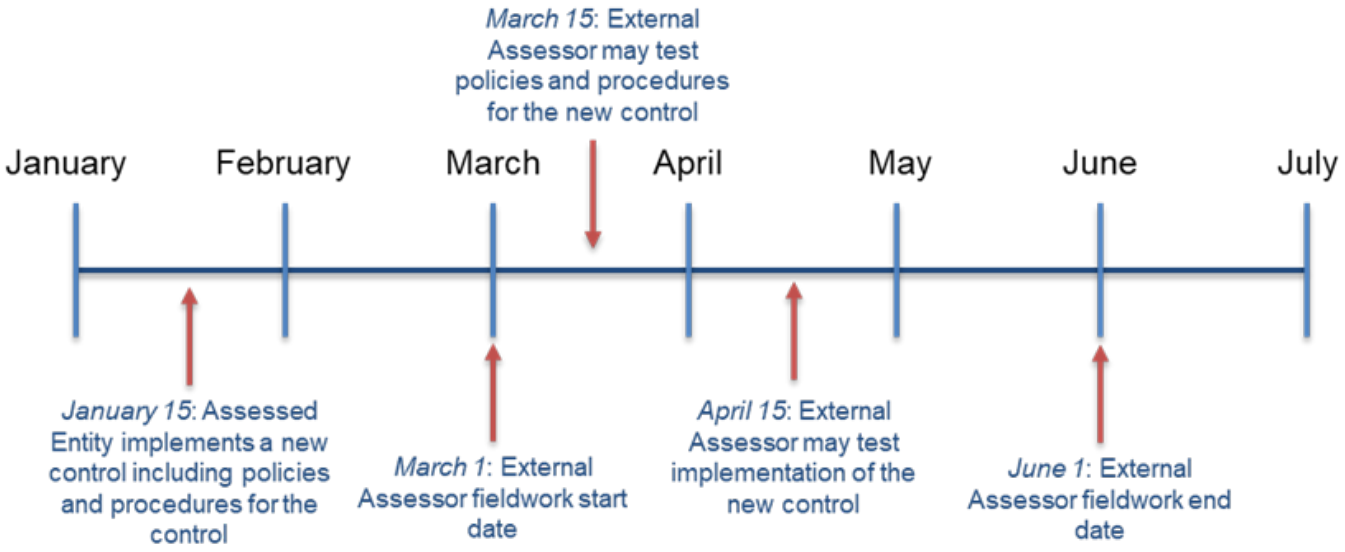
11.2.8 All controls established by the Assessed Entity in support of each of the HITRUST requirement statements must be implemented for a minimum of 90 days prior to testing (i.e., 90-day incubation period). This includes either a newly implemented control or a control remediated due to deficiencies. The control must have been operating in its current state for a consecutive 90 days (or more) before it can be tested as an implemented control.

11.2.9 When an Assessed Entity utilizes a service provider that is responsible for performing a HITRUST requirement, the Assessed Entity does not need to wait the 90-day incubation period if it is able to demonstrate the service provider's control has been implemented at least 90 days (e.g., for other

customers of the service provider). If the service provider already has a HITRUST certification or other third-party report that demonstrates implementation of the corresponding HITRUST requirement(s), the Assessed Entity may immediately utilize inheritance or rely on the third-party report. See Chapter 12. Reliance & Third-Party Coverage for additional information on inheritance and reliance.

11.2.10 Policies and procedures within the organization must be implemented for a minimum of 60 days prior to being considered by the External Assessor during the fieldwork period (i.e., 60-day incubation period). As the maximum fieldwork length is 90 days, it is possible for the Assessed Entity to remediate any policy and/or procedure deficiencies identified by the External Assessor within the first 30 days of fieldwork. If remediated within the first 30 days of fieldwork, the policies and/or procedures may be utilized to support scoring after the 60-day incubation period has completed, but prior to the end of the 90-day fieldwork period.

The following is a visual timeline of a newly implemented control.



11.2.11 If the incubation period has not been met as noted in criteria 11.2.8 or 11.2.10, the Assessed Entity must score the requirement statement based on the control state prior to remediation. There is no ability to partially score a requirement statement for meeting less than the full incubation period.

11.3 Working Papers & Evidence

Working Papers

External Assessors must create working papers based on the artifacts collected during the validated assessment which were used to support the External Assessor's review and validation of the Assessed Entity's scoring.

11.3.1 Each requirement statement that includes sample-based testing must have a testing lead sheet. The testing lead sheet must:

- Reference the population evidence (including creation date and source)
- Include the population size, population date range and sample size
- Document the sampling approach
- List the attributes tested (addressing all illustrative procedure elements / evaluative elements within the requirement statement) including description of the test procedure
- List the items selected for testing (with identifier back to the population and references to evidence for each sampled artifact)
- Include the results of testing for each sampled item and corresponding attribute(s)

11.3.2 For the *Policy* and *Procedure* maturity levels, there must be clear references to the evidence supporting the scores. The Assessed Entity or External Assessor should map each requirement statement's evaluative element to the location within the document (e.g., section, page #, paragraph, etc.) where it describes the corresponding policy and/or procedure.

11.3.3 For the *Measured* and *Managed* maturity levels, there must be clear references to the supporting measure(s), metric(s) and/or risk treatment plan supporting the scores. Additionally, documentation must demonstrate how criteria of a measure, metric, or risk treatment plan were achieved (for criteria, see Chapter 9.4 Measured Maturity Level and Chapter 9.5 Managed Maturity Level). In cases where sampling was performed the same testing lead sheet requirements in criteria 11.3.1 must be followed, along with all requirements in Chapter 11.4 Population & Sampling.

Evidence

Evidence must be collected to support the scores documented within the assessment.

Evidence is the information obtained by performing procedures during a HITRUST assessment. Evidence may include distinct types of information that influence the nature and/or extent of audit procedures needed to reach a conclusion on the requirement statement score. The various types of information include:

- Verbal information: Information obtained via responses to inquiries during the assessment.
- Observed information: Information obtained via observation (e.g., datacenter visit or a screenshot of a system configuration setting observed on a screen).
- Paper documents: Information obtained using documents (e.g., an original IT Service Level Agreement or a policy/procedure).
- Electronic information: Information obtained using electronic documents (e.g., a scanned version of a signed approval form) or data stored in an IT system (e.g., system-generated user access lists or change tickets from a ticketing system).

HITRUST has specific requirements related to evidence used during an assessment as indicated below.

11.3.4 Persuasiveness of the evidence relates to the External Assessor obtaining appropriate evidence that is sufficient for the auditor to draw reasonable conclusions. The External Assessor may rely on evidence that is persuasive rather than conclusive. The External Assessor must use professional judgment and professional skepticism in evaluating the quantity and quality of the evidence, and thus its sufficiency and appropriateness, to support the results.

11.3.5 The External Assessor must obtain more than verbal information to obtain sufficient evidence to support its procedures. Inquiry alone does not provide sufficient evidence to evaluate the maturity level of the corresponding requirement statement.

11.3.6 Evidence is more reliable (and persuasive) if there are multiple items of consistent supporting evidence obtained from different sources or of a different nature than from evidence considered individually. For example, corroborating information by observing a wireless access point in a data center may increase the reliability of a network diagram obtained from management containing the wireless access point. Alternatively, when evidence obtained from one source is inconsistent with that obtained from another, additional procedures must be performed to reconcile the discrepancy.

11.3.7 All evidence collected that supports the requirement statements scores within a validated assessment must be uploaded to MyCSF and properly referenced within the Test Plan and/or MyCSF. A validated assessment's collective body of working papers is considered incomplete if validation of only a portion of an assessment's scope and/or requirement statements are reflected in the working papers. The only exception is if the assessment will be undergoing Live QA (see Chapter 14.3 Live QA).

11.3.8 Observations and inspections performed to test the operation of a control at a point in time (e.g., configuration screenshots, system parameters, audit logs, etc.) must be performed within the fieldwork period. The evidence provided by the Assessed Entity to the External Assessor supporting those observations and inspections must include a corresponding date within the fieldwork period. The evidence supporting any observation and/or inspection must be uploaded into MyCSF (see Chapter 14.1 Quality Assurance Process).

11.3.9 Policy and procedure documents used to support scoring must be current, final (non-draft), and

periodically reviewed by the Assessed Entity in accordance with its requirements. The documents attached as evidence in MyCSF must include all relevant sections of the final, approved policy or procedure documents to support scoring of the corresponding requirement statements.

11.3.10 Policy and procedure documents may be obtained by the External Assessor prior to the start of the fieldwork period but must be reviewed and validated by the External Assessor within the fieldwork period.

11.3.11 External Assessors must link supporting evidence individually to each of the related requirement statements as well as the related control maturity level(s) within MyCSF. The External Assessor may **not**:

- Only list and/or reference the supporting evidence in a Test Plan and/or lead sheet (instead of linking the evidence in MyCSF).
- Use zip files that contain all evidence for a particular domain and/or requirement statement. (NOTE: sample-based evidence for the same test may be in a zip file if properly labeled to identify each sample item)
- Embed all evidence for a particular domain and/or requirement statement within a spreadsheet.

11.3.12 The External Assessor must include evidence documenting the date when each evidence artifact was generated. For each type of evidence, this date will be:

- Verbal Information: Date of the inquiry response
- Observed Information: Date of the observation
- Paper Documents: Date when the document was provided by the Assessed Entity
- Electronic Information: Date when the electronic record or system-generated report/document was generated by the corresponding system of record.

11.3.13 Evidence is expected to be submitted in English. Where translations of all evidence are not possible, the Assessed Entity and/or External Assessor must provide written translations from a translation service for all items selected for review during the Quality Assurance process.

11.3.14 The MyCSF assessment object will continue to retain all working papers and evidence until expiration of the certification. Assessed entities will not be able to delete the object and/or evidence within the object until expiration of the certification. For details on the HITRUST data retention policy, see Chapter 5.1 r2 Validated Assessment Workflow and Chapter 5.2 i1 and e1 Validated Assessment Workflow *Assessment Object Archiving*.

11.3.15 Assessed entities may be able to archive an assessment prior to certificate expiration with approval from HITRUST. However, HITRUST will continue to retain access to the assessment evidence and work papers until expiration of the certification. For archiving approval prior to expiration of the

certification, the Assessed Entity must contact HITRUST Support (support@hitrustalliance.net) with its rationale for the request.

11.3.16 Regardless of the evidence collection method (e.g., manual or automated), the evidence must meet all HITRUST requirements.

Evidence Generated by Intermediate Software Platforms

When External Assessors receive evidence supporting the requirement statement scores in a HITRUST assessment, they must consider the persuasiveness and reliability of the evidence, as noted in HITRUST Assessment Handbook criteria 11.3.4 and 11.3.6. As stated within the criteria, this must include an evaluation of the quality of the evidence, including its sufficiency and appropriateness.

HITRUST allows the transmission of assessment evidence from authorized intermediate software platforms into MyCSF. An intermediate software platform is a platform operated and configured by a third-party to manage an Assessed Entity's compliance efforts through integrations with the Assessed Entity's systems, tools and/or service providers. When an Assessed Entity outsources the generation of assessment evidence to a third-party there are risks of misconfiguration within these platforms that must be addressed by the External Assessor during the Assessed Entity's HITRUST assessment.

11.3.17 If the intermediate software platform:

i. Utilized integration parameters and/or queries to generate the evidence directly from the Assessed Entity's system(s), supporting tool(s), and/or service provider's system(s) or supporting tool(s), AND

ii. Transmitted the assessment evidence from the intermediate software platform directly into MyCSF,

then the below criteria must be followed to evaluate the evidence quality (in addition to all current guidance within the HITRUST Assessment Handbook). The criteria listed below are intended to validate both completeness and accuracy of evidence generated and transmitted via an intermediate software platform.

The below criteria are not required to be applied to evidence generated by the Assessed Entity and directly uploaded into the intermediate software platform. In this instance, the intermediate software platform is acting as a conduit for the transfer of the Assessed Entity's evidence into MyCSF (similar to the Assessed Entity directly uploading evidence into MyCSF). Evidence generated by the Assessed Entity in this manner should continue to follow all other HITRUST Assessment Handbook criteria related to evidence quality.

11.3.18 The External Assessor must indicate in MyCSF (e.g., within a test plan, separate workpaper, etc.) when evidence in a HITRUST assessment was provided via an intermediate software platform utilizing integration parameters and/or queries to generate the evidence directly from the Assessed Entity's system(s), supporting tool(s), and/or service provider's system(s) or supporting tool(s).

11.3.19 All procedures supporting evidence quality must be documented within MyCSF by the External Assessor. There is no required format for the documentation (e.g., within the test plan, separate

workpaper, etc.) but any supporting procedures must be attached to the requirement statement(s) containing the linked evidence and reference the corresponding evidence.

11.3.20 All evidence quality procedures must be performed within the fieldwork period or no more than 30 days prior to the start of fieldwork. The evidence must continue to meet all fieldwork timing requirements within the HITRUST Assessment Handbook.

11.3.21 Evidence quality procedures may be performed once for multiple evidence files when identical integration parameter and/or queries were used to generate the evidence.

11.3.22 The External Assessor must validate appropriate scope coverage for the evidence. As the evidence is generated via an integration originating from the intermediate software platform (without direct Assessed Entity oversight), there is a risk the integration is configured with the incorrect system and/or tool.

This validation could include inspection of the intermediate software platform's integration with the Assessed Entity's or service provider's system to confirm evidence collection from the accurate system(s) or supporting tool(s). When performing this approach, the inspection should identify if the defined integration parameter and/or query is with the appropriate system and/or tool.

For example: If "System A" uses "Active Directory server A" to manage its password settings, the External Assessor may inspect the intermediate software platform's integration parameter has been correctly defined to integrate with "Active Directory server A" to obtain the password settings (rather than another location, such as "Active Directory server B").

External Assessors may utilize alternate methods for scope validation if it appropriately validates that the evidence was generated from the correct system and/or tool.

11.3.23 The External Assessor must validate the integration parameters and/or queries used to generate the evidence were accurately configured. As the evidence is generated via an integration originating from the intermediate software platform (without direct Assessed Entity oversight), there is a risk that incorrect parameters and/or queries could result in the evidence containing incomplete or missing data.

This validation could include inspection that the parameters and/or queries were appropriately designed in the intermediate software platform. This inspection should verify the correct parameter and/or query configuration, such as data and/or record requests, dates, and/or appropriate request exclusions.

For example: If the intermediate software platform generates a population of changes to "System A" across a period of nine months, the External Assessor is expected to inspect the defined query included the request for all expected "System A" changes with correctly defined dates corresponding to the expected population.

If an Assessed Entity has documentation supporting the initial setup of a parameter and/or query, the External Assessor may use this as evidence if they can validate systematically that the design and evidence source has not been modified in the intermediate software platform (e.g., validation through a

system change date, log, etc.). However, the initial configuration must be re-inspected every two years at a minimum.

11.3.24 If the External Assessor is unable to validate the integration parameters and/or queries used to generate the evidence were accurately configured (as described in criteria 11.3.23), the External Assessor must corroborate the provided evidence with the Assessed Entity's system(s), supporting tool(s), and/or service provider's system(s) or supporting tool(s) to reasonably conclude the completeness and accuracy of the provided evidence (e.g., using record counts, re-production of evidence, etc.).

When multiple evidence files have been generated using identical parameters and/or queries within the intermediate software platform, the External Assessor may corroborate a sample (following the HITRUST sampling methodology) of evidence files to confirm accuracy of the integration parameter and/or query.

11.3.25 The External Assessor may not rely on any conclusions made by the intermediate software platform on whether the evidence achieves a specific HITRUST requirement and/or maturity score. The External Assessor must reach independent conclusions through a review of the underlying evidence utilized by the intermediate software platform to reach its conclusion. This evidence must meet all criteria outlined here and within the HITRUST Assessment Handbook.

An Assessed Entity may also be utilizing an intermediate software platform to monitor the implementation and effectiveness of a control. The Assessed Entity may use this monitoring as a measurement in support of scoring at the *Measured* maturity level if it meets the criteria of a measure or metric (see Chapter 9.4 Measured Maturity Level) and the criteria below.

11.3.26 When an Assessed Entity is using an intermediate software platform to monitor its control performance for the *Measured* maturity level, it must also have a process to validate the intermediate software platform's performance and calculation of the measure or metric (as defined in criteria 9.4.1, vi). This process must include a periodic review (minimum once every 12 months) of the measure or metric's integration parameter and/or query (as described in criteria 11.3.22 – 11.3.24) to ensure the parameters and/or queries have been correctly defined for the correct system(s) or supporting tool(s) and/or have not been modified since the previous review. The External Assessor must obtain evidence of this review to support the Assessed Entity's *Measured* maturity score.

The criteria above is not considered to be an exhaustive approach to evaluating the quality of evidence within a HITRUST assessment. External Assessors must perform the procedures they deem necessary to gain sufficient assurance around the quality of any evidence within a HITRUST assessment.

11.4 Population & Sampling

External Assessors are often required to perform sampling to validate management's scoring. The first step in the sampling process is to identify the population. The population for the assessment scope may use common process aggregation to group those systems or auditable business units that are subject to the same controls into a single population. When possible, this may be a more efficient approach than separately testing those populations. This is often the case where IT general controls are being tested and common IT processes such as change management or password administration support multiple systems. For populations, the following requirements must be met:

11.4.1 Each sample-based test must be designed appropriately to detect potential errors. For example, the population should not be obtained from a source that only contains items that already adhere to the control being tested (e.g., a test around whether anti-virus is installed should not have a sample selected from the anti-virus console since that will never yield a deviation).

11.4.2 Assessors are expected to use a sample-based test when testing the *Implemented* maturity level for a requirement statement and the illustrative procedures for the *Implemented* maturity level indicates to 'select a sample'.
NOTE: HITRUST has not contemplated within the illustrative procedures all situations where the External Assessor may need to perform sampling to address the requirement statement. The External Assessor may determine that a sample-based test is necessary to validate the HITRUST requirement even when not specifically stated within the illustrative procedures (or when a sampling badge is not present).

11.4.3 For i1, e1, and r2 (CSF v11 and later) assessments, HITRUST has included sampling badges on the requirement statement within MyCSF where sampling is expected.

11.4.4 For all validated assessments, the External Assessor is expected to document its rationale when they decide it is not necessary to perform a sample-based test (when the HITRUST requirement statement's *Implemented* Illustrative Procedure in MyCSF indicates that a sample-based test is expected to be performed).

11.4.5 There may be situations where the External Assessor will perform a sample-based test at the *Measured* or *Managed* maturity level. In those situations, the External Assessor must follow the HITRUST Population and Sampling guidance outlined in this chapter.

11.4.6 The population used to select a sample must be homogeneous. This similarity may allow certain populations to be aggregated if it follows a common process subject to the same controls. When aggregating populations with different characteristics, each process must be reviewed to validate the homogeneity, and the rationale must be documented. For example, if testing change approvals for a sample of changes, the External Assessor may determine to combine the population for two different change ticketing tools. The rationale for combining the populations may be determined by performing walkthroughs of each tool and identifying the approvals for both tools follow the same process under the same control owner.

Sample-based tests are designed to test if an attribute has been performed *historically* (e.g., period of time testing), or if that attribute is *currently* in place (e.g., point in time testing). HITRUST considers the following distinction between these types of tests:

- When an External Assessor performs a sample-based test to determine if the population has *historically* met defined attributes for a period of time, HITRUST refers to this as a "time-based" test and/or population.
- When an External Assessor performs a sample-based test to determine if a population is *currently* meeting one or more defined attributes, HITRUST refers to this as an "item-based" test and/or population.

The generation and testing of "time-based" and "item-based" populations are expected to meet the criteria defined below. See Appendix A-16 Sample-based Testing Examples for additional examples.

11.4.7 For "time-based" populations (e.g., daily backups, population of change tickets over a period of time, list of new hires/terminations), the following criteria must be met:

- The period used for the "time-based" population must be at least 90 consecutive days.
- If the period used for the "time-based" population ends more than 180 days prior to the start of the fieldwork period the selected sample must cover a population period of 180 days or more. If the population covers a period less than 180 days, a second sample must be selected for testing using an additional population to achieve a minimum of 180 days of coverage.
- The period of the "time-based" population may not begin more than one year prior to the start of the fieldwork period.

Samples selected from "time-based" populations may be tested by the External Assessor prior to the start of the fieldwork period (if the above timing criteria have been met).

Example acceptable testing scenarios assuming a fieldwork start date of July 1, 2026:

- Population used for sampling may be April 1, 2026 – June 30, 2026 (Population covers 90 consecutive days and is less than 180 days from the start of fieldwork)
- Population used for sampling may be July 1, 2025 – December 31, 2025 (Population covers the required 180 days (since it is more than 180 days from the start of fieldwork), and is not more than one year from start of fieldwork).
- Populations used for sampling may be August 1, 2025 – December 31, 2025 and June 1, 2026 – June 30, 2026 (Since the population ending December 31, 2025 covers less than 180 days, an additional sample using a population of 30 consecutive days achieves the minimum 180 days of coverage).

11.4.8 For "time-based" populations, when the population does not include a date within the fieldwork period, an additional item must be sampled within the fieldwork period to validate the control is operating

as expected.
NOTE: If the External Assessor is unable to select an additional item due to non-performance of the control within the fieldwork period, the External Assessor may select the most recent occurrence of the control prior to the start of the fieldwork period. The External Assessor must include evidence of the non-performance of the control within the fieldwork period and document this approach within the testing documentation.

11.4.9 “Item-based” populations generated at a point-in-time (e.g., population of assets, list of current employees) may be generated no more than 30 days prior to the start of the fieldwork period (e.g., as part of the planning procedures).

11.4.10 Samples selected from “item-based” populations may not be provided to the Assessed Entity until the fieldwork start date, as these are point in time tests where the corresponding evidence for each sampled item must be generated and tested within the fieldwork period.

11.4.11 Sampled items that are no longer able to be tested within the fieldwork period (e.g., decommissioned assets) must be re-selected.

11.4.12 When a control has not been performed by the Assessed Entity within one year prior to the start of fieldwork, there is no population that can be tested. The External Assessor must confirm the non-occurrence of the control using a review of evidence greater than inquiry (e.g., if there were no system changes during the period, the External Assessor should review the change management log to validate that statement OR if there were no new hires, the External Assessor should review the validity of that statement in the Human Resources employment system). After corroborating the inquiry, the full *Implemented* score may be used for that requirement. See Appendix A-8: Testing & Evidence FAQs & Examples for example potential validations of zero populations.

11.4.13 After the population has been identified, the External Assessor must determine the appropriate sample size. HITRUST has documented the following minimum requirements for sampling within the HITRUST scoring rubric:

Sample-based Testing Requirements

Sampling Scenario	Minimum Number of Items to Test
Testing a manual control operating at a defined frequency	**The expected frequency of the control must first be defined and then apply the following minimum requirements:** • Daily controls: 25 days • Weekly controls: 5 weeks • Monthly controls: 2 months • Quarterly controls: 2 quarters • Semi-annual controls: 2 halves • Annual controls: 1 year (most recent control occurrence)
Testing a manual control operating at an undefined frequency (i.e., "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 is a minimum of 3 items **Population period:** • Minimum of 90 days prior to the date of testing with a maximum of one-year prior to the date of testing
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 system behaves as configured, the outcome / result of the configuration must be tested
Sampling from point-in-time populations (e.g., endpoints, servers, current employee list)	Observe the sampling guidance provided for the "Testing a manual control with an undefined frequency" scenario provided above

11.4.14 Where an External Assessor organization has its own internal guidance on sample sizes, they must meet the minimum amounts specified by the HITRUST sampling guidance but can perform more sampling as necessary according to its methodology.

11.4.15 The sampling method utilized may be any type of probability sampling chosen by the External Assessor (e.g., random, systematic, haphazard, etc.) however the rationale for the method used must be documented.

11.4.16 Evidence must be uploaded to MyCSF for each sample selection within the sample-based test.

11.4.17 Electronic markups should be included on at least one piece of evidence (or clearly documented elsewhere) demonstrating where each of the tested attributes is located, to allow reviewers to understand how the testing was performed. When the evidence is homogeneous, markups on additional pieces of evidence are not necessary. However, if additional evidence artifacts vary from the initial evidence that included markup, additional markups must be included.

11.4.18 An automated control is a control performed by systems—not people—based on configurations, rulesets, or programming. An example of an automated control is a forced password expiration by the system after the number of days specified in the associated configuration.

11.4.19 For automated controls, testing must include evidence of both the configuration of the tool/system and a sample of one showing the tool/system is operating as expected. For example, to test that passwords demonstrate appropriate complexity, the testing approach must address:

- Configuration in the system showing the complexity settings.
- Test of one user demonstrating that they are unable to set the password unless it has met the complexity requirements.

For an automated control testing example, see Appendix A-11: Automated Control Testing Example.

11.4.20 If a control contains both manual and automated elements, the manual element(s) must be tested using the population and sampling requirements for a manual control, while the automated element may be tested using the automated control guidance. For example, a user access review may:

- Perform an automated comparison between the HR system list of terminated employees and the system users to identify accounts to be removed. This part of the control may be tested using the automated control guidance.
- Require a manual review to determine whether the access level for each user account is appropriate. This part of the control is tested using the HITRUST manual population and sampling guidance.

11.5 Documenting Exceptions

During the assessment process, HITRUST understands that control gaps may exist in the environment. The HITRUST control maturity model allows an entity to achieve certification with a small amount of control gaps across maturity levels when other corresponding requirement statements have been met. When an Assessed Entity has not met certain requirements, this typically results in a Corrective Action Plan (CAP) or Gap in the assessment and final report. For more information on CAPs and Gaps, see Chapter 13.9 CAPs and Gaps.

11.5.1 Each exception noted by the External Assessor during testing must result in a corresponding action on the assessment results. The External Assessor must determine the impact of each exception within the overall scoring of the assessment results. Typically, exceptions will result in a reduction in either "Strength" and/or "Coverage" scores when calculating the final maturity score using the HITRUST Scoring Rubric. For examples of calculating exceptions in scoring, see Appendix A-6: Rubric Scoring – Policy, Procedure, and Implemented.

11.5.2 Exceptions noted by the External Assessor during validated assessment fieldwork leading to scores of less than 100% (fully compliant) on the *Policy*, *Procedure*, or *Implemented* control maturity levels should be captured in MyCSF's "Assessor Comment" fields and/or within accompanying work papers. The documentation should be at sufficient level to enable reviewers, such as the External Assessor's QA Reviewer, the Engagement Lead, the Engagement Executive, and HITRUST Quality Assurance, to reconcile to control maturity levels, corrective action plans (CAPs), and working papers.

11.5.3 When documenting exceptions within the work papers, External Assessors must include the corresponding treatment of the exception and rationale.

11.5.4 Any conditions noted by the External Assessor necessitating a change in scoring should be discussed and agreed with management of the Assessed Entity.

For additional information on testing & evidence, see Appendix A-8: Testing and Evidence FAQs & Examples.

12. Reliance & Third-Party Coverage

The following sections outline the requirements for obtaining coverage over third-parties which impact controls within the scope of the assessment.

12.1 Third-Party Coverage

Recently completed audits and/or assessments covering some or all control areas included in the scope of a HITRUST validated assessment can possibly be leveraged (relied upon or inherited) by the External Assessor. Reliance on the results of such efforts can benefit the Assessed Entity as well as the External Assessor, as duplicative assessment-related requests and interviews can be minimized.

The decision to rely on the work of others lies solely with the External Assessor, as the External Assessor is ultimately accountable for validating an Assessed Entity's implementation of the HITRUST CSF. When using the work of others, the External Assessor should take care to design a validated assessment testing strategy that ensures they are still sufficiently involved in the validated assessment. When designing the testing strategy, the External Assessor must understand what reliance/inheritance capabilities are possible for all third parties in scope of the validated assessment.

12.1.1 The Assessed Entity and/or External Assessor must identify all in-scope third-parties during validated assessment planning and determine the testing strategy for the corresponding third-party prior to fieldwork.

12.1.2 When an Assessed Entity and/or External Assessors is unable to utilize the below testing approaches to obtain coverage of the in-scope third-party, scoring in the assessment must reflect that those requirement statements were not compliant for the corresponding third party.

12.1.3 For the i1 and e1 assessment types, Assessed Entities have the ability to carve out third-parties from the scope of the assessment. This must be properly documented within the Scope of the Assessment webform. For more information, see Chapter 7 Scoping the Assessment.

12.1.4 Assessed Entities should adopt policies requiring their third-parties to maintain each of the relevant HITRUST requirements within the CSF framework.

HITRUST recognizes four distinct strategies which can be used by an External Assessor to approach testing of third-parties:

- Reliance on Assessment Results Using Inheritance
- Reliance on Audits and/or Assessments Performed by a Third-Party
- Reliance on Testing Performed by the Assessed Entity
- Direct Testing of Third-Party Controls

12.2 Reliance on Assessment Results Using Inheritance

HITRUST provides Assessed Entities with a method for placing reliance on previously assessed HITRUST-compliant control environments by utilizing inheritance. Inheritance may reduce and/or eliminate the need for duplicative control assessment testing by Assessed Entities and/or External Assessors during a HITRUST assessment.

The inheritance function provides Assessed Entities and External Assessors the ability to inherit previously assessed HITRUST control testing maturity scores (and pertinent commentary) from any other qualified "inheritable" HITRUST assessment. HITRUST requirement statements may be inherited into/from any version of the HITRUST CSF (cross-version inheritance).

While performing a HITRUST assessment Assessed Entities have the option to use ***internal*** and/or ***external*** types of inheritance:

- ***Internal*** inheritance uses the inheritance functionality to share assessment results between assessments of a single organization (e.g., between a shared IT service and a business unit).

- ***External*** inheritance uses the inheritance functionality to share assessment results between assessments of different organizations (e.g., between a CSP and its tenants).

12.2.1 Inheritance into a validated or readiness assessment (for any assessment type) is allowed from the following assessment types while in the *Certified* status:

- HITRUST Essentials, 1-year (e1) Validated Assessment
- HITRUST Implemented, 1-year (i1) Validated Assessment
- HITRUST Risk-based, 2-year (r2) Validated Assessment

If an assessment is in the *Not Certified* status, inheritance (or reliance) is allowed if it is a complete validated-only report within one year from the report date. Assessments with a status of *Expired*, *Suspended*, or *Revoked* are not inheritable (and may not be relied upon). See Chapter 15.1 HITRUST Reporting for additional information on the various assessment and certification statuses.

12.2.2 Inheritance from a readiness or incomplete validated assessment (for any assessment type) is only allowed into a readiness assessment (utilizing internal inheritance). Inheritance from those assessments is not allowed into a validated assessment since it has not completed the HITRUST Quality Assurance review process (see Chapter 14 Undergoing Quality Assurance).

An Assessed Entity will fall into one of the following roles during the inheritance process:

- **Inheritance User** (also may be called a "Tenant"): The Assessed Entity which owns the "inheriting" assessment. The Inheritance User is placing reliance on controls that were previously assessed and

validated in a separate HITRUST assessment. The separate assessment may be owned by another organization (external inheritance) or the same organization (internal inheritance).

- **Inheritance Provider**: The Assessed Entity which owns the “inheritable” HITRUST assessment.

HITRUST has established the following requirements for **Inheritance Users**:

12.2.3 Inheritance Users may directly apply internal inheritance scores to the corresponding requirement statement. See MyCSF Help | User Guide for detailed instructions.

12.2.4 Internal inheritance (or external inheritance from the same subscriber) from an e1 or i1 expiring within 6 months or an r2 assessment expiring within 12 months must be approved by HITRUST and have an appropriate rationale. This is intended to avoid extending a certification beyond the assurance limitations of the previously performed assessment. The Assessed Entity and/or External Assessor should contact HITRUST support (support@hitrustalliance.net) for additional guidance.

12.2.5 Inheritance from an e1, i1 or r2 assessment into the same assessment type with an identical scope is not allowed without prior approval by HITRUST. The Assessed Entity and/or External Assessor should contact HITRUST support (support@hitrustalliance.net) for additional guidance.

12.2.6 Inheritance Users must submit all external inheritance requests to the Inheritance Provider using the automated approval workflow process. See MyCSF Help | User Guide for detailed instructions.

12.2.7 For external inheritance requests, the Inheritance User must use the HITRUST Shared Responsibility Matrices (SRMs) that are available for download from MyCSF or the HITRUST website (HITRUST Shared Responsibility and Inheritance Program – HITRUST Alliance) to help identify which requirement statements can be inherited based on their corresponding SRM Type designations.

12.2.8 Inheritance Users must use the SRM specific to the service provider in scope of its assessment when available. When the service provider does not offer a provider-specific SRM, the Inheritance User must use the baseline SRM template.

12.2.9 The SRM may not be used to support scoring within the validated assessment. Reliance on a service provider’s HITRUST assessment must be done utilizing inheritance or attaching a HITRUST validated assessment report.

12.2.10 Inheritance Users must submit all inheritance requests to the “inheriting” HITRUST assessment prior to the end of the 90-day assessment fieldwork period and no more than 30 days prior to the start of fieldwork.

12.2.11 Inheritance Users must have a valid business justification for use of inheritance supported by a strategy and approach for the appropriate level of control reliance.

12.2.12 Requirement statements that have been marked as ‘Not Applicable (N/A)’ by the Inheritance Provider, but marked inheritable in the SRM, may be inherited by the Inheritance User in their HITRUST

assessment. For scoring information, see Chapter 8.3 Not Applicable (N/A) Requirement Statements.

HITRUST has established the following requirements for **Inheritance Providers**:

12.2.13 For an Inheritance Provider to allow external inheritance requests, it must enable the use of external inheritance and consent to external Inheritance User terms and conditions. See MyCSF Help | User Guide for detailed instructions.

12.2.14 Inheritance Providers should process (approve or reject with comment) external inheritance requests in a timely manner to help ensure Assessed Entities are able to apply all approved external inheritance requests before the end of the 90-day assessment fieldwork period.

12.2.15 Inheritance Providers must validate the following when considering approving or rejecting an external inheritance request:

- Request is from a valid Customer of the Inheritance Provider.
- The Customer has purchased/contracted with the Inheritance Provider the service(s) in scope of the assessment.
- The inheritance weight is within the boundaries the Inheritance Provider has established or the rationale for a higher weight has been agreed with the Inheritance Provider.

12.2.16 If the Inheritance Provider has questions or concerns on an inheritance request, it should engage directly with the Inheritance User in a timely manner.

12.2.17 Inheritance Providers are eligible to create and publish a HITRUST SRM tailored for its “inheritable” HITRUST assessment. The HITRUST SRM provides a mechanism for Inheritance Providers to communicate expectations to Inheritance Users to streamline inheritance request processing (e.g., partial inheritance weight limits, support contact information, and processing lead-time or Service Level Agreements (SLAs), if applicable).

12.2.18 A HITRUST assessment that reaches its expiration date will automatically unpublish on the expiration date of the certification, which disables the assessment’s inheritability.

12.2.19 Prior to an assessment being unpublished, Inheritance Providers should respond to all open inheritance requests.

12.2.20 Inheritance Providers should publish their recertified assessment for inheritance in a timely manner to minimize any downtime impact on their Inheritance Users. Inheritance Providers can work directly with their HITRUST Customer Success Manager (CSM) or contact HITRUST Support (support@hitrustalliance.net) to migrate any outstanding external inheritance requests (i.e., with status of created or submitted and not approved or rejected) from an expired assessment to a new HITRUST assessment.

12.2.21 A bridge certificate (see Chapter 15.8 Bridge Assessments) does not extend the expiration date of a HITRUST report. As a result, an "inheritable" HITRUST assessment with a bridge certificate will not extend the assessment's inheritability.

12.2.22 If an Inheritance Provider obtains a new certification of the same assessment type and scope before the expiration date of the prior certification, the prior certification will no longer be inheritable as it will be considered *Expired*. See Chapter 15.1 HITRUST Reporting for additional information on the various certification statuses.

Inheritance scoring

Requirement statements must be scored for each service provider that manages performance of the corresponding HITRUST requirement statement within an Assessed Entity's assessment (unless the service provider is carved out – see Chapter 7.3 Carve-outs). In situations where control performance responsibility is shared between the Assessed Entity and/or one or more Inheritance Providers, the Assessed Entity and/or its External Assessors should determine a corresponding amount of responsibility for each party based on its role within the scope of the assessment. In situations where there is one service provider that is responsible for a particular requirement statement in its entirety, the Assessed Entity may be able to request full inheritance from the provider. However, in situations where the responsibility is shared, either between the Assessed Entity and a Service Provider or between multiple Service Providers, the Inheritance User (i.e., Assessed Entity) will utilize partial inheritance instead of full inheritance.

For partial inheritance, the Inheritance User assigns a percentage to each corresponding responsible party (i.e., Assessed Entity or Inheritance Provider(s)) on a per requirement statement basis to produce a weighted average which represents the resulting maturity score for each requirement statement. After assigning the corresponding weights, MyCSF will automatically calculate the score based on the assigned weights and inherited scores. HITRUST offers Assessed Entities and its External Assessors an Inheritance Calculator tool to preview how inheritance scores and weights impact assessment scoring.

HITRUST has established the following requirements for inheritance scoring:

12.2.23 In situations where an SRM allows inheritance (either partial or full), inheritance may not be used if the Assessed Entity has the sole responsibility, authority, and accountability over the control's implementation and enforcement to achieve control compliance.

12.2.24 Full inheritance may only be asserted if responsibility for performance of a requirement statement, in its entirety, is functionally outsourced to the Inheritance Provider, and therefore, the Assessed Entity is completely reliant upon the Inheritance Provider. In addition, the corresponding SRM for the Inheritance Provider (or baseline SRM when the provider does not have an SRM) should indicate the full inheritance is allowed. In cases where the SRM does not allow full inheritance, the Inheritance User must agree with the Inheritance Provider to utilize full inheritance.

12.2.25 Partial inheritance must be used if responsibility for performance of a control to address a HITRUST requirement statement is shared, either between the Assessed Entity and the Inheritance Provider(s), or between multiple Inheritance Providers (if fully outsourced).

12.2.26 To assign an appropriate inheritance weight percentage, the Inheritance User must determine the percentage of the assessment scope and/or control responsibility which is outsourced, and whether that responsibility is fully or partially covered, by the Inheritance Provider's scoring. The defined weight percentage may or may not be the maximum percentage allowed by the Inheritance Provider and/or HITRUST SRM since it is based on the corresponding control responsibility. The Inheritance User must agree with the Inheritance Provider for any weight percentage above the maximum allowed in the SRM. For examples of inheritance calculations, please see Appendix A-12: Inheritance FAQs & Examples.

12.2.27 The percentage weights assigned by the Inheritance User between the Assessed Entity and/or Inheritance Provider(s) must include a documented rationale within the MyCSF requirement statement validated by the External Assessor. The rationale should be based on the amount of responsibility for each party related to the control environment and scope of the assessment. Since responsibilities may vary per control, requirement statements may have different weights (and rationales).

12.2.28 For external inheritance, the Inheritance User cannot modify the Inheritance Provider's originating control maturity scores from the "inheritable" HITRUST assessment once applied to the "inheriting" HITRUST assessment. Inheritance Users may modify scores applied using internal inheritance.

Since requirement statements marked as 'N/A' are not scored, the following provides an explanation of how inheriting an 'N/A' impacts the Assessed Entity's assessment scoring calculation:

- **Full (100% weight) Inheritance 'N/A' Scoring:** The inherited requirement statement is marked as 'N/A' within the Assessed Entity's assessment and not scored. It is excluded from the aggregate domain maturity score. The inherited 'N/A' rationale is included in the final report.

- **Partial Inheritance 'N/A' Scoring:** The inherited requirement statement is not marked as 'N/A' within the Assessed Entity's assessment and the directly tested (non-inherited) portion of the requirement statement is scored. The inherited requirement statement is not included in the numerator or denominator during the scoring calculation (for both the requirement statement and domain scoring).

For further information and examples on inheritance, please see Appendix A-12: Inheritance FAQs & Examples. For the latest version of the Shared Responsibility Matrix, see HITRUST Shared Responsibility and Inheritance Program – HITRUST Alliance.

12.3 Reliance on Audits and/or Assessments Performed by a Third-Party

The results of recently completed audits performed by a third-party auditor against the scoped environment can—at the External Assessor's discretion—be relied upon to reduce the extent of the External Assessor's direct testing. The following requirements must be met for reliance to be placed on the results of third-party audits:

12.3.1 A valid business justification must exist for relying on the third-party report. For example, it is inappropriate to rely on a SOC 2 Type II report covering a service provider not used by the Assessed Entity.

12.3.2 A formal, final report documenting the results of the third-party audit must exist prior to the end of the External Assessor's fieldwork period. Third-party audits failing to produce a final report inclusive of the following elements should not be relied upon by the External Assessor:

i. a description of the audit's scope;

ii. the timeframe that the testing covers (for period-of-time reports), the date that the final report was issued (for point-in-time reports), or the timeframe that the report is valid (for forward-looking reports);

iii. the auditor's procedures performed;

iv. the conclusions reached for each control/requirement tested; and

v. the compliance gaps/testing exceptions noted.

12.3.3 The third-party auditor must be independent of management and objective of the controls and processes audited. "Objectivity" refers to a lack of bias, judgment, or prejudice, and "independent" means not being influenced or controlled by others in matters of opinion, conduct, etc. Only third-party audits performed by individuals sufficiently independent of the Assessed Entity and objective of the controls/ requirements tested should be relied upon.

12.3.4 Third-party audits older than one year in age should not be relied upon. This one-year reliance threshold is determined by comparing the start date of the External Assessor's fieldwork to the following:

- For point-in-time reports (such as a PCI DSS ROC): To the date of the third-party auditor's final report.
- For period-of-time reports (such as a SOC 2 Type II report): To the end date of the reporting period.
- For future-looking certifications (such as a HITRUST certification): To the certification date or to the date of the most recent surveillance audit/interim assessment.

NOTE: If a recurring third-party report is in process but has not been issued by the end of the assessment's fieldwork window, the External Assessor may attach the previous third-party report as a placeholder and submit the assessment. However, HITRUST will open a task during QA and requires the updated third-party report to be provided (and any scores updated) prior to close of the QA process.

12.3.5 The External Assessor and HITRUST must both be authorized recipients of the third-party audit report. While the External Assessor and HITRUST do not need to be explicitly named as authorized recipients, the owner of the report must be allowed to distribute the report to such parties. This requirement exists specifically to avoid situations in which reliance was placed on a report that cannot be shared with HITRUST, thus restricting HITRUST's ability to perform meaningful QA procedures. Reliance cannot be placed on third-party audit reports for which neither HITRUST nor the External Assessor are authorized to receive. For example:

- The AICPA specifically states for SOC 1 reports: "Use of these reports is restricted to the management of the service organization, user entities, and user auditors." As HITRUST (and likely the External Assessor) is not a member of any of those recipient groups, a SOC 1 report cannot be used as a valid report for third-party reliance.

12.3.6 The scope of the third-party audit (in terms of systems, facilities, and business units) must overlap with that of the HITRUST validated assessment. Third-party audits of only systems or organizational elements outside the scope of the validated assessment should not be relied upon.

12.3.7 The controls assessed in the third-party audit must overlap with that of the HITRUST validated assessment. Third-party audits of only controls or compliance requirements outside the scope of the validated assessment should not be relied upon.

12.3.8 When designing a reliance strategy, the External Assessor must map the requirement statements and evaluative elements included in the HITRUST validated assessment to the controls/requirements tested in the third-party audit. In the absence of this mapping, the External Assessor cannot form a meaningful reliance strategy and therefore lacks an adequate basis for reliance. To support HITRUST's QA efforts, this mapping as well as the third-party audit report must be attached to or referenced in MyCSF.

For example: An External Assessor would not be able to use a PCI AoC (Attestation of Compliance) for reliance as it does not include detailed testing procedures within the report. However, an External Assessor may use a PCI RoC (Report on Compliance) if it is able to map the report's procedure(s) to a corresponding HITRUST requirement statement's evaluative element(s).

12.3.9 The depth/rigor of testing performed by the third-party auditor must reasonably align with the testing expectations placed upon External Assessors by HITRUST. Only those audits and assessments featuring tests of control design / operation / implementation / effectiveness using audit procedures such as inspection of evidentiary matter and sampling (utilizing statistically meaningful sample sizes as applicable) are suitable for reliance. For example, procedures executed by a service organization's auditor during a SOC 2 Type I examination should not be relied upon given a SOC 2 Type I examination's lack of substantive testing.

12.3.10 The third-party audit report must be prepared in accordance with the publicly available corresponding professional standards. A third-party audit report that is not prepared in accordance with the corresponding professional standards should not be relied upon.

12.3.11 HITRUST reserves the right to reject the use of a third-party audit report when there are concerns on the performance, competence and/or objectivity of the third-party auditor.

12.3.12 When reliance is placed on a third-party audit report to reduce the extent of the External Assessor's direct testing, the External Assessor's workpaper documentation must include:

- The third-party audit report upon which reliance was placed. The report must be attached to or referenced within MyCSF.
- The type or focus of the third-party audit (e.g., SOC 2 Type II).
- The third-party audit's final report date and timeframe covered.
- The scope of the assessment that is covered by the third-party audit report.
- The External Assessor's mapping of the requirement statements and evaluative elements included in the HITRUST validated assessment to the controls/requirements tested in the third-party audit.
- Procedures performed and results of testing in the third-party report for the control(s) mapped to the HITRUST requirement statement, including any noted exceptions and External Assessor's treatment of exceptions in the HITRUST maturity scoring.

12.4 Reliance on Testing Performed by the Assessed Entity (i.e., Internal Assessors)

In advance of a validated assessment, an Assessed Entity may perform assessment procedures against the HITRUST CSF internally, either using an organizational function (e.g., Internal Audit) or using an outside party (e.g., an authorized External Assessor, a professional services firm possessing a HITRUST readiness license). The individuals performing this testing are referred to as “Internal Assessors” and their function/team is referred to as the “Internal Assessor Function.” The results of recently completed testing performed by Internal Assessors can—at the External Assessor’s discretion—be relied upon by the External Assessor to reduce the extent of the External Assessor’s direct testing.

Please note that only External Assessors are eligible to validate scores on a validated assessment. However, if the Assessed Entity chooses to perform testing that can be leveraged by its External Assessor, HITRUST has established guidance which:

- Establishes a framework for the External Assessor—at its discretion—to rely on that testing.
- Defines the requirements that must be met by both by the Assessed Entity and by the External Assessor for reliance to occur.
- Sets forth requirements which prevent over-reliance and undue reliance on an Internal Assessor’s testing.

12.4.1 Regardless of the amount of reliance placed upon the work of an Internal Assessor function, the External Assessor must lead and/or participate in walkthroughs of the Assessed Entity’s control environment.

In addition, the following requirements must be met in order for an External Assessor to place reliance on an Internal Assessor’s testing:

12.4.2 Testing performed on behalf of management by an outside party lacking a license to use the HITRUST CSF in a commercial context should not be relied upon by the External Assessor. If an outside party performed or was engaged to act as an Internal Assessor (i.e., using a “facilitated self-assessment”), that outside party must be either:

i. A professional services firm designated as an Authorized External Assessor,

ii. In possession of a HITRUST readiness license specific to the engagement, or

iii. An agent of management (e.g., a loan staff, staff augmentation, or contractor arrangement.)

12.4.3 The Internal Assessor function must be approved by HITRUST via an application process. See Internal Assessors for more information. Testing performed by an organizational function not previously

authorized by HITRUST should not be relied upon by the External Assessor.

12.4.4 The Internal Assessor's testing conclusions (i.e., per requirement statement, per maturity level scoring) must be entered into MyCSF. Also, accompanying work papers must be attached to or referenced in MyCSF.

12.4.5 The Internal Assessor function must be objective of the controls and processes being tested. "Objectivity" refers to a lack of bias, judgment, or prejudice. Example situations where objectivity is not considered to exist include:

- When the Internal Assessor function and the function being assessed (e.g., IT) roll up to the same executive.

- When the Internal Assessors are involved in the design, implementation, or operation of the controls being tested.

12.4.6 The Internal Assessor must be competent with respect to the HITRUST CSF, the HITRUST Assurance Program, and the overall HITRUST validated assessment process. "Competence" is the set of demonstrable characteristics and skills that enable, and improve the efficiency of, performance of a job. Testing performed by individuals lacking the necessary competence should not be relied upon by the External Assessor.

12.4.7 All Internal Assessors must hold an active CCSFP credential for testing to be relied upon by the External Assessor (i.e., 100% of hours incurred by the Internal Assessor function must be incurred by a CCSFP). If this 100%-hour threshold is not met, the External Assessor should not rely on the Internal Assessor function's testing.

12.4.8 The Internal Assessor's testing cannot be based on evidence more than 90 days old. Internal Assessor testing using evidence greater than 90 days old should not be relied upon by the External Assessor. This 90-day age threshold is determined by comparing External Assessor's validated assessment fieldwork start date to:

i. The date the associated evidence was produced / generated / captured (for point-in-time evidence such as screenshots of configurations),

ii. The end date of the population date range (for period-of-time populations such as the listing of newly hired employees), or

iii. The date of the observation (for observation-based tests).

12.4.9 The scope of the Internal Assessor's testing (in terms of systems, facilities, and business units) must mirror that of the HITRUST validated assessment. An Internal Assessor's testing of out-of-scope systems, facilities and organizational elements should not be relied upon by the External Assessor.

12.4.10 Internal Assessors are not required to test all requirement statements within the HITRUST

validated assessment. External Assessors must perform direct testing for any requirement statements not relied upon or tested by the Internal Assessor. Additionally, there is no limit on the amount of requirement statement testing performed by an Internal Assessor that an External Assessor may rely upon.

12.4.11 The depth / rigor of testing performed by the Internal Assessor must adhere to the HITRUST's testing expectations placed upon External Assessors. Specifically, the Internal Assessor's testing must be performed in accordance with requirements set forth in this document. Internal Assessor testing which fails to adhere to HITRUST's assessment requirements should not be relied upon by the External Assessor.

12.4.12 The testing documentation and supporting work papers produced by the Internal Assessor must adhere to HITRUST's assessment documentation requirements placed upon External Assessors. Specifically, the Internal Assessor's testing must be documented in accordance with requirements set forth in Chapter 11 Testing & Evidence Requirements. Poorly documented testing performed by Internal Assessors should not be relied upon by the External Assessor.

12.4.13 The External Assessor must gain assurance through review of the Internal Assessor testing that the testing was adequately executed. To gain comfort that the Internal Assessor's tests were adequately executed, the External Assessor:

i. must document its review performance of the Internal Assessor's work papers (including its reperformance approach and methodology) and

ii. must reperform (by inspection of those work papers) a portion of the Internal Assessor's testing. NOTE: "Reperforming" an Internal Assessor's testing involves inspecting, in detail, the evidence examined by the Internal Assessor and reconciling the information therein to (a) the conclusions reached by the Internal Assessor, and (b) to information gleaned via the External Assessor's walkthroughs of the control environment.

12.4.14 When reperforming an Internal Assessor's testing, the External Assessor must gain reasonable comfort that the Internal Assessor collected the same evidence, tested the same attributes, and reached the same conclusions.

12.4.15 When placing reliance on an Internal Assessor's sample-based test, the External Assessor must reperform at least 20% of the Internal Assessor's sample testing (rounding up to the nearest whole number as necessary).

12.4.16 If reperformance of the Internal Assessor's testing yields results that call into question the adequacy of the Internal Assessor's testing or accompanying documentation, the External Assessor should either not place reliance on that testing, supplement the Internal Assessor's testing to address the identified testing gap(s), or allow the Internal Assessor the opportunity to remediate the testing gap.

12.4.17 When reliance is placed on an Internal Assessor's testing to reduce the extent of the External Assessor's direct testing, the External Assessor's documentation, as captured in MyCSF, must clearly include:

i. An identification of the requirement statements where reliance on the Internal Assessor's testing was placed.

ii. Confirmation that External Assessor reperformed the Internal Assessor's testing and addressed identified testing flaws by either:

a. not placing reliance on the flawed testing,
b. supplementing the testing to address the identified testing flaws, or
c. allowing the Internal Assessor the opportunity to remediate the flawed testing.

12.4.18 For sample-based tests being relied upon, an identification of which and how many sample(s) were reperformed by the External Assessor along with the conclusions reached by the External Assessor for each reperformed item is required. When reliance is placed on an Internal Assessor's testing to reduce the extent of the External Assessor's direct testing, the Internal Assessor's documentation, as captured in MyCSF, must clearly reflect / include:

i. The scoring levels reached by the Internal Assessor on a per requirement statement, per maturity level basis.

ii. A populated Internal Assessor timesheet reflective of the hours incurred by the Internal Assessor function.

iii. The Internal Assessor's work papers/supporting evidence (either attached to or referenced).

12.5 Direct Testing of Third-Party Controls

HITRUST understands that in certain instances, the third-party does not have a HITRUST assessment nor a report providing coverage of the expected requirements. In these situations, the External Assessor is only able to provide scoring of the third party's maturity level by direct testing of the requirement statements at the corresponding entity. HITRUST will accept this testing as long as the same testing rigor was utilized when testing the Assessed Entity. See Chapter 11 Testing & Evidence Requirements for testing expectations.

13. Assessment Submission Process

When performing a validated assessment, there are several required items that the Assessed Entity and External Assessor must complete in addition to its scoring and validation of the assessment. These deliverables include the following:

- QA Reservation
- Audits and Assessments Utilized
- Validated Report Agreement
- Automated Quality Checks
- Test Plan
- External Assessor Time Sheet
- QA Checklist
- Management Representation Letter
- CAPs and Gaps

NOTE: A readiness assessment does not require all the above deliverables to be completed. When the Assessed Entity completes the *Answering Assessment* phase, the readiness assessment may be submitted to HITRUST.

13.1 Quality Assurance (QA) Reservation

HITRUST utilizes a reservation system within the MyCSF platform, allowing Assessed Entities to schedule the start of Quality Assurance (QA) procedures for all HITRUST validated assessment types.

During the QA reservation process, the Assessed Entity must indicate the date that they plan to submit the assessment to HITRUST and, based on the planned submission date, select an available QA Block during which HITRUST will begin QA review procedures on the assessment. QA Blocks are one-week periods where HITRUST will begin QA procedures on the assessment. Reservation slots occur within QA Blocks, and each QA Block contains a set number of reservation slots. MyCSF displays the QA Blocks that are available to reserve.

HITRUST encourages Assessed Entities to make their reservations as early as possible to secure their requested date because the reservation system will allow reservations up to one year in advance.

HITRUST begins QA procedures on the submitted assessment during the QA Block period. Assessed Entities should typically expect to hear from HITRUST within seven to ten business days after the end of the QA Block. Failure to hear from HITRUST during the week of the scheduled QA Block does not indicate that QA has not started.

Key requirements for the QA reservation process:

13.1.1 All Assessed Entities must make a QA reservation to submit their HITRUST r2, i1 or e1 validated assessment. The Assessed Entity may book a QA reservation during the following phases of the assessment workflow: *Answering Assessment*, *Performing Validation*, *Inputting CAPs and Signing Representation Letter*, and *Reviewing CAPs*.

13.1.2 A validated assessment report credit is required to make a reservation.

13.1.3 Reservations may be made up to one year in advance of the current date.

13.1.4 Prior to booking a reservation, Assessed Entities must acknowledge the cancellation policy. The cancellation policy outlines the date by which the Assessed Entity can make a modification or cancel the reservation without incurring a fee.

13.1.5 The submission date of the assessment, which is the date the assessment must be submitted to HITRUST, must be entered into MyCSF as part of the reservation process. Assessed Entities should work with their External Assessors to plan their submission date. Failure to submit the assessment by the submission date will result in cancellation of the reservation and a change fee being billed to the Assessed Entity. A new reservation will need to be made in order to submit the assessment to HITRUST.

13.2 Audits and Assessments Utilized

The Audits and Assessments Utilized webform is completed by the Assessed Entity and External Assessor to document reliance placed on the work of others by either the usage of the inheritance feature within MyCSF or reliance on third-party attestation reports in support of the validation procedures performed by the External Assessor.

13.2.1 *Inheritance*: When inheritance is applied to a requirement statement by the Assessed Entity, MyCSF automatically adds the associated HITRUST assessment that was inherited from and populates that HITRUST assessment's details into the Audits and Assessments Utilized webform (including the assessment name, type, report date, and assessment domains for which external inheritance was utilized). The External Assessor will be required to complete the assessed organization name field and map the inherited HITRUST assessment to related in-scope platforms and facilities within the Audits and Assessments Utilized webform.

13.2.2 *Reliance*: For any third-party attestation reports being relied upon, the External Assessor or Assessed Entity (depending on who uploaded the document) must tag the report within the Documents repository or within the requirement statement (if uploading the document within a particular requirement statement) by checking the box labeled, "Is this an attestation report issued by a third party?" After tagging the document as an attestation report issued by a third party, the External Assessor or Assessed Entity populates the various report details, including assessed organization, report type, and report dates. The External Assessor or Assessed Entity must map the utilized third-party attestation report to the related in-scope platforms and facilities within the Audits and Assessments Utilized webform. NOTE: Each document should be uploaded to MyCSF only once to ensure the Audits and Assessments Utilized webform does not contain duplicate entries.

13.2.3 The Audits and Assessments Utilized webform may only include information related to the assessment's usage of inheritance and/or reliance. Reports used to support direct testing of a requirement statement (such as Penetration Tests, Vulnerability Assessments, Risk Assessments, etc.) should not be included in the Audits and Assessments Utilized webform.

NOTE: If the offline assessment template is utilized, the External Assessor or Assessed Entity also may tag documents as attestation reports issued by a third party by selecting "Yes" in the "Third Party Report?" column within the Documents tab of the offline assessment workbook. After uploading the offline assessment, the External Assessor or Assessed Entity will follow the remaining steps within the webform.

13.3 Validated Report Agreement

The Validated Report Agreement (VRA) is an agreement that must be signed by both the Assessed Entity and HITRUST prior to submission of the assessment to HITRUST. The VRA for all HITRUST validated assessment types is completed via MyCSF using an electronic signature workflow.

The VRA webform can be completed by the Assessed Entity during the following phases of the assessment workflow: *Answering Assessment*, *Performing Validation*, *Inputting CAPs and Signing Representation Letter*, and *Reviewing CAPs*.

13.3.1 The Assessed Entity must complete the VRA webform by entering the name, job title, and email address of the individual who will sign the VRA as well as the address of the organization.

13.3.2 A designated individual at the Assessed Entity must electronically sign the VRA. The signer of the VRA is not required to have a MyCSF account.

13.3.3 HITRUST must sign the VRA prior to submission of the assessment to HITRUST. After being signed by the Assessed Entity, the VRA is automatically routed to HITRUST for signature.

The Assessed Entity and External Assessor should allow up to one business day for the VRA to be signed by HITRUST. The Assessed Entity may contact its HITRUST Customer Success Manager (CSM) or HITRUST Support (support@hitrustalliance.net) with any questions related to signing of the VRA. Once signed by both parties, the VRA will automatically be loaded into MyCSF and emailed to the individual who signed it.

13.4 Automated Quality Checks

During the pre-submission phases of the assessment workflow, MyCSF runs a set of automated quality checks that provide an early warning of potential quality concerns in the assessment. As the Assessed Entity and External Assessor work on the assessment, MyCSF displays potential quality issues (PQIs), resulting from the automated quality checks.

13.4.1 All PQIs identified by the automated quality checks are presented within the assessment in MyCSF with a description of the issue, the flagged comment or scoring, recommendations on how to address, as well as the option to override/accept the issue and to provide an accompanying explanation.

13.4.2 All PQIs must be addressed or overridden/accepted (with explanation) before the assessment can proceed to the next phase of the assessment workflow. For example, PQIs identified during the Answering Assessment phase must be addressed or overridden/accepted before the assessment can proceed to the Performing Validation phase and PQIs identified during the Performing Validation phase must be addressed or overridden/accepted before the assessment can proceed to the Inputting CAPs and Signing Rep Letter phase.

13.4.3 Each PQI that is overridden by the Assessed Entity must be approved by the External Assessor. All overridden PQIs will be reviewed during HITRUST Quality Assurance review and may require further clarification from the Assessed Entity and/or External Assessor.

Running quality analytics during the pre-submission phases of the assessment workflow allows for more timely detection and communication of potential concerns and allows for an opportunity to remediate the potential issues prior to the submission of the assessment to HITRUST.

13.5 Test Plan

13.5.1 During the planning phase of a validated assessment effort, the External Assessor must prepare a Test Plan which outlines the anticipated testing of all in-scope requirement statements and serves as the blueprint for the performance of the validated assessment. For detailed requirements on the Test Plan, see Chapter 11 Testing & Evidence Requirements.

13.5.2 The Test Plan must be uploaded to MyCSF by the External Assessor during the Performing Validation phase of the assessment workflow.

An Excel-based Test Plan template is available for use by External Assessors performing i1 or e1 validated assessments. This template can be downloaded from the Test Plan upload page in MyCSF. The use of the template is not required. (The template is not currently available for r2 validated assessments due to the ability to tailor r2 requirements based on the Assessed Entity's factor responses.)

NOTE: The Test Plan template is not available within assessments for Assessed Entities with Report-Only access to MyCSF. For such assessments, the External Assessor must manually build its Test Plan.

13.6 External Assessor Time Sheet

Each validated assessment must include a documented External Assessor Time Sheet. The External Assessor team should work with the Assessed Entity during planning to determine the assessment fieldwork testing period and confirm the start date and end date of the fieldwork period.

13.6.1 The time reported within the timesheet must include all time spent on performance of the engagement by the External Assessor.

13.6.2 The time sheet must accurately reflect the start and end dates of the External Assessor's fieldwork period.

- Fieldwork start date: The first day the External Assessor team starts reviewing the collected support data.

- Fieldwork end date: The date the External Assessor team completes its testing procedures and no new support data is received. *

*NOTE: The External Assessor may optionally perform its QA review and/or assessment wrap-up procedures within two weeks following the fieldwork end date. However, no new testing or evidence collection is permitted during this period.

13.6.3 The time sheet must include the names, roles, CCSFP number, and number of hours worked for each individual from the External Assessor who worked on the assessment.

13.6.4 Prior to completing the External Assessor Time Sheet, the Engagement Executive and QA Reviewer must be assigned on the assessment's Name & Security page in MyCSF. The user making the assignments must select an individual holding a CCSFP certification for Engagement Executive and an individual holding a CHQP certification for QA Reviewer.

13.6.5 The External Assessor Time Sheet must be completed during the *Performing Validation* phase of the assessment workflow.

13.6.6 The External Assessor is required to have 50% of time incurred on the engagement performed by HITRUST CCSFPs.

13.7 QA Checklist

13.7.1 Prior to submitting a validated assessment to HITRUST, the External Assessor's Engagement Executive and Quality Assurance Review Executive are required to perform a quality assurance review of the assessment's documentation.

13.7.2 This pre-submission QA review should be driven by the items in the QA Checklist within MyCSF. The review focuses on whether the HITRUST requirements were observed.

13.7.3 The QA Checklist in MyCSF is required to be electronically completed by the Engagement Executive and Quality Assurance Review Executive during the *Performing Validation* phase of the assessment workflow after the Test Plan has been uploaded and the External Assessor Time Sheet has been completed.

13.8 Management Representation Letter

The Management Representation Letter (Rep Letter) for HITRUST r2, i1, and e1 validated assessments is completed via MyCSF using an electronic signature workflow.

13.8.1 The HITRUST r2, i1, or e1 validated assessment report date is determined by the date on the Rep Letter.

13.8.2 The Rep Letter webform in MyCSF is completed by the Assessed Entity during the *Performing Validation* phase after the External Assessor team's fieldwork period has ended and the External Assessor Timesheet has been completed or during the *Inputting CAPs and Signing Rep Letter* phase of the assessment workflow. All testing performed by the External Assessor must be complete before the Assessed Entity may sign the Rep Letter.

13.8.3 The Assessed Entity completes the Rep Letter webform by:

i. Setting the Rep Letter date.

ii. Entering the name, job title, and email address of the individual who will sign the Rep Letter.

iii. Uploading the organization's logo.

13.8.4 The date on the Rep Letter must meet the following requirements:

- The date must be on or within two weeks following the end date of the External Assessor's fieldwork period on the External Assessor Time Sheet (unless the Assessed Entity completed a bridge assessment).
- The date may not be after the date the assessment was submitted to HITRUST for processing.
- If the Assessed Entity completed a bridge assessment (see Chapter 15.8 Bridge Assessments), the date must be the bridge certificate date, which is the expiration date of the prior certification.

13.8.5 A request to electronically sign the Rep Letter is automatically sent to the designated management representative for signature via email. The signer of the Rep Letter may be any designated individual from the Assessed Entity's organization and is not required to have a MyCSF account.

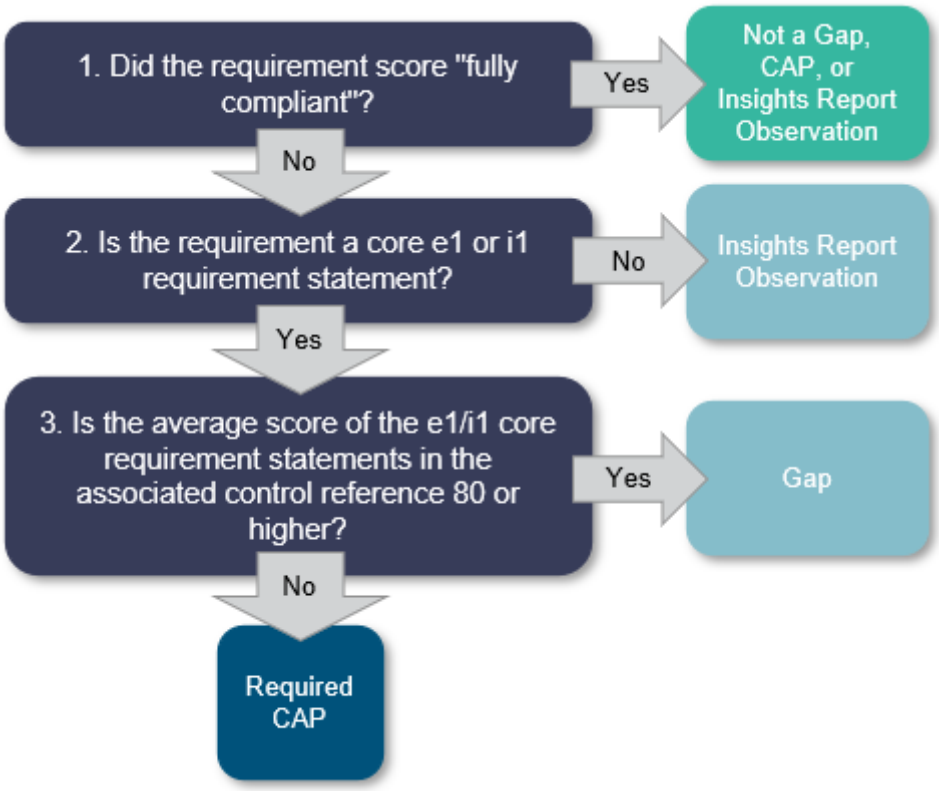
13.8.6 Once signed, the Rep Letter will automatically be loaded into MyCSF and emailed to the individual who signed it.

13.9 CAPs and Gaps

13.9.1 For i1 or e1 validated assessments, HITRUST requires Assessed Entities to define Corrective Action Plans (CAPs) for all requirement statements meeting the following criteria:

i. Requirement statements that score less than “fully compliant” and
ii. Associated control reference average score is less than 80 when considering only the core e1 or i1 requirement statements. Any requirement statements added by included Compliance factors are not considered in this average score.

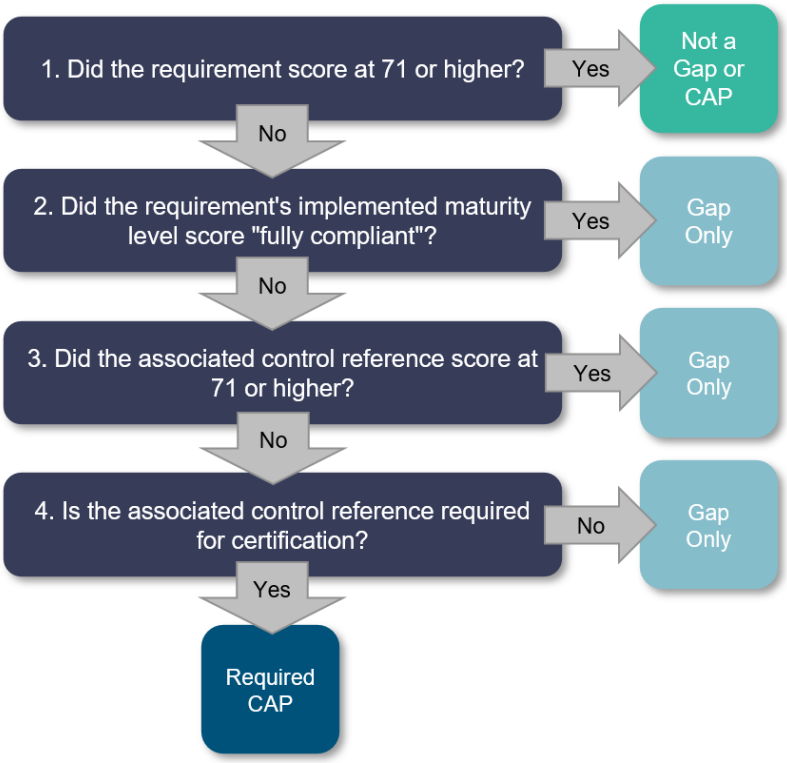
Instances in which a core i1 or e1 requirement statement scores less than “fully compliant” and the associated control reference averages 80 or higher are identified as gaps instead of CAPs. The following diagram illustrates the process for identifying gaps and CAPs in i1 or e1 validated assessments.



13.9.2 For r2 validated assessments, HITRUST requires Assessed Entities to define corrective action plans (CAPs) for all requirement statements meeting the following criteria:

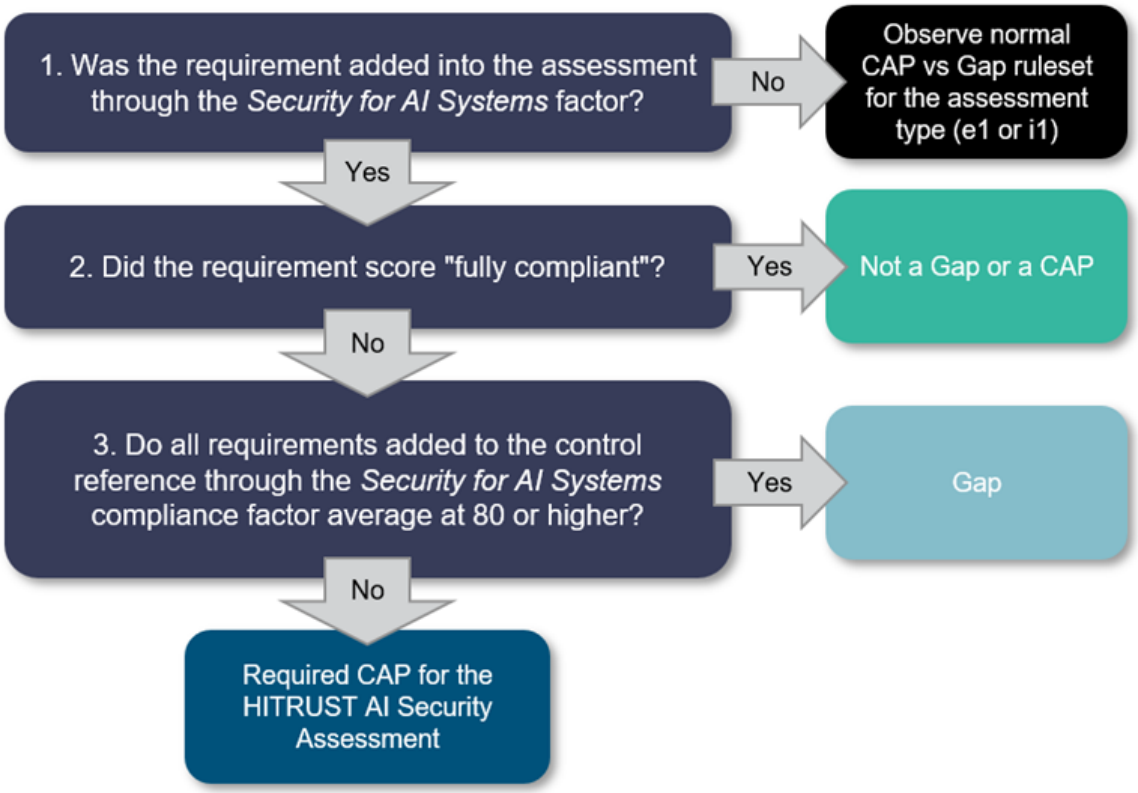
i. Requirement statement’s overall score is less than 71,
ii. Requirement statement’s *Implemented* maturity level scores less than “fully compliant”,
iii. Associated control reference (e.g., 00.a) is required for HITRUST Risk-based, 2-year (r2) certification, and
iv. Associated control reference averages less than 71.

Instances in which a requirement statement scores less than 71 and one or more of the CAP criteria are not met are identified as gaps instead of CAPs. The following diagram illustrates the process for identifying gaps and CAPs in r2 validated assessments.

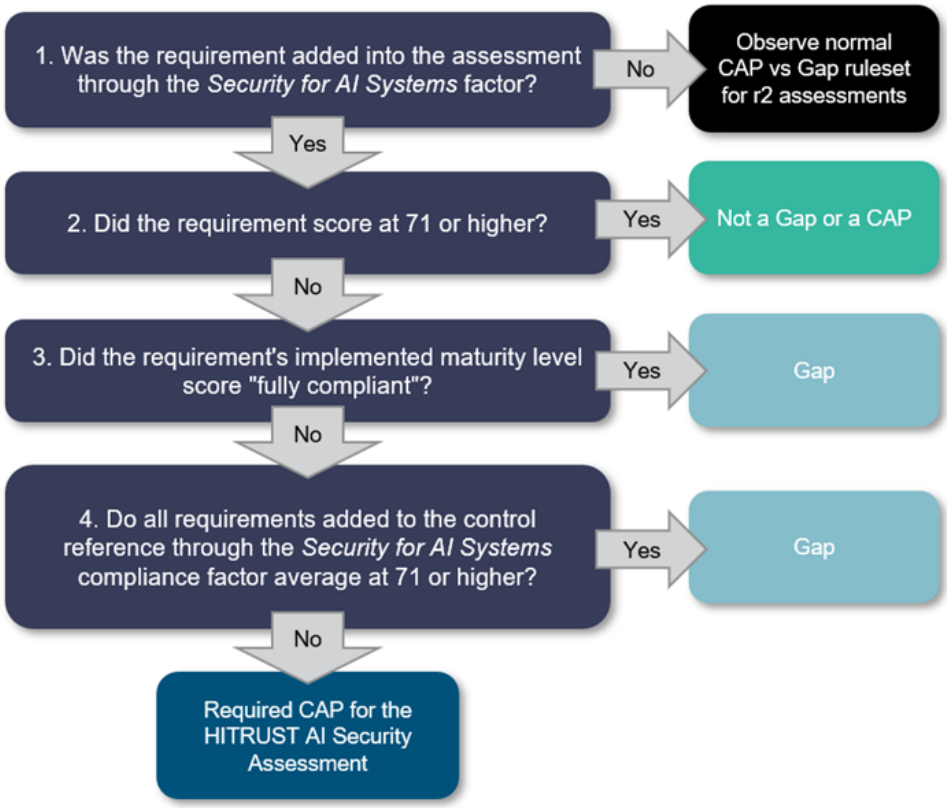


13.9.3 The ai1 or ai2 assessment will utilize the underlying HITRUST e1, i1 or r2 assessment's CAP and Gap logic. See the flowcharts below for detailed criteria.

HITRUST ai1 CAP/Gap workflow:



HITRUST ai2 CAP/Gap workflow:



13.9.4 When an r2, i1, or e1 assessment enters the Inputting CAPs and Signing Rep Letter phase, any

requirement statements requiring CAPs are identified in MyCSF using the “CAP Required” requirement statement-level response status.

13.9.5 For each requirement statement with the status “CAP Required”, the Assessed Entity must enter a corrective action plan which describes the specific steps that are planned to correct the identified deficiency. The Assessed Entity enters its corrective action plans by completing the CAP form in MyCSF, which includes (at a minimum) the following information:

- **Name** – A name to identify the CAP.

- **Corrective Action** – A description of the planned corrective action that is specific, measurable, and clear enough to provide value to readers of the HITRUST report. All deficient levels and evaluative elements must be addressed by the corrective action.

- **Status** – The current status of the corrective actions; selected from the following:
  - Not Started: Corrective actions have not yet begun
  - Started – At Risk: Corrective actions have begun, but are at risk to not be completed by the scheduled completion date
  - Started – On Track: Corrective actions have begun and are on track to be completed by the scheduled completion date
  - Completed: Corrective actions have been completed

- **Point of Contact / Owner** – The name and/or job title of the point of contact or owner of the corrective action plan.

- **Scheduled Completion Date** – The date when the planned corrective actions are scheduled to be completed.

For additional information on writing CAPs, see Appendix A-13: Well-written CAP Examples.

13.9.6 For requirement statements with the status “CAP Required” that have a score of 62 or higher, the Assessed Entity may optionally accept the risk rather than plan for the remediation of the deficiency. To determine whether to accept the risk of a deficiency or define a corrective action plan, the Assessed Entity must perform and document a risk analysis, taking into consideration the likelihood and impact of the risk as well as the existence of mitigating controls.

13.9.7 When the assessment enters the *Reviewing CAPs* phase, any requirement statements for which the Assessed Entity has entered a required CAP are identified by the requirement statement-level response status “Awaiting CAP Review”.

13.9.8 For each requirement statement identified as “Awaiting CAP Review,” the External Assessor must review the linked CAPs for specificity, clarity, spelling, and grammar. Additionally, for each CAP where the Assessed Entity has not elected to accept the risk, the External Assessor must review the ability of the Assessed Entity to demonstrate progress against the CAP.

13.9.9 When using inheritance, the Assessed Entity may inherit scores from its service providers which results in one or more CAPs. A CAP which is the responsibility of the Assessed Entity's service provider to remediate must be completed by the Assessed Entity in the same manner as all other CAPs.

13.10 Check-in Process

Upon submission to HITRUST, all assessments undergo the *Check-in* process in which HITRUST performs automated QA checks and a high-level manual review of the assessment, accompanying required documents, and webforms (Organization Information, Scope of the Assessment, Factors, VRA, Management Representation Letter, Test Plans, External Assessor Time Sheet, QA Checklist, and Audits and Assessments Utilized) to determine if the assessment is ready for a HITRUST QA Analyst to review.

Depending on the results of HITRUST's check-in review, there are three possible outcomes:

- When the results of the check-in review determine that the assessment is ready for a HITRUST QA Analyst to review, HITRUST accepts the assessment, and it enters the *Pending Quality Assurance* phase.

- When the check-in review identifies a small number of potential issues, typically related to the required documents and webforms, HITRUST creates check-in tasks within the assessment for the External Assessor and Assessed Entity to address. After the necessary check-in tasks are created by HITRUST, the assessment enters the *Addressing Check-In Tasks* phase.

- When the check-in review identifies a larger number of potential issues HITRUST reverts the assessment back to the Performing Validation phase and gives the External Assessor and Assessed Entity a set of pre-QA quality recommendations to use to address potential issues. In the event this occurs:

13.10.1 A workbook outlining the pre-QA quality recommendations is uploaded by HITRUST into MyCSF, and the External Assessor and Assessed Entity are notified via email. The External Assessor and Assessed Entity must address the pre-QA quality recommendations and resubmit the assessment.

NOTE: In this scenario, the External Assessor must be careful to ensure that the assessment is resubmitted to HITRUST prior to the Wednesday before the beginning of the reserved QA block. If the assessment is not resubmitted by that date, the assessment's QA Reservation will be cancelled, and the Assessed Entity will be required to make a new QA reservation.

13.10.2 When the assessment is resubmitted to HITRUST, it will enter the *Performing Check-In* phase for a second check-in review to occur. If there continues to be a larger number of potential issues during the second check-in, the assessment may enter the Escalated QA Process. For additional information on Escalated QA, see Chapter 14.4 Escalated QA.

13.11 Addressing Check-in Tasks

When the assessment enters the *Addressing Check-In Tasks* phase, the Assessed Entity and External Assessor must address the tasks created by HITRUST during check-in. Throughout this phase, the External Assessor and Assessed Entity will receive periodic emails that summarize all new and open items that must be addressed during the *Addressing Check-In Tasks* phase. Below are requirements for this phase:

13.11.1 If the action taken to address a task adds requirement statements to the assessment, those requirement statements must be scored by the Assessed Entity and validated by the External Assessor prior to resubmission of the assessment.

13.11.2 If the action taken to address a task adds required CAPs to the assessment, those CAPs must be entered by the Assessed Entity and reviewed by the External Assessor.

13.11.3 When all tasks have been returned to HITRUST and all new requirement statements and/or CAPs have been reviewed by the External Assessor, the assessment automatically enters the *Reviewing Pending Check-In Tasks* phase, during which HITRUST will review the actions taken to address the check-in tasks. HITRUST may accept the assessment or send tasks that have not been appropriately addressed back to the External Assessor.

13.11.4 The External Assessor and Assessed Entity must send all tasks back to HITRUST and address all additional requirement statements and CAPs prior to the Wednesday before the beginning of the reserved QA block. If all items are not resolved and HITRUST has not accepted the assessment by the beginning of the reserved QA block, the assessment's QA reservation will be cancelled, and the Assessed Entity will be required to make a new QA reservation.

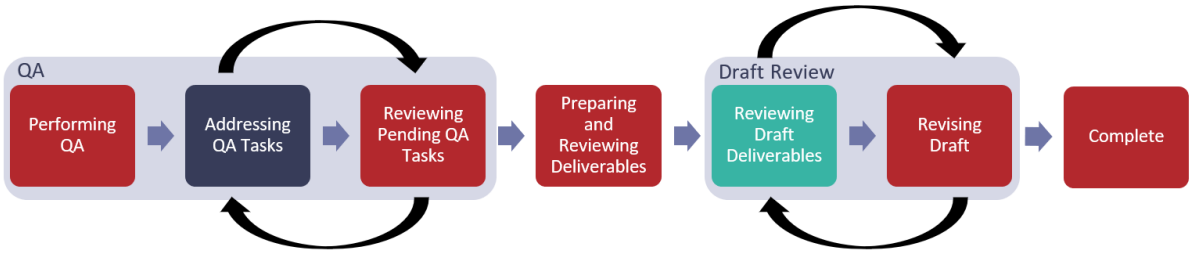
When HITRUST's check-in process indicates that the assessment is ready for QA review, HITRUST accepts the assessment, and it enters the *Pending Quality Assurance* phase. At that time, the Assessed Entity personnel and External Assessors assigned to the assessment are notified that the assessment has been accepted and is pending QA review. The QA review will begin the week of the reserved QA block.

14. Undergoing Quality Assurance (QA)

The following sections describe the HITRUST Quality Assurance (QA) process for validated assessments.

14.1 Quality Assurance Process

As described in Chapter 13.10 Check-in Process, when HITRUST's check-in process identifies that the assessment is ready for QA review, HITRUST accepts the assessment, and it enters the *Pending Quality Assurance* phase.



All accepted assessments are assigned to a HITRUST QA Analyst, and the assessment enters the *Performing QA* phase when the HITRUST QA Analyst begins the QA review of the assessment. At this time, Assessed Entity personnel and External Assessors assigned to the assessment, are notified via email and MyCSF homepage notification that the QA review has begun. The email notification contains the name and email address of the HITRUST QA Analyst assigned to the assessment.

During this phase, the HITRUST QA Analyst will re-perform a sample of work performed by the External Assessor, including the following:

- **Pre-Assessment:** A review of information captured on the Organization Information, Scope of the Assessment, Assessment Options, and Factors pre-assessment pages.
- **Required Documents and Webforms:** A review of information captured in the Management Representation Letter, Test Plans, External Assessor Time Sheet, and Audits and Assessments Utilized required documents and webforms.
- **Risk-based Sample of Core Requirement statements (Core QA):** A selection of requirement statements where HITRUST re-performs the External Assessor's testing against the stated control maturity scoring. In e1 and i1 combined assessments, HITRUST reviews independent QA samples for the core e1 and i1 requirement statement and each added Compliance factor.
- **Sample of Measured and Managed Scores:** A selection of requirement statements containing scoring on the *Measured* and *Managed* levels are subject to additional QA procedures (only applicable for r2 assessments utilizing the *Measured* or *Managed* maturity levels).
- **Not Applicable Rationales**: A review of all requirements marked as Not Applicable. For HITRUST expectations on N/A rationale, see Chapter 8.3 Not Applicable (N/A) Requirement Statements.
- **CAPs:** A review of all CAP responses. For HITRUST expectations on CAP responses, see Chapter

13.9 CAPs and Gaps.

- **Overridden Potential Quality Issues (PQIs):** A review of all PQIs that were overridden by the Assessed Entity or External Assessor to ensure that the override is appropriate.

If the HITRUST QA Analyst identifies any exceptions or questions during its review, QA Tasks will be prepared in MyCSF for the External Assessor and Assessed Entity to address (see Chapter 14.2 QA Tasks). Once the HITRUST QA Analyst enters all QA tasks, the assessment is moved to the *Addressing QA Tasks* phase.

NOTE: If the QA review identifies more significant concerns within the assessment than normal, the assessment will be submitted to the HITRUST Quality team to enter the escalated QA process, See Chapter 14.4 Escalated QA.

14.1.1 During the *Addressing QA Tasks* phase, the Assessed Entity and External Assessor must address the QA tasks created by HITRUST.

14.1.2 If the action taken to address a task adds requirement statements to the assessment, those requirement statements must be scored by the Assessed Entity and validated by the External Assessor.

14.1.3 If the action taken to address a task adds required CAPs to the assessment, those CAPs must be entered by the Assessed Entity and reviewed by the External Assessor.

When all tasks have been returned to HITRUST and all new requirement statements and/or CAPs have been reviewed by the External Assessor, the assessment automatically enters the *Reviewing Pending QA Tasks* phase.

HITRUST reviews the QA Tasks addressed by the Assessed Entity and External Assessor, closes all tasks that have been resolved, and sends any QA tasks still needing more information back to the External Assessor with additional comments or instructions. If a task is assigned to the External Assessor or Assessed Entity during this phase, the assessment automatically returns to the *Addressing QA Tasks* phase.

After all QA Tasks have been resolved by the Assessed Entity and External Assessor and closed by HITRUST, the QA review of the assessment is complete, and the assessment moves to the *Preparing and Reviewing Deliverables* phase.

During the *Preparing and Reviewing Deliverables* phase, HITRUST prepares and reviews the draft reports. All draft reports will be submitted for additional review by Assurance management and Quality team. If there no concerns from the review of the draft report, the HITRUST QA Analyst uploads the draft reports to MyCSF. This causes the assessment to enter the *Reviewing Draft Deliverables* phase. For additional information on reporting and draft report requirements, see Chapter 15.1 HITRUST Reporting.

14.2 QA Tasks

As a HITRUST QA Analyst performs the QA review of the assessment described above, QA Tasks are created for the External Assessor and Assessed Entity to address in MyCSF. The following sections describe the process to respond to QA Tasks.

Each HITRUST validated, interim, bridge, and readiness assessment contains an Assessment Task Management page that can be accessed within an assessment. The Assessment Task Management page is where all tasks for a particular assessment can be addressed and where the status of open and pending tasks can be tracked. When the Assessment Task Management page is accessed by an Assessed Entity or External Assessor user, the My Task Queue displays all open tasks assigned to the user's group.

In addition to the assessment-specific Task Management page, Assessed Entity and External Assessor users may access a global Task Management page from the top navigation bar of MyCSF to view tasks within all assessments to which the user has access. When accessing either the global Task Management page or an assessment-specific Task Management page, the user may sort and filter the tasks displayed based on the task type, current assigned group, status, and more.

14.2.1 The External Assessor and Assessed Entity must address QA tasks promptly.

There are two types of tasks that may be assigned during the QA process:

- *General Tasks:* HITRUST requests or instructions describing an action item for the External Assessor or Assessed Entity to address a QA concern.

- *Proposed Tasks:* HITRUST proposed change that must be considered by the Assessed Entity or External Assessor to address a QA concern.

During QA, HITRUST initially assigns all General tasks to the External Assessor. This allows the External Assessor to review each general task and take one of the following next steps:

- *Address the task:* When a general task is sent to the External Assessor, it may address the task by making the requested update on the relevant assessment page. After making the requested update, the External Assessor must leave a comment within the task to state the update that was made and should send the task back to HITRUST.

- *Leave a comment within the task and send it back to HITRUST:* If the External Assessor would like to respond to the task by leaving a comment or question for the HITRUST QA Analyst, the External Assessor may enter its comment within the task and send the task back to HITRUST.

- *Send the task to the Assessed Entity to be addressed:* When the general task is a request by HITRUST to update the Organization Information Webform, Scope of the Assessment Webform, Factors, requirement statement scoring or applicability, N/A rationale, Management Representation Letter, VRA, or a CAP response, the general task should be sent to the Assessed Entity for r2

assessments. For i1 and e1 assessments the External Assessor may be able to address these tasks directly after consultation with the Assessed Entity.

When the External Assessor has assigned a general task to the Assessed Entity, the Assessed Entity may take one of the following next steps:

- *Leave a comment within the task and send it back to the External Assessor:* If the Assessed Entity would like to respond to the task by leaving a comment or question for the External Assessor or the HITRUST QA Analyst, the Assessed Entity may enter its comment within the task and send the task back to the External Assessor.

- *Address the task:* When the general task includes a request from HITRUST to update the Organization Information Webform, Scope of the Assessment Webform, Factors, requirement statement scoring or applicability, N/A rationale, Management Representation Letter, VRA, or a CAP response, the Assessed Entity may address the task by making the requested update. Depending on the instructions within the task, the requested update is either made within the task itself or on the relevant page of the assessment. After addressing the task, the Assessed Entity must leave a comment within the task to state the update that was made and should send the task back to the External Assessor.

General tasks may be sent back and forth between the Assessed Entity and External Assessor as many times as needed for the task to be addressed. When the task has been addressed, the External Assessor must send the task to HITRUST. After the general task has been sent back to HITRUST by the External Assessor, HITRUST may close the task if it has been appropriately resolved or may leave a comment in the task to explain any additional action needed and send the task back to the External Assessor.

A proposed task allows HITRUST to propose a specific value for a field. For this type of task, the Assessed Entity or External Assessor can only apply the value proposed by HITRUST and cannot change any other fields within MyCSF.

For example, a proposed task can be used to change a:

- Technical Factor answer from ‘No’ to ‘Yes’ or vice versa.
- Geographical Factor answer from drop-down menu options.
- Requirement statement which has been scored to Not Applicable.
- Maturity level score to a specific proposed value.

During QA, HITRUST initially assigns all proposed tasks to the External Assessor. This allows the External Assessor to review each proposed task and take one of the following next steps:

- *Apply the Proposed Change:* The External Assessor may apply any changes proposed by HITRUST. This includes proposed tasks to change factor responses and requirement statement scoring. The External Assessor must discuss any proposed changes with the Assessed Entity prior to applying them. After applying the change proposed within the task, the task is automatically sent back to HITRUST. If a proposed change adds additional requirements to the assessment (e.g., factor change)

or additional required CAPs (e.g., certain scoring changes), the Assessed Entity users with access to the assessment are notified of the change via email and MyCSF notifications. The notifications outline whether a factor response or requirement statement score was changed, the email address of the individual who applied the proposed change, and whether there is a new requirement statement or CAP to be addressed.

- *Reject the Proposed Change:* If the External Assessor does not agree with the proposed change, the External Assessor may reject the proposed change. When rejecting the proposed change, the External Assessor is required to enter a comment within the task to explain why the change was rejected. The task is automatically sent back to HITRUST.

- *Send the task to the Assessed Entity to be addressed:* If the External Assessor would like the Assessed Entity to review the task and make the decision to either apply or reject the proposed change, the External Assessor may send the task to the Assessed Entity.

When the External Assessor has assigned a proposed task to the Assessed Entity, the Assessed Entity may take one of the following steps:

- *Apply the Proposed Change:* The Assessed Entity may apply any changes proposed by HITRUST. This includes proposed tasks to change factor responses and requirement statement scoring. After applying the change proposed within the task, the task is automatically sent back to HITRUST. If a proposed change adds additional requirements to the assessment (e.g., factor change) or additional required CAPs (e.g., certain scoring changes), the Assessed Entity users with access to the assessment are notified of the change via email and MyCSF notifications. The notifications outline: whether a factor response or requirement statement score was changed; the email address of the individual who applied the proposed change; and whether there is a new requirement statement or CAP to be addressed.

- *Reject the Proposed Change:* If the Assessed Entity does not agree with the proposed change, the Assessed Entity may reject the proposed change. When rejecting the proposed change, the Assessed Entity is required to enter a comment within the task to explain why the change was rejected. The task is automatically sent back to HITRUST.

When the proposed task has been either applied or rejected by the Assessed Entity or the External Assessor, it is automatically sent back to HITRUST. HITRUST may close the task if it has been appropriately resolved or may leave a comment in the task to provide additional explanation or answer a question and send the task back to the External Assessor. If a proposed task has been rejected and a different change needs to be proposed, HITRUST creates a new proposed task. Additionally, if any new issues are identified during QA, a new proposed task is created.

The Assessed Entity and External Assessor should also be aware that the actions taken to resolve a general or proposed task may generate additional requirement statements or CAPs that must be addressed before QA is completed. When any requirement statements or CAPs within the assessment require attention during QA, the Task Management page displays a banner to indicate that there are requirement statements or CAPs requiring input or validation. The banner contains a link to the assessment homepage where those

requirement statements and CAPs are identified by the requirement statement response status. The following scenarios are examples of when a requirement statement or CAP may require attention during QA:

- When a requirement statement score is updated via a task, the requirement statement will have a status of External Assessor Review Pending to allow the External Assessor to review and thumb up the updated score and link documents as needed.

- When a factor response is updated via a task, additional requirement statements may be added to the assessment in the status Response Needed for New Statement to allow the Assessed Entity to score the requirement statement and the External Assessor to review and link documents.

- When a requirement statement score is lowered via a task, new required CAPs may be generated. Any requirement statements requiring CAPs during QA have a status of CAP Required to allow the Assessed Entity to enter a CAP and the External Assessor to review the CAP.

14.3 Live QA

Live QA is a process which differs from the normal QA process because supporting evidence for an assessment is provided via screen share sessions. Due to the requirements necessary to perform Live QA, this process will extend the length of time for an assessment to traverse the QA process and for an Assessed Entity to receive its report.

14.3.1 An assessment qualifies for a Live QA session if the Assessed Entity, due to legal, regulatory, or corporate policies, is not able to upload the supporting evidence required for each requirement statement within the MyCSF portal.

14.3.2 If required supporting documentation was not provided during check-in, the HITRUST QA Analyst will review with the Assessed Entity and/or External Assessor if Live QA is necessary for the assessment. If so, the assessment is accepted and tagged for Live QA.

14.3.3 Only supporting evidence and/or narratives that violate the Assessed Entity's legal, regulatory, or corporate policies may be withheld from MyCSF. All other required assessment documentation, including completed Test Plans, testing results (after removing proprietary data) and file names of linked evidence (see criteria 14.3.4), must be included. HITRUST will not accept the assessment or perform Live QA until all necessary information has been included with the assessment.

14.3.4 The External Assessor must link in each requirement statement the references to the supporting documents which were reviewed during the assessment. These references must indicate the corresponding maturity level for each document.

14.3.5 When QA starts, the HITRUST QA Analyst will perform the initial review of the assessment excluding the Core QA or "Measured & Managed" sampled requirement statements and submit the initial feedback to the External Assessor via MyCSF tasks. In parallel the HITRUST QA Analyst will initiate the process of scheduling the Live QA sessions via tasks.

NOTE: Live QA sessions are scheduled after the initial QA review is completed.

14.3.6 Prior to the Live QA session, the External Assessor and/or Assessed Entity may address the tasks the HITRUST QA Analyst has sent related to scope, organization information, N/A requirement statements, CAP response details, and any other questions related to the assessment.

14.3.7 The External Assessor team must be prepared to display any working papers/supporting documentation reviewed during the assessment's fieldwork that are requested by HITRUST during the Live QA session.

NOTE: The Assessed Entity may optionally attend the Live QA session with the External Assessor.

14.3.8 During the Live QA session, the HITRUST QA Analyst will perform the following:

- The Core QA and *Measured* & *Managed* (if necessary) sampled requirement statements will be selected during the session.

- The HITRUST QA Analyst will review one requirement at a time. For each selected QA sample item, the Analyst will ask to see the documents linked to a requirement statement for the maturity level being reviewed.

- The External Assessor will share the screen and display documents as requested by the HITRUST QA Analyst.

- The HITRUST QA Analyst will discuss their questions about the content being displayed with the External Assessor.

- The outcome will either be that the HITRUST QA Analyst agrees with the scoring or proposes scoring adjustments. If scoring adjustments are proposed, these must be agreed upon before moving to the next requirement statement.

The steps will be repeated continuously for each requirement statement until the support evidence for all maturity levels of the sampled requirement statement have been verified.

NOTE: The scoring evaluation by the HITRUST QA Analyst is final. Additionally, if the HITRUST QA Analyst notes additional concerns than normal in the assessment or with the scoring of sampled requirements during the Live QA, the assessment may be escalated to the HITRUST Quality team as part of the Escalated QA process (see Chapter 14.4 Escalated QA).

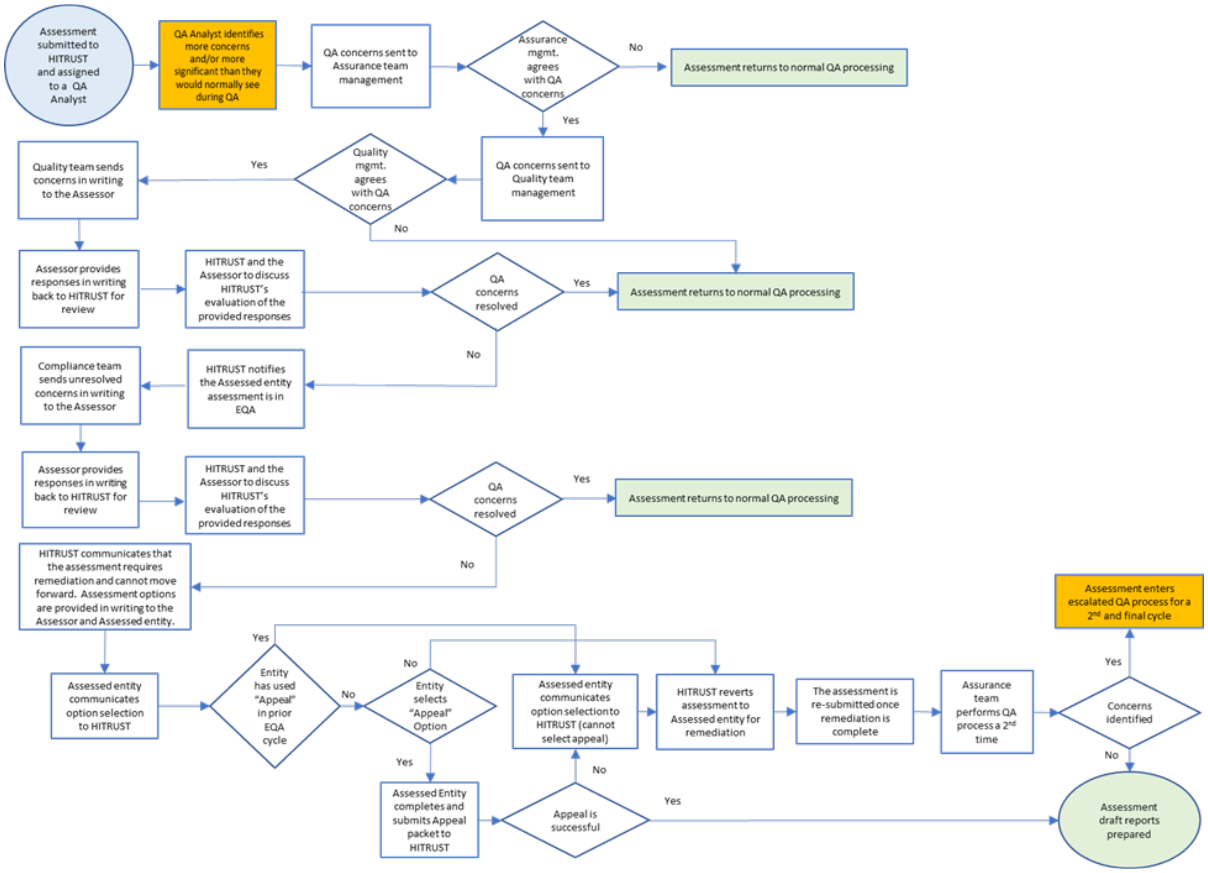
14.4 Escalated QA

HITRUST typically raises questions to the External Assessor related to questions and concerns throughout the QA process. However, the HITRUST QA Analyst occasionally identifies a higher volume and/or severity of concerns in an assessment than is typically expected. When this occurs, the submission enters HITRUST's Escalated QA process (EQA). An assessment only enters Escalated QA if HITRUST believes that the nature of the concerns may be pervasive enough to affect scoring across the validated assessment.

HITRUST's EQA process is in place to:

- Determine whether the control maturity scores accurately reflect the Assessed Entity's implementation of the HITRUST CSF
- Identify whether the External Assessor sufficiently validated the Assessed Entity's implementation of the HITRUST CSF using its testing procedures for the scope of the assessment
- Determine that the HITRUST methodology outlined in this Assessment Handbook was followed throughout the assessment process

When concerns are noted that can impact the issuance of a report meeting HITRUST's quality standards, HITRUST works to resolve these concerns. As a result of the additional inspection and investigation required during EQA, the expected delivery of the Assessed Entity's report will be delayed due to the extended process outlined below.



14.4.1 In the EQA process, the External Assessor team must respond to HITRUST's identified questions and concerns. HITRUST allows the External Assessor team multiple opportunities to describe its validation procedures and scoring rationale. The EQA process includes the following steps:

i. HITRUST communicates the identified concerns in writing to the External Assessor team.

ii. The External Assessor team provides responses in writing back to HITRUST for review.

iii. HITRUST will set up a meeting with the External Assessor to discuss HITRUST's evaluation of the provided responses.

iv. The External Assessor will provide a second set of responses in writing back to HITRUST for review.

v. HITRUST will set up a second meeting with the External Assessor to discuss HITRUST's final evaluation of the provided responses.

14.4.2 In EQA, the HITRUST Quality team is attempting to understand the procedures performed by the External Assessor during fieldwork to validate the assessment scoring. As a result, the External Assessor must not perform any new procedures to validate the assessment scores.

14.4.3 When providing responses to HITRUST's questions, the External Assessor may not introduce new evidence that was not assessed during fieldwork.

14.4.4 HITRUST's EQA process allows the External Assessor team up to two "rounds" (following the above steps) to resolve HITRUST's questions and concerns. If HITRUST's questions and concerns are not resolved after the first round, HITRUST notifies the Assessed Entity that its validated assessment is undergoing EQA and encourages them to work closely with the External Assessor team for the remainder of the process.

14.4.5 The External Assessor can resolve HITRUST's questions or concerns by demonstrating that the scores are supportable. This can be achieved using a variety of methods depending on the noted concerns. Examples of resolutions for typical concerns include:

- Referencing the exact location of the evidence reviewed by the External Assessor that supports the assessment scoring.
- For policies and procedures, mapping each requirement statement's evaluative elements to the corresponding wording in the policy or procedure where the evaluative element(s) is addressed.
- For sampling concerns, demonstrating the rationale and sampling approach used follows HITRUST sampling guidance.
- For non-occurrence of controls, referencing the additional procedures (beyond inquiry) that were performed to validate the non-occurrence.
- For third-party coverage, referencing the testing or reliance procedures that were performed which addresses the corresponding requirement statement's evaluative elements.

14.4.6 Potential outcomes from HITRUST's questions and concerns may include:

- HITRUST agreeing the score is supportable by the additional information provided by the External Assessor. No change will be required to the assessment.
- HITRUST confirming with the External Assessor that the score should be lowered. This score must be lowered when the assessment is returned to the Assessed Entity.
- HITRUST agreeing with the External Assessor that a requirement should be Not Applicable, rather than scored. This change must be made when the assessment is returned to the Assessed Entity.
- HITRUST confirming with the External Assessor that a requirement should have been scored rather than marked as Not Applicable. This change should be made, and the corresponding testing performed when the assessment is returned to the Assessed Entity.

14.4.7 The External Assessor should maintain communication with the Assessed Entity throughout the EQA process on the status and issues. While the questions are related to the procedures performed by the External Assessor, the Assessed Entity is welcome to participate in the meetings and/or it may request to be included on messages to the External Assessor throughout the process.

NOTE: HITRUST will provide regular communication to the Assessed Entity throughout the EQA process of the current assessment status.

Possible EQA Outcomes & Options

14.4.8 If HITRUST's questions and concerns are sufficiently resolved, the assessment exits the EQA process and re-enters HITRUST's normal QA process.

14.4.9 HITRUST determines whether the concerns were or were not sufficiently resolved by considering whether the outcomes of HITRUST's questions and concerns are likely to be pervasive across the validated assessment, or if any remaining concerns are likely isolated occurrences. This determination is agreed upon by HITRUST Quality and Assurance management.

14.4.10 In cases where a determination is unclear, HITRUST may review an additional sample of requirements with the External Assessor.

14.4.11 When HITRUST agrees that the assessment may move back to the normal QA process, no additional QA will be performed. The assessment will be handed over to a HITRUST QA Analyst who will work with the External Assessor on any necessary changes resulting from the EQA process, and validate all other information needed to prepare the draft report.

14.4.12 If the External Assessor is unable to sufficiently resolve HITRUST's questions and concerns, HITRUST will not issue a HITRUST validated assessment report or HITRUST certification. Instead, HITRUST presents the following options (detailed below) to both the External Assessor and the Assessed Entity:

i. Appeal the EQA Decision
ii. Remediate the Assessment
iii. Re-perform the Assessment

Appeal the EQA Decision

In this Option, the Assessed Entity can appeal the Quality team's evaluation of the assessment. At the Assessed Entity's request, HITRUST will convene the appeals board of HITRUST personnel consisting of HITRUST leadership team members who are familiar with the certification process, but who were not involved in the QA of the validated assessment. HITRUST expectations for appealing the decision include the following:

14.4.13 The Assessed Entity may appeal if it does not agree with HITRUST's conclusion that there were pervasive issues in the External Assessor's testing across the validated assessment.

NOTE: HITRUST QA does not determine if an Assessed Entity's environment is certifiable so an appeal should not use that as a basis. HITRUST QA is performed to determine whether the External Assessor testing is sufficient to support the validated assessment's scores.

14.4.14 The Assessed Entity and/or External Assessor must prepare a written statement documenting the

basis for the appeal that includes:

- The specific requirements that were sampled for QA and control maturity levels that were considered to have unresolved concerns.
- The rationale why the Assessed Entity and/or External Assessor believes the existing documentation in the assessment supports the scoring in the assessment and/or addresses the concerns identified by HITRUST during QA.
- References to evidence mentioned during the EQA process that demonstrate how the scoring is supported.
- Any additional information that will assist the HITRUST appeals board with making its determination.

14.4.15 When an Assessed Entity selects the 'Appeal' option, the Assessed Entity will submit its documentation to the VP of Quality, who will provide all documentation to the HITRUST Appeals Board. The Appeals Board will provide its response back to the Assessed Entity via email within 30 days of submission.

If the appeal is successful, the assessment will move back to normal QA processing. The date of the report and/or certification which may result from this assessment will still be the original Management Representation Letter date.

If the appeal is unsuccessful, the Assessed Entity will be required to select one of the remaining two options outlined below.

Remediate the Assessment

In this option, the Assessed Entity will adjust the maturity scoring within the necessary requirement statements to lowered scores reflecting the testing performed during the assessment, or additional documentation will be added from the fieldwork period supporting the requirement statement's score.

14.4.16 The Assessed Entity will typically remediate the assessment by either *lowering scores to supportable levels* and/or *adding "historical" documentation* from the fieldwork period that supports the Assessed Entity's scores. HITRUST may also request the Assessed Entity to remove Compliance factor(s) from the assessment if it is determined that their removal will resolve the concerns identified by HITRUST. If the Compliance factor is related to an insight report or add-on certification the Assessed Entity will no longer be eligible to receive the corresponding report and/or add-on certification as part of the assessment.

14.4.17 *Lowering scores to supportable levels*:

- The scores across the entire assessment must be reviewed to determine whether they should be lowered, not just the requirements sampled during EQA.

- The assessment's control maturity scores can be lowered to those that the External Assessor believes are supportable by the existing, previously collected assessment documentation (e.g., screenshots, policies, access listings) linked to each requirement at the time the assessment was submitted to HITRUST.

- Lowering requirement maturity scoring has its drawbacks that include (i) several CAPs will likely result, and (ii) certification may not be possible if the control maturity scores are lowered past a certain point.

14.4.18 *Adding "Historical" Documentation*:

- The External Assessor may retain requirement maturity scoring by bolstering the assessment's documentation across the entire assessment.

- "Historical" assessment documentation, which reflects the environment during the time of the previously performed validated assessment up to the Management Representation Letter date, can be used to provide better support for the existing requirement maturity scores.

- This "historical" assessment documentation must depict the control environment during the time of the validated assessment. Examples include previous copies of written policies and procedures, help desk tickets created within the period, populations spanning the period, point-in-time screenshots paired with change logs spanning the period, etc.

- All newly collected historical evidence must be collected in accordance with the requirements outlined in Chapter 11 Testing & Evidence Requirements.

- Upon re-submission, the Assessed Entity and/or External Assessor must notify HITRUST of the requirement statements where evidence was added to bolster the scoring.

14.4.19 *Compliance factor removal*:

- This option is utilized to allow the Assessed Entity to still obtain a HITRUST validated assessment report when concerns are limited to the testing and/or scoring for requirement statements related to the included Compliance factor(s).

- The Assessed Entity will update the Factors webform by removing the requested Compliance factor selection and refreshing the assessment which will result in removal of requirement statements which correspond to the Compliance factor.

- Scoring and documentation for the remaining requirement statements must remain unchanged.

- When selecting this option, the Assessed Entity will be unable to obtain a corresponding report which includes the Compliance factor without performing a new validated assessment.

14.4.20 When using the option to remediate the assessment, the date of the report and/or certification will

retain the original Management Representation Letter date.

Re-perform the Assessment

In this option, the Assessed Entity will fully re-perform the validated assessment. Brand new assessment documentation (e.g., freshly collected screenshots, updated policies, current access lists) reflective of the current environment can be used to provide better support for the control maturity scores. This option should be chosen if the External Assessor thinks (i) the scores in the assessment accurately depict the environment's control maturity, and (ii) newly collected supporting evidence will increase the likelihood of a successful QA outcome. If this option is chosen:

14.4.21 The External Assessor must:

- Test and document all newly collected evidence in accordance with the requirements outlined in Chapter 11 Testing & Evidence Requirements,
- Ensure all supporting evidence in the revised submission, not just those associated with the requirements selected for QA, is not older than 90 days, and
- Agree with (i.e., "thumbs-up") the control maturity scores reflected in MyCSF.

14.4.22 The date of the report and/or certification which may result from this revised assessment object will not be the original Management Representation Letter date; instead, a new representation letter will need to be signed and dated after the end of the new fieldwork period.

Assessment Re-submission

If either the "Remediate the Assessment" or "Re-perform the Assessment" options are selected, HITRUST will re-perform QA on a new sample of requirements after assessment remediation is completed and has been re-submitted to HITRUST.

If the Assessed Entity chooses to move forward on any of the assessment options other than Appeal:

- HITRUST will revert the assessment object so it can be amended.
- The Assessed Entity is free to continue to use its current External Assessor, or the Assessed Entity may engage a new HITRUST External Assessor of the Assessed Entity's choosing.
- After the desired changes are made within the assessment object, and the External Assessor has completed its validation procedures, HITRUST will again perform a QA review. If significant QA concerns again arise, the assessment will once more enter the EQA process a second (and final) time.
- HITRUST cannot guarantee that remediation performed against the assessment object will result in a favorable outcome. If the re-submission moves into EQA and HITRUST's concerns are unable to be resolved during the second EQA process, HITRUST will not return the assessment back to the

Assessed Entity. Instead, the Assessed Entity may appeal (if not previously appealed after the first EQA outcome) or agree to declare the assessment as a “Failed QA”.

After a “Failed QA”, HITRUST will provide a “Failed QA” letter to the Assessed Entity and close the assessment object without issuing a report. To obtain a HITRUST certification, the Assessed Entity will need to perform a new validated assessment effort using a new object in MyCSF with new supporting evidence.

15. Reporting & Maintaining a HITRUST Certification

This page is intentionally left blank.

15.1 HITRUST Reporting

HITRUST provides reports for each of the following assessments (example HITRUST reports are available at MyCSF Help):

- HITRUST Essentials, 1-year (e1) Readiness Assessment
- HITRUST Essentials, 1-year (e1) Validated Assessment
- HITRUST Implemented, 1-year (i1) Readiness Assessment
- HITRUST Implemented, 1-year (i1) Validated Assessment
- HITRUST Risk-based, 2-year (r2) Readiness Assessment
- HITRUST Risk-based, 2-year (r2) Validated Assessment

15.1.1 For HITRUST Essentials, 1-year (e1) Validated, HITRUST Implemented, 1-year (i1) Validated and HITRUST Risk-based, 2-year (r2) Validated Assessments, the requirement statements average scores per domain must meet the threshold required to attain a certification.

15.1.2 The i1 and e1 require the core e1 and i1 requirement statements in each domain to score at least an 83, while the r2 requires each domain to score at least a 62 to achieve certification. Note that in the r2 assessment, the domain scores considered for certification include all requirement statements in the assessment. The i1 and e1 only take into consideration the core requirement statements for certification (i.e., excluding requirement statements added for a combined assessment). For scoring examples, see Appendix A-15: Certification Threshold Scoring Examples.

Upon achieving the required score, the corresponding Certification Report (HITRUST Essentials 1-year (e1) Certification Report, HITRUST Implemented 1-year (i1) Certification Report or HITRUST Risk-based, 2-year (r2) Certification Report) and copies of the certification letter are issued. The copies of the certification letter include one copy with the certification letter and scope of the assessment and one copy with only the certification letter. This is intended to allow Assessed Entities to share only the necessary details of the certification with their relying parties.

15.1.3 For assessments that do not meet the required certification average score threshold, a HITRUST Essentials, 1-year (e1) Validated Assessment Report, HITRUST Implemented, 1-year (i1) Validated Assessment Report or HITRUST Risk-based, 2-year (r2) Validated Assessment Report are issued, respectively. HITRUST refers to these non-certified reports as “validated-only” reports and each report will state that certification thresholds were not met.

15.1.4 The HITRUST Essentials, 1-year (e1) Certification Report and HITRUST Implemented, 1-year (i1) Certification Report are valid for 12 months if there are no significant changes or security events related to the in-scope environment.

15.1.5 The HITRUST Risk-based, 2-year (r2) Certification Report is valid for 24 months, with a requirement to complete an interim assessment at the 12-month anniversary (see Chapter 15.4 Interim Assessment), and if there are no significant changes (see Chapter 15.6 Significant Changes) or security events (see Chapter 15.3 Security Events & Fraud)

related to the in-scope environment.

Certification Status

Each certification associated with a HITRUST validated assessment (including HITRUST CSF, NIST, and AI certifications) will have one of the following statuses:

- *Not Certified*: A validated assessment which did not achieve the necessary scores for certification resulting in a “validated-only” report. In addition, a validated assessment which has not yet reached the workflow status of ‘Complete’ will be considered as *Not Certified*, even if the submitted validated assessment has achieved the necessary scores for certification.

- *Certified*: A validated assessment in the workflow status of ‘Complete’ which achieved the necessary scoring threshold for certification.

- *Expired*: A validated assessment which was *Certified* but reached the date of expiration. This also includes *Certified* assessments which were replaced by another *Certified* assessment of the same assessment type prior to its normal expiration.

- *Suspended*: A previously *Certified* validated assessment undergoing investigation by HITRUST or remediation activities by the Assessed Entity for potential non-compliance (e.g., not performing the interim on a timely basis, breach investigation, etc.).

- *Revoked*: A previously *Certified* validated assessment which expired early due to non-compliance with HITRUST requirements.

15.1.6 An Assessed Entity may not have two *Certified* assessments of the same assessment type with the same primary scope (to avoid misrepresentation and/or inheritance of results which do not reflect the most recent assessment of the security environment). Upon completion of a new validated assessment of the same assessment type and scope which achieves certification, any prior certification will be considered as *Expired*.

15.1.7 An Assessed Entity may not distribute a certification in the *Suspended* or *Revoked* status.

15.1.8 An assessment in the *Expired*, *Suspended*, or *Revoked* status may not be published for inheritance.

NIST Certification

HITRUST offers two separate NIST Cybersecurity Framework (CSF) certifications depending on the HITRUST CSF version used for the underlying r2 assessment:

- For r2 validated assessments created using HITRUST CSF version 11.3.2 or earlier, a complimentary report based upon NIST CSF v1.1 will be provided with each completed HITRUST r2 assessment. Complimentary NIST CSF v1.1 reports are not available for HITRUST CSF versions 11.4.0 or later.

- For r2 validated assessments created using HITRUST CSF version 11.4.0 or later, a NIST CSF v2.0 report is available as an optional purchased add-on. To obtain the NIST CSF v2.0 report, an Assessed Entity must select the corresponding compliance factor, NIST Cybersecurity Framework 2.0, within the “Factors” webform (see Chapter 6.7 Factors).

HITRUST certification of the Organization’s NIST Cybersecurity Framework implementation is based on the NIST Cybersecurity Framework (either NIST Cybersecurity Framework v1.1 or v2.0) and presented via HITRUST’s NIST Cybersecurity Framework Scorecard. The Scorecard reflects the aggregated scores for the underlying HITRUST CSF controls as they are mapped by HITRUST to the NIST Cybersecurity Framework Core Subcategories.

15.1.9 A NIST Cybersecurity Framework Certification Report (v1.1 or v2.0) is issued if the average score of the NIST-mapped HITRUST CSF requirements is 70 or higher on each Core Function and Category.

15.1.10 A NIST Cybersecurity Framework validated-only (i.e., non-certified) report is issued if the average score of the NIST-mapped HITRUST CSF requirements does not achieve a score of 70 on one or more Core Functions and Categories, or if the underlying r2 certification was not achieved.

15.1.11 The NIST Cybersecurity Framework Report is not available with a HITRUST Essentials, 1-year (e1) Validated Assessment or HITRUST Implemented, 1-year (i1) Validated Assessment.

HITRUST AI Security Assessment with Certification (ai1 or ai2)

HITRUST offers a HITRUST AI Security Assessment, ai1 (when combined with an e1 or i1 assessment) and ai2 (when combined with an r2 assessment), which is designed to deliver an AI security assessment and accompanying certification for deployed AI systems, which includes any system with integrated AI functionality. For additional details on the types of AI which can be certified, see AI Security and Assessment Certification Help.

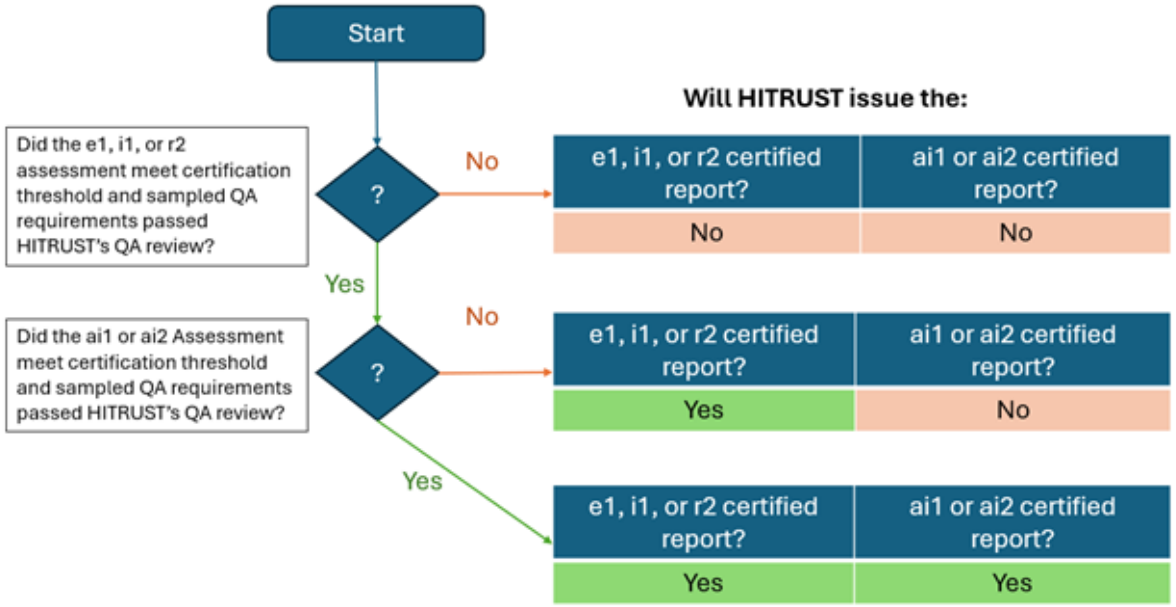
This certification is available for organizations performing an e1, i1 (including i1 rapid) or r2 assessment using version 11.4.0 and later of the HITRUST CSF who select the “Cybersecurity for AI Systems” Compliance factor (see Chapter 6.7 Factors). For additional details on certification eligibility, see A-19: AI Security Certification Eligibility.

Upon selecting the factor and answering the factor tailoring questions, the corresponding assessment will include the necessary HITRUST requirement statements to support the ai1 or ai2 certification.

15.1.12 The ai1 or ai2 certification is awarded if the average control maturity scores of all AI security requirement statements tailored into the assessment through the “Cybersecurity for AI Systems” compliance factor achieve a minimum of 83 in ai1 assessments or 62 in ai2 assessments.

15.1.13 The ai1 or ai2 certification is dependent on achievement of the underlying HITRUST e1, i1 or r2 certification. This is due to the need to consider the security of the supporting technology layers used to deliver the AI functionality (e.g., the application leveraging the AI model, the cloud services used to deliver that application, the data center that those cloud services reside in).

NOTE: The underlying HITRUST e1, i1 or r2 certification can be achieved regardless of whether the necessary scores for the ai1 or ai2 certification have been achieved. See below for diagram depicting the possible outcomes.



Upon achieving criterion 15.1.12 and 15.1.13, the corresponding ai1 or ai2 report and copies of the certification letter are issued. These will be issued in addition to the deliverables for the underlying HITRUST e1, i1 or r2 certification. HITRUST ai1 or ai2 assessments which do not meet the required certification criteria will receive a non-certified “validated-only” report stating that certification thresholds were not met.

Assessed Entities who maintain an existing HITRUST e1, i1 or r2 certification and were unable to perform an ai1 or ai2 assessment may still be able to achieve an ai1 certification without completing a new e1, i1 or r2 validated assessment. For an example approach, see A-18: Example Add-on Certification Approach for Existing HITRUST Certifications.

Insights Reports

A separate Insights Report may be provided with HITRUST e1, i1, or r2 validated assessments which include Compliance factors eligible for Insights Reporting. The Insights Reports provide easy-to-understand and reliable compliance reporting over the authoritative sources assessed. These reports include the precise HITRUST control mapping against the specific authoritative source, communicate coverage and compliance with the authoritative source, and identify the requirement statements for which a control observation was identified. Note that the availability of Insights Reports depends on the CSF version used in the assessment.

For additional information on the current available Insights Reports, Assessed Entities may contact their CSM or HITRUST Support (support@hitrustalliance.net).

HITRUST Reporting Process

When the QA process is complete the draft reports are built, reviewed, and posted by HITRUST.

15.1.14 The Assessed Entity has 30 days to review the draft reports.

15.1.15 Changes to scope, factors, and scoring may not be requested via draft report revisions. Additionally, new evidence may not be introduced during the reporting phases.

15.1.16 After the Assessed Entity has reviewed the draft reports, they may either:

- ***Approve the Draft Reports:*** If the Assessed Entity does not request revisions to the draft reports, it can approve the draft reports by selecting the “Approve HITRUST CSF Draft Report” button within the HITRUST CSF Reports section of the assessment.

- ***Request Revisions:*** If the Assessed Entity would like to request revisions to the draft reports, it may do so by selecting the “Request Revision” button within the HITRUST CSF Reports section of the assessment. This initiates a webform that allows the Assessed Entity to prepare each revision request individually.

15.1.17 If the Assessed Entity does not approve the draft reports or request revisions within 30 days, the draft reports are automatically approved by MyCSF.

Upon approval from the Assessed Entity, HITRUST will prepare and post the final reports, and the Assessed Entity and External Assessor will be notified that the final reports are available. Additionally, the HITRUST marketing team will send a press kit to the Assessed Entity.

15.2 Report Re-Issuance

HITRUST does not re-issue any report once the final reports are posted without extenuating circumstances for the re-issuance. Please note the following criteria:

15.2.1 A name change at the Assessed Entity does not necessarily qualify for report re-issuance. The name of the report must match the Management Representation Letter which is based upon the name of the Assessed Entity as of the date of the letter.

15.2.2 Assessed Entities needing a report re-issued will need to submit an exception request to HITRUST Support (support@hitrustalliance.net) and meet the following criteria to be considered for reissuance:

i. Assessed Entity must be an active MyCSF subscriber with access to the completed assessment (assessment cannot be archived).

ii. The final report must have been issued within the last 6 months.

iii. The exception request must describe the circumstances and rationale for the re-issuance which HITRUST will review to determine whether to approve the re-issuance.

15.2.3 If an exception is approved, the Assessed Entity may incur a cost and should contact its HITRUST CSM to obtain pricing information and initiate the re-issuance process.

15.2.4 If an organization has a name change, it should contact its HITRUST CSM to request a change to its MyCSF account. All name changes must be approved by HITRUST. If the name change is due to an acquisition, divestiture, or merger, HITRUST will request additional information to determine if there is an impact to any current HITRUST certifications. See Chapter 15.6 Significant Changes for additional information.

15.3 Security Events & Fraud

There are certain circumstances that may result in HITRUST certifications being suspended or revoked. These circumstances can include a security event at the Assessed Entity (including data breaches), fraud from either the Assessed Entity and/or External Assessor, or misrepresentations by the Assessed Entity and/or External Assessor.

15.3.1 When the Assessed Entity identifies a security event (including any data breaches), involving the environment in-scope of its HITRUST certification, it is required to notify HITRUST when either: a) the Assessed Entity has confirmed the security event, or b) the investigation has been open or ongoing for sixty (60) days from the date when the Assessed Entity identified the incident as a potential security event or data breach. The Assessed Entity and/or its External Assessor may submit the notification through HITRUST Support (support@hitrustalliance.net) or contact its CSM for alternate notification approaches (e.g., encrypted communication).

15.3.2 A security event includes any event which may call into question the Participant's continued compliance with the HITRUST CSF, as provided in the issued HITRUST validated assessment report, or which leads to unauthorized access to the Participant's system or data housed therein.

15.3.3 A data breach is a security event in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, used, disclosed, or accessed in an unauthorized fashion and/or by an individual or organization unauthorized to do so and compromises the privacy or security of the data.

15.3.4 In case of a reported security event, an investigation by HITRUST will take place within 30 days of the Assessed Entity notifying HITRUST. The duration of the investigation may be extended by HITRUST if more time is required to determine the cause and assess the significance of the control failure(s) and its impact on Assessed Entity's certification.

15.3.5 In order to expedite the investigation, the security event notification to HITRUST should include the cause and scope of the security event, including whether the security event: 1) involved any of the platforms/systems within the primary scope of the assessment (see Chapter 7.2 Required Scope Components for description of the primary scope); and 2) was caused due to previously assessed HITRUST requirement statements not operating and/or being properly performed.

15.3.6 During the investigation, the Assessed Entity must provide additional information requested by HITRUST related to the cause and/or scope of the security event. If necessary, HITRUST may request the Assessed Entity to have an independent Assessor perform an investigation to provide further clarity on the root cause of the security event as it relates to the requirement statements and environment under certification.

15.3.7 During the investigation, HITRUST will request the Assessed Entity and/or External Assessor to identify and re-evaluate requirement statement(s) related to the security event. HITRUST will evaluate the Assessed Entity's maturity score(s) for those requirement statement(s), at time of failure, to determine if it deviated from the requirement statement(s)' maturity score(s) during the Assessed Entity's validated

assessment.

15.3.8 If the maturity score(s) deviated to a level below what was required for certification, HITRUST may suspend or revoke the Assessed Entity's certification. If the maturity score(s) deviated below the Assessed Entity's prior maturity score(s), but not below the certification threshold, HITRUST may suspend the certification.

15.3.9 If HITRUST suspends the Assessed Entity's certification, HITRUST will provide the Assessed Entity with the necessary process for removal of the suspension. For example, if certain requirement statement(s) were found to no longer be operational resulting in the security event, HITRUST may request the Assessed Entity to remediate the impacted requirement statement(s) and have the requirement statement(s) re-tested by an External Assessor (after any necessary incubation period). The requirement statement(s) must achieve scores greater than or equal to the scores from the validated assessment prior to removal of the suspension.

15.3.10 During suspension of the HITRUST certification, the Assessed Entity may not allow external or internal inheritance and may not communicate that they are HITRUST certified.

15.3.11 If HITRUST revokes the Assessed Entity's certification, the Assessed Entity may perform a new full validated assessment 90 days after remediation of all controls related to the security event. If the Assessed Entity performs a new r2, i1, or e1 validated assessment after a security event, it must modify the Management Representation Letter in the new assessment to reflect the circumstances of the security event. HITRUST will review and approve the necessary Management Representation Letter updates.

15.3.12 If the security event occurred prior to the Assessed Entity's interim assessment, the External Assessor must include a "thumbs down" to the question in MyCSF stating "The External Assessor inquired of management of the Assessed Entity and was told that no security breaches have occurred within the scoped and assessed environment that required reporting to a federal or state agency by law or regulation since the certification effective date." In addition, the External Assessor must include a document stating the procedures performed as a result of the security event and results of its procedures.

15.3.13 If fraud and/or misrepresentation is suspected at any time during the validated assessment process or certification period, HITRUST will investigate the activity and circumstances surrounding the concern. The Assessed Entity and/or External Assessor is expected to cooperate with HITRUST throughout the investigation.

15.3.14 When fraud and/or misrepresentation has been identified at any point during the validated assessment process or certification period, HITRUST will revoke the certification and reserves the right to remove either the Assessed Entity and/or External Assessor from the HITRUST program.

15.4 Interim Assessment

For an entity to maintain its r2 certification, an interim assessment must be completed and submitted to HITRUST in the 90-day window leading up to the one-year anniversary of the certification issuance date.

For annual MyCSF subscribers, the interim assessment is automatically generated by MyCSF 90 days prior to the required submission date. Assessed Entities with an annual MyCSF subscription can manually generate the object 120 days prior to the required submission date.

Non-subscribers will automatically receive an interim assessment notice 90 days prior to the required submission date and will need to contact HITRUST Support (support@hitrustalliance.net) to generate the interim assessment and obtain access. NOTE: The access will only last for 60 days.

The assessment will consist of one randomly selected requirement statement from each of the assessment domains plus all requirement statements that resulted in required CAPs. When an Assessed Entity has obtained an add-on certification (e.g., ai2) as part of its r2 assessment, the interim will also contain a sample of previously assessed requirement statements from the corresponding add-on certification.

HITRUST determines whether the Assessed Entity has met the criteria to retain its certification(s)*, which includes:

- No significant changes to the scope of the current certification (see Chapter 15.6 Significant Changes)
- No security events have taken place impacting the certified environment (see Chapter 15.3 Security Events & Fraud)
- No degradation of the control posture within the certified environment (i.e., no lowering of maturity scores within the sampled requirement statements)
- Sufficient progress on the CAPs documented during the validated assessment

*NOTE: When an Assessed Entity has an add-on certification within an assessment (e.g., ai2), these criteria must be met independently for the add-on certification and underlying r2. For example, there may be situations where there was degradation of the control environment for AI systems resulting in the inability to retain the ai2 certification, but the r2 certified environment has not degraded, allowing the Assessed Entity to retain its r2 certification. However, please note an add-on certification cannot be retained if the underlying certification has been revoked.

HITRUST's interim assessment guidelines and expectations to determine whether the criteria have been met include the following:

15.4.1 The External Assessor must inquire with management of the Assessed Entity whether any significant changes occurred since the certification effective date in the Assessed Entity's business or security policies, processes, controls, hosting locations, or technologies that may impact the Assessed

Entity's ability to meet the certification criteria.

15.4.2 Where a significant change has occurred, the External Assessor and/or Assessed Entity must consult with HITRUST to determine its impact, and testing requirements for the impacted requirement statements. HITRUST will provide direction on the steps necessary to address the change within the interim assessment. For additional details on significant changes, see Chapter 15.6 Significant Changes.

15.4.3 The External Assessor must inquire with management of the Assessed Entity whether any security events have occurred within the scoped and assessed environment that required reporting to a federal or state agency by law or regulation since the certification effective date. If a security event has occurred, the Assessed Entity must follow the process outlined in Chapter 15.3 Security Events & Fraud before HITRUST will issue the interim report.

NOTE: If it is confirmed that either a significant change or security event has occurred, the External Assessor should include a 'thumbs down' for the corresponding question in the interim assessment questionnaire overview. The External Assessor should also attach a document within the assessment which describes the situation and actions performed (as agreed with HITRUST).

15.4.4 The External Assessor must perform full testing/validation procedures for all selected requirement statements, working with the Assessed Entity to re-score the randomly selected requirement statements in MyCSF. These validation procedures must be documented in the MyCSF tool in the Assessed Entity's interim assessment.

15.4.5 When scores have been lowered for the selected requirement statements in the interim (from the validated assessment scores), the External Assessor must determine if the scoring change reflects a degradation in the control environment. The External Assessor may expand its validation procedures to reach a conclusion on the control environment.

15.4.6 If the External Assessor has identified HITRUST requirements which require remediation as a result of control degradation, the External Assessor must contact HITRUST Support (support@hitrustalliance.net) to discuss next steps. Depending on the severity and pervasiveness of the control degradation, HITRUST may suspend the certification to allow remediation of the corresponding HITRUST requirements or revoke the certification (which would require performance of a new validated assessment after the Assessed Entity has completed remediation).

15.4.7 Based on the results of all tests performed during the interim assessment, the External Assessor must indicate if they are aware of any reason to revoke the Assessed Entity's certification prior to the two-year certification anniversary. If the External Assessor has concerns around continuing the Assessed Entity's certification, it must contact HITRUST Support (support@hitrustalliance.net) to discuss next steps.

15.4.8 The External Assessor must request the Assessed Entity to update the status of required CAPs in MyCSF to reflect the current state of the CAP.

15.4.9 The External Assessor must review the status and progress of CAPs that were included in the initial assessment and conclude whether the entity is making sufficient progress on the CAPs. For

purposes of CAP progress, barring extenuating circumstances, 50% or more of required CAPs must be started and/or complete.

15.4.10 The interim assessment must be submitted to HITRUST by the External Assessor on or within 90 days prior to the one-year anniversary of the organization's r2 certification date. Upon acceptance of the assessment, HITRUST will perform a Quality Assurance review of the submitted assessment. The QA review includes HITRUST review of a random selection of requirement statements. The QA review will be performed using the scoring rubric that was used during the corresponding validated assessment. Non-submission of an interim assessment by the deadline will result in suspension and/or revocation of the Assessed Entity's certification.

15.4.11 HITRUST does not accept interim assessments with incomplete testing of the sampled requirements. Incomplete testing includes any expected procedures not performed by the External Assessor or a lack of sufficient evidence received from the Assessed Entity to complete testing procedures. Any incomplete interim assessments will be reverted back to the Assessor for additional testing. If this causes the interim to be submitted after the submission deadline, HITRUST may suspend the Assessed Entity's certification until the interim assessment is completed.

15.4.12 In the event of questions from HITRUST during QA, tasks will be opened for the External Assessor to address, similar to the QA process outlined in Chapter 14.2 QA Tasks.

15.4.13 If, at the conclusion of QA review, HITRUST concludes that the Assessed Entity should retain its certification, HITRUST will issue a letter to the Assessed Entity that indicates its certification is still valid. If HITRUST concludes that the Assessed Entity no longer meets the requirements, a letter will be sent to the Assessed Entity asking it to remove any references to its HITRUST certification from its literature and website.

Interim Assessment Testing

As mentioned above, the External Assessor is expected to fully test the randomly selected requirement statements that did not result in required CAPs, as they were tested in the supported validated assessment. The following additional expectations and guidelines apply for interim testing:

15.4.14 The External Assessor must use full sampling where sampling is required. Please note that all External Assessor fieldwork expectations for validated assessments related to timing of validation procedures, performance of validation procedures, and creation of working papers apply to interim assessments (although a Test Plan is not required for the interim assessment).

15.4.15 The External Assessor must assess the nature of any changes to policies and procedures for the selected requirement statements to determine whether they continue to fully address all elements within the corresponding requirement statement. Minor changes that are editorial in nature will not impact scoring during the interim assessment.

CAP Review and Progress

As mentioned above, the Assessed Entity is expected to have made sufficient progress at interim on the CAPs noted in its HITRUST validated report. The following expectations and guidelines for External Assessors apply for interim CAP testing:

15.4.16 All testing of HITRUST requirement statements in support of CAP remediation must follow the HITRUST testing expectations in Chapter 11 Testing & Evidence Requirements.

15.4.17 The compliance state for requirement statements in the interim assessment that must be reviewed is “CAP Required”. Testing must be performed on all CAPs that are in any state other than NOT STARTED.

15.4.18 CAPs that indicate a STARTED status but are not yet COMPLETE should have testing performed that shows the progress towards remediation that has been made. If appropriate, scoring should be updated to reflect the corresponding progress. The testing performed must validate the documented progress toward remediation.

15.4.19 Project planning activities are not evidence of progress toward remediation so items like creating a project plan or work tickets are not considered progress towards remediation. Verifiable artifacts that may be used as evidence include, but are not limited to, meeting minutes, email and text communications regarding remediation approach, draft versions of documents, configuration changes with corresponding change management documentation.

15.4.20 Scoring of a requirement statement that has a linked CAP with a status of COMPLETE is expected to be 100/100/100 for the *Policy*, *Procedure* and *Implemented* maturity levels, respectively. The only exception to this is where risk has been accepted by the Assessed Entity. Risk may be accepted when a requirement statement scores 62 or greater. Assessed Entities have the option to remediate to this level and accept the remainder of the risk. If the risk is accepted to complete a CAP, management must include its risk analysis and rationale that supports its decision.

15.4.21 A remediated CAP must also follow the 90-day incubation period requirements (see criteria 11.2.8 in Chapter 11.2 Testing Requirements).

15.4.22 Testing is performed by the External Assessor to confirm remediation of a CAP. This testing is not required to include those maturity levels and/or evaluative elements that were fully tested during the validated assessment and resulted in a fully compliant score. The External Assessor may rely on the validated assessment scoring results when determining the final score of the requirement statement.

15.4.23 If an Assessed Entity has not demonstrated sufficient progress towards addressing its CAPs, HITRUST may delay providing the interim report or suspend or revoke the Assessed Entity’s certification. HITRUST takes into consideration the number of CAPs, complexity, and length of time since the Assessed Entity entered its CAPs to determine sufficient progress.

15.4.24 An e1 or i1 certification for the same assessment scope may be performed in lieu of an interim

assessment if there have been no significant changes and/or security events within the certified environment. The date of the e1 or i1 certification must fall within the interim fieldwork timeline (no later than the one-year anniversary of the r2 and no more than 90 days prior to the one-year anniversary). The Assessed Entity and/or External Assessor must contact HITRUST support (support@hitrustalliance.net) to confirm eligibility and report the intention to use this approach.

15.5 Rapid Assessments

The HITRUST i1 and e1 rapid assessments allow Assessed Entities and their External Assessors to apply a rapid sampling approach to eligible sets of requirement statements in order to demonstrate that the control environment has not materially degraded since the previous certification was obtained. Upon successfully demonstrating that the control environment has not materially degraded, the Assessed Entity is permitted to roll forward scores from the previously certified i1 or e1 assessment for the remaining requirement statements in the set; thus, reducing the amount of testing required to complete the assessment.

i1 Rapid Assessment Overview

After completing an i1 combined validated assessment in year 1, the assessed entity may be eligible to complete an i1 rapid assessment in year 2. The i1 rapid assessment will allow the rapid sampling approach, described below, to be applied independently to the core i1 requirement statements and any compliance factor that includes more than 60 requirement statements. If any compliance factors included in the combined assessment included 60 or fewer requirement statements, those requirement statements must all be assessed in the i1 rapid assessment

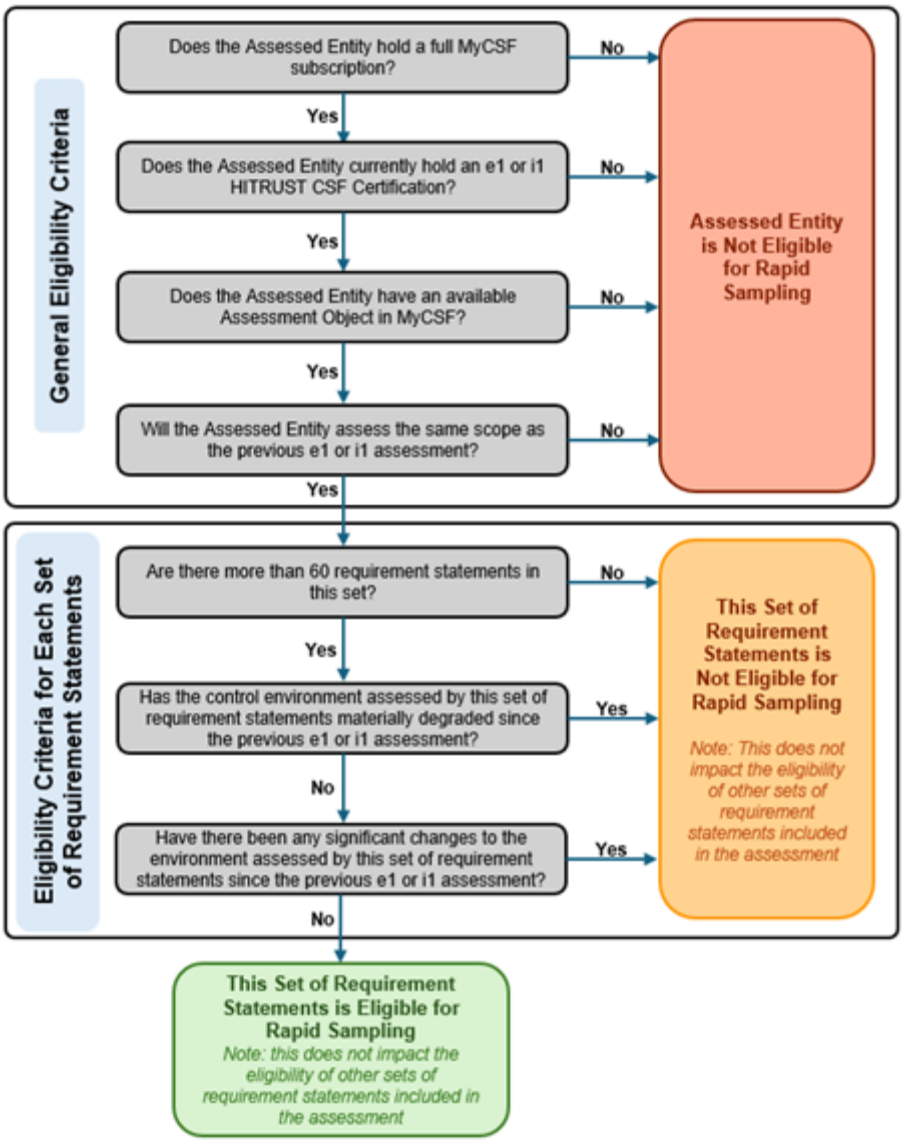
e1 Rapid Assessment Overview

After completing an e1 combined validated assessment in year 1, if the combined assessment included a compliance factor that adds more than 60 requirement statements to the assessment, the assessed entity may be eligible to complete an e1 rapid assessment in year 2. The e1 rapid assessment will allow the rapid sampling approach, described below, to be applied independently to any compliance factor that includes more than 60 requirement statements. The core e1 requirement statements and any compliance factors that include 60 or fewer requirement statements must all be assessed in the e1 rapid assessment.

15.5.1 The i1 and e1 Rapid Assessment results in the same i1 or e1 assessment reports (HITRUST CSF Reports and Insights Reports) and i1 or e1 certification as a full i1 or e1 assessment (valid for one year from the date on the i1 or e1 certification).

i1 and e1 Rapid Assessment Eligibility

Eligibility to apply the rapid sampling approach is determined individually for each set of requirement statements included in the assessment (where a “set” is the set of e1 core, i1 core, and each set of requirement statements added by a single Compliance factor).



Eligibility for each set of requirement statements is determined as follows:

Core Requirements

15.5.2 e1 core requirement statements are never eligible for the rapid sampling approach due to the number of requirement statements in the set being 60 or fewer.

15.5.3 i1 core requirement statements may be eligible for the rapid sampling approach based on the Assessed Entities ability to meet the eligibility criteria below.

Authoritative Source Requirements

15.5.4 Compliance factors that include 60 or fewer requirement statements are never eligible for the rapid sampling approach due to the number of requirements in the set being 60 or fewer.

15.5.5 Compliance factors that include more than 60 requirement statements may be eligible for the rapid

sampling approach based on the Assessed Entities ability to meet the eligibility criteria below

Eligibility Criteria

15.5.6 For the Assessed Entity to be eligible to apply the rapid sampling approach it must have an eligible MyCSF Subscription which allows rapid assessments and have an available object in MyCSF.

15.5.7 For the Assessed Entity to be eligible to apply the rapid sampling it must have an active e1 or i1 certification resulting from the performance of a full e1 or i1 validated assessment using CSF v11 or later.

15.5.8 The Assessed Entity must meet the same Management Representation Letter criteria for the e1 or i1 rapid assessment as described in Chapter 13.8 Management Representation Letter and sign the letter on or prior to expiration of the previous certification to avoid a gap in certification dates. **There is no ability to extend e1 or i1 certifications past the one year expiration**.

15.5.9 For the Assessed Entity to be eligible to apply the rapid sampling approach it must assess the same scope assessed in the prior e1 or i1 assessment.

15.5.10 The rapid assessment will be generated no greater than 120 days prior to expiration of the current e1 or i1 certification (an eligibility questionnaire will be provided to the Assessed Entity 180 days prior to expiration).

15.5.11 If all of the General Eligibility Criteria are met, then for each set of requirement statements potentially eligible for rapid sampling, the following criteria will determine if that particular set of requirement statements may be sampled.

- The set contains more than 60 requirement statements
- The control environment assessed by this particular set of requirement statements has not materially degraded since the previous e1 or i1 assessment was performed.
- No significant changes have occurred since the previous e1 or i1 certification date in the Assessed Entity's business or security policies, processes, controls, hosting locations, or technologies.

15.5.12 When an Assessed Entity is eligible to apply the rapid sampling approach to at least one set of requirement statements and ineligible to apply the rapid sampling approach to others, an i1 or e1 rapid assessment may be performed. Within the rapid assessment, the eligible sets of requirement statements will be sampled, while the ineligible sets will be assessed in full.

NOTE: Even if eligible to perform an i1 or e1 rapid assessment, an Assessed Entity may still choose to perform a full i1 assessment in lieu of the i1 rapid assessment.

Rapid Sampling Approach

For each set of requirement statements that is determined to be eligible for the rapid sampling approach to be applied, the following section describes the selection of requirement statements that are required to be evaluated during the rapid assessment.

15.5.13 If the e1 or i1 Rapid Assessment is created using a newer CSF version than that which was utilized for the Assessed Entity's previous e1 or i1 assessment, there may be additional requirement statements included in this set of requirement statements due to the HITRUST threat analysis and other updates to the CSF.

15.5.14 A sample of 60 requirement statements that were scored in the parent e1 or i1 Assessment from this set. Note that the i1 core sample of 60 requirement statements will include all requirement statements that required a CAP in the previous i1 assessment.

15.5.15 All requirement statements from this set that were marked as N/A during the previous e1 or i1 assessment.

All other requirement statements in the set are not required to be assessed. By default, these requirement statements appear within the assessment in a read-only state and include the scores that were entered in the previous e1 or i1 Assessment. If the Assessed Entity would like to show improvement on a requirement statement that is not already required to be assessed in the e1 or i1 Rapid Assessment, the Assessed Entity may optionally include any of these requirement statements by toggling the requirement statement from read-only to an editable state.

Detection of Control Degradation

During the performance of the e1 or i1 Rapid Assessment, MyCSF monitors the scoring of the sampled requirement statements in the Rapid Assessment and compares them to the parent e1 or i1 assessment to determine whether any scores have been lowered. The control degradation detection process described below and illustrated in the below flowchart is applied independently to each set of sampled requirement statements.

15.5.16 For each sample of 60 requirement statements, if scores are lowered for ***two or fewer*** requirement statements, the sample is accepted and no further testing of requirement statements in that set is required.

15.5.17 If MyCSF detects either ***three or four*** requirement statements in a single sample of 60 requirement statements with lower scores in the Rapid Assessment, the Assessed Entity and External Assessor have the option to expand the sample of requirement statements to assess an additional sample of 60 requirement statements from the set or assess the set of requirement statements in full if there are fewer than 60 additional requirement statements in the set to assess.

- **Case I – three lowered scores:** If the Assessed Entity opts to expand the sample by an additional 60 requirement statements, MyCSF will allow ***two or fewer*** requirement statements with lower scores in the additional sample. If MyCSF detects three or more requirement statements with lower scores in the additional sample, that set of requirements must be assessed in full.

- **Case II – four lowered scores:** If the Assessed Entity opts to expand the sample by an additional 60 requirement statements, MyCSF will allow ***one or fewer*** requirement statements with lower scores in the additional sample. If MyCSF detects two or more requirement statements with lower scores in the

additional sample, that set of requirements must be assessed in full.

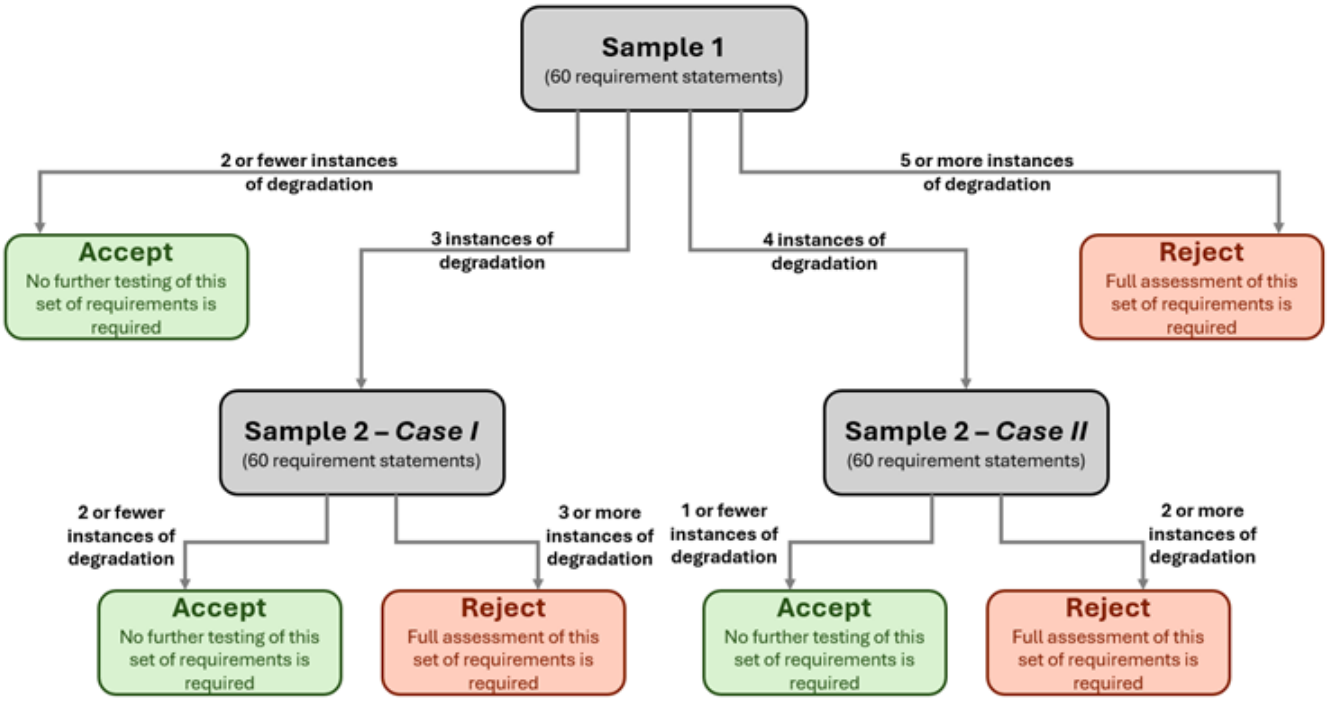
15.5.18 If MyCSF detects ***five or more*** requirement statements with lower scores in a single sample of 60 requirement statements, that set of requirement statements must be assessed in full.

15.5.19 Upon acceptance of the assessment, HITRUST will perform a Quality Assurance review of the submitted assessment. The QA review includes HITRUST review of a random selection of requirement statements from each set of requirement statements (where a "set" is the set of e1 core, i1 core, and each set of requirement statements added by a single Compliance factor).

15.5.20 If scores are lowered during the QA review process, HITRUST will consider whether the scores have been lowered due to an issue with the operation of the control or due to an error in testing approach or documentation. Scores lowered due to an error in testing approach or documentation are not considered to be control degradation. Only scores lowered due to an issue with the operation of the control will count toward the threshold for control degradation.

15.5.21 If scores are lowered due to an issue with control operation, there is a possibility that the threshold for number of scores lowered to indicate material degradation is met during the QA review process. If this occurs, the Assessed Entity and External Assessor must expand the sample of requirement statements evaluated in the e1 or i1 rapid assessment or complete a full e1 or i1 assessment according to the previous guidelines.

The following diagram provides a visual workflow of the control degradation detection process within an e1 or i1 rapid assessment. This control degradation detection process is applied independently to each set of sampled requirement statements (i.e. the core requirement statements and each added Compliance factor).



15.6 Significant Changes

A HITRUST certification is only valid for the system(s), facility(s) and supporting infrastructure included in-scope of an Assessed Entity's validated assessment and the corresponding certification letter and validated report. However, HITRUST understands that Assessed Entities may have fast-changing environments which require maintaining a continuous HITRUST certification. As a result, HITRUST has developed a collaborative process that enables Assessed Entities to maintain their certification when they have identified developments that may impact their current certification ("Significant Changes").

15.6.1 When an Assessed Entity has identified a significant change that may impact its current certification, it must notify HITRUST (support@hitrustalliance.net) to determine the steps that can be taken to maintain its certification.

15.6.2 A change is considered significant when it is likely to impact the security or privacy posture of the Assessed Entity's system(s), facility(s) or supporting infrastructure in-scope of its certification. Examples of activities that might be considered a significant change include*:

- Moving from an on-premises data center into a public cloud environment.
- Moving an in-scope facility to a different physical location.
- Decommissioning a data center and moving all assets to a different data center.
- Replacing in-scope applications or platforms (e.g., moving from SAP to Oracle EBS).
- Changing an in-scope system to use a different back-end system (e.g., using a NoSQL backend instead of a relational database).
- Moving away from an outsourced IT model by standing up an internal IT function.
- Changes in responsibility for performance or oversight of the in-scope control activities (e.g., outsourcing, insourcing, change in service providers).
- New functionality in an in-scope platform enabling it to be accessed from a public location.
- Acquisitions, divestitures, mergers, reorganizations, or other changes in control of an Assessed Entity, or the sale of all or substantially all of the assets of an Assessed entity, where controls over in-scope systems are no longer being operated by the Assessed Entity who originally obtained the certified report.
- Change in a "Factor" question response within the validated assessment.
- Changing the AI model assessed in an ai1 or ai2 certification.

*NOTE: This list is intended to demonstrate example changes in an environment that could result in a certification inaccurately representing the previously assessed environment. This list is not intended to be comprehensive, and not all changes in this list may result in a significant change.

Significant changes are reported so HITRUST certifications continue to accurately reflect the assessed environment, benefiting both the Assessed Entity and its relying parties. The path required to maintain certification is highly dependent on the nature of the change, timing of the change (within the Assessed Entity's certification cycle), and impact on the certification.

15.6.3 Upon notifying HITRUST that the organization may have a significant change, HITRUST will review the circumstances of the change with the Assessed Entity and/or External Assessor. HITRUST may request an evaluation performed by the External Assessor to identify the HITRUST requirements which should be re-assessed. In order to make this determination, the Assessed Entity and/or External Assessor should consider and provide the following information to HITRUST:

- New components within the primary scope (e.g., applications, operating systems, databases, facilities, networks) which were not part of the previous assessment.
- HITRUST requirements where the Assessed Entity's underlying control(s) policy, process and/or operation has changed.
- HITRUST requirements where the Assessed Entity's control owners are within a different department and/or organization.
- New HITRUST requirements which should be assessed as a result of the change.

15.6.4 When an Assessed Entity has a change requiring inheritance and/or reliance from a service provider (e.g., migrating the hosted environment to a cloud service provider) it may immediately inherit and/or rely on any HITRUST requirements performed by the service provider and assessed within a HITRUST *Certified* assessment (where permitted by the service provider). A HITRUST certification validates the control environment has been in place for at least 90 days which permits this ability to immediately inherit and/or rely on these requirements.

15.6.5 Changes to secondary scope components (see Chapter 7.2 Required Scope Components) previously assessed may be considered significant if they impact the previously assessed control policies, processes, or implemented controls within the organization.

For example: If an Assessed Entity replaces its change management tool, but the replacement does not impact its change management processes (e.g., how the organization documents, tests and approves its changes), that would not be considered a significant change. However, if an Assessed Entity changes a recovery location where its backups are stored, relevant backup storage controls (e.g., "Backups are stored in a physically secure remote location") may need to be re-assessed since they would not have been assessed in the current certification.

If additional testing is required by the Assessed Entity due to the significant change, HITRUST may reach the conclusion to include additional testing as part of the interim assessment. Such additional testing is dependent on the timing of the change within the Assessed Entity's certification cycle (as not all changes occur close to interim) and nature of the change (there may not be sufficient time to complete all necessary

additional testing by the interim deadline).

If an Assessed Entity introduces a new system and/or facility not currently in-scope of its HITRUST certification, this is considered a scope expansion. Scope expansions are not considered significant changes since the current certification remains accurate by reflecting the in-scope environment included in the initial certification report. Although the new scope may potentially be introduced into the same environment included within the current HITRUST certification, the new scope would not be HITRUST certified as it was not in-scope of the corresponding validated assessment.

15.6.6 If the Assessed Entity requires the new scope to be HITRUST certified, this will require a new validated assessment on the areas within the scope expansion.

15.6.7 If there are requirement statements in this new assessment which were addressed in its corresponding validated assessment, the Assessed Entity may have the ability to utilize reliance or inheritance from the previously completed HITRUST assessment to avoid re-testing those requirement statements. The certification being relied upon or inherited must be an active certification prior to submission date to be able to utilize this capability. For additional details on reliance, see Chapter 12 Reliance and Third-party Coverage.

15.7 Re-certification

15.7.1 The HITRUST Essentials, 1-year (e1) Certification Report and HITRUST Implemented, 1-year (i1) Certification Report are valid for 12 months from the date of the report, after which the Assessed Entity will be required to re-assess. Any certifications added into an e1 or i1 assessment (e.g., ai1) are also valid for 12 months from the date of the report. NOTE: The date of the report is the same date as the Management Representation Letter (see Chapter 13.8 Management Representation Letter).

15.7.2 The HITRUST Risk-based, 2-year (r2) Certification Report is valid for 24 months from the date of the report, after which the Assessed Entity will be required to re-assess. Any certifications added into a r2 assessment (e.g., ai2, NIST CSF) are also valid for 24 months from the date of the report. To maintain the two-year certification(s), the Assessed Entity must complete an interim assessment at the 12th month mark (see Chapter 15.4 Interim Assessment for additional details).

15.7.3 If the re-assessment fieldwork testing is not complete with a signed Management Representation Letter by the last day of the certification period, the Assessed Entity will have a certification gap. A certification gap is the period between the day the certification expires and the date of the re-certification. During the certification gap, the Assessed Entity is not considered to be HITRUST certified.

15.7.4 HITRUST does not, under any circumstances, extend the expiration date of a HITRUST certification.

For Assessed Entities that have circumstances where they may not be able to submit their r2 validated assessment by the expiration date of the prior certification, HITRUST provides a mechanism to extend the submission date using a bridge assessment (see Chapter 15.8 Bridge Assessments). The bridge assessment allows for up to 90 days after expiration of the prior r2 certification to submit the validated assessment to maintain the HITRUST certification without a certification gap (bridge assessments are not available for i1 or e1 certifications).

15.8 Bridge Assessments

A HITRUST bridge assessment allows an organization to maintain a form of HITRUST certification status for an additional 90 days even if its validated assessment recertification date has passed. A HITRUST bridge assessment results in a HITRUST bridge certificate if all the conditions in this Chapter are met. The HITRUST bridge certificate links an Assessed Entity's expiring HITRUST r2 validated assessment with its re-certification by offering a limited level of assurance during the period when the next HITRUST r2 validated assessment is being completed. Bridge certificates do not extend the expiration date of HITRUST validated reports with certification and are considered a separate certification.

The HITRUST bridge assessment is:

- A forward-looking certificate issued by HITRUST.
- Valid for 90 days from the expiration date of the Assessed Entity's previous HITRUST r2 certification.
- A letter meant to accompany the previous/expired HITRUST certification report.
- Includes the environment for any add-on certification(s) included within the prior r2 assessment (e.g., ai2).
- A means for the organization to demonstrate that:
    - The scoped control environment is unlikely to have degraded since the expiration of the prior certification,
    - The scoped control environment is unlikely to degrade significantly for the duration of this certificate, and
    - It intends to complete the next HITRUST validated r2 assessment prior to the expiration of the HITRUST bridge certificate.

The HITRUST bridge assessment is not:

- An extension to the Assessed Entity's existing certification which still expires on the two-year certification anniversary, or
- A replacement for a traditional HITRUST certification as it does not provide an equivalent level of assurance.
- Available for an i1 or e1 certification.

15.8.1 Eligibility for a bridge assessment is determined based on the following criteria:

i. The Assessed Entity must currently hold an active HITRUST r2 validated report with certification.

ii. The Assessed Entity has not already missed its recertification date by more than 30 days.

iii. No reportable breaches at the Assessed Entity have occurred in the scoped control environment since the HITRUST certification was issued (see Chapter 15.3 Security Events & Fraud).*

iv. No significant changes in the scoped control environment have occurred since the HITRUST certification was issued (see Chapter 15.6 Significant Changes).*

v. The Assessed Entity intends to complete a full validated r2 assessment prior to the expiration of the HITRUST bridge certificate.

*NOTE: If the Assessed Entity has had a reportable breach or significant change, it should contact HITRUST Support (support@hitrustalliance.net) to determine whether it may still be eligible to perform a bridge assessment.

15.8.2 To obtain a HITRUST bridge assessment object, the Assessed Entity must contact its HITRUST Customer Success Manager (CSM) for approval.

15.8.3 HITRUST bridge assessment objects can be created and submitted no more than 60 days before and up to 30 days after the expiration date of the Assessed Entity's HITRUST r2 certification.

Bridge Assessment Process

15.8.4 A HITRUST External Assessor tests 19 requirement statements randomly selected by the HITRUST MyCSF platform. The External Assessor is expected to test all maturity levels that will be included in the r2 validated assessment for the 19 requirement statements. When an Assessed Entity has obtained an add-on certification (e.g., ai2) as part of its r2 assessment, the bridge assessment will also contain a sample of previously assessed requirement statements from the corresponding certification.

NOTE: When an Assessed Entity has obtained an add-on certification within an assessment (e.g., ai2), the Assessed Entity must successfully validate both the r2 and add-on sample of requirements to achieve the bridge certificate. Only one bridge certificate will be issued for the entire environment previously in scope of the assessment.

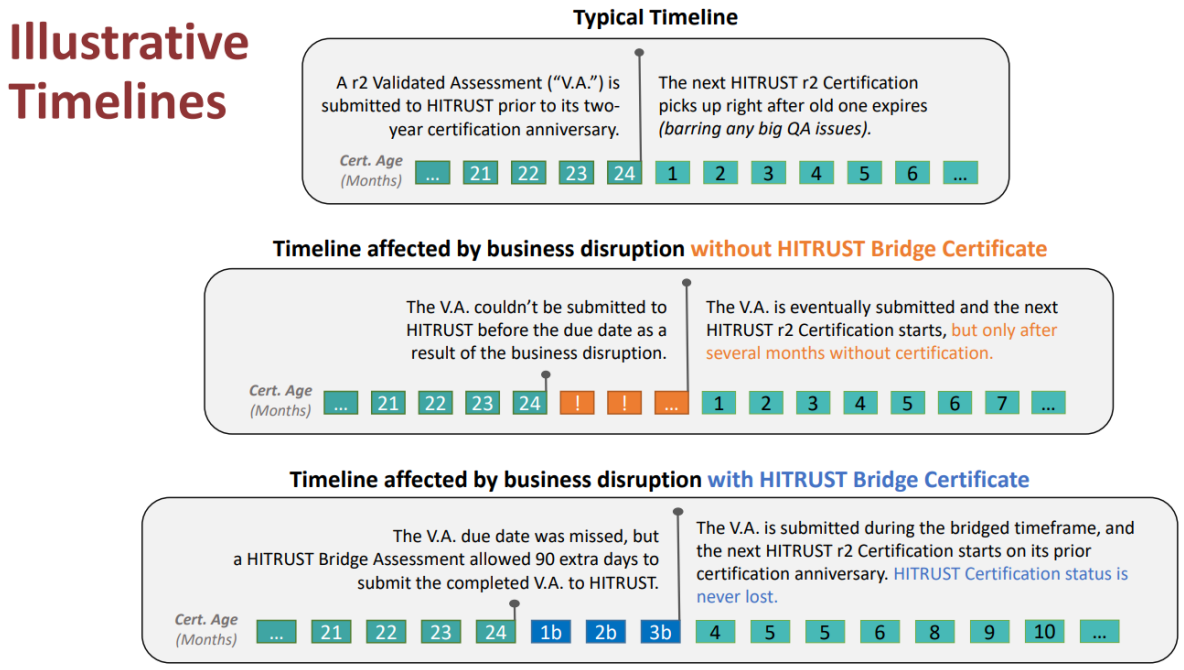
15.8.5 Requirement statements that were inherited in the expiring validated assessment must demonstrate that the assessment that was inherited is still active and in good standing. The External Assessor should acquire the interim letter from the service provider(s) if the HITRUST certification is still active. The External Assessor should acquire the HITRUST certification letter if the service provider(s) certification has been renewed. In these cases, the scoring and evidence from the bridge assessment may not be transferred to the new HITRUST r2 validated assessment but will require a new inheritance request be submitted during validation.

15.8.6 HITRUST will perform a QA review of the External Assessor's testing. QA will be performed to the same level and rigor and against the same scoring rubric as full assessments.

Upon successful completion of the QA review, HITRUST issues a HITRUST bridge certificate, which is dated the expiration date of the prior HITRUST r2 validated report. The test results used during the bridge

assessment may be included for the corresponding requirement statements in the validated assessment without needing to be reperformed (i.e., HITRUST does not require re-testing of these 19 requirement statements).

15.8.7 The Assessed Entity must submit its completed validated assessment to HITRUST prior to expiration of the HITRUST bridge certificate (i.e., no later than 90 days after the previous certification's expiration). The 90 days covered by the HITRUST bridge certificate are deducted from the new HITRUST certification's 24-month validity period resulting in the new certification being dated as of the original re-certification date.



For additional information on bridge assessments, see HITRUST CSF Bridge Assessment.

15.9 Emerging Mitigation Process (EMP)

The HITRUST CSF framework is Cyber Threat Adaptive (CTA) to ensure organizations have controls in place to address current threats. As part of the CTA process, HITRUST regularly reviews current threat intelligence data that has been associated with MITRE ATT&CK techniques, and utilizes the MITRE ATT&CK mitigations to identify the controls within the CSF framework necessary for each assessment type. As cyber threats evolve over time, HITRUST may identify new threats as part of the CTA process. When a new urgent threat is identified which needs to be addressed through a new mitigation, HITRUST will expedite the consideration and inclusion of additional requirement statements within the HITRUST CSF through the Emerging Mitigation Process (EMP). Please note the EMP is not launched for each newly identified threat as most threats will have existing mitigations (and corresponding HITRUST requirements) within the HITRUST CSF. The EMP will only be launched when HITRUST identifies an urgent and serious threat requiring a prioritized response.

The introduction of new requirement statements initiated through the EMP will impact each Assessed Entity differently depending on where it is within its certification cycle. This chapter outlines the EMP steps and expectations for an Assessed Entity when HITRUST must introduce new requirement statements through the EMP process.

Please note the EMP is separate from HITRUST's standard review and update process for the HITRUST CSF framework. If HITRUST identifies a new threat through EMP which is not currently addressed in the HITRUST CSF framework, it should be considered a situation where Assessed Entities must be mindful of the potential impact within its environment since the corresponding risk may not have previously been considered within its HITRUST assessment.

NOTE: For a more detailed discussion around HITRUST's CTA approach, see A-4 Cyber Threat Adaptive Control Specification in the HITRUST Risk Management Handbook.

HITRUST Community Notification

Upon activation of the EMP, HITRUST would first notify the HITRUST community that a new mitigation was identified. As part of the mitigation, HITRUST would include detailed information on the threat, potential risks and additional requirement statement(s) being added to HITRUST assessments as part of the mitigation.

15.9.1 Upon receipt of the HITRUST notification, Assessed Entities should perform a self-assessment to determine susceptibility to the threat. If an Assessed Entity determines that it has an exposure to the threat, it should implement the new HITRUST requirement.

CSF Version Release Process

Activation of the EMP will result in any new requirement statement(s) being added as an errata release for each CSF version currently available for assessment creation (e.g.: v11.0.x, v11.1.x, v11.2.x). Due to the increased risk of a newly identified threat, HITRUST will impose a creation and submission deadline for prior

CSF versions which do not include the requirement statement(s).

15.9.2 HITRUST will announce creation and submission deadlines for previous CSF versions which do not include the HITRUST requirement statement(s) added through the EMP. The following upgrade processes will be utilized:

- All new e1, i1, and r2 assessments created after the notification deadline will use an errata version that includes the requirement statement(s).
- Any existing e1, i1, and r2 assessments not yet submitted to HITRUST may optionally be upgraded to the new errata version. If these assessments are not submitted by the announced submission deadline, they must be upgraded to the new errata version.
- The new requirement statement(s) will also be included in any r2 interim assessments created after the community notification deadline.
- Existing interim assessments and interim assessments created prior to the announced deadline will not include the new requirement statement(s).

15.9.3 When any new requirement statement(s) related to the EMP release is assessed within an r2 interim assessment, the interim letter will include a statement indicating the requirement statement(s) was included in the interim assessment as well as the requirement statement score(s). If a new requirement statement related to the EMP release scored less than 62, HITRUST will require a CAP to be entered in MyCSF and state in the letter that a CAP was provided. For more information on CAPs, see Chapter 13.9 CAPs and Gaps..

15.10 HITRUST Treatment of Non-compliance

HITRUST expects all Assessed Entities and External Assessors to meet the criteria described within this Assessment Handbook. Assessed Entities and External Assessors may contact their HITRUST CSM or HITRUST Support (support@hitrustalliance.net) with questions on the criteria.

15.10.1 If criteria are not met that impact the scoring and/or certification results in an assessment, the Assessed Entity and/or External Assessor must make any corrections requested by HITRUST.

15.10.2 If criteria are not met that may mislead the reader of a HITRUST report to reach inaccurate conclusions, the Assessed Entity and/or External Assessor must make any corrections requested by HITRUST.

15.10.3 If an External Assessor does not meet the HITRUST assessment or testing criteria defined in this Assessment Handbook, HITRUST may request or perform one or more of the following actions based on the nature, quantity, and severity of the infractions:

- Remediation of the non-compliant assessment
- Rejection of the non-compliant assessment
- Written warnings of non-compliance
- Non-compliance meetings between HITRUST and External Assessor firm's leadership
- External Assessor firm corrective action plans
- Tracking and reporting of non-compliance in External Assessor performance reports

15.10.4 If an Assessed Entity or External Assessor has questions on the Assessment Handbook content or believes it is unable to meet certain criteria it may contact their HITRUST CSM or HITRUST Support (support@hitrustalliance.net) for additional guidance.

15.10.5 Requests for exceptions to criteria within this Assessment Handbook must be sent to HITRUST Support (support@hitrustalliance.net). Any request for an exception to criteria in this handbook must include:

- Criterion number for which the exception is being requested
- Rationale for the exception
- Where possible, description of an alternative approach or mitigating factors which may address risks of not adhering to the HITRUST criterion

15.10.6 At HITRUST's discretion, it may provide alternatives to achieving the defined criteria in this Assessment Handbook. Any alternative solutions approved by HITRUST are granted on a one-time basis.

Appendix A: FAQs & Examples

A-1: Carve-out Scoring Details

For i1 and e1 validated assessments, the External Assessors and Assessed Entities have two options to address situations in which a requirement statement is fully or partially performed by a service provider (such as by a cloud service provider):

- ***The Inclusive method,*** whereby requirement statements performed by the service provider are included within the HITRUST assessment and addressed utilizing full or partial inheritance, reliance on third-party assurance reports, and/or direct testing (see Chapter 12 Reliance & Third-Party Coverage for additional details).

- ***The Carve-out method,*** whereby requirement statements performed by the service provider remain included within the HITRUST assessment but marked as Not Applicable (N/A). The N/A includes supporting commentary that specifies that the requirement statement is fully performed by a party other than the Assessed Entity (for fully outsourced controls) or describes the excluded partial performance of the control (for partially outsourced controls).

NOTE: For all r2 assessments, the inclusive method must be used.

For i1 and e1 validated assessments utilizing the Carve-Out method, the Scope of the Assessment details within MyCSF will be updated to reflect the carve-out. For example, under the “Services Outsourced for In-Scope Platforms and Facilities” table, the Assessed Entity and/or the External Assessor will select “Excluded” from a “Consideration in this Assessment” dropdown menu.

Applying the inclusive and carve-out methods for the same service provider within the same assessment object is not permitted (see Chapter 7.3 Carve-outs). Therefore, only one method can be selected for each service provider relevant to the Assessed Entity’s assessment scope.

For example, if an Assessed Entity’s infrastructure is hosted and managed by a Cloud Service Provider (CSP) within an i1 or e1 assessment object, it may decide to carve-out the CSP. In this case, the following must be updated within the assessment object.

1. Scope of the Assessment – In the “Platforms / Systems” table, the “Exclusions from Scope” column must be updated to reference the CSP.
2. Scope of the Assessment – In the “Services Outsourced for In-scope Platforms and Facilities” table, the CSP must be added and “Excluded” should be selected within the menu dropdown in the “Consideration in this Assessment” column.
3. All requirement statements that the CSP fully manages will be marked Not Applicable (N/A), and the rationale should always note that the CSP is out of scope due to the carve-out approach.
4. For all requirement statements the excluded CSP partially manages, the Assessed Entity will assess and score its percentage and N/A the CSP portion.

A-2: Mixed Applicability Errors

HITRUST identifies “Mixed Applicability” errors within an assessment when inconsistent responses have been identified in the submission. “Mixed Applicability” errors typically occur due to

- inconsistent responses to factor questions or
- inconsistent responses across requirement statements that address the same topic.

1. Inconsistent responses to factor questions

If a reductive factor question is answered ‘Yes’, the requirement statements related to that factor question topic are not removed from the assessment. In this case, if there are a significant number of requirement statements related to the reductive factor topic answered as N/A, HITRUST will check whether the related factor should actually be answered as ‘No’. A ‘No’ response will remove the requirement statements from the assessment.

For example, if the factor question related to electronic signatures “Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment?” is answered ‘Yes’, but the corresponding requirement statements related to electronic signatures in the assessment are all marked N/A then HITRUST will check whether the factor should be answered as ‘No’.

2. Inconsistent responses across requirement statements that address the same topic

There will be a “Mixed Applicability” error if responses for related requirement statements were assessed inconsistently throughout the assessment object.

For example, a “Mixed Applicability” error will be raised if the requirement statement responses in domain 4 were scored as Not Applicable (N/A) with the rationale “mobile devices are not permitted in the environment”, but in domain 13, the requirement statement “Personnel using mobile computing devices are trained on the risks, the controls implemented, and their responsibilities (e.g., shoulder surfing, physical protections).” was scored.

The “Mixed Applicability” error will be flagged in the assessment, and HITRUST will review the inconsistencies with the External Assessor to ensure that all requirement statements were answered consistently.

A-3: Not Applicable (N/A) Examples

For any requirement statement marked as N/A, the Assessed Entity must provide a clear and concise rationale to support why the requirement statement is not applicable to the in-scope environment. The rationale should directly address the requirement statement and the current state of the in-scope environment. The following examples include acceptable N/A rationales for the corresponding situation:

Requirement Statement	In-scope environment background	Rationale for N/A
0302.09o2Organizational.1 The organization protects and controls media containing sensitive information during transport outside of controlled areas.	The Assessed Entity does not maintain any portable media within its in-scope facilities.	Removable media devices are not used or permitted within the in-scope environment. Therefore, the organization will not have any media to protect nor transport.
19243.06d1Organizational.15 The organization specifies where covered and/or confidential information can be stored.	The Assessed Entity is a business associate and does not process, manage, or store covered or confidential information.	“XYZ” is a business associate, not a covered entity. It does not process, manage nor store any covered or confidential information.
0504.09m2Organizational.5 Firewalls are configured to deny or control any traffic from a wireless environment into the covered and/or confidential data environment.	The Assessed Entity has no wireless access points within the in-scope environment.	“XYZ” does not have or utilize any wireless access points within the in-scope environment.
1699.09l1Organizational.10 Workforce members roles and responsibilities in the data backup process for Bring Your Own Device (BYOD) are identified and communicated to the workforce; in particular, users are required to perform backups of organizational and/or client data on their BYOD devices.	The Assessed Entity does not allow the use of any personal devices within the in-scope environment, so there are no BYOD devices.	“XYZ” does not permit any personal devices within the in-scope environment.
19165.07e1Organizational.13 The organization physically and/or electronically labels and handles sensitive information commensurate with the risk of the information or document. Labeling reflects the classification according to the rules in the information classification policy.	The Assessed Entity does not manage or store sensitive information within the in-scope environment.	“XYZ” does not manage or store any sensitive information within the in-scope environment.

A-4: Never N/A Examples

There are certain requirement statements that HITRUST has determined can typically not be marked N/A. The following examples include requirement statements HITRUST expects to be scored along with HITRUST's rationale for not being able to mark the requirement statements as N/A:

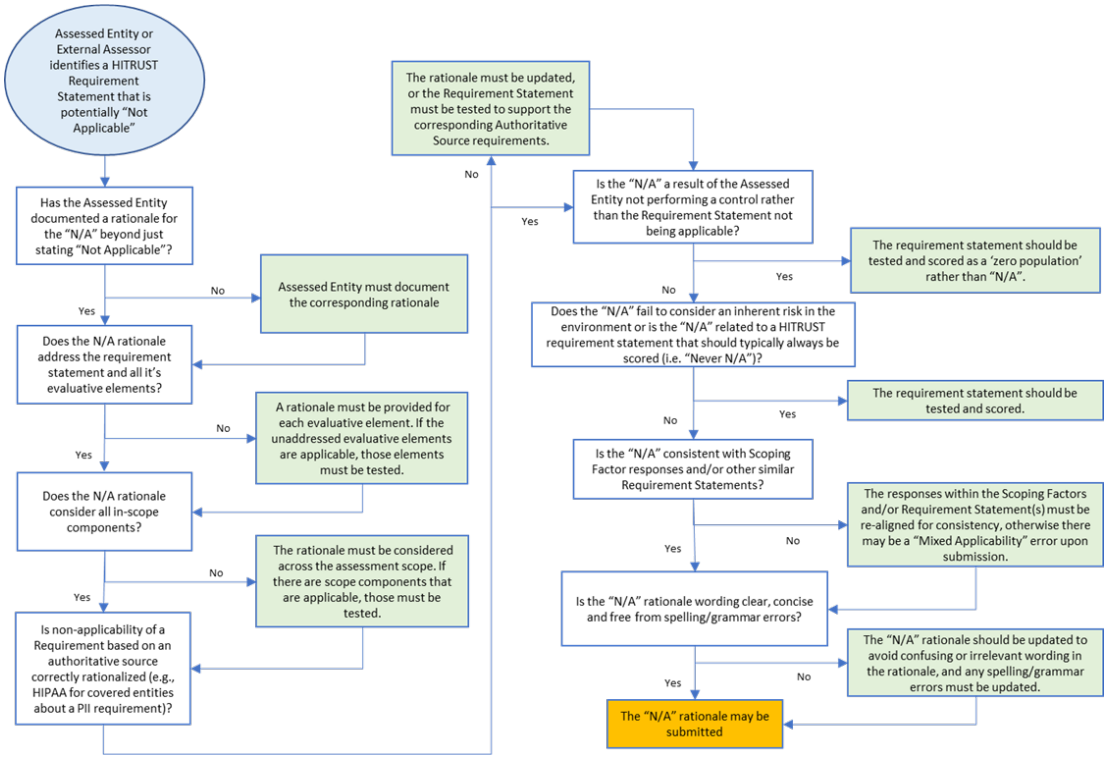
HITRUST CSF Requirement Statement	Example (Incorrect) Assessment N/A Rationale	HITRUST Rationale for not allowing N/A	Suggested Testing Approach
0505.09m2Organizational.3 Quarterly scans are performed to identify unauthorized wireless access points, and appropriate action is taken if any unauthorized access points are discovered.	"The in-scope facility does not use wireless access."	The requirement statement expects a detective control to identify unauthorized wireless access points connected to the in-scope network(s). (NOTE: A similar rationale applies to other monitoring requirement statements within a HITRUST assessment)	The requirement statement should be tested for all in-scope networks.
0403.01×1Organizational.5 The organization (1) monitors for unauthorized connections of mobile devices.	"Mobile devices are not allowed in the scoped environment."	The requirement statement expects a detective control to identify unauthorized mobile device connections.	The requirement statement should be tested.
0828.09m2Organizational.8 Technical scanning tools and solutions (1) are implemented. Scans (2) are performed on a quarterly basis to identify unauthorized components/devices.	"The company has outsourced its vulnerability scanning."	Unless the third-party was carved-out (only allowed for i1 and e1), a third-party performing the control does not make a requirement statement not applicable. The requirement statement expects scanning solutions and scans to be performed on the in-scope environment, regardless of who performs it.	For an r2, the third-party's performance of the requirement statement should be tested. For an i1 or e1, the third-party can be carved-out which will allow an N/A.
1119.01j2Organizational.3 Periodic monitoring (1) is implemented to ensure that installed equipment does not include unanticipated dial-up capabilities.	"The company does not maintain equipment with dial-up capabilities."	The requirement statement expects a detective control to identify a system with dial-up capabilities where the company was not aware.	The requirement statement should be tested.
0858.09m2Organizational.12 The organization (1) monitors	"The in-scope facility does not	For #1, The requirement statement expects a detective control to identify	The requirement statement should be

for all authorized and unauthorized wireless access to the information system and (2) prohibits installation of wireless access points (WAP) unless explicitly authorized, in writing, by the CIO or his/her designated representative.	use wireless access points."	unauthorized wireless access. For #2, the requirement contemplates that the organization must have a requirement for a wireless access point's installation in the future. This can be more prohibitive than the HITRUST requirement but there still must be a requirement.	tested.
19134.05j1Organizational.5 The public has access to information about the organization's security and privacy activities and is able to communicate with its senior security official and senior privacy official.	"The company does not deal with the public" OR "The scoped environment does not have public facing components, application, and/or systems"	The rationale assumes 'general public' only. The requirement is not solely dependent on interacting with the 'general public.' This requirement statement applies if the company has customers.	The requirement should be tested by the Assessed Entity taking its customers and/or users into consideration.
19180.09z1Organizational.2 The organization designates individuals authorized to post information onto a publicly accessible information system, and trains these individuals to ensure that publicly accessible information does not contain nonpublic information.	"No publicly accessible systems are in scope of the assessment"	This is an entity-level control which applies to the organization as a whole. Publicly accessible systems include the company website or company social media sites (e.g., LinkedIn, facebook, etc.)	The requirement should be tested by the Assessed Entity taking its public media and data protection policy/ procedures into consideration.
19249.06b1Organizational.2 The organization establishes restrictions on the use of open source software. Open source software used by the organization is legally licensed, authorized, and adheres to the organizations secure configuration policy.	"The scope of the assessment doesn't include open source software."	This is an entity-level control which applies to the organization as a whole. Open source software is typically accessible by organization employees so appropriate limitations should be implemented.	The requirement should be tested by the Assessed Entity taking the ability for employees to access open source software into account.
Domain 18 Physical & Environmental Security	"The company hosts all information in	Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which	If the service provider is not carved-out, Physical

	the cloud so there are no physical and environment security requirements.”	should be addressed in the assessment (unless carved-out in an i1 or e1 assessment).	Security requirement statements must be scored either by direct testing or relying on testing of the service provider (i.e., reliance or inheritance).

A-5: N/A Decision Tree

For organizations that have adopted the HITRUST CSF and have answered the assessment factors correctly, the majority of HITRUST requirement statements should apply to the environment. If there are many requirement statements marked as N/A within an assessment it may indicate the N/A designation was incorrectly applied. For assistance in determining whether the N/A designation was correctly applied, see the following decision tree for additional guidance.



A-6: Rubric Scoring – Policy, Procedure, and Implemented

The following examples outline how to use the HITRUST scoring rubric to identify the appropriate Policy, Procedure, and Implemented strength and coverage over a number of scenarios. Before reading the examples, please review Chapter 9: Control Maturity Levels and the HITRUST CSF Control Maturity Scoring Rubric.

For examples pertaining to the *Measured* and *Managed* maturity levels, see A-7: Rubric Scoring – Measured and Managed.

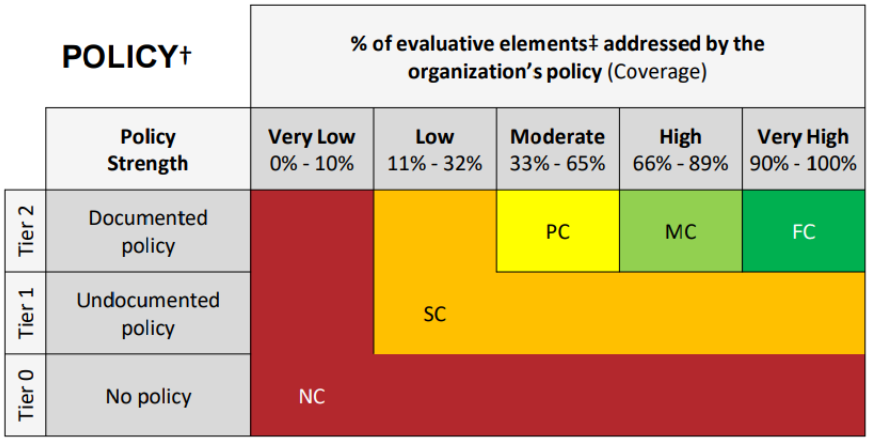
Example #1

Scenario
BUID: 0410.01×1system.12 | CVID:0271.0
If it is determined that encryption is not reasonable and appropriate, the organization documents its
1. rationale, and
2. acceptance of risk.

Evaluation

Policy:

A “Mobile Device Policies and Procedures” document states, “All PHI, PII, and sensitive data shall be encrypted,” and also states, “All mobile devices, laptops, smartphones, and other portable media shall be encrypted.”



Policy Strength: In this scenario, a documented mobile device policy exists (see Chapter 9.1 Policy Maturity Level) so the *Policy* strength appears to be “Tier 2 – Documented Policy”.

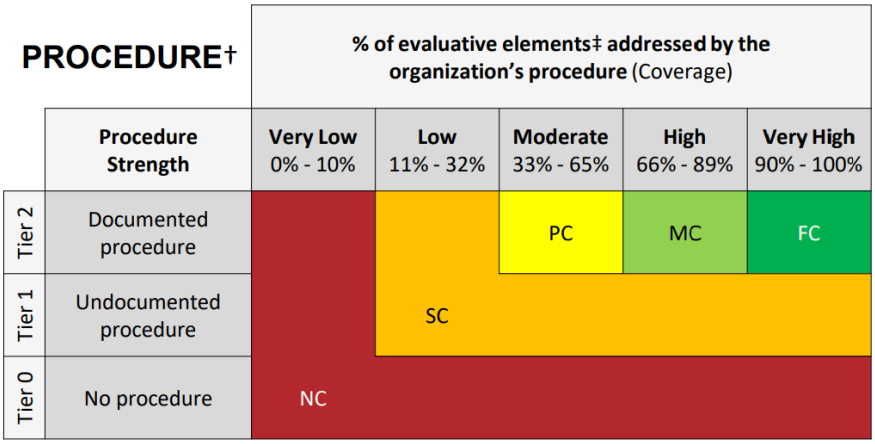
Policy Coverage: While the policy does talk about encrypting mobile devices, it does not address the documentation of A) rationale and B) acceptance of risk, when the organization deems that encryption is not reasonable and appropriate. Therefore, the *Policy* coverage is 0/2 = 0% or “Very Low”.

Policy Score: Use the strength and coverage to determine the final *Policy* score according to the rubric. “Tier 2” strength and “Very Low” coverage indicate a score of ***Non-Compliant*** or 0%.

Alternative Approach – Once it is determined that the Mobile Device Policies and Procedures document does not address this requirement statement’s evaluative elements, the External Assessor may opt to investigate whether an undocumented policy exists (see Chapter 9.1 Policy Maturity Level). In this scenario, the implementation testing described below indicates that there is not an undocumented policy that is consistently observed. This alternative approach therefore results in a *Policy* strength of “Tier 0 – No Policy”, which always indicates a score of ***Non-Compliant*** or 0%. Note that both approaches result in the same *Policy* score.

Procedure:

The Mobile Device Policies and Procedures document states, “All PHI, PII, and sensitive data shall be encrypted,” and also states, “All mobile devices, laptops, smartphones, and other portable media shall be encrypted.”



Procedure Strength: To determine the appropriate *Procedure* score, first identify the *Procedure* strength. The “Mobile Device Policies and Procedures” document doesn’t actually contain any procedures (despite the name) as it does not describe the operational aspects of how to perform the requirements. Therefore, a documented procedure does not exist and the External Assessor may investigate whether an undocumented procedure exists (see Chapter 9.2 Procedure Maturity Level).

The External Assessor’s inquiries of various members of the workforce showed that no consensus exists on what to do if it is determined encrypting a mobile device is not reasonable and appropriate. Further, the implementation testing described below confirms that there are no undocumented procedures that are consistently observed. Therefore, *Procedure* strength is “Tier 0 – No Procedures”.

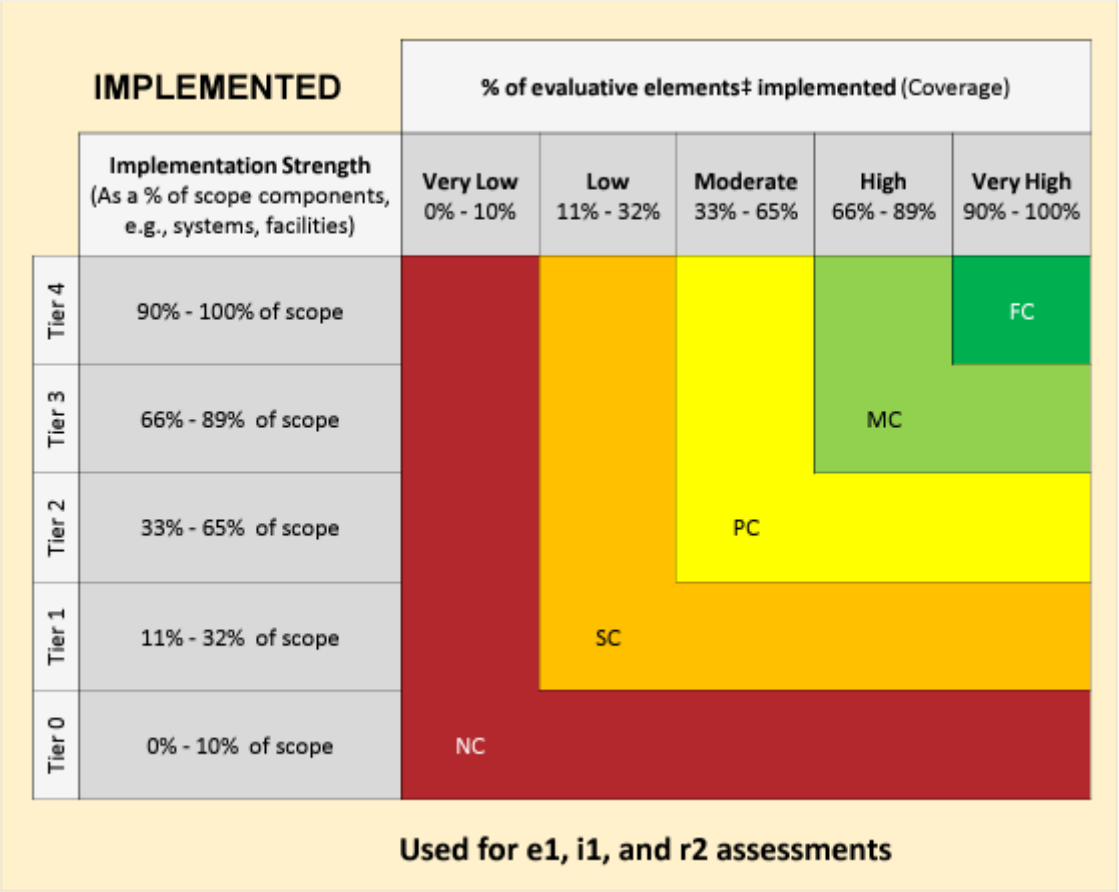
Procedure Coverage: Since *Procedure* strength is “Tier 0”, there is no need to determine *Procedure*

coverage.

Procedure Score: “Tier 0” strength always indicates a final *Procedure* score of ***Non-Compliant*** or 0%.

Implemented:

A comparison of a system-generated population of mobile devices (including laptops and phones) against the IT asset inventory (deemed complete by the testing of another requirement statement) showed that 75 of the organization’s 100 mobile devices are encrypted. However, the organization has not documented the rationale for its failure to encrypt the remaining 25 mobile devices.



Implemented Coverage: To determine implementation coverage, identify the percentage of the evaluative elements implemented. In this example, there was no documentation of rationale or acceptance of risk for the 25 mobile devices that were not encrypted. Therefore, neither of the two evaluative elements has been implemented and coverage is 0% or “Very Low”.

Implemented Score: In this case, the final *Implemented* score can be determined from the coverage since the testing demonstrated the requirement statement was not being performed. “Very Low” coverage will always result in a score of ***Non-Compliant*** or 0%.

Example #2

Scenario
BUID: 1814.08d1Organizational.12 | CVID:0732.0
Appropriate fire extinguishers
1. are located throughout the facility, and
2. are no more than fifty (50) feet away from critical electrical components.
Fire detectors (e.g., smoke or heat activated) are installed on and in the
3. ceilings and
4. floors.

Evaluation

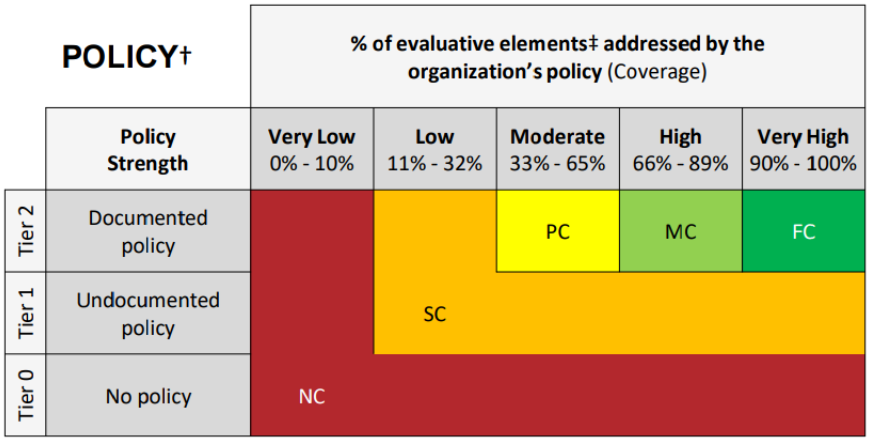
In this scenario, the evaluation for each maturity level indicates varied strength and coverage across the three scoping components (Office, DC1, and DC2).

Policy:

The Assessed Entity has a “Data Center Environmental Protections Policy”, but this policy is only applicable to data centers (not office buildings).

- The Data Center Environmental Protections Policy states, “Fire detectors must be installed in the ceilings. Clearly marked fire extinguishers must be placed throughout the facility.” There is no mention of fire detectors installed in the floors and no further mention of placement of fire extinguishers relative to critical electronics.

- Further, no policies exist addressing environmental protections in corporate offices, which is unsurprising given no fire protections were noted during an office tour.



In this example, the steps outlined in the HITRUST rubric for “varied scope on each level” will be used to determine the final score for the Policy maturity level.

Step 1) Decompose/separate scope into individual components against which the rubric can be applied.

This scenario has three individual scope components:

1. Office
2. DC1
3. DC2

Step 2) Apply the HITRUST CSF control maturity scoring rubric to each individual scope component.

1. Office

   Policy Strength: In this scenario, no policy exists for the Office, so the *Policy* strength is “Tier 0 – No Policy”.
   Policy Score: In this case, the *Policy* score can be determined from the strength alone. “Tier 0 – No Policy” strength always indicates a score of ***Non-Compliant*** or 0%.

2. DC1

   Policy Strength: In this scenario, a documented policy exists for DC1, so the *Policy* strength appears to be “Tier 2 – Documented Policy”.
   Policy Coverage: To determine the *Policy* coverage, consider the percentage of evaluative elements covered for DC1. Evaluative elements 1 and 3 are covered by the policy, so the percentage of evaluative elements covered is 2/4 = 50%. This indicates “Moderate” coverage.
   Policy Score: Use the strength and coverage to determine the *Policy* score according to the rubric. “Tier 2” strength and “Moderate” coverage indicate a score of ***Partially Compliant*** or 50%.

3. DC2

   Policy Strength: In this scenario, a documented policy exists for DC2, so the *Policy* strength appears to be “Tier 2 – Documented Policy”.
   Policy Coverage: To determine the *Policy* coverage, consider the percentage of evaluative elements covered for DC2. Evaluative elements 1 and 3 are covered by the policy, so the percentage of evaluative elements covered is 2/4 = 50%. This indicates “Moderate” coverage.
   Policy Score: Use the strength and coverage to determine the *Policy* score according to the rubric. “Tier 2” strength and “Moderate” coverage indicate a score of ***Partially Compliant*** or 50%.

Step 3) Calculate an average score.

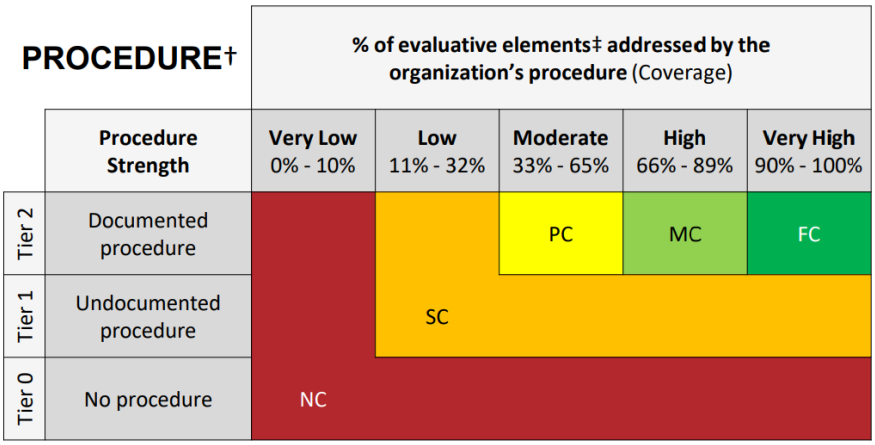
(0% + 50% + 50%)/3 = 33.3%

Step 4) Refer to the “Range of Average Scores” in the legend of the HITRUST rubric to determine the rating.

Since 33.3% falls within the range of 33% – 65%, the final *Policy* score is ***Partially Compliant*** or 50%.

Procedure:

For the two data centers, the Assessed Entity has a written “Data Center Fire Protections Procedure” addressing operational aspects of how to install and maintain fire detectors on the ceilings and fire extinguishers throughout the facilities. The policies and procedures do not specify that fire extinguishers must be placed no more than fifty (50) feet away from critical electrical components or that fire detectors must be installed in the floors. Further, no procedures exist addressing environmental protections in corporate offices, which the External Assessor found unsurprising given no fire protections were noted.



Step 1) Decompose/separate scope into individual components against which the rubric can be applied.

This scenario has three individual scope components:

1. Office
2. DC1
3. DC2

Step 2) Apply the HITRUST CSF control maturity scoring rubric to each individual scope component.

1. Office

   Procedure Strength: In this scenario, no procedure exists for the Office, so the *Procedure* strength is “Tier 0 – No Procedure”.
   Procedure Score: In this case, the *Procedure* score can be determined from the strength alone. “Tier 0 – No Procedure” strength always indicates a score of ***Non-Compliant*** or 0%.

2. DC1

   Procedure Strength: In this scenario, a documented procedure exists for DC1, so the *Procedure* strength appears to be “Tier 2 – Documented Procedure”.
   Procedure Coverage: To determine the *Procedure* coverage, consider the percentage of evaluative elements covered for DC1. Evaluative elements 1 and 3 are covered by the procedure, so the percentage of evaluative elements covered is 2/4 = 50%. This indicates “Moderate” coverage.
   Procedure Score: Use the strength and coverage to determine the *Procedure* score according to the rubric. “Tier 2” strength and “Moderate” coverage indicate a score of ***Partially Compliant*** or

50%.

3. DC2

   Procedure Strength: In this scenario, a documented procedure exists for DC2, so the *Procedure* strength appears to be “Tier 2 – Documented Procedure”.
   Procedure Coverage: To determine the *Procedure* coverage, consider the percentage of evaluative elements covered for DC2. Evaluative elements 1 and 3 are covered by the procedure, so the percentage of evaluative elements covered is 2/4 = 50%. This indicates “Moderate” coverage.
   Procedure Score: Use the strength and coverage to determine the *Procedure* score according to the rubric. “Tier 2” strength and “Moderate” coverage indicate a score of ***Partially Compliant*** or 50%.

Step 3) Calculate an average score.

(0% + 50% + 50%)/3 = 33.3%

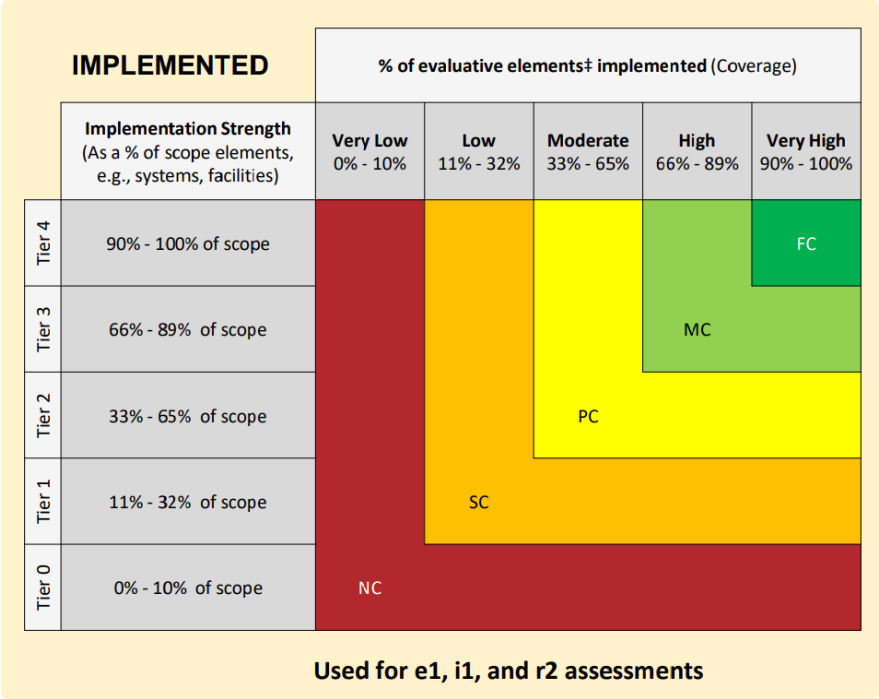
Step 4) Refer to the “Range of Average Scores” in the legend of the HITRUST rubric to determine the rating.

Because 33.3% falls within the range of 33% – 65%, the final *Procedure* score is ***Partially Compliant*** or 50%.

Implemented:

During the visit to each in-scope facility the External Assessor noted the following;

1. Office tour, no fire extinguishers or detectors were present.
2. A DC1 tour revealed that fire extinguishers are present throughout the facility and no more than fifty (50) feet away from critical electrical components and that fire detectors aren’t installed.
3. A DC2 tour yielded no exceptions. All evaluative elements were met.



For the *Implemented* Maturity level, the scoring does not need to be decomposed into separate scope components since the *Implemented* strength takes into account the overall scope against the evaluative elements.

The Requirement statement's *Implemented* strength is evaluated by considering the Assessed Entity's control application across the assessment scope. The tier in the rubric for *Implemented* strength can be calculated based on the number of scope components where the control is being applied. The application of these controls can be determined utilizing corresponding observations, inspections, or walkthroughs for each scope component.

In this example, it was determined that the controls for this requirement statement were not being applied for the Office location. However, the controls were being applied at each of the Data Centers. As a result, the *Implemented* strength will be calculated at (0% + 100% + 100%)/3 = 67%, or *Tier 3*.

The maturity rating for *Implemented* coverage can be readily computed by leveraging a single table for coverage.

Example 2 Assessment Results for Coverage – Implemented

Evaluative Elements	Office	DC1	DC2
Fire Extinguishers Throughout	Not Implemented	Implemented	Implemented
Fire Extinguishers < 50'	Not Implemented	Implemented	Implemented
Fire Detectors in Ceilings	Not Implemented	Not Implemented	Implemented
Fire Detectors in Floors	Not Implemented	Not Implemented	Implemented

Coverage	0%	50%	100%

A simple average yields 50% ((0% + 50% +100%)/3), or “Moderate” for *Implemented* coverage.

Implementation Score: On the *Implemented* rubric, the intersection of “Tier 3” Strength and “Moderate” Coverage is 50% or ***Partially Compliant***.

Example #3

Scenario
BUID: 06.09b1System.2 | CVID:0271.0
Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently

1. *Documented,*
2. *Tested, and*
3. *Approved.*

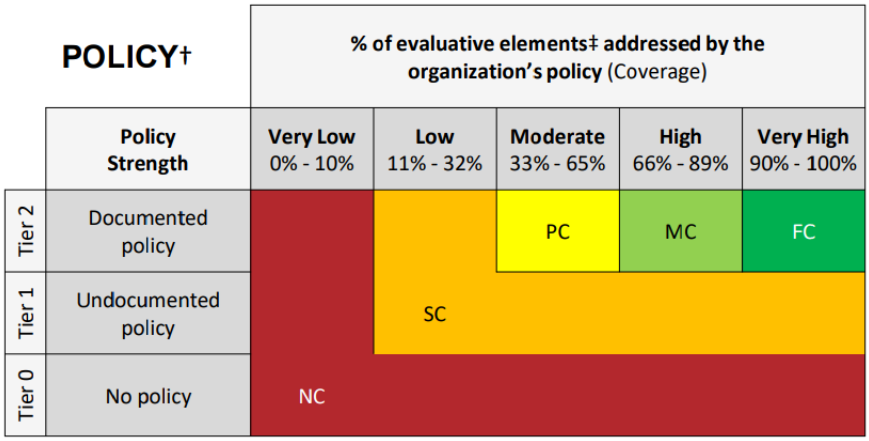
The scope identified for testing included: Application #1, Operating System #1, Database #1, and Network #1.

Evaluation

Policy:

The Assessed Entity has two separate Change Management policies:

- Change Management Policy #1 is documented for Application #1, Operating System #1, and Database #1 and states that changes must be documented, tested, and approved. (All three elements are covered)
- Change Management Policy #2 is documented for Network #1 and states that changes must be documented and approved. Since testing of changes is not explicitly stated in the policy, only 2 of 3 elements are covered.



Policy Strength: In this scenario, a documented policy exists for all four scope components, so they are all scored at “Tier 2”. Since they are scored at the same tier on the rubric, the *Policy* coverage scores can be averaged to determine the overall score for the *Policy* Maturity Level.

Policy Coverage: To determine the *Policy* coverage, consider the percentage of evaluative elements covered for each scope component.

Example 3 Assessment Results for Coverage – Policy

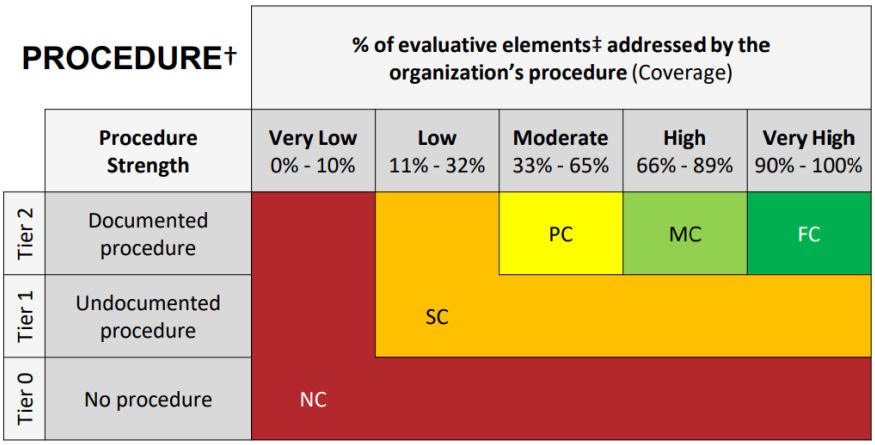
Evaluative Elements	Application #1	Operating System #1	Database #1	Network #1
Changes are documented	Covered	Covered	Covered	Covered
Changes are tested	Covered	Covered	Covered	Not Covered
Changes are approved	Covered	Covered	Covered	Covered
Coverage	100%	100%	100%	67%

An average of the scores indicates overall coverage is 91.75% which is “Very High” *Policy* coverage.

Policy Score: Use the strength and coverage to determine the final *Policy* score according to the rubric. “Tier 2” strength and “Very High” coverage indicate a score of ***Fully Compliant*** or 100%.

Procedure:

It was determined that a Change Management Procedure was in place stating how to document, test, and approve changes for Application #1, Operating System #1, and Database #1. There was no documented Change Management procedure in place for Network #1. However, the External Assessor determined, via walkthrough and observations of the Change Process, that the Change Management process was well-understood by the Network Administrators and that it required change documentation, testing, and approvals for all Network changes.



Procedure Strength: In this scenario, a documented procedure exists for three of the four scope

components, so those three (Application #1, Operating System #1 and Database #1) are scored at “Tier 2”. However, the procedure for Network changes was not documented. Since it was observed to be performed and well-understood by those performing the procedure, it can be scored at a “Tier 1 Undocumented procedure”.

Procedure Coverage: To determine the *Procedure* coverage, consider the percentage of evaluative elements covered for each scope component.

Example 3 Assessment Results for Coverage – Procedure

Evaluative Elements	Application #1	Operating System #1	Database #1	Network #1
Changes are documented	Covered	Covered	Covered	Covered
Changes are tested	Covered	Covered	Covered	Covered
Changes are approved	Covered	Covered	Covered	Covered
Coverage	100%	100%	100%	100%

In this instance, an alternate method will be utilized for calculating the rubric score since there were differing strength scores. This calculation will also show how weighting may be utilized in scoring.

Since Application #1, Operating System #1, and Database #1 all follow the same Change Management Procedure, these will have the same score. The Change Management process for those three applications has a score of 100% or *Fully Compliant* (“Tier 2” Strength and “Very High” Coverage).

The Change Management Process for Network #1 is scored at 25% or *Somewhat Compliant* (“Tier 1” strength and “Very High” coverage).

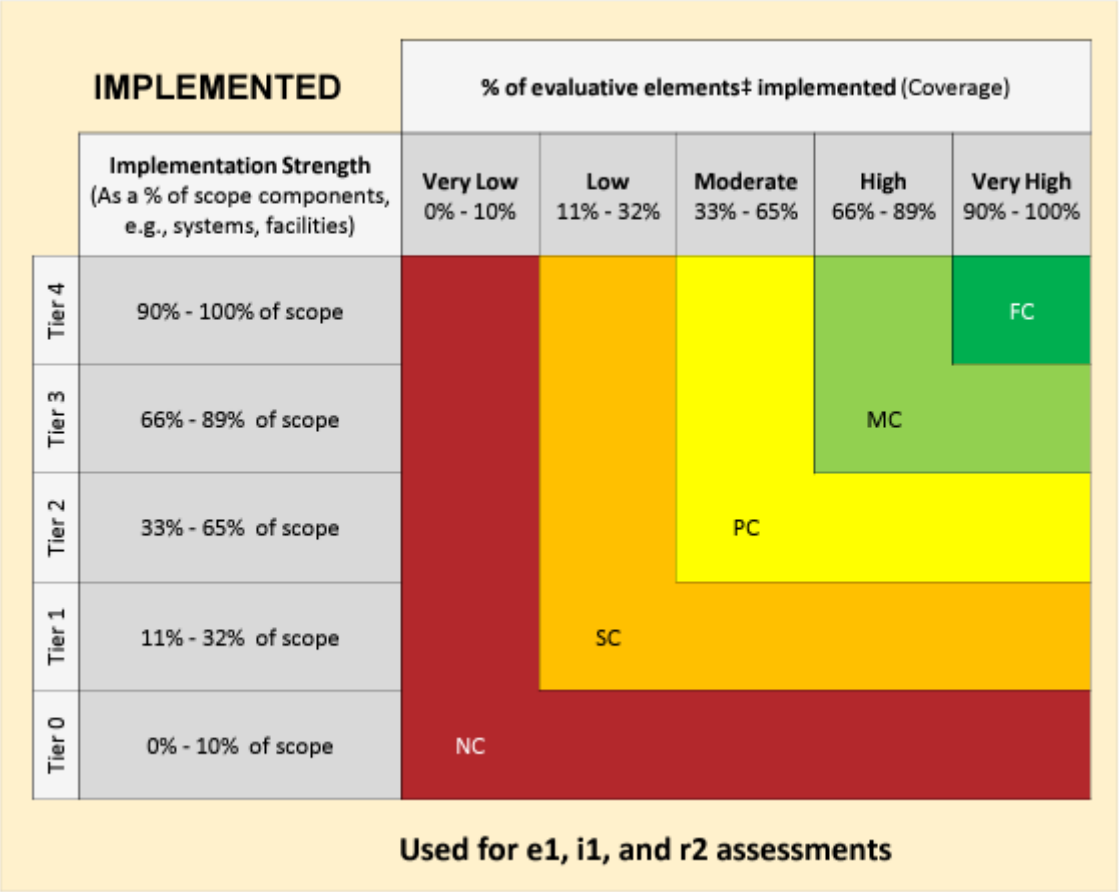
Procedure Score: In this example, there are rubric scores of *Fully Compliant* and *Somewhat Compliant*. Since 3 of the 4 scope components follow the change management process scored at *Fully Compliant*, a weight of 75% can be used for that score. The Network change management process of *Somewhat Compliant* will be weighted at 25%. After combining these scores, we reach a score of (.75)100 + (.25)25 = 81.25%, or ***Mostly Compliant***.

Implemented:

During testing of the Change Management process, the External Assessor noted that:

For *Change Management Process #1 (Application #1, Operating System #1, and Database #1)*: Ten (10) Changes were sampled, it was determined that 5 of 10 were properly documented, 3 of 10 were properly tested, and 3 of 10 were approved.

For *Change Management Process #2 (Network #1)*: Ten (10) Changes were sampled, it was determined that 2 of 10 were properly documented, 1 of 10 were properly tested, and 1 of 10 were approved.



While the same scoring approach for the *Implemented* level can be taken as in example #2, this example will highlight an alternate acceptable scoring approach (which may be easier for those requirements) by combining scope components and evaluative elements into one table.

In this example, the testing results for each evaluative element will be entered into a table with the scope components listed on the *Implementation Strength* axis and the evaluative elements on the *Implementation Coverage* axis.

Example 3 Assessment Results for Coverage – Implemented

Scope Components	Changes are Documented	Changes are Tested	Changes are Approved
Application #1	50%	30%	30%
Operating System #1	50%	30%	30%
Database #1	50%	30%	30%
Network #1	20%	10%	10%

Implemented Score: The above table combines the strength and coverage to determine the final *Implemented* score according to the rubric. If the above scores are averaged (370%/12), a score of 31% is achieved, which corresponds to an overall rating of ***Somewhat Compliant***.

A-7: Rubric Scoring – Measured and Managed

For background information on the *Measured* and *Managed* maturity levels, see Chapter 9 Control Maturity Levels and the HITRUST CSF Control Maturity Scoring Rubric.

We have supporting documentation for a measure that includes all measure criteria except (iv) identify who is responsible for gathering the data. What is the *Measured* strength?
"Tier 0 – No measurement used". ALL of the *Measured* criteria must be met to reach tiers 1 – 4.

The *Managed* coverage is calculated as a percentage of issues identified. How do I calculate *Managed* coverage if no issues have been identified in the past year?
When zero issues have been identified, the *Managed* coverage is "Very High".

We used a third-party report (e.g., SOC report, PCI RoC) to support a 50% or higher score for the *Managed* maturity level. Why has this raised a QA concern?
To achieve a 50% score for the *Managed* maturity level, the *Managed* strength must be Tier 2 or higher. This requires a risk treatment process that meets at least one of the following risk treatment criteria:

(i) initial involvement of an appropriate level of management or a defined escalation or review process to be observed if/when the appropriate level of management is not initially involved,

(ii) a defined mechanism to track issues, risks, and risk treatment decisions, or

(iii) cost, level of risk, and mission impact are considered in risk treatment decisions.

A third-party report does not typically meet any of the above risk treatment criteria.

Can the *Managed* score ever be higher than the *Measured* score?
Yes. While the *Managed* score cannot exceed the *Measured* coverage, the *Managed* score may exceed the *Measured* score. The following example outlines a scenario where the *Measured* score is 25% and *Managed* score is 75%.

Measured: For a requirement statement with four evaluative elements, the External Assessor determines that the organization has an operational measure ("Tier 1" Strength) that addresses all four evaluative elements ("Very High" Coverage). This indicates a *Measured* score of 25%.

Managed: The operational measure identified one issue in the past year that was remediated ("Very High" Coverage) using the organization's documented risk treatment process. The risk treatment process met two of the three formal risk treatment process criteria ("Tier 3" Strength). This indicates a *Managed* score of 75%.

In this scenario, it is acceptable that the *Managed* score of 75% exceeds the *Measured* score of 25% because the *Managed* score does not exceed the *Measured* coverage of 100% or Very High. In the event the *Measured* "coverage" was 50% ("Moderate") and the *Managed* score was calculated at 75%, then the

Managed score will need to be lowered to the *Measured* “coverage” score of 50%, or *Partially Compliant*.

Example #1

Scenario

BUID: 1814.08d1Organizational.12 | CVID: 0732.0

Fire extinguishers and detectors are installed according to applicable laws and regulations.

Policy Illustrative Procedures:

Examine policies and/or standards related to the protection against environmental threats to determine if

1. *appropriate fire extinguishers are located throughout the facility,*
2. *and are no more than fifty (50) feet away from critical electrical components;*

and fire detectors (e.g., smoke or heat activated) are installed on and in the

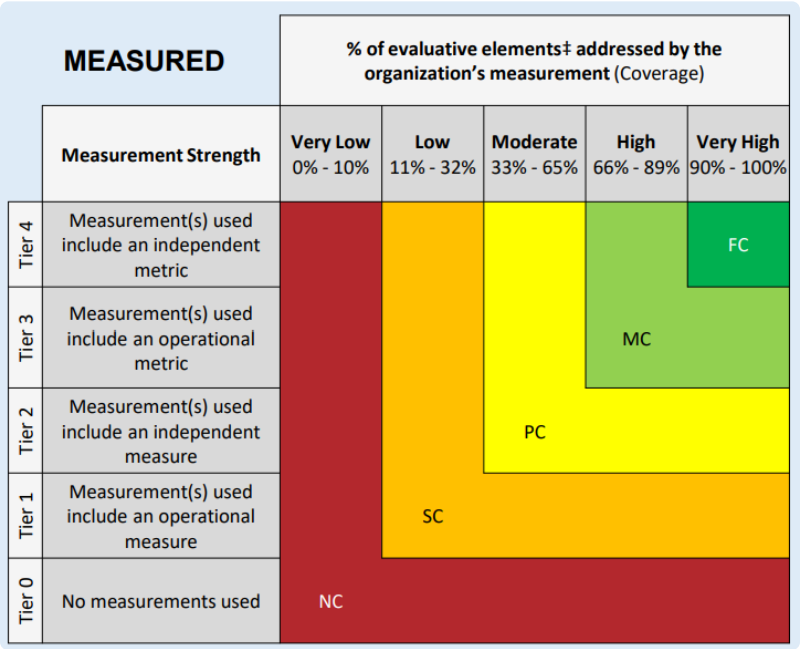
3. *ceilings*
4. *and floors.*

The scope for this assessment includes a corporate office (“Office”), and two data centers (“DC1” and “DC2”).

Evaluation

Measured:

Internal Audit or “IA” (which is in no way tied to the operation of this requirement) tests that fire extinguishers at the DCs exist and are maintained on an annual basis. IA’s test documentation contains details of who gathered the data, what was tested, the frequency of testing, how the test was performed, and the result. IA also has a written procedure on communicating audit findings to executive management, which is always observed. However, IA doesn’t include any comparison of testing results across time periods and doesn’t identify any thresholds or performance targets.



Measured Strength: To determine the strength, first identify whether the measure or metric criteria are met (see Chapter 9.4 Measured Maturity Level).

To be classified as a measure for HITRUST assessment purposes, supporting documentation must:

(i) address the control's operation/performance,
(ii) specify an appropriate frequency,
(iii) define what is measured,
(iv) identify who is responsible for gathering the data,
(v) describe how the data is recorded,
(vi) describe how the measurement is performed/calculated, and
(vii) specify how often the measure is reviewed and by whom.

In this example, all of the above criteria for a measure are met by IA's test documentation. Next, look at the metric criteria to determine whether the tests performed by IA can be considered a metric (see Chapter 9.4 Measured Maturity Level).

To be classified as a metric for HITRUST assessment purposes, the measurement must meet ALL requirements for a measure (listed above) AND:

(i) be tracked over time, and
(ii) have explicitly stated (not implied), established thresholds (i.e., upper and/or lower bounds on a value) or targets (i.e., targeted goals, what the organization is trying to achieve).

In this example, IA doesn't include any comparison of testing results across time periods and doesn't identify any thresholds or performance targets. Therefore, the testing performed by IA is classified as a measure, not a metric. This means that the *Measured* strength is either "Tier 1 – Operational Measure" or "Tier 2 – Independent Measure" (see Chapter 9.4 Measured Maturity Level). Since the IA team is in no way tied to the operation of this requirement, their testing is independent. Thus, the *Measured* strength is "Tier 2 – Independent Measure".

Measured Coverage: To determine *Measured* coverage, identify the percentage of the evaluative elements measured.

Example 1 Assessment Results for Coverage – Measured

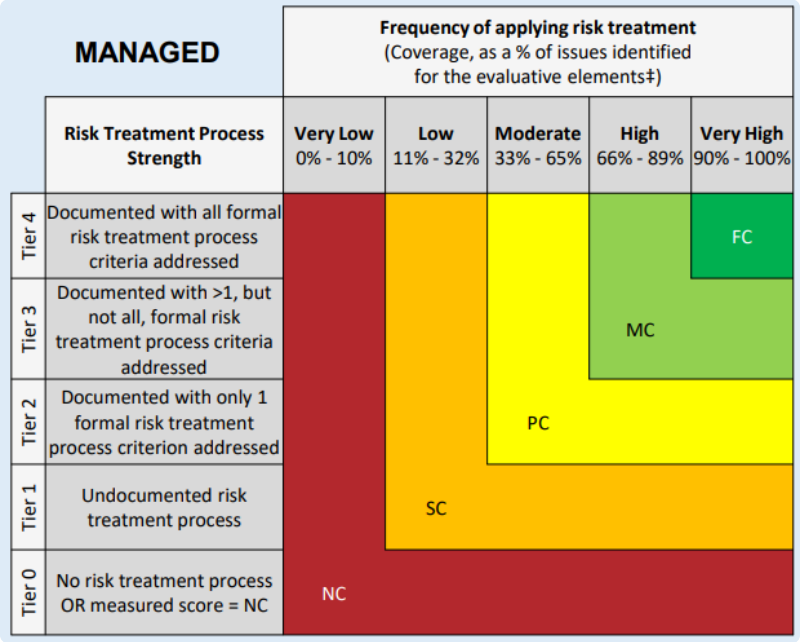
Element of the Requirement	Office	DC1	DC2
Fire extinguishers throughout	Not Measured	Measured	Measured
Fire extinguishers < 50'	Not Measured	Measured	Measured
Fire detectors in ceilings	Not Measured	Not Measured	Not Measured
Fire detectors in floors	Not Measured	Not Measured	Not Measured
Coverage	0%	50%	50%

A simple average of the scores indicates overall coverage of the elements is 33.3%, which is “Moderate” coverage.

Measured Score: Use the strength and coverage to determine the final *Measured* score according to the rubric. “Tier 2” strength and “Moderate” coverage indicate a score of ***Partially Compliant*** or 50%.

Managed:

The Assessed Entity has a “Risk Treatment Procedure” that describes the process for tracking issues, risks, and risk treatment decisions across the organization. In the past year, no issues were identified in IA’s testing of whether fire extinguishers at the DCs exist and are maintained.



Managed Strength: Managed strength is determined by how many of the formal risk treatment criteria listed below are addressed (see Chapter 9.5 Managed Maturity Level).

To be classified as a risk treatment process for HITRUST assessment purposes, the process must include:

(i) initial involvement of an appropriate level of management or a defined escalation or review process to be observed if/when the appropriate level of management is not initially involved,
(ii) a defined mechanism to track issues, risks, and risk treatment decisions, and
(iii) cost, level of risk, and mission impact are considered in risk treatment decisions.

In this example, only criterion (ii) is addressed. Therefore, the strength is “Tier 2 – Documented with 1 formal risk treatment process criterion addressed”.

Managed Coverage: The coverage is calculated as the frequency of applying risk treatment as a percentage of issues identified (see Chapter 9.5 Managed Maturity Level). In this example, no issues have been identified in the past year, so coverage can be considered Very High.

Managed Score: Use the strength and coverage to determine the final *Managed* score according to the rubric. “Tier 2” strength and “Very High” coverage indicate a score of ***Partially Compliant*** or 50%.

A-8: Testing & Evidence FAQs & Examples

During QA, HITRUST may identify testing and evidence that does not sufficiently support the scoring within the validated assessment. The following questions and scenarios are related to testing and evidence along with clarification on HITRUST's expectations for each situation.

If the organization's policy and/or procedure did not specifically cover all evaluative elements, but in general the documentation meets the 'spirit' or 'intent' of the requirement statement, does that support a fully compliant score?

No. Per the HITRUST rubric, each requirement statement's *Policy* and/or *Procedure* maturity level is scored using a maturity model that evaluates strength and evaluative element coverage. If the company's policy and/or procedure does not specifically address all evaluative elements even at Tier 2 strength, a score of 100% is not supported.

For example, the company's documented policy formally addressed three of five evaluative elements, while the remaining two evaluative elements are inferred. The maturity score will be calculated as follows:

- Strength: Tier 2 because the policy was documented.
- Coverage: Moderate coverage because three of five (60%) evaluative elements were explicitly addressed in the policy. The remaining two evaluative elements are not specifically addressed by the policy and/or procedure since they were inferred.

Based upon the strength and coverage, a score of ***Partially Complaint*** (50%) would be supported.

We tested a sample as noted in our Test Plan and linked the testing lead sheet to the requirement. Why am I required to provide the supporting evidence for each sample item contained in the lead sheet?

The HITRUST QA Analyst must be able to view all supporting documents in order to re-perform scoring. As a result, a lead sheet alone and/or example of one is insufficient to support the work performed by the External Assessor.

We are being asked for corroborating evidence to support a population of zero. How do we prove a negative?

HITRUST expects a *reasonable* level of relevant due diligence performed during fieldwork corroborating any inquiry. The External Assessor should evaluate the nature of the requirement statement, and inspect the relevant system(s) of record that might be available to view a history of the requirement statement's operation. The following examples include potential evidence that can support a zero population:

HITRUST CSF Requirement Statement	Assessed Entity Comments	Potential Validation of Zero Population
0120.05a1Organizational.4 "Capital planning and investment requests include the resources needed to implement the security	The Assessed Entity reports there have been no security	For validation, the External Assessor may inspect procurement/purchase records, change control records, and/or

program, employ a business case (or Exhibit 300 and/or 53 for federal government); and the organization ensures the resources are available for expenditure as planned."	program expenditures in the past year.	budget records.
1117.01j1Organizational.23 "Remote access by vendors and business partners (e.g., for remote maintenance) is disabled/deactivated when not in use."	The Assessed Entity reports there have been no instances where vendor partners and business partners remotely accessed the environment.	For validation, the External Assessor may inspect change control records, break/fix incident tickets, and/or third-party contracts to determine if remote services have been provided.
1539.11c2Organizational.7 "Incident response is formally managed and include specific elements."	The Assessed Entity reports there have been no incidents since the control was implemented 12 months ago.	For validation, the External Assessor may inspect incident registers covering a 12-month period (even if empty), examine legal records pertaining to incident communication to external parties, or examine customer inquiry records pertaining to incident disclosures.

We used a vendor whitepaper to support a score of 100%. Why has this raised a QA concern?
While a whitepaper, admin guide, user guide, or sales sheet describes controls that *can* be implemented for a particular solution, it is not a policy or procedure owned by the Assessed Entity nor is it evidence of a control's implementation. Therefore, this type of evidence is insufficient to support scoring independently. For additional information on acceptable evidence for a HITRUST assessment see Chapter 11.3 Working Papers & Evidence.

We used a third-party report (e.g., SOC report, PCI Compliance report, or ISO 27001 report) to support a 100% score for the *Implemented* maturity level. Why has this raised a QA concern?
This may be due to one or more of the following reasons:

- The External Assessor used a SOC 1 report, which is not acceptable per requirement 12.3.5 in Chapter 12.3. SOC 1 reports contain a restricted use paragraph in the Auditor's Opinion that limits distribution of the report to the service organization, the service organization's customers, and their auditors. All other parties, including HITRUST, are not authorized to use the report.

- The External Assessor used a SOC 2 Type I report, which is not acceptable per requirement 12.3.9 in Chapter 12.3. Only those audits and assessments featuring tests of control design / operation / implementation / effectiveness utilizing audit procedures such as inspection of evidentiary matter and sampling (utilizing statistically meaningful sample sizes as applicable) are suitable reliance. For example, procedures executed by a service organization's auditor during a SOC 2 Type I examination should not be relied upon given a SOC 2 Type I examination's lack of substantive testing.

- The External Assessor used a SOC 3 report, which is not acceptable per requirement 12.3.9 in Chapter 12.3. SOC 3 reports do not include detail of tests of control design / operation / implementation / effectiveness utilizing audit procedures such as inspection of evidentiary matter and sampling.

- The External Assessor used a PCI Attestation of Compliance (AoC) Criteria, which is not acceptable per requirement 12.3.9 in Chapter 12.3. Only those audits and assessments featuring tests of control design / operation / implementation / effectiveness utilizing audit procedures such as inspection of evidentiary matter and sampling (utilizing statistically meaningful sample sizes as applicable) are suitable for reliance.
  The External Assessor may utilize a PCI RoC which provides a Report on Compliance (RoC) and is issued by a Qualified Security Assessor (QSA). The report details an organization's security posture, environment, systems, and protection of cardholder data.

- The External Assessor only provided the one-page ISO 27001 certification letter, which is not acceptable per requirement 12.3.9 in Chapter 12.3. Only those audits and assessments featuring tests of control design / operation / implementation / effectiveness utilizing audit procedures such as inspection of evidentiary matter and sampling (utilizing statistically meaningful sample sizes as applicable) are suitable for reliance. HITRUST expects the External Assessor to provide the full ISO 27001 certification report with a mapping to the corresponding HITRUST requirement statements.

- The External Assessor did not provide a mapping of the SOC 2 Type II, PCI RoC, or ISO certification report's testing to the evaluative elements found in the requirement statement. HITRUST must be able to identify at a granular level how the testing performed in the SOC 2 Type II addresses each evaluative element in the HITRUST requirement statement.

- The External Assessor provided a mapping of the SOC 2 Type II, PCI RoC, or ISO certification report, but the report did not test all evaluative elements found in the requirement statement. The SOC2 Type II report must provide sufficient detail to demonstrate that each evaluative element in the HITRUST requirement statement was tested.

- The External Assessor used a SOC 2 Type II, PCI RoC, or ISO certification report, but the scope did not match the HITRUST assessment scope.

We included the necessary sample selection and evidence of testing the requirement statement. However, the HITRUST QA Analyst opened a task stating the evidence did not appear to support a score of 100% for the *Implemented* maturity level.

HITRUST requirements are written at a granular level to address the various risks and threats for each organization. External Assessors should ensure their testing is performed at that granular level and specifically addresses the wording in the requirement statement for each evaluative element. Additionally, the testing should be performed in alignment with the testing listed within the illustrative procedures for the *Implemented* maturity level. The following scenarios include situations where an External Assessor may receive a question from a HITRUST QA Analyst:

Scenario

BUID: 0104.02a1Organizational.12 | CVID: 0297.0

Policies and/or standards related to user roles and responsibilities include:

1. implementing and acting in accordance with the organization's information security policies;

2. protecting assets from unauthorized access, disclosure, modification, destruction, or interference;

3. executing particular security processes or activities;

4. ensuring responsibility is assigned to the individual for actions taken;

5. reporting security events or potential events or other security risks to the organization; and

6. security roles and responsibilities are defined and clearly communicated to users and job candidates during the pre-employment process.

Illustrative Procedure for the Implemented Maturity Level:

For example, examine the relevant security policies and confirm that roles and responsibilities have been formally defined in the policy.

1. Further, select a sample of new hires and confirm that the policy was clearly communicated and acknowledged by the employee during the pre-employment process.

Assessor Testing

In this scenario, the External Assessor selected a sample of new hires. For each new hire, the External Assessor uploaded a signed acknowledgment and reviewed that the evaluative elements were addressed in the acknowledgments. Each acknowledgment was signed by the new employee on their 1st day of employment.

HITRUST Evaluation

During the review of the testing performed by the External Assessor, the HITRUST QA Analyst was able to confirm most evaluative elements were addressed in the policy and signed acknowledgments. However, the acknowledgments were signed by the new employee on their 1st day of employment, but not during the pre-employment process as required by evaluative element #6. Therefore, testing was not in alignment with the illustrative procedures for *Implemented*. When scoring the requirement statement, the External Assessor must reduce the corresponding score for the *Implemented* maturity level since only 5 of 6 evaluative elements were tested.

Scenario

BUID: 0709.10m1Organizational.1 | CVID: 1369.0

Once a potential technical vulnerability has been identified, the organization identifies the

1. associated risks and

2. the actions to be taken.

Further, the organization

3. performs the necessary actions to correct identified technical vulnerabilities in a timely manner.

BUID: 0787.10m2Organizational.14 | CVID: 1369.0

The organization

1. requires patches installed in the production environment to also be installed in the organization's disaster recovery environment in a timely manner, as defined by the organization.

Assessor Testing

In this scenario, the External Assessor scored the *Implemented* maturity level for "0709" using the same

documents linked to “0787”. The External Assessor’s rationale is that the installation of patches demonstrates the risks of vulnerabilities were addressed and actions were taken to address the vulnerabilities.

HITRUST Evaluation

The HITRUST CSF is a framework for managing information security and privacy risks, which is comprised of granular requirements derived from Authoritative Sources. While 0709.10m1Organizational.1 and 0787.10m2Organizational.14 are similar they are not identical.

- 0709.10m1Organizational.1: The illustrative procedure for the Implemented maturity level calls for selecting a sample of system vulnerabilities identified by the organization and examining evidence to confirm that a risk assessment was performed to identify associated risks. Further, confirming that action plans were identified and carried out.

- 0787.10m2Organizational.14: The illustrative procedure for the Implemented maturity level calls for selecting a sample of patches installed in the production environment and confirming they are also installed in the organization’s disaster recovery environment, and that the installation was performed in a timely manner, as defined by the organization.

Please note the granular differences when comparing the two requirements. Applying patches is an example of carrying out an action plan, but it is not inclusive of all system vulnerability action plans, which is tested in requirement in “0709”. For instance, an action plan to address system vulnerabilities might be to simply retire the system rather than a patch as in the case of a system that is no longer supported by the manufacturer and the risk of continuing to use unsupported systems exceeds the organization’s risk tolerance. Requirement “0787” is intended to address the risk of the Disaster Recovery environment not operating in the same manner as the production environment with the same level of security.

As a result, the testing performed for requirement “0787” does not support scoring for requirement “0709”.

A-9: Off-site Validation Procedures

In cases where on-site testing will not be performed, the External Assessor should engage with their Assessed Entity to:

- Develop and agree upon possible alternate assessment procedures for instances where an on-site observation is normally performed.
- Ensure that the Assessed Entity understands it is vital that the External Assessor has sufficient, appropriate evidence to support validation of management's implementation of the HITRUST CSF. Where an External Assessor is unable to obtain such evidence, they will be unable to agree with "Fully Compliant" scoring.

In situations where Assessors leverage alternative validation procedures other than on-site testing, assessment documentation must clearly reflect the nature, timing, and extent of the alternative procedures employed.

When performing a HITRUST assessment, the External Assessor must ensure that all validation procedures it performs provide the necessary level of assurance over the Assessed Entity's implementation of the HITRUST CSF. Even when alternate test procedures are employed and a validated assessment is performed remotely, External Assessors must take all necessary steps to ensure that the reliability and integrity of the assessment process are maintained.

HITRUST has identified the following requirement statements for which the *Implemented* maturity level is typically validated via on-site observation. For each requirement statement, HITRUST has volunteered possible alternate procedures to validate implementation in lieu of on-site observations. The underlying theme throughout these suggested alternate test procedures is to consider less traditional supporting artifacts—such as maintenance records, installation documentation, facility diagrams, etc.—which collectively evidence both the installation and ongoing operation of the associated requirement statements.

HITRUST CSF Requirement Statement	Possible Alternate Implementation Validation Procedures
1815.08d2Organizational.123: Fire prevention and suppression mechanisms, including workforce training, are provided.	Inspect documentation reflecting the existence of and placement location of fire suppression equipment, potentially including: • Facility placement diagrams • Fire suppression system maintenance records • Service tickets from initial fire suppression system installations • Post-installation inspection reports • Fire Chief inspection reports
0503.09m1Organizational.6: Wireless access points are placed in secure locations.	Inspect documentation reflecting the secure placement/location of wireless access points, potentially including: • Facility wiring diagrams • Facility diagrams

	• Service tickets from initial installation and/or ongoing maintenance of WAPs which may describe placement location • Screenshots of camera feeds • Badge/card reader access history • Badge/card reader access reports
1114.01h1Organizational.123: Covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors.	Inspect documentation generated by management using procedures performed by management to monitor for consistent observance and enforcement of clean desk, clean screen, and clean printer requirements, potentially including: • Populated periodic clean-desk walkthrough checklists • Reports from sanctioning personnel for failing to observe these requirements
1192.01l1Organizational.1: Access to network equipment is physically protected.	Inspect documentation evidencing the location of on-premises networking equipment and the physical protections in place for these locations, potentially including: • Facility wiring diagrams • Facility diagrams • Camera footage • Service tickets from initial installation and/or ongoing maintenance of networking equipment installations which may describe placement location • Service tickets from initial physical security equipment installations which may describe placement location • Facility floor plans/diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) • Badge/card reader access history • Badge/card reader access reports
1801.08b1Organizational.124: Visitor and third-party support access is recorded and supervised unless previously approved.	Inspect documentation evidencing the protections observed for site visitations, potentially including: • Camera footage • Logs from visitor check-in/check-out systems • Service tickets from initial installation and ongoing maintenance of visitor badge printers • Scans of hard-copy visitor check-in/check-out logs • Reports from sanctioning personnel for failing to properly record and supervise visitors
1802.08b1Organizational.3: Areas where sensitive information (e.g., covered	Inspect documentation evidencing the physical protections in place for areas where sensitive information is stored or processed, potentially including: • Camera footage

information, payment card data) is stored or processed are controlled and restricted to authorized individuals only.	• Service tickets from initial installation and/or ongoing maintenance of physical security systems • Facility floor plans/diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) • Badge/card reader access history • Badge/card reader access reports • Logs of alerts generated by the physical security system such as forced entry alerts, door held open alerts, etc. • Logs generated by rounds performed by guards or floor marshals
1845.08b1Organizational.7: For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards that the organization determines necessary for areas officially designated as publicly accessible.	Inspect documentation evidencing the physical protections in place for areas where information systems reside, potentially including: • Camera footage • Service tickets from initial installation and/or ongoing maintenance of physical security systems • Facility floor plans/diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement) • Badge/card reader access history • Badge/card reader access reports • Logs of alerts generated by the physical security system such as forced entry alerts, door held open alerts, etc. • Logs generated by rounds performed by guards or floor marshals
1814.08d1Organizational.12: Fire extinguishers and detectors are installed according to applicable laws and regulations.	Inspect documentation reflecting the existence of and placement location of fire detection and suppression equipment, potentially including: • Facility placement diagrams • Fire detection and suppression system maintenance records • Service tickets from initial fire detection and suppression system installations • Post-installation inspection reports • Fire Chief inspection reports
18127.08l1Organizational.3: Surplus equipment is stored securely while not in use and disposed of or sanitized when no longer required.	Inspect documentation evidencing the physical protections in place for areas where surplus equipment is stored while not in use, potentially including: • Camera footage • Service tickets from initial installation and/or ongoing maintenance of physical security systems • Facility floor plans/diagrams showing physical access points with description of associated access control mechanisms (e.g., manual locks, system locks via key card, and or biometric reader placement)

	• Badge/card reader access history • Badge/card reader access reports • Logs of alerts generated by the physical security system such as forced entry alerts, door held open alerts, etc. • Logs generated by rounds performed by guards or floor marshals • Asset inventories reflecting the physical location of surplus equipment
1817.08d3Organizational.12: Water detection mechanisms are in place with master shutoff or isolation valves accessible, working and known.	Inspect documentation reflecting the existence and placement location of water detection and control mechanisms potentially including: • Service tickets from initial installation and/or ongoing maintenance of water detection and control mechanisms • Post-installation inspection reports

A-10: Policy & Procedure FAQs & Examples

Our company has obligations to adhere to many different frameworks and/or regulations. We already have established policies. We now have a business need to perform a HITRUST assessment with the goal of achieving a HITRUST certification. Can we use our existing policies for the validated assessment, or do we need to create a separate set of HITRUST policies?

An Assessed Entity may leverage existing policy sets. It is not mandatory to create a new and/or separate set of policies. The HITRUST CSF leverages good security hygiene and leading practices that substantially cover authoritative sources, such as: NIST SP 800-171, HIPAA Security Rule, GLBA Safeguards Rule, U.S. Department of Labor EBSA Cybersecurity Program Best Practices, and Health Industry Cybersecurity Practices (HICP). Many organizations find success in establishing a foundation based upon the HITRUST CSF and adding, as needed, organization relevant policies. Conversely, the existing policy sets can be leveraged and adding, as needed, HITRUST CSF relevant policies not specifically addressed in the organization's existing policies.

We would like to use the HITRUST requirement statements verbatim as our policies. Is that allowable?

This is allowable. However, for "Fully Compliant" *Policy* scoring in HITRUST CSF version 9.x assessments, the evaluative elements noted in the illustrative procedures for *Policy* must be incorporated. For "Fully Compliant" *Policy* scoring in HITRUST CSF version 11.x assessments, policies related to each evaluative element within the requirement statements must be incorporated.

There are many HITRUST requirement statements in which a procedure would seem obvious to our workforce. Can we simply use policy language for the procedure language?

HITRUST requirement statements are scored according to maturity levels. A procedure that might be understood by the staff from reading a policy, but a procedure addressing the policy that is not formally documented will lead to an undocumented *Procedure* score assuming the procedure was consistently observed. (See Chapter 9.2 Procedure Maturity Level)

We used a third-party report to support *Implemented* scores of 100%. However, the third-party report didn't address policies and procedures. How can we score these?

Controls tested in third-party reports may address the operation of a control which will allow it to support scores at the *Implemented* level in a HITRUST assessment. However, these controls often do not sufficiently address whether the Service Provider maintained policies or procedures for all evaluative elements within a HITRUST requirement statement. In these instances, the Assessed Entity may maintain its own policies and procedures describing the expectations of the Service Provider to support scoring (similar to its own policies and procedures, these must also address all evaluative elements within each requirement statement).

The evaluative elements in a requirement statement within an e1 or i1 assessment refer to the organization having a documented policy or procedure. Does this mean that we would be testing the existence of the policy or procedure at the *Implemented* maturity level?

Yes. Although an i1 or e1 assessment does not include the Policy or Procedure maturity levels, HITRUST has identified the existence of certain policies and procedures as key baseline controls in those

assessments. As a result, the External Assessor should follow the illustrative procedure for the *Implemented* maturity level and ensure that all evaluative elements have been appropriately tested including the existence of any expected policies or procedures.

In the HITRUST scoring rubric, it states that a documented procedure must address the "operational aspects of how to perform the requirement statement." What is meant by this statement?

Each procedure should be documented at a sufficient level of detail to enable a knowledgeable and qualified individual to perform the requirement.

Examples of the operational aspects of "how" to perform the evaluative elements contained in a requirement statement may include documents that discuss:

- Tools / technology / system of record usage
- People or teams involved to carry out procedure
- Workflow description and/or description
- Technical / system / application configurations
- Check list items aligning to the requirement evaluative elements
- Triggering event(s) or condition(s) that would cause a need for the requirement to be carried out/ operated
- Runbooks/step by step instructions

Procedures are not required to include all the items listed above, nor is the listing above exhaustive. The following examples include procedures and the corresponding HITRUST evaluation:

Scenario (Acceptable Procedure)

BUID: 00501.09m1Organizational.10 | CVID: 0926.1

Prior to authorizing the implementation of wireless access points, the organization changes

1. *vendor default encryption keys,*
2. *default SNMP community strings on wireless devices,*
3. *default passwords/passphrases on access points, and*
4. *other security-related wireless vendor defaults, if applicable.*

Assessed Entity Procedure:

"The network team is responsible for all aspects of the wireless infrastructure. Cisco Meraki and Netgear are used to deploy and manage WAPs.

Per company policy, the network team must ensure:

** vendor default encryption keys are changed;*

** default SNMP community strings on wireless devices are changed;*

** default passwords/passphrases on access points are changed;*

The network team records the wireless solution's security related features and any default settings are changed before being deployed into the production environment. WAP configuration(s) are checked quarterly to ensure consistent alignment to company configuration policy. Configuration and compliance check results are reviewed by the network manager and archived on the network department's intranet site.

Additionally, the network manager is notified by the HR team when staff changes occur and ensures that wireless infrastructure encryption keys are changed."

HITRUST Evaluation

This appears to be a fully compliant procedure because it articulates an operational discussion by describing:

- Who is carrying out the requirement – The network team uses Cisco and Netgear tools and technology
- When – at the deployment of WAPs
- What – Changing:

  i. vendor default encryption keys – using tools and technology

  iii. default SNMP community strings on wireless devices – using tools and technology

  iv. default passwords/passphrases on access points – using tools and technology

  v. other security-related wireless vendor defaults, if applicable (this is achieved by stating the workflow to be followed “The network team records the wireless solution’s security related features and any default settings are changed before being deployed into the production environment”)

Scenario (Unacceptable Procedure)

BUID: 0501.09m1Organizational.10 | CVID: 0926.1

Prior to authorizing the implementation of wireless access points, the organization changes

1. *vendor default encryption keys,*
2. *default SNMP community strings on wireless devices,*
3. *default passwords/passphrases on access points, and*
4. *other security-related wireless vendor defaults, if applicable.*

Assessed Entity Procedure:

“When the IT department is configuring a WAP, use the ABC Corporation random password generation tool to generate a new password and change the default administrator password on the WAP to one that was newly generated. The network team should record the wireless solution’s security related features.”

HITRUST Evaluation

This is not a compliant procedure because it addresses only one evaluative element (changing of default password) and assumes this is completed prior to authorizing the implementation of the access point (rather than specifically stating it must be done prior to authorization of the wireless access point).

A-11: Automated Control Testing Example

As noted in Chapter 11.4 Population & Sampling, Automated controls are those controls performed by systems—not people—based on configurations, rulesets, or programming. An example of an automated control is forced password expiration after the number of days specified in the associated configuration.

For automated controls, testing must include evidence of both the configuration of the tool/system and a sample of one showing the tool/system is operating as expected. The following example includes a scenario and potential automated control testing approach.

Scenario
BUID: 1116.01j2Organizational.6 | CVID: 0121.0
The authentication of remote users is implemented using
1. a password or passphrase and
2. at least one of the following methods: a cryptographic based technique; biometric techniques; hardware tokens; software tokens; a challenge/response protocol; or certificate agents.
The Assessed Entity is using a VPN software for users to remotely access the in-scope platform. The VPN software requires the user to login using their password and a software authenticator tool on their phone prior to granting access.

Potential Automated Control Testing Approach
In this scenario, a potential automated control testing approach must address:

- The Configuration of the VPN software, and
- Walkthrough of one user remotely accessing the in-scope platform.

The External Assessor should review that the VPN software was configured to:

- Grant access to the corresponding IT environment (the environment where the in-scope platform will be accessed)
- Require a password for users to login
- Require the user to successfully authenticate via the software authenticator.

The External Assessor will then need to perform sufficient observation and/or inspection of one user accessing the in-scope platform using the VPN software, validating the VPN required a password and software authentication before granting access.

A-12: Inheritance FAQs & Examples

Why use inheritance instead of other methods of control reliance on previously assessed requirement statements?

The HITRUST Shared Responsibility and Inheritance Program offers Assessed Entities a unique and innovative alternative method for placing reliance on previously assessed HITRUST-compliant control environments by utilizing inheritance.

- Inheritance eliminates the need for duplicative control assessment testing that can save Assessed Entities (and their External Assessors) considerable time, effort, and cost when planning, performing, and validating a HITRUST assessment.

- For relying parties, traditional manual reliance methods are problematic and time-consuming when a third-party service provider's offline compliance reports lack sufficient transparency needed for scoring HITRUST assessments or force external control carve-outs when reports are not shared. This problem is solved by utilizing inheritance in conjunction with the HITRUST Shared Responsibilities Matrix® (SRM) when relying on third-party service providers that are HITRUST certified and getting clarity over how control responsibility is shared.

- For Assessed Entities (and their External Assessors), users gain the ability to inherit previously-assessed requirement statement testing (and pertinent commentary) from any other qualified "inheritable" HITRUST assessment. Further, cross-version inheritance is supported which allows requirement statements to be inherited into/from HITRUST assessments generated from any version of the HITRUST CSF. This is enabled by MyCSF which can systematically identify and link to cross-version control matches that span any supported version of the HITRUST CSF.

Who is allowed to use inheritance, and does it depend on whether I use the external or internal types of inheritance?

HITRUST customers with an eligible MyCSF subscription can use and publish for inheritance. The Assessed Entity may contact their HITRUST CSM or HITRUST Support (support@hitrustalliance.net) to determine eligibility.

Which HITRUST assessments support use of inheritance?

The following assessment types (and assessment status) can qualify as "inheritable" HITRUST assessments:

- For external inheritance, Assessed Entities can inherit from "published" Risk-based, 2-year (r2), Implemented, 1-year (i1) and Essentials, 1-year (e1) Validated Certified and Validated-Only (Non-Certified) Assessments that are complete and with a report date posted.

- For internal inheritance, Assessed Entities can inherit from their own Risk-based, 2-year (r2), Implemented, 1-year (i1) and Essentials, 1-year (e1) Validated Certified, and Validated-Only (Non-Certified) that are complete (and with a report date posted for validated assessments).

Can I inherit from a targeted, current state (tC) assessment?
No.

Is it possible to inherit from a Risk-based, 2-year (r2) type of HITRUST assessment into an Implemented, 1-year (i1) or Essentials, 1-year (e1) HITRUST assessment (and vice versa)?
Yes. As specified in Chapter 12 Reliance & Third-Party Coverage), requirement statements can be inherited between the various assessment types (Risk-based, 2-year (r2), Implemented, 1-year (i1) and Essentials, 1-year (e1)). However, when inheriting from an "inheritable" i1 or e1 into an "inheriting" r2, only the *Implemented* maturity score can be inherited. It is therefore incumbent upon the Assessed Entity to be prepared to cover the remaining control maturity scores that cannot be inherited (e.g., *Policy*, *Procedure*, *Implemented* if partially inherited, and *Measured* or *Managed*, if applicable).

When using external inheritance, when is it appropriate to request full versus partial inheritance, and if partial, what should be the appropriate inheritance weight?
When using external inheritance, Assessed Entities should have a documented strategy and approach for placing the appropriate level of control reliance ("inheritance weights") for those requirement statements that are covered by (or shared with) third-party service providers. As stated in criteria 12.2.26 (see Chapter 12.2 Reliance on Assessment Results Using Inheritance) the Inheritance User must determine the percentage of the assessment scope and/or control responsibility which is outsourced, and whether that responsibility is fully or partially covered, by the Inheritance Provider's scoring. The percentage is based on the following:

- The use of full inheritance is appropriate when a third-party service provider performs 100% of the requirement statement on behalf of the Assessed Entity.

- The use of partial inheritance is appropriate when either of the following apply:
  - The Assessed Entity performs a portion (< 100%) of the requirement statement and the remaining is covered by one or more third-party service providers.
  - Multiple third-party service providers split performance of 100% of the requirement statement on behalf of the Assessed Entity.

Assessed Entities can use HITRUST SRMs as a baseline inheritance guideline, available for download from MyCSF or the HITRUST website, to help identify which requirement statements can be inherited based on their corresponding SRM Type designations. Assessed Entities can also use HITRUST's interactive Inheritance Calculator to test out various full and partial inheritance scenarios via: https://help.mycsf.net/inheritance-calc/.

Can I inherit requirement statements that are marked as N/A? If so, how are they scored within the HITRUST assessment?
Yes. External and internal inheritance is allowed for requirement statements marked as N/A but are scored differently depending on whether full or partial inheritance was applied:

- Full inheritance: The requirement statement is not included when calculating the domain-level aggregate score within the qualified "inheriting" HITRUST assessment.

- Partial inheritance: The final score is derived from the "applicable" portion of the requirement

statement that was scored by the Assessed Entity (or inherited from another third-party service provider), ignoring the inherited portion marked as N/A. The resulting final score is included when calculating the domain-level aggregate score within the qualified "inheriting" HITRUST assessment.

For external inheritance, it is a good practice for Assessed Entities to reference HITRUST SRMs that are tailored for Inheritance Providers (if available). The HITRUST SRMs tailored for Inheritance Providers include a standardized set of N/A commentary providing Assessed Entities with supplemental context and guidance for the appropriate application of "inheritance weights" for requirement statements marked as N/A.

For additional user guidance on the use and scoring of requirement statements marked as N/A, refer to Chapter 8.3 Not Applicable (N/A) Requirement Statements and 12.2 Reliance on Assessment Results Using Inheritance. To explore various inheritance scenarios with requirement statements marked as N/A, visit HITRUST's interactive Inheritance Calculator via: https://help.mycsf.net/inheritance-calc/.

Can I pick and choose which of the requirement statement's control maturity scores to inherit (i.e., only inherit the *Policy* and *Procedure* control maturity scores but not *Implemented*, *Measured*, and *Managed*)?

No. When using either external or internal inheritance, the entire set of maturity scores that have been assessed for a specific requirement statement are inherited into a HITRUST assessment. However, if only the Implemented maturity level is available in the Inheritance User's assessment (i.e., in an i1 or e1) the Assessed Entity may inherit only the *Implemented* maturity score from the Inheritance Provider. Additionally, if the Inheritance Provider performed an i1 or e1 then only the *Implemented* maturity score will be available for the Inheritance User to inherit.

I created and then submitted several external inheritance requests to an Inheritance Provider, but they have not yet been approved. How long is a reasonable timeframe to wait and is there a way to ask for a status update or if there is an SLA for the timely processing of external inheritance requests?

All inheritance requests within a qualified "inheriting" HITRUST assessment (see Chapter 12.2 Reliance on Assessment Results Using Inheritance) must be:

1. "created" and "submitted" by the Assessed Entity,
2. "approved" by the Inheritance Provider, and
3. "applied" by the Assessed Entity (using the built-in automated workflow process within MyCSF)

In order to utilize testing results from the Inheritance Provider, each inheritance request must be completed prior to the end of the 90-day assessment fieldwork period. It is therefore incumbent upon Assessed Entities to submit external inheritance requests as soon as possible upon initiating the HITRUST assessment process and Inheritance Providers should also make reasonable efforts to process external inheritance requests in a timely manner.

If Assessed Entities have "submitted" external inheritance requests, but have not received a response (approval or rejection with comment) from the Inheritance Provider within a reasonable timeframe (i.e., 10 or more business days), Assessed Entities have the following escalation options:

a) Assessed Entities may contact the Inheritance Provider directly using the customer support contact information included in the Inheritance Provider's HITRUST SRM (if available), or

b) The Assessed Entity may contact their HITRUST CSM or HITRUST Support (support@HITRUSTalliance.net).

I am unable to request external inheritance from a third-party service provider included in the scope of my HITRUST assessment. Why is that the case?

Assessed Entities may be unable to utilize external inheritance due to one of the following situations:

- The third-party service provider may not be HITRUST certified, or its HITRUST certification may have lapsed. If the third-party service provider is not (or no longer) HITRUST certified, utilizing external inheritance is not possible.

- The third-party service provider may not have an eligible MyCSF subscription, or the third-party service provider may have an eligible MyCSF subscription but it has not yet "published" the HITRUST assessment. In either case, Assessed Entities are encouraged to notify HITRUST if there are any third-party service providers that should be external Inheritance Providers via the MyCSF UserVoice online user feedback forum.

- The third-party service provider is already an Inheritance Provider with a "published" HITRUST assessment, however, the requested requirement statement(s) cannot be inherited. This will occur when the Inheritance Provider did not have the corresponding requirement statement(s) within their validated assessment, which may occur because:
    - The assessment factors used to generate the HITRUST assessment object for the Inheritance Provider did not bring that requirement statement into its validated assessment, and/or
    - The version of the HITRUST CSF used to generate the HITRUST assessment object for the Inheritance Provider did not contain that requirement statement.

A-13: Well-written CAP Examples

CAPs are required for all requirement statements that meet the criteria outlined within Chapter 13.9 CAPs and Gaps. A well-written CAP will include all the required information described in criteria 13.9.4 within that Chapter.

Scenario #1
CAP as a result of the *Implemented* maturity score only.
BUID: 1239.09aa1System.4
Retention policies for audit logs are specified by the organization and the audit logs are retained accordingly.
Maturity Scores: *Policy* (100%), *Procedure* (100%), *Implemented* (50%)

CAP Example #1
A well-written CAP will identify the point of contact (POC) or Owner, the scheduled completion date, the corrective action and provide the CAP status.

- *Point of Contact (POC)/Owner:* Name or Position (James Smith or Information Security Officer)
- *Scheduled Completion Date:* June 30, 2023
- *Corrective Action:* Organization XYZ will update the audit log configuration settings to ensure the system retains audit logs according to the organization's established retention policy and log management standards.
- *Status:* Not Started

Scenario #2
CAP as a result of the *Process* and *Implemented* maturity scores.
BUID: 0943.09y1Organizational.1
Data involved in electronic commerce and online transactions is checked to determine if it contains covered information.
Maturity Scores: *Policy* (100%), *Procedure* (0%), *Implemented* (0%)

CAP Example #2

- *Point of Contact (POC)/Owner:* Name or Position (James Smith or Information Security Officer)
- *Schedule Completion Date:* December 31, 2023
- *Corrective Action:* Organization XYZ will review and update the procedures to check data involved in online transactions contains covered information. Organization XYZ will document monthly performance of the data checks in a log and Information Security Officer will review logs on a quarterly basis to validate the checks are occurring as expected.
- *Status:* Not Started

Scenario #3

CAP as a result of the *Policy*, *Process*, and *Implemented* maturity scores.
BUID: 11190.01t1organizational.3
Bring your own device (BYOD) and/or company-owned devices are configured to require an automatic lockout screen, and the requirement is enforced through technical controls.
Maturity Scores: *Policy* (0%), *Procedure* (0%), *Implemented* (25%)

CAP Example #3

- *Point of Contact (POC)/Owner:* Name or Position (James Smith or Information Security Officer)
- *Schedule Completion Date:* June 30, 2023
- *Corrective Action:* Organization XYZ will define a BYOD management policy and procedure that will include the requirement to configure an automatic screen lockout that is enforced through technical controls. The technical support team will review to ensure the configuration is applied on all BYOD devices utilized within the in-scope environment.
- *Status:* Started – On Track

A-14: Scoping Approaches

An Assessed Entity determining the scope of its assessment has several possibilities on where it sets its scope boundary. The following examples include potential scoping approaches that may be undertaken by the Assessed Entity. (NOTE: This list is intended to provide examples of scoping approaches and not intended to be comprehensive guidance on all possible scoping scenarios.)

- **Enterprise:** This is where the assessment scope includes all the organization's networks, IT platforms, and supporting infrastructure. This approach is beneficial when the entire organization has adopted the HITRUST CSF Framework.

- **IT Service or Platform-focused:** In this approach, the assessment is scoped to one or more specific IT services or IT platforms and their supporting infrastructure. There are several use cases for this approach, including:
    - *Regulatory compliance:* If an Assessed Entity is seeking a HITRUST certification to demonstrate compliance with a particular standard, the organization should identify those IT services or platforms that need to be in compliance. For example, if the organization intends to use the HITRUST HIPAA compliance pack or the NIST CSF scorecard to demonstrate compliance then the organization should carefully ensure the scope meets the regulatory expectations.
    - *Building blocks:* If the Assessed Entity is in progress of adopting the HITRUST CSF, they may elect to focus on obtaining HITRUST certification for certain IT services or platforms first and then move to other IT services or platforms after those areas have adopted the HITRUST CSF.
    - *Contract-focused:* If the Assessed Entity has contractual obligations to maintain a HITRUST certification, they may elect to focus on those relevant IT platforms and supporting infrastructure that support that contract.

- **Enclave-focused:** This is similar to the "IT Service or Platform-focused" approach but may be broader since the assessment is scoped to the relevant IT platforms and supporting infrastructure used by one or more specific enclaves (e.g., business units, network segments, hosted environments). The use cases are similar to those in the "IT Service or Platform-focused" approach.

- **Shared IT services:** In this approach, the assessment is scoped to some or all aspects of the organization's shared IT services. This approach may be useful when there are multiple separate assessments able to inherit from the Assessed Entity's centralized shared IT services.

- **Follow-the-data:** All platforms and supporting infrastructure traversed by a specific type of sensitive information. If the key concern for the organization is protecting a specific set of sensitive data, the organization may elect to identify all IT Systems, Networks, Facilities, and Infrastructure where that data resides and/or transmits to perform its HITRUST assessment.

A-15: Certification Threshold Scoring Examples

Assessed Entities must achieve scores above a particular threshold to obtain a HITRUST certification.

The i1 and e1 assessments require the core i1 or e1 requirement statements in each domain to score at least an 83. Any requirement statements that are not part of the i1 or e1 core, but were included in the assessment due to an added Compliance factor are not considered in the domain score calculations. The following example shows the calculation for the average domain score for one sample domain.

Requirement Statement	Core i1 Requirement Statement	Mapped to an Included Compliance Factor	Score included in Domain Average Score Calculation	Requirement Statement Scoring
Requirement Statement 1	Yes	No	Yes	75%
Requirement Statement 2	Yes	No	Yes	75%
Requirement Statement 3	Yes	No	Yes	100%
Requirement Statement 4	Yes	Yes	Yes	100%
Requirement Statement 5	**No**	Yes	**No**	25%
			Domain Average used for CSF Certification Determination	**87.5%**

The r2 assessment requires each domain to score at least a 62 to achieve certification. All requirement statements within a domain are averaged together to determine the domain score. The following examples include potential scoring scenarios for r2 assessments (certification with no CAPs or Gaps, certification with Gaps, certification with CAPS, and no certification).

r2 Scenario #1 Certification with no CAPs or Gaps

		Requirement Statement Scoring
Domain	**Control Reference**	**Numeric Score**
01 Information Protection Program	00.a ISMP	72
01 Information Protection Program	00.a ISMP	80
01 Information Protection Program	00.a ISMP	82
02 Endpoint Protection	09.j Controls Against Malicious Code	72
02 Endpoint Protection	09.ab Monitoring System Use	83
05 Wireless Protection	09.ab Monitoring System Use	72
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	02.d Management Responsibilities	80
19 Data Protection & Privacy	02.d Management Responsibilities	72

In this example, all ten requirement statements scored at 72 or greater. **No gaps are present.**

	Domain-level Scoring (Drives Certification Outcome)
Domain	Average Numeric Score
01 Information Protection Program	78
02 Endpoint Protection	78
05 Wireless Protection	72
19 Data Protection & Privacy	79

(All other domains excluded for the purposes of this example but are necessary for certification)

Because all domains achieved an average score greater than 62, **certification can be achieved.**

r2 Scenario #2 Certification with Gaps

		Requirement Statement Scoring
Domain	**Control Reference**	**Numeric Score**
01 Information Protection Program	00.a ISMP	68
01 Information Protection Program	00.a ISMP	80
01 Information Protection Program	00.a ISMP	82
02 Endpoint Protection	09.j Controls Against Malicious Code	72
02 Endpoint Protection	09.ab Monitoring System Use	83
05 Wireless Protection	09.ab Monitoring System Use	72
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	02.d Management Responsibilities	80
19 Data Protection & Privacy	02.d Management Responsibilities	70

In this example, two of the ten requirement statements scored at 70 or lower. As such, **two gaps are present.**

	Domain-level Scoring (Drives Certification Outcome)
Domain	Average Numeric Score
01 Information Protection Program	77
02 Endpoint Protection	78
05 Wireless Protection	72
19 Data Protection & Privacy	78

(All other domains excluded for the purposes of this example but are necessary for certification)

Because all domains achieved an average score greater than 62, **certification can be achieved.**

r2 Scenario #3 Certification with CAPs

		Requirement Statement Scoring
Domain	**Control Reference**	**Numeric Score**
01 Information Protection Program	00.a ISMP	40
01 Information Protection Program	00.a ISMP	80
01 Information Protection Program	00.a ISMP	82
02 Endpoint Protection	09.j Controls Against Malicious Code	80
02 Endpoint Protection	09.ab Monitoring System Use	83
05 Wireless Protection	09.ab Monitoring System Use	80
19 Data Protection & Privacy	11.c Responsibilitiesand Procedures	81
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	02.d Management Responsibilities	90
19 Data Protection & Privacy	02.d Management Responsibilities	91

In this example, one of the many requirement statements in Domain 01 scored a 40.

	Domain-level Scoring (Drives Certification Outcome)
Domain	Average Numeric Score
01 Information Protection Program	68
02 Endpoint Protection	82
05 Wireless Protection	80
19 Data Protection & Privacy	86

(All other domains excluded for the purposes of this example but are necessary for certification)

The three requirement statements in Domain 01 average out to a domain-level score of 68.
This assessment can still achieve certification but required CAP(s) are likely to exist.

r2 Scenario #4 No Certification

		Requirement Statement Scoring
Domain	**Control Reference**	**Numeric Score**
01 Information Protection Program	00.a ISMP	89
01 Information Protection Program	00.a ISMP	80
01 Information Protection Program	00.a ISMP	82
02 Endpoint Protection	09.j Controls Against Malicious Code	80
02 Endpoint Protection	09.ab Monitoring System Use	75
05 Wireless Protection	09.ab Monitoring System Use	25
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	11.c Responsibilities and Procedures	81
19 Data Protection & Privacy	02.d Management Responsibilities	90
19 Data Protection & Privacy	02.d Management Responsibilities	91

In this example, the only requirement statement in the wireless domain scored a 25.

	Domain-level Scoring (Drives Certification Outcome)
Domain	Average Numeric Score
01 Information Protection Program	84
02 Endpoint Protection	78
05 Wireless Protection	25
19 Data Protection & Privacy	86

(All other domains excluded for the purposes of this example but are necessary for certification)

There is only one requirement statement in the Wireless Protection domain, so the domain scores a 25 as well. Because the domain scored less than a 62, **this assessment cannot achieve certification.**

A-16: Sample-based Testing Examples

Populations used for a sample-based test will either be selected from a list of items at a point in time ("item-based") or over a period of time ("time-based"). As described in criteria 11.4.10, the "item-based" populations tested at a point in time must be tested within the fieldwork period. Those "time-based" samples selected to test a HITRUST requirement over a period of time must meet the date requirements outlined in criteria 11.4.7 and 11.4.8 (see Chapter 11.4 Population & Sampling). Below are examples of sample-based tests and whether the test and/or population would be considered "item-based" or "time-based".

HITRUST CSF Requirement Statement	Illustrative Procedure for Implemented Sample-based Test (Partial text for example purposes)	Test/Population Type
BUID: 06.09B1SYSTEM.2: CVID: 2368.0 Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently 1 documented, 2. tested, and 3. approved.	Select a sample of changes made to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) and confirm that they were documented, tested, and approved.	*Time-based*: This test will sample changes over a historic period of time to validate the control operation.
BUID: 0201.09J1ORGANIZATIONAL.124: CVID: 0873.0 Technologies are implemented for the 1. timely installation of anti-malware protective measures, 2. timely upgrade of anti-malware protective measures, and 3. regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans… [truncated for brevity].	Select a sample of endpoint devices (desktops, laptops, servers, BYOD, etc.), determine if anti-malware software is installed, operating, and up-to-date.	*Item-based:* This test will sample from a current list of endpoints to validate: 1. Each sampled endpoint currently has installed anti-malware software, 2. The anti-malware software on each sampled endpoint is operating (e.g., active), and 3. The anti-malware software on each sampled endpoint contains the most recent updates and signatures.

BUID: 1301.02E1ORGANIZATIONAL.12: CVID: 0333.0 Security awareness training 1. commences with a formal induction process designed to introduce the organization's security and privacy policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee is hired Ongoing training includes… [truncated for brevity]	Select a sample of employees and determine if each was trained on the organization's security and privacy policies at the time of hire and annually thereafter.	*Item-based:* Although the evidence may be historic, the population being sampled from is a current list of employees, so this should follow the item-based population timing criteria.
BUID: 1015.01D1SYSTEM.1: CVID: 0074.0 Users 1. acknowledge receipt of passwords.	Select a sample of users that received new passwords and examine evidence to confirm that an acknowledgement was received from the user upon receipt. A sample of users can be selected from population of new user access requests to determine control implementation.	*Time-based:* This test will sample new users over a historic period of time.
BUID: 1002.01D1SYSTEM.1: CVID: 0067.0 Passwords 1. are prohibited from being displayed when entered.	Examine the password configuration settings for a sample of systems/ applications and confirm that they have been configured to not display passwords in plain text.	*Item-based:* This test will sample from the current in-scope systems to validate password configuration at a point in time.

A-17: Expected AI Expertise for External Assessors

Given the rapid emergence of AI technologies and the associated data privacy and security risks, independent assessments by qualified external assessors are crucial. The assessment team should have diverse skills, including knowledge of AI systems and industry-specific security requirements. These guidelines outline the essential expertise required to perform such assessments, including a deep understanding of AI technology and cybersecurity principles, risk management skills, and regulatory compliance knowledge.

While no single external assessor may meet all of the following attributes, these attributes should be met by the combined expertise, knowledge, and experience of the collective external assessor team. These attributes are additive to the requisite expertise, knowledge, and experience necessary to competently perform cybersecurity consulting and/or attestations outside of the AI context.

NOTE: Each Assessed Entity is expected to perform their own due diligence to validate the necessary experience of an External Assessor prior to engaging with them to perform a HITRUST assessment.

Essential expertise

- Understanding of AI technologies and their business context
    - Knowledge of AI model types (e.g., open source vs. not, predictive AI vs. generative AI), platforms, patterns (e.g., RAG), and technical architectures
    - Knowledge and expertise of the team performing the assessment should align with the complexity of the environment being assessed, and ongoing education should be implemented to continuously understand the latest developments
    - Familiarity with AI development frameworks and tools, as well as with the AI software development lifecycle
    - Understanding the business drivers for the rapid emergence of AI in the marketplace
    - Understanding of the risks associated with the adoption of AI without proper risk mitigation techniques

- Cybersecurity expertise
    - Proficiency in securing AI systems, models and data
    - Demonstrated knowledge/familiarity/awareness with the AI security standards, guidelines, and publications mapped in the HITRUST assessment.

- Risk Management Skills
    - Ability to identify and assess risks associated with AI implementations
    - Experience in developing risk mitigation strategies for AI initiatives

- Professional certifications relating to AI
    - (Not specifically recommended due to the novelty of the subject matter in the governance, risk, and compliance domain)

Specific knowledge

- AI security threats
  - Awareness of common security threats to AI systems
  - Understanding of potential vulnerabilities in AI models and datasets
  - Understanding of expanded attack surface for AI enabled systems
  - Understanding of impacts associated with compromised vulnerabilities

- Regulatory compliance
  - Knowledge of relevant AI-specific regulations (e.g., EU AI Act) and standards (e.g., ISO 42001)
  - Knowledge/familiarity in ensuring AI systems comply with regulatory requirements

Experience

- Prior assessments
  - Experience conducting engagements focusing on security and/or risk assessment of AI systems.
    - If unable to meet this attribute due to the novelty of the subject matter in the governance, risk, and compliance domain, consider a letter/attestation to file describing actions taken to overcome this experience shortcoming (e.g., through required pre-engagement training)
  - Track record of evaluating risk management controls in AI projects

Industry experience

- Familiarity with various industries implementing AI technologies
- Understanding of sector-specific security and compliance requirements for AI

A-18: Example Add-on Certification Approach for Existing HITRUST Certifications

As HITRUST introduces new available add-on certifications (e.g., ai1 or ai2) there may be Assessed Entities who already maintain the underlying e1, i1 or r2 certification and would like to obtain the HITRUST add-on certification. Since a new add-on certification may only be available for CSF versions later than the Assessed Entity's current certification, and it would require testing additional HITRUST requirements to obtain the certification, these situations require a customized approach. Each Assessed Entity should contact its HITRUST CSM or HITRUST support (support@hitrustalliance.net) to confirm the appropriate approach for obtaining the additional certification.

The following is an example of an approach for an Assessed Entity with a current valid r2 certification (NOTE: below circumstances may vary depending on the add-on certification, assessment type, timing and inheritance approach for the assessment):

1. The current r2 certification holder will create a new e1 assessment object using HITRUST CSF version 11.4.0 or later with the same scope as the certified assessment.

2. The e1 assessment object must then be tailored to include the "Cybersecurity for AI Systems" Compliance factor (see Chapter 6.7 Factors) while performing all other pre-assessment procedures (e.g., pre-assessment webforms, QA reservation, etc.).

3. During the assessment, the Assessed Entity may use internal inheritance to inherit the e1 core requirement statement scores from its prior r2 certified assessment into the e1 assessment object (see Chapter 12.2 Reliance on Assessments Using Inheritance).

4. The Assessed Entity and External Assessor must score and validate the ai1 requirements added into the e1 assessment from the "Cybersecurity for AI Systems" Compliance factor (and any other e1 core requirements which could not be inherited).

5. Any HITRUST requirements performed by a service provider which cannot be directly tested by the External Assessor should utilize external inheritance (when appropriate based on shared responsibilities).

6. If there are HITRUST requirements performed by a service provider that cannot be tested or inherited (e.g., a service provider has not completed its ai1 or ai2 certification), the requirements for that service provider may utilize carve-outs (see Chapter 7.3 Carve-outs) as long as the HITRUST AI security assessment is an ai1.

7. Upon completion of the assessment, it should follow the standard submission processes for an e1 assessment (See Chapter 13. Assessment Submission Process).

8. Upon successful completion of QA, HITRUST will provide the HITRUST ai1 certification reports (see Chapter 15.1 HITRUST Reporting).

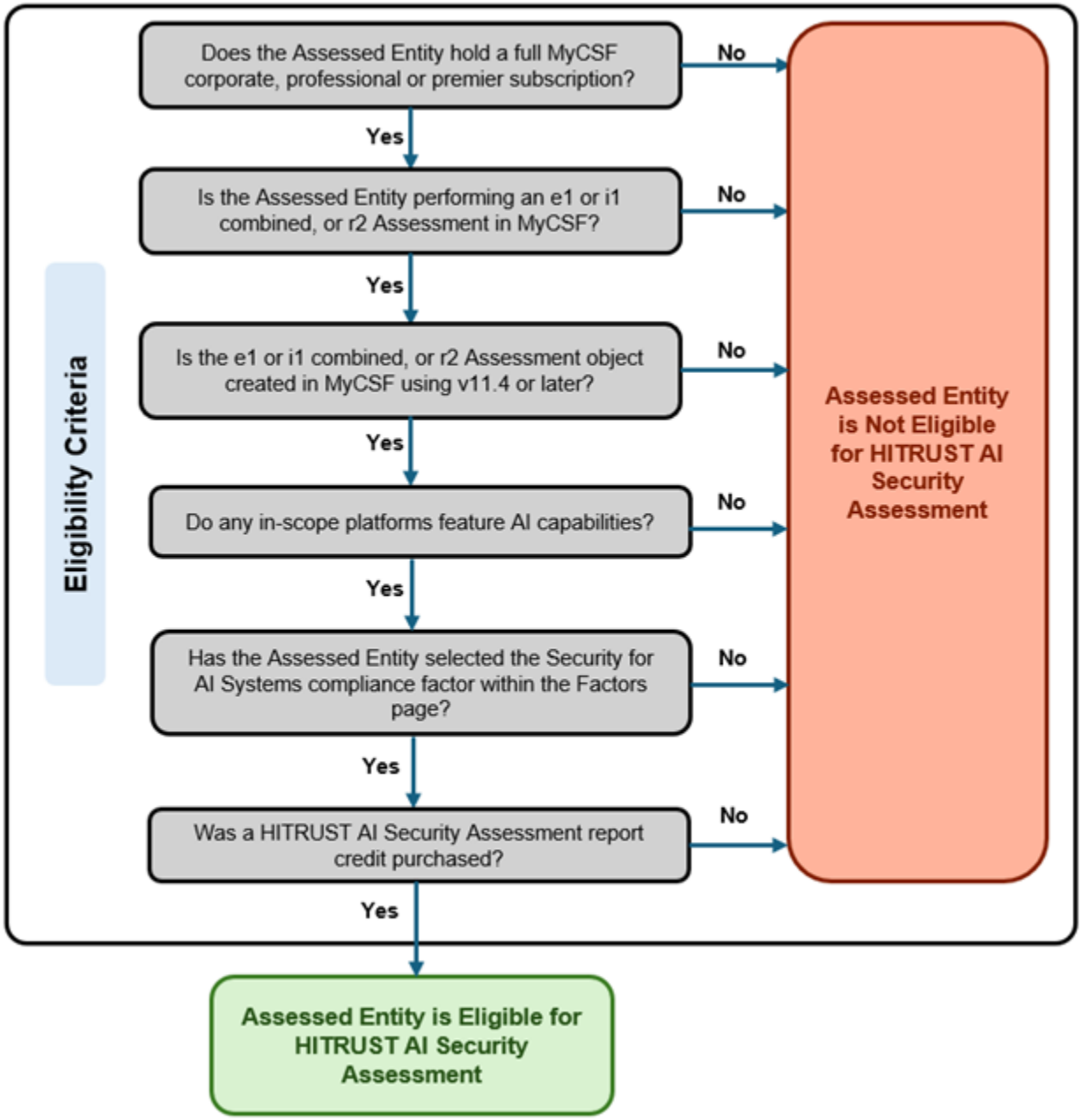
NOTE: The above approach can also be used by Assessed Entities who wish to complete an r2 assessment but need to carve-out a service provider for its HITRUST AI Security Assessment. The Assessed Entity would follow step #1 after completing its r2 assessment (NOTE: the initial r2 assessment would not include selection of the “Cybersecurity for AI Systems” Compliance factor, and would not carve-out any in-scope service providers).

A-19: AI Security Certification Eligibility

Any organization performing an e1, i1 or r2 assessment may also perform an HITRUST AI Security Assessment for its corresponding AI platform and achieve an ai1 (when combined with an e1 or i1 assessment) or ai2 (when combined with an r2 assessment) certification if it meets the necessary criteria. The ai1 and ai2 assessments are designed to equip organizations with a capability to demonstrate fundamental cybersecurity risks of deployed AI systems are being addressed.

Eligibility Criteria

The diagram below depicts the assessment types and associated CSF library version that qualify for an ai1 or ai2 assessment.



AI Certification Intended Audience

The table below describes a subset of AI personas listed by ISO/IEC 22989:2022, with an indication of whether the persona can perform an ai1 or ai2 Assessment.

AI Persona	Description	Can perform this assessment
AI providers	An AI provider is an organization or entity that provides products or services that use one or more AI systems. Encompasses: • AI platform providers: Provide services that enable other organizations to deliver AI-enabled products or services. • AI product providers: Provide AI-enabled services or products directly usable by end-user / end-customer.	**Yes**
AI developers	Concerned with the development of AI services and products (for example, model designers, model verifiers).	**No** The AI Application Deployer that instantiates what an AI developer built can obtain this certification, but the software development function cannot. HITRUST cannot certify the AI application/system development function. HITRUST only certifies implemented systems.
AI customers/ users	Users of an AI product or service.	**No** A SaaS user organization cannot obtain an ai1 or ai2 Certification over the SaaS product. The SaaS provider must certify the system.
AI partners	Provide products and/or services in the context of AI (e.g., datasets, technical development services, evaluation/assessment	**No**

	services).	

A-20: Never N/A Registry

For the core HITRUST requirement statements, HITRUST has identified a list of requirements that are expected to never be scored as Not Applicable (see Chapter 8.3 Not Applicable (N/A) Requirement Statements). These requirements are expected to always be scored, even if there is a zero population for testing (see criteria 11.4.12 for scoring zero populations). If any of the below requirement statements are marked N/A in an assessment, the HITRUST QA Analyst will open a QA task (see Chapter 14.2 QA Tasks) requesting the requirement statement to be scored. In the event that an Assessed Entity and/or its External Assessor believes there is a unique circumstance for one of the below requirement statements to be marked as N/A, it may follow the exception process outlined in criteria 15.10.5 (see Chapter 15 HITRUST Treatment of Non-compliance).

An item appearing on the below list may still be marked N/A for the Assessed Entity if the scoring is provided through inheritance and/or reliance on one or more service providers (see Chapter 12 Reliance & Third-party Coverage). In addition, the Assessed Entity may utilize a carve-out for these requirements in the event it is an e1 or i1 assessment and the service provider has been carved out of the assessment scope (see Chapter 7.3 Carve-outs).

There may be HITRUST requirement statements not listed below which may also generate QA tasks when marked as N/A. Please note that each evaluative element within the HITRUST requirement statement must have an appropriate rationale to be considered as N/A.

HITRUST Baseline Unique ID (BUID)	HITRUST Requirement Statement	HITRUST Rationale for not allowing N/A
0101.00a1Organizational.123	The organization has a formal information security management program (ISMP) that is documented and addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP is based on an accepted industry framework, considers all the control objectives of the accepted industry framework, documents any excluded control objectives of the accepted industry framework and the reasons for their exclusion, and is updated at least annually or when there are significant changes in the environment.	Entity-level requirement (all Assessed Entities must have an ISMP)
0104.02a1Organizational.12	Policies and/or standards related to user roles and responsibilities include: implementing and acting in accordance with the organization’s information security policies; protecting assets from unauthorized access,	Entity-level requirement

	disclosure, modification, destruction, or interference; executing particular security processes or activities; ensuring responsibility is assigned to the individual for actions taken; reporting security events or potential events or other security risks to the organization; and security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.	
0109.02d1Organizational.4	Employees, contractors, and third-party users are: properly briefed on their information security roles and responsibilities prior to being granted access to covered and/or confidential information or information systems; provided with guidelines to state security expectations of their role within the organization; motivated and comply with the security policies of the organization; achieve a level of awareness on security relevant to their roles and responsibilities within the organization; conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and continue to have the skills and qualifications appropriate to their roles and responsibilities.	Entity-level requirement
01109.02b1Organizational.7	The organization screens individuals requiring access to organizational information before authorizing access.	Entity-level requirement
0113.04a1Organizational.2	The organization's information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management's commitment; describe management and workforce members' roles and responsibilities; and establish the organization's approach to managing information security.	Entity-level requirement
0114.04b1Organizational.1	The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Security policies are communicated throughout the organization.	Entity-level requirement
0117.05a1Organizational.1	A senior-level information security official is appointed. The senior-level information security official is responsible for ensuring the organization's information	Entity-level requirement

	security processes are in place, communicated to all stakeholders, and consider and address organizational requirements.	
0126.05b1Organizational.1	Security activities (e.g., implementing controls, correcting nonconformities) are coordinated in advance and communicated across the entire organization where necessary.	Entity-level requirement
0135.02f1Organizational.56	The organization's formal sanctions process: includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action; identifies the individual sanctioned; and identifies the reason for the sanction. The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. The organization notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated.	Entity-level requirement
0151.02c1Organizational.23	The organization ensures that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The organization develops and documents access agreements for organizational systems. Privileges are not granted until the terms and conditions have been satisfied and agreements have been signed.	Entity-level requirement
0173.05c1Organizational.45	The organization clearly allocates and assigns responsibilities to identify and protect individual IT assets in accordance with the security policies. Where necessary, the organization supplements policies with more detailed guidance for specific assets and facilities. When security responsibilities are delegated to others, the individual originally assigned these responsibilities remains accountable, and the organization determines that any delegated tasks have been correctly performed.	Entity-level requirement
0180.05h1Organizational.4	An independent review of the information security management program and information security controls is conducted at least annually or whenever there is a	Entity-level requirement

	material change to the business practices that may implicate the security or integrity of records containing personal information.	
0181.06a1Organizational.12	All relevant statutory, regulatory, and contractual requirements, including the specific controls and individual responsibilities to meet these requirements, are explicitly defined and formally documented (e.g., in policies and procedures, as appropriate) for each information system type, and communicated to the user community as necessary through documented security training and awareness programs.	Entity-level requirement
0183.07b1Organizational.1	All information systems are documented. Documentation of all information systems includes a method to determine accurately and readily the: assigned owner of responsibility; owner's contact information; and purpose (e.g., through labeling, coding, and/or inventory).	Entity-level requirement
0193.09a1System.3	Operating procedures and the documented procedures for system activities are treated as formal documents. Changes to operating procedures and the documented procedures for system activities are authorized by management.	Entity-level requirement
0201.09j1Organizational.124	Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code	There will always be at least one endpoint in scope of testing.

	before use or file types that are unnecessary for the organization's business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.	
0207.09j1Organizational.6	Centrally managed spam protection mechanisms are employed at information system entry and exit points, workstations, servers, and mobile computing devices on the network. Spam protection mechanisms detect and take action on unsolicited messages transported by electronic mail, transported by electronic mail attachments, transported by Web accesses, transported by other common means, and inserted through the exploitation of information system vulnerabilities. Malicious code and spam protection mechanisms are centrally managed and updated when new releases are made available in accordance with the organization's configuration management policy and procedures.	There will always be at least one endpoint in scope of testing.
0210.01g1Organizational.1	All users are made aware of: the security requirements and procedures for protecting unattended equipment; their responsibilities for terminating active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver); their responsibilities for logging-off mainframe computers, servers, and office PCs when the session is finished (e.g., not just switch off the PC screen or terminal); and their responsibilities for securing PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g., password access) when not in use.	There will always be at least one user and/or endpoint in scope of testing.

0217.09j1Organizational.7	The organization configures malicious code and spam protection mechanisms to: perform periodic scans of the information system according to organization guidelines; perform real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and block malicious code, quarantine malicious code, or send alerts to an administrator in response to malicious code detection.	There will always be at least one endpoint in scope of testing.
0226.09k1Organizational.2	The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.	There will always be at least one endpoint in scope of testing.
0265.09m1Organizational.2	The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.	There will always be at least one endpoint in scope of testing.
02962.09j1Organizational.5	The organization augments endpoint protection strategies with additional solutions—including those built into the operating system if available—to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).	There will always be at least one endpoint in scope of testing.
0403.01×1Organizational.5	The organization monitors for unauthorized connections of mobile devices.	The requirement statement expects a detective control to identify unauthorized mobile device connections.
0505.09m1Organizational.11	Quarterly scans are performed to identify unauthorized	The

	wireless access points. Appropriate action is taken if any unauthorized access points are discovered.	requirement statement expects a detective control to identify unauthorized wireless access points connected to the in-scope network(s).
06.09b1System.2	Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.	All assessments will have an in-scope environment where this applies.
0601.06g1Organizational.124	Annual compliance assessments are conducted. Compliance reviews are conducted by security, privacy, and/or audit individuals, and incorporate reviews of documented evidence. If any non-compliance is found as a result of the review, managers will: determine the causes of the non-compliance; evaluate the need for actions to ensure that non-compliance do not recur; determine and implement appropriate corrective action; and review the corrective action taken.	All assessments will have an in-scope environment where this applies.
0613.06h1Organizational.12	The organization performs annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools. If any non-compliance is found as a result of a technical security configuration compliance review, the organization: determines the causes of the non-compliance; evaluates the need for actions to ensure that non-compliance do not recur; determines and implements appropriate corrective action; and reviews the corrective action taken.	All assessments will have an in-scope environment where this applies.
0627.10h1System.45	Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational	All assessments will have an in-

	systems to take advantage of the latest security functions. The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse.	scope environment where this applies.
0636.10k1Organizational.3	The organization formally addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management.	Entity-level requirement
0666.10h1System.5	The organization maintains an up-to-date list of authorized software that is required in the enterprise for any business purpose on any business system.	Entity-level requirement
0667.10h1System.6	The organization is required to deploy application allow listing technology that allows systems to run software only if it is authorized to execute (allow listed) and prevents execution of all other software on the system in accordance with the allow list and rules authorizing the terms and conditions of software program usage.	Entity-level requirement
06900.09d1System.2	The organization ensures separation between production and non-production (development, test/ quality assurance) environments is established and controls are implemented to prevent operational issues.	Expectation is that the organization or its service provider will always have a non-production environment (e.g. dev or test) where this would be tested (e.g., for testing changes, patches, etc.)
07.07a1Organizational.8	Organizational inventories of IT assets are periodically (annually at minimum) reviewed to ensure completeness and accuracy.	Entity-level requirement.
07.10m1Organizational.2	The organization deploys automated software update tools in order to ensure that systems are running the most recent security updates provided by the software vendor, and installs software updates manually for systems that do not support automated software	All assessments will have an in-scope environment

	updates.	where this applies.
07.10m1Organizational.3	Information systems are periodically scanned to proactively (annually at minimum) identify technical vulnerabilities.	All assessments will have an in-scope environment where this applies.
0701.07a1Organizational.7	The organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites). The organization documents the importance of these inventoried assets. The asset inventory includes: all systems connected to the network; the network devices themselves; desktops; servers; network equipment (routers, switches, firewalls, etc.); printers; storage area networks; Voice Over-IP telephones; multi-homed addresses; virtual addresses; mobile phones, regardless of whether they are attached to the organization's network; tablets, regardless of whether they are attached to the organization's network; laptops, regardless of whether they are attached to the organization's network; other portable electronic devices [i.e., other than mobile phones, tablets, and laptops] that store or process data, regardless of whether they are attached to the organization's network; and approved bring your own device (BYOD) equipment.	Entity-level requirement
0701.07a1Organizational.8	The asset inventories include: type or classification of the asset; format of the asset; location of the asset; backup information of the asset; license information of the asset; a business value of the asset; and data on whether the device is a portable and/or personal device. The asset inventory record is used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department. The asset inventory records: the network addresses; the machine name(s); the purpose of each system; an asset owner responsible for each device; and the department	Entity-level requirement.

	associated with each device. The inventory does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned. Records of property assigned to employees is reviewed and updated annually.	
0704.07a1Organizational.8	The organization creates, documents, and maintains a process and procedure to physically inventory capital assets (at least annually), physically inventory non-capital assets, reconcile IT asset inventory information on hand for capital assets, reconcile IT asset inventory information on hand for non-capital assets. Organizational inventories of IT assets are updated during installations, equipment removals, system changes.	Entity-level requirement
0704.07a1Organizational.9	The asset inventory includes the: unique identifier and/or serial number of the IT asset; information system of which the component is a part; type of information system component (e.g., server, desktop, application); manufacturer/model information of the IT asset; operating system type and version/service pack level of the IT asset; presence of virtual machines; application software version/license information; physical location (e.g., building/room number) of the IT asset; logical location (e.g., IP address, position with the IS architecture) of the IT asset; Media access control (MAC) address of the IT asset; data ownership and custodian by position and role; operational status of the IT asset; primary and secondary administrators of the IT asset; and primary user of the IT asset.	Entity-level requirement.
0709.10m1Organizational.1	Once a potential technical vulnerability has been identified, the organization identifies the associated risks and the actions to be taken. Further, the organization performs the necessary actions to correct identified technical vulnerabilities in a timely manner.	Entity-level requirement
0715.10m1Organizational.4	Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.2 or later, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).	All assessments will have an in-scope environment where this applies.

0732.09r1Organizational.3	The access list for system documentation is kept to a minimum and is authorized by the application owner.	All assessments will have an in-scope environment where this applies.
0778.10m1Organizational.5	The organization regularly compares the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	All assessments will have an in-scope environment where this applies.
08.09m1Organizational.8	The organization prevents enterprise assets from accessing known malicious addresses and domains on the Internet (for example by means of browser configurations, DNS sinkholing, and/or use of a subscription service), unless there is a clear, documented business need and the organization understands and accepts the associated risk.	All assessments will have an in-scope environment where this applies.
0802.01i1Organizational.2	The organization: determines who is allowed to access which network and networked services; specifies the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system); at a minimum, manages all enterprise devices remotely logging into the internal network, with remote control of their configuration; at a minimum, manages all enterprise devices remotely logging into the internal network, with installed software; at a minimum, manages all enterprise devices remotely logging into the internal network, with patch levels; publishes minimum security standards for access to the enterprise network by third-party devices (e.g., subcontractors/vendors); performs a security scan before allowing access; identifies the ports necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure; identifies the services necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure; and	All assessments will have an in-scope environment where this applies.

	identifies the similar applications (e.g., protocols) necessary for business and provides the rationale–or identifies compensating controls implemented–for those protocols to be non-secure.	
0805.01m1Organizational.12	Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of: enforcing security policies, being configured to filter traffic between these domains, and blocking unauthorized access in accordance with the organization's access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered and/or confidential information systems environment.	All assessments will have an in-scope environment where this applies.
0814.01n1Organizational.12	At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception). The organization restricts the ability of users to connect to the internal network in accordance with the access control policy and the requirements of its business applications.	All assessments will have an in-scope environment where this applies.
0815.01o1Organizational.1	The organization ensures that security gateways (e.g., a firewall) are used to validate source and destination addresses at internal and external network control points. The organization designs and implements network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The application-layer filtering proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a disallow list, or applying lists of allowed sites that can be accessed through the proxy while blocking all other sites. The organization forces outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Internal directory services and internal IP addresses are protected and hidden from	All assessments will have an in-scope environment where this applies.

	any external access. Requirements for network routing control are based on the access control policy.	
0816.01w1System.1	The sensitivity of an application is explicitly identified, and documented by the application/system owner. Applications are not limited to only the in-scope applications. Supporting tools in the environment are also expected to be addressed.	All assessments will have an in-scope environment where this applies.
0820.01k1System.3	The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection. Network devices that require authentication mechanisms use shared information (e.g., MAC or IP address) to control remote network access and access control lists to control remote network access.	All assessments will have an in-scope environment where this applies.
0825.09m1Organizational.14	Technical tools such as intrusion detection systems (IDS)/intrusion prevention systems (IPS) are implemented and operating at the network perimeter and key points within the network. Implemented and operating technical tools include IDS and IPDS deployed on the wireless side of the firewall (WIDS). The IDS/IPS is updated on a regular basis, including the engines, baselines and signatures.	All assessments will have an in-scope environment where this applies.
0835.09n1Organizational.1	The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored. The right to audit is agreed by management for each network service provider. The security arrangements necessary for particular network services' security features, service levels, and management requirements, are identified and documented.	The expectation is that all Assessed Entities would have some type of company providing network services (e.g., ISP)
09.09v1Organizational.7	The organization uses an email filtering solution to recognize and block suspicious emails and unnecessary file types before they reach employee inboxes.	This is an entity level control with the focus on protections

		around employee email in order to prevent phishing/ malware at the organization level, not just within the in-scope environment.
0905.10g1Organizational.12	All cryptographic keys are protected against modification, loss, and destruction. Secret/private keys, including split-keys, are protected against unauthorized disclosure. Equipment used to generate, store, and archive keys is physically protected.	All Assessed Entities will be using encryption within the in-scope environment so the protection of those keys must be tested.
0913.09s1Organizational.5	Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security (TLS) 1.2 or later; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TSL VPNs: SSL Portal VPN; SSL Tunnel VPN.	All organizations must have a defined encryption procedure for data in transit.
0945.09y1Organizational.3	Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL).	Not limited to ecommerce, this is related to all online transactions.
0954.10d1System.1	The information system provides mechanisms to protect the authenticity of communications sessions.	All assessments will have an in-scope environment

		where a communication session will take place requiring authentication
10.01d1System.10	Password policies applicable to the organization's information systems are documented and enforced through technical controls.	All assessments will have an in-scope environment where this applies.
1003.01d1System.3	User identities are verified prior to performing password resets.	Entity-level requirement.
1011.01f1Organizational.1	The organization ensures users are made aware of the organization's password policies and requirements, are made aware to keep passwords confidential, avoid keeping a record (e.g., paper, software file, or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved, change passwords whenever there is any indication of possible system or password compromise, do not share individual user accounts or passwords, do not provide their password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks), do not use the same password for business and non-business purposes, and select quality passwords.	Entity-level requirement.
1013.01r1System.2	The password management system stores passwords in protected (e.g., encrypted or hashed) form, transmits passwords in protected (e.g., encrypted or hashed) form, stores password files separately from application system data, enforces a choice of quality passwords, enforces password changes, and maintains a record of previous user passwords and prevents re-use.	All organizations will have to manage passwords for their in-scope environment.
1023.01d1System.11	The organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts before deploying any new devices in a networked	Organizations will have area(s) where default password

	environment.	would need to be changed.
10902.01d1System.12	Authentication credentials are provided using a secure method.	All organizations will have to manage authentication credentials for their in-scope environment.
11.01e1System.2	The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).	All organizations will have to manage accounts for their in-scope environment.
11.01p1System.5	A policy applicable to the organization's information systems addressing account lockout after consecutive unsuccessful login attempts is documented and enforced through technical controls.	All assessments will have an in-scope environment where this applies.
11.01q1System.3	The organization requires multi-factor authentication for network and local access to privileged accounts.	All organizations will have to manage accounts for their in-scope environment.
1101.01a1Organizational.1245	Access control rules and rights for each user or group of users are based on clearly defined requirements for information dissemination and authorization (e.g., need-to-know, need-to-share, least privilege, security levels, and information classification). The policy further defines logical and physical access control rules and rights for each user or group of users are considered together and clearly defined in standard user access profiles (e.g., roles). The access control program takes into account security requirements of individual	All organizations will have users where access needs to be managed.

	business applications and business units and ensures standard user access profiles for common jobs roles in the organization.	
1105.09c1Organizational.2	Access authorization (e.g., access requests, approvals, and provisioning) is segregated among multiple individuals or groups.	All organizations will have users where access needs to be managed.
1107.01b1System.2	Default and unnecessary accounts are removed, disabled, or otherwise secured.	All organizations will have area(s) where default or unnecessary accounts need to be managed.
1114.01h1Organizational.123	Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use. Documents containing covered or critical information are removed from printers, copiers, and facsimile machines immediately. When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).	All organizations will have critical and/or confidential information that needs to be managed and/or workstations that must be secured.
11143.02i1Organizational.3	The organization ensures logical and physical access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in responsibility, or employment.	All organizations have access to be managed.
11149.02g1Organizational.2	The organization has a documented termination checklist that identifies all the steps to be taken and assets to be collected.	All organizations have

		terminations that must be managed.
11152.02h1Organizational.1	The termination process includes the return of all previously issued software in the termination process, all corporate documents in the termination process, all equipment in the termination process, and all other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media in the termination process.	All organizations have terminations that must be managed.
11183.01c1System.3	System administrators only use accounts with privileged access when performing administrative duties and use a separate user account with standard user access rights when performing non-privileged activities (e.g., Internet browsing, email, or similar activities).	All organizations have systems / applications that must be managed by an administrator.
1123.01q1System.2	Each user ID in the information system (including non-privileged, privileged, seeded, and service accounts) is assigned to a specific, named individual to maintain accountability.	All organizations will have an information system with user IDs.
1143.01c1System.123	The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).	All organizations will have an information system with privilege(s) to manage.
1151.01c1System.2	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users and tracks and monitors privileged role assignments.	All organizations will have an information

		system with privileged account(s).
1194.01l1Organizational.2	Ports, services, and applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled or removed.	All assessments will have a computer and/or network system in scope.
1203.09aa1System.2	Audit records include a unique user ID, unique data subject ID (if applicable), function performed, and date/time the event was performed.	All organizations will have audit records to manage.
12101.09ab1System.2	The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.	All organizations will have audit records to manage.
12148.06i1Organizational.1	The organization determines which of the following auditable events require auditing on a continuous basis in response to specific situations: user log-on and log-off (successful or unsuccessful); configuration changes; application alerts and error messages; all system administration activities; modification of privileges and access; account creation, modification, or deletion; concurrent log on from different workstations; and override of access control mechanisms.	All organizations will have audit records to manage.
1223.09ac1System.1	Access to audit trails / logs is safeguarded from unauthorized access and use.	All organizations will have audit records to manage.
1235.06j1Organizational.1	Access to information systems audit tools is protected to prevent any possible misuse or compromise.	All organizations will have audit records established by tool(s).

1239.09aa1System.4	Retention policies for audit logs are specified by the organization and the audit logs are retained accordingly.	All organizations will have audit records to manage.
1270.09ad1System.12	The organization ensures that proper logging is enabled in order to audit administrator activities. The organization ensures system administrator logs and operator logs are reviewed on a regular basis.	All organizations will have audit records to manage.
1272.09ae1System.13	Faults reported by users or by system programs related to problems with information processing or communications systems are logged. Error logging is enabled if this system function is available.	All assessments will have an information system in scope.
1295.09af1System.2	The organization uses at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.	All assessments will have a server and/or network equipment in scope.
13.02e1Organizational.6	Dedicated phishing awareness training is developed as part of the organization’s onboarding program, is documented and tracked, and includes the recognition and reporting of potential phishing attempts.	All organizations have employees and/or individuals they may need to onboard.
1304.02e1Organizational.7	The organization provides role-based security-related training, especially for personnel with significant security responsibilities (e.g., system administrators), prior to accessing the organization’s information resources, when required by system or environment changes, when entering into a new position that requires additional role-specific training, and no less than annually thereafter.	All organizations have employees and/or individuals they may need to onboard.
1306.06e1Organizational.5	All employees and contractors are informed in writing that violations of the security policies will result in	All organizations

	sanctions or disciplinary action.	have employees and/or individuals they may need to onboard.
1307.07c1Organizational.124	The organization establishes and makes readily available to all information system users a set of rules that describe their responsibilities and expected behavior with regard to information and information system usage. Acceptable use addresses rules for electronic mail and Internet usages and guidelines for the use of mobile devices, especially for the use outside the premises of the organization. The organization includes in the rules of behavior containing explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.	All organizations will have information system users.
1308.09j1Organizational.5	The organization prohibits users from installing unauthorized software, including data and software from external networks, and disables any auto-run features which allow file execution without user authorization (such as when files are downloaded from the Internet or when removable media is inserted). Users are made aware and trained on requirements relating to prohibition of installing unauthorized software, including data and software from external networks.	All organizations will have information system users.
13998.02e1Organizational.2	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, prior to accessing any system’s information.	All organizations will have information system users.
1408.08e1System.1	Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions (e.g., reliability, availability, and response times for the provision of services), security controls, and other aspects of services management (e.g., monitoring, auditing, impacts to the organization’s resilience, and change management).	Entity-level requirement. If the organization does not have a service provider the requirement

		should still be scored (but treated as a zero population).
1411.09f1System.1	The organization ensures a periodic review of service-level agreements (SLAs) is conducted at least annually, and compared against the monitoring records.	Entity-level requirement. If the organization does not have a service provider the requirement should still be scored (but treated as a zero population).
1506.11a1Organizational.2	A point of contact is established for the reporting of information security events. It is ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response. The organization also maintains a list of third-party contact information (e.g., the email addresses of their information security officers), which can be used to report a security incident.	Entity-level requirement. Not contingent on a security event having occurred.
1535.11b1Organizational.12	The organization has an easy-to-use, available, and widely accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents.	Entity-level requirement
1560.11d1Organizational.1	The information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents, and update the incident response and recovery strategy.	Entity-level requirement. If no security incidents have occurred, this would be scored as zero population.

1561.11c1Organizational.4	The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); procedures defining roles and responsibilities; incident handling procedures (business and technical); communication; reporting and retention; and references the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation).	Entity-level requirement
1563.11d1Organizational.2	The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, and training and testing exercises. The organization implements the resulting changes to incident response procedures, training exercises, and testing exercises accordingly.	Entity-level requirement
1569.11e1Organizational.12	The organization collects, retains, and presents evidence to support legal action (either civil or criminal) in accordance with the laws of the relevant jurisdiction(s).	Entity-level requirement
1589.11c1Organizational.5	The organization tests and/or exercises its incident response capability regularly.	Entity-level requirement
1602.12c1Organizational.4567	Business continuity plans: identify the necessary capacity for information processing during contingency operations, e.g., during an information system disruption, compromise or failure; identify the necessary capacity for telecommunications during contingency operations; identify the necessary capacity for environmental support during contingency operations; identify the essential missions and business functions; identify the contingency requirements associated with essential missions and business functions; provide recovery objectives; provide restoration priorities; provide recovery and restoration metrics; address contingency roles; assign individuals to contingency responsibilities; and contain the contact information of individuals assigned to contingency responsibilities.	Entity-level requirement

1611.09h1System.2	The organization has allocated sufficient storage capacity to reduce the likelihood of exceeding capacity and the impact on network infrastructure (e.g., bandwidth).	All assessments will have an information system and/or network infrastructure in scope.
1616.09l1Organizational.16	Backup copies of information and software are made regularly at appropriate intervals in accordance with an agreed-upon backup policy, are made when equipment is moved (relocated), and are tested regularly at appropriate intervals in accordance with an agreed-upon backup policy. Restoration procedures are tested regularly at appropriate intervals in accordance with an agreed-upon backup policy.	All assessments will have information and/or software in scope.
1617.09l1Organizational.23	A formal definition of the level of backup required for each system is defined and documented including the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory, and business requirements. The organization formally defines and documents how each system is completely restored from backup.	All assessments will have an information system in scope.
1618.09l1Organizational.45	Backups are stored in a physically secure remote location and at a sufficient distance to make them reasonably immune from damage to data at the primary site. Physical and environmental controls are in place for the backup copies.	All assessments will have backups from the in scope information system.
1632.12a1Organizational.1	The organization: identifies all the assets involved in critical business processes; considers the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management; ensures the safety of personnel and the protection of information assets and organizational property; and formulates and documents business continuity plans addressing information security requirements in line with the agreed business continuity strategy.	Entity-level requirement
1634.12b1Organizational.1	The organization identifies the critical business	Entity-level

	processes requiring business continuity.	requirement
1666.12d1Organizational.1235	The organization creates, at a minimum, one business continuity plan. The organization ensures each plan: has an owner; describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security; specifies the escalation plan; specifies the conditions for the escalation plan's activation; and specifies the individuals responsible for executing each component of the plan.	Entity-level requirement
1677.12e1Organizational.6	Responsibility is assigned for regular reviews of at least a part of the business continuity plan at a minimum, annually.	Entity-level requirement
1701.03a1Organizational.12345678	The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	Entity-level requirement
1704.03b1Organizational.12	The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals and when major changes occur in the environment, and	Entity-level requirement

	the results reviewed annually.	
17126.03c1Organizational.2	The organization implements an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks.	Entity-level requirement
1734.03d1Organizational.2	The risk management process is integrated with the change management process.	Entity-level requirement
1739.05d1Organizational.3	Management formally authorizes (approves) new information assets and facilities for processing (use) before commencing operations and periodically reviews and updates authorizations (approvals) at a frequency defined by the organization – but no less than three years.	Entity-level requirement. If no new assets and facilities then it would be treated as a zero population.
1744.05f1Organizational.23	The organization includes key contacts including phone numbers and email addresses as part of its incident management and/or business continuity plan. The organization designates a point of contact to review the list at least annually to keep it current.	Entity-level requirement
1749.05g1Organizational.1	Membership in organization-defined special interest groups or forums/services are considered as a means to: improve knowledge of best practices and stay up to date with relevant security information; ensure the understanding of the information security environment is current and complete (e.g., threat monitoring/ intelligence services); receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; gain access to specialist information security advice; share and exchange information about new technologies, products, threats, or vulnerabilities; and provide suitable liaison points when dealing with information security incidents.	Entity-level requirement
1767.07d1Organizational.2	The organization establishes a classification schema to differentiate between various levels of sensitivity and value. Information assets are classified according to their level of sensitivity as follows: Level 1: Low-sensitive information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of employees, clients, and partners. This includes information regularly made available to	Entity-level requirement

	the public via electronic, verbal, or hard copy; Level 2: Sensitive information that may not to be protected from public disclosure but if made easily and readily available, the organization will follow its disclosure policies and procedures before providing this information to external parties; Level 3: Sensitive information intended for limited business use that can be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of employees, clients, or partners; Level 4: Information that is deemed extremely sensitive and is intended for use by named individuals only. This information is typically exempt from public disclosure. Users of information systems will be notified and made aware when the data they are accessing contains PII.	
1769.09i1System.12	Requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. The organization ensures new information systems, upgrades, and new versions are only migrated into production after obtaining formal acceptance from management.	Entity-level requirement.
1781.10a1Organizational.23	Specifications for the security control requirements include security controls to be incorporated in the information system, and supplemented by manual controls as needed. Further, security control requirements are considered when evaluating software packages, either developed or purchased.	Entity-level requirement
18108.08j1Organizational.1	The organization formally addresses purpose, scope, roles associated with, responsibilities associated with, management's commitment to, coordination among organizational entities associated with, and compliance with the organization's equipment maintenance program. Formal, documented procedures exist to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed

		in the assessment (unless carved-out in an i1 or e1 assessment).
18127.08l1Organizational.3	The organization ensures that surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless carved-out in an i1 or e1 assessment).
18128.08m1Organizational.12	The organization ensures equipment, information, and software are not taken off-site without prior authorization. The organization ensures employees, contractors, and third-party users who have authority to permit off-site removal of assets are clearly identified.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the

		assessment (unless carved-out in an i1 or e1 assessment).
1845.08b1Organizational.7	For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points to the facility, maintains physical access audit logs, and provides security safeguards the organization determines are necessary for areas officially designated as publicly accessible.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless carved-out in an i1 or e1 assessment).
1857.08c1Organizational.1	Relevant health and safety regulations and standards are taken into consideration when securing facilities.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment

		(unless carved-out in an i1 or e1 assessment).
1863.08d1Organizational.4	The organization develops, disseminates, and reviews/updates annually a formal, documented physical and environmental protection policy. The physical and environmental protection policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization develops formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless carved-out in an i1 or e1 assessment).
1867.08e1Organizational.12	The arrangements for working in secure areas include controls for the employees, contractors, and third-party users working in the secure area, as well as other third-party activities taking place there. Personnel are aware of the existence of, or activities within, a secure area on a need to know basis.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless

		carved-out in an i1 or e1 assessment).
1880.08g1Organizational.6	The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, and considers the physical and environmental hazards in its risk mitigation strategy.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless carved-out in an i1 or e1 assessment).
1888.08h1Organizational.456	An uninterruptable power supply (UPS) to support orderly close down is required for equipment supporting critical business operations. Power contingency plans cover the action to be taken on failure of the UPS. The organization ensures UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer’s recommendations.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless carved-out in

		an i1 or e1 assessment).
1899.08i1Organizational.1	The organization protects power equipment and power cabling for the information system from damage and destruction.	Assessments will have at least one in-scope facility. Even if the information is hosted in the cloud, the cloud service provider maintains a physical presence which should be addressed in the assessment (unless carved-out in an i1 or e1 assessment).
1908.10c1System.5	The organization: develops and documents system and information integrity policy and procedures; disseminates the system and information integrity policy and procedures to appropriate areas within the organization; and reviews and updates defined system and information integrity requirements no less than annually.	Entity-level requirement
19131.05e1Organizational.45	Requirements for confidentiality and non-disclosure agreements are reviewed at least annually and when changes occur that influence these requirements. Confidentiality and non-disclosure agreements comply with all applicable laws and regulations for the jurisdiction to which it applies.	Entity-level requirement
19142.06c1Organizational.8	Guidelines are issued and implemented by the organization on the ownership, classification, retention, storage, handling, and disposal of all records and information.	Entity-level requirement
19180.09z1Organizational.2	The organization designates individuals authorized to	This is an

	post information onto a publicly accessible information system, and trains these individuals to ensure that publicly accessible information does not contain nonpublic information.	entity-level requirement which applies to the organization as a whole. Publicly accessible systems include the company website or company social media sites (e.g., LinkedIn, Facebook, etc.)
19204.10i1System.1	The use of operational databases containing covered and/or confidential information for non-production (e.g., testing) purposes is avoided; however, if covered and/or confidential information is used for testing purposes, all sensitive details and content is removed or modified beyond recognition (i.e., de-identified) before use.	If covered / confidential information is not used for non-production then the organization is addressing the requirement.
19249.06b1Organizational.2	The organization establishes restrictions on the use of open source software. Open source software used by the organization is legally licensed, authorized, and adheres to the organizations secure configuration policy.	This is an entity-level requirement which applies to the organization as a whole. Open source software is typically accessible by organization employees so appropriate limitations should be

		implemented.
19922.06f1Organizational.2	The encryption policy addresses the type and strength of the encryption algorithm and when used to protect the confidentiality of information. The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards.	Entity-level requirement

Appendix B: Summary of Changes

This page is intentionally left blank.

B-1: Version 1.0

In addition to minor wording updates and clarification, the changes between the exposure draft and version 1.0 of the Assessment Handbook include the key modifications summarized in the table below.

Chapter	Modification
1. Introduction	Added reference to HITRUST Glossary of Terms and Acronyms.
3.1 Assessed Entity	Updated to include the Assessed Entity responsibilities outlined in the Management Representation Letter.
3.2 Assessors	Updated with previously documented and communicated readiness assessment, readiness license and internal assessor requirements.
3.3 Independence Requirements	Clarified types of remediation activities that are not authorized for External Assessors.
6. Pre-Assessment	Added Chapter numbers for each pre-assessment webform.
6.5 Scope of the Assessment	Included the requirements for description of a platform.
6.7 Factors	Included the requirement for a rationale when a factor question is answered “No”.
7.1 Assessment Scoping	Included visual timeline for system implementation requirement; Added criteria 7.1.4 to clarify HITRUST rationale for reporting facility(s).
7.2 Required Scope Components	Clarified the potential for other component types to be included as a primary scope components; Clarified definition of primary and secondary scope components; 7.2.4 – Added example, Added NOTE clarifying that components may exist as both a primary and secondary scope component; 7.2.7 – Clarified that additional facility(s) not hosting the in-scope platform that are included in scope must present a risk to the in-scope platform; Added new criteria 7.2.12 for clarification on how to determine scope when requirement statement language may conflict with Assessment Handbook guidance; 7.2.14 – Added testing expectations and definitions for bastion host, jump server and VDI; 7.2.15 – Clarified that laptops are not classified as portable media; Other Scoping Topics – Added criteria 7.2.23 – 7.2.25 to provide guidance and expectations on sampling of scope components.
7.3 Carve-outs	Clarified definition of carve-out.
8.1 Requirement Statement Background	Included additional information on Illustrative Procedures (previously documented in HITRUST whitepapers) including criteria 8.1.1 for an External Assessor to use the Illustrative Procedures to support its testing approach.

8.2 Alternate Controls	Added chapter 8.2 on the HITRUST Alternate Control process and requirements.
9.5 Managed Maturity Level	Added criteria 9.5.2 to explain an undocumented risk treatment process.
10.1 HITRUST Scoring	Added criteria 10.1.1 – 10.1.3 to explain HITRUST expectations for weighting of scope components.
11.2 Testing Requirements	11.2.8 – Clarified 90 day control operation requirement; 11.2.9 – Added visual timeline of a newly implemented control.
11.3 Working Papers & Evidence	Temporary removal of criteria related to completeness and accuracy (for further refinement); 11.3.8 – Clarified date requirements for evidence supporting observations and inspections; 11.3.9 – Clarified requirements for policy and procedure documents; 11.3.11 – Clarified expectations for appropriate evidence linking; Temporary removal of criteria requiring evidence documenting the source of each population.
11.4 Population & Sampling	Temporary removal of criteria requiring evidence documenting the source of each population; Temporary removal of criteria related to completeness and accuracy of the population (for further refinement); 11.4.9 – Added time limit of 30 days to population generation prior to fieldwork; Removed HITRUST criteria to re-validate population size within fieldwork period (if generated prior to fieldwork); Added criteria 11.4.11 to re-select sample items that are selected and not able to be tested; Added criteria 11.4.16 to clarify that evidence must be uploaded for all sample selections.
11.5 Documenting Exceptions	Added criteria 11.5.1 and 11.5.3 to clarify HITRUST expectations when an exception has been identified during testing.
12.1 Third-Party Coverage	Added criteria 12.1.4 to clarify HITRUST expectations for Assessed Entities as it relates to third-parties.
12.2 Reliance on Assessment Results Using Inheritance	Re-organized and re-worded Chapter 12.2 for easier interpretation of HITRUST expectations.
13.2 Audits and Assessments Utilized	Added criteria 13.2.3 to clarify what should and should not be included.
13.8 Management Representation Letter	Added criteria 13.8.4 to include the Rep Letter date requirements.
14.3 Live QA	Added criteria 14.3.3 to clarify what information may and may not be withheld from

	MyCSF for LiveQA; Added criteria 14.3.7 to communicate HITRUST expectations for the External Assessor during LiveQA.
14.4 Escalated QA	Added criteria 14.4.13 to clarify the purpose of an appeal.
15.3 Security Events & Fraud	Added criteria 15.3.10 to clarify how an External Assessor should answer the interim assessment question related to security breaches.
15.4 Interim Assessment	Added criteria 15.4.5 and 15.4.6 to clarify the impact of lowering scores in an interim assessment; Added criteria 15.4.19 and 15.4.20 to clarify testing approach for remediated CAPs; 15.4.21 – Added items that HITRUST takes into consideration to determine sufficient progress.
15.5 Rapid Assessments	Added diagram to provide visual workflow of the control degradation detection process.
15.9 HITRUST Treatment of Non-compliance	Added Chapter 15.9 to describe potential outcomes when criteria in the Assessment Handbook are not met.
Appendix A-4: Never N/A Examples	Updated table to include additional examples.
Appendix A-7: Rubric Scoring – Measured and Managed	Updated with additional FAQs.
Appendix A-10: Policy & Procedure FAQs & Examples	Updated with additional FAQs.
Appendix A-12: Inheritance FAQs & Examples	Updated with additional FAQs.
Appendix A-15: Certification Threshold Scoring Examples	New Appendix to provide various certification scoring scenarios.

B-2: Version 1.1

In addition to minor wording updates and clarification, the changes between version 1.0 and version 1.1 of the Assessment Handbook include the key modifications summarized in the table below.

Chapter	Modification
1.0 Introduction	Added link to the MyCSF Help website.
3.2 Assessors	Added paragraph summarizing skill expectations for staffing HITRUST assessments, including expected AI skills.
3.3 Independence Requirements	3.3.5 and 3.3.6 – Included Internal Assessors in the independence requirements
4. Assessment Types	Updated the description of e1 and i1 assessments to include the newly released enhancement that allows Assessed Entities to include other authoritative sources in those assessments. Added a characteristic to the table comparing e1, i1, and r2 assessments to address the ability to obtain Insights Reports over added authoritative sources.
4.1 Readiness Assessments	Updated the description of e1 and i1 readiness assessments to include the newly released enhancement that allows Assessed Entities to include other authoritative sources in those assessments.
4.2 Validated Assessments	Updated the description of e1 and i1 readiness assessments to include the newly released enhancement that allows Assessed Entities to include other authoritative sources in those assessments. Included a description of Insights Reports associated with e1, i1, and r2 assessments.
5.1 r2 Validated Assessment Workflow	Updated chapter 5.1 to describe only the r2 Validated Assessment Workflow. Included a description of the process to request Insights Reports during the Complete phase of the r2 Validated Assessment Workflow.
5.2 e1 and i1 Validated Assessment Workflow	Added chapter 5.2 to describe the enhanced e1 and i1 Validated Assessment Workflow that allows for Compliance factors to be included in the assessment for the purpose of obtaining Insights Reports over the included authoritative sources. The e1 and i1 Validated Assessment Workflow includes the following new phases: • Pre-QA Assessment Results Review • Addressing HITRUST CSF Reporting Tasks • Reviewing Pending HITRUST CSF Reporting Tasks • Preparing Additional Report Drafts • Reviewing Additional Report Drafts • Revising Additional Report Drafts • Addressing Additional Reporting Tasks • Reviewing Additional Reporting Tasks

5.3 r2 Readiness Assessment Workflow	Chapter 5.2 Readiness Assessment Workflow was renamed to accommodate the addition of chapter 5.2 e1 and i1 Validated Assessment Workflow described above and to address only r2 Readiness Assessments.
5.4 e1 and i1 Readiness Assessment Workflow	Added chapter 5.4 to describe the e1 and i1 Readiness Assessment Workflow which includes a new phase, *Assessment Results Review.*
5.5 Interim and Bridge Assessment Workflow	Chapter 5.3 Interim and Bridge Assessment Workflow was renamed to Chapter 5.5 Interim and Bridge Assessment Workflow. The content of this chapter is unchanged.
5.6 Assessment Status Dashboard	Chapter 5.4 Assessment Status Dashboard was renamed to Chapter 5.6 Assessment Status Dashboard. The content of this chapter is unchanged.
5.7 MyCSF Assessment Status Notifications	Chapter 5.5 MyCSF Assessment Status Notifications was renamed to Chapter 5.7 MyCSF Assessment Status Notifications. The content of this chapter is unchanged.
6.2 Name & Security	Added criteria 6.2.3 to clarify that only one organization may be listed in the Name & Security Webform and corresponding HITRUST assessment report.
6.5 Scope of the Assessment	6.5.2 – Added expectation that the Assessed Entity includes in the description whether the platform/system incorporates an AI model.
6.7 Factors	6.7.1 – removed the statement that factor questions are not available on i1 or e1 assessments. 6.7.4, 6.7.5, and 6.7.6 – Added criteria to explain the use of the factor webform in i1 and e1 assessments.
7.1 Assessment Scoping	7.1.1 – Added that the installation and configuration must include all primary scope components of the system (e.g., operating system, database, etc.) for the entire 90-day period. 7.1.1 – Added the definition of ‘production environment’ as a footnote.
7.2 Required Scope Components	Added scoping considerations for the AI Security Assessment.
7.3 Carve-outs	Added a note for organizations performing an r2 who need to carve-out a service provider for their ai certification.
8.1 Requirement Statement Background	8.1.1 – Added “NOTE: Regardless of the illustrative procedure wording, the External Assessor must ensure testing coverage of the entire requirement statement” Removed the statement that e1 and i1 assessments do not contain Compliance factors.
9.4 Measured Maturity Level	9.4.2 – Added clarification that the measure review must occur annually at a minimum.
11.2 Testing Requirements	11.2.9 – Added criteria to describe the treatment of the 90-day incubation period

	for implementation when a service provider is responsible for performing a requirement.
11.3 Working Papers & Evidence	11.3.11 – Clarified that sample-based evidence for the same test may be in a zip file or embedded in a spreadsheet if properly labeled to identify each sample item. Added 11.3.16 – “Regardless of the evidence collection method (e.g., manual or automated), the evidence must meet all HITRUST requirements.”
11.4 Population & Sampling	Added additional descriptions for “item-based” and “time-based” testing and populations. 11.4.8 – Added a note describing the process if the External Assessor is unable to select an additional sample during the fieldwork period due to non-performance of the control.
12.4 Reliance on Testing Performed by the Assessed Entity	12.4.10 – Added criteria to clarify that Internal Assessors are not required to test all requirement statements within the assessment. 12.4.13 – Added criteria to clarity that there is no limit to the amount of testing performed by an Internal Assessor that an External Assessor may rely upon.
13.9 CAPs and Gaps	13.9.1 – Added clarification that only the core e1 and i1 requirement statements are included in the CAP determination for e1 and i1 assessments. Inserted 13.9.3 with the AI Security certification CAP and gap logic.
14.1 Quality Assurance Process	In the description of the Core QA sample, explained that in e1 and i1 assessments with included Compliance factors, HITRUST reviews a Core QA sample for each factor.
14.4 Escalated QA	Inserted 14.4.19 to describe the option if HITRUST requests the removal of a compliance factor to remediate an assessment.
15.1 HITRUST Reporting	15.1.2 – Updated to explain that the e1 and i1 certification determination is based only on the core e1 or i1 requirement statements. Added content around NIST 2.0 certification. Added content describing the AI Security certification. Added a description on Insights Report in e1, i1, and r2 assessments.
15.2 Report Re-Issuance	Added 15.2.4 to provide instructions for when an organization has a name change.
15.3 Security Events & Fraud	Added 15.3.2 with the HITRUST definition of a security event.
15.4 Interim Assessment	Added information in the introductory paragraphs around the interim approach for add-on certifications in an r2 assessment (e.g., ai2). Below 15.4.3, included a note specifying the External Assessor approach in an interim if a security event or significant change has been identified. 15.4.9 – Included a requirement that the interim assessment must be submitted on or within 90 days prior to the one-year anniversary of the organization’s r2 certification date.

15.5 Rapid Assessment	Re-titled Rapid Recertification to Rapid Assessment Updated entire Chapter to reflect the ability to perform a rapid assessment on a combined e1 or i1 assessment. 15.5.4 – 15.5.7 – Criteria in the HITRUST CSF requirements included in i1 Rapid Assessments were updated to address the treatment of requirement statements added due to any included Compliance factors. 15.5.8 – 15.5.14 – New sections Leveraging the e1 Rapid Assessment, and HITRUST CSF requirements included in e1 Rapid Assessments containing the following new criteria have been added to address the e1 Rapid Assessment. 15.5.15 – 15.5.20 – Criteria in the Detection of Control Degradation section have been updated to include the e1 assessment.
15.6 Significant Changes	Added a change in AI model as a potential significant change. Added 15.6.3 to reflect additional steps upon notification to HITRUST of potential significant change. Included a description and example for the treatment of changes to secondary scope components.
15.7 Re-certification	15.7.1 and 15.7.2 – Added validity timeframe for add-on certifications.
15.8 Bridge Assessments	15.8.4 – Added bridge approach when the r2 certification contains an add-on certification (e.g., ai2).
15.9 Emerging Mitigation Process	Added new Chapter describing EMP approach and expectations.
15.10 HITRUST Treatment of Non-compliance	15.10.5 – Added criteria to describe exception approval process and requirements. Re-numbered to 15.10 due to new 15.9 Chapter
A-3: Not Applicable (N/A) Examples	Added N/A Example 19165.07e1Organizational.13.
A-4: Never N/A Examples	Added Examples 19180.09z1Organizational.2 and 19249.06b1Organizational.2
A-15: Certification Threshold Scoring Examples	Included an additional example for an i1 or e1 assessment domain average score calculation.
A-16: Sample-based Testing Examples	Added a new appendix to demonstrate the differences between ‘time-based’ and ‘item-based’ populations.
A-17: Expected AI Expertise for External Assessors	Added a new appendix to define expected AI expertise for External Assessors.
A-18: Example Add-on Certification Approach for Existing HITRUST	Added a new appendix to demonstrate an approach for add-on certification for existing HITRUST certifications.

Certifications	
A-19: AI Security Certification Eligibility	Added a new appendix to define eligibility criteria for AI security certification.

B-3: Version 1.2

In addition to minor wording updates and clarification, the changes between version 1.1 and version 1.2 of the Assessment Handbook include the key modifications summarized in the table below.

Chapter	Modification
4.2 Validated Assessments	Added “In an i1 or e1 validated assessment, the requirement statement scores for any added authoritative sources do not impact scoring towards achievement of the underlying i1 or e1 certification.” to the 3rd paragraph (this is not a change from current process)
6.5 Scope of the Assessment	Added criteria 6.5.2 to clarify that the scope entered into the scoping webform must align with the reported scope in the certification.
6.7 Factors	Added 6.7.5 to clarify the current process around scoring for an i1 or e1 when an authoritative source is added as a factor.
7.1 Assessment Scoping	Added a bullet to the top of the list of scoping considerations: “Expectations of the Assessed Entity’s security program by the Assessed Entity, stakeholders relying on the Assessed Entity, and general public”.
7.2 Required Scope Components	7.2.13: Added wording in the example to assist with interpretation.
7.2 Required Scope Components	7.2.15: Added a bullet to top of list of expectations when using a bastion host, jump server, or VDI and excluding those endpoints from testing. Note that this expectation that the technology is restricting data from leaving the environment is not a change from prior expectations.
7.2 Required Scope Components	7.2.16: Added “However, the technology they enable (e.g., USB devices, CD/DVD burners) should be considered when evaluating requirements within this domain.” at the end of the note around use of laptops to clarify.
8.2 Alternate Controls	Added wording in this chapter to assist with interpretation. Updated wording from ‘compensating’ control to ‘alternate’ control to reflect that any variation in the control being applied must address the same risks the current control addresses.
8.3 Not Applicable (N/A) Requirement Statements	Updated wording at the end of the chapter to include references to the new Appendix ‘A-20’.
11.1 Testing Approach	11.1.6: Added this criteria to reflect the current HITRUST evidence expectation when testing on-site observations. (this is not a change from current HITRUST QA expectations)
11.3 Working Papers &	11.3.8: Added “The evidence supporting any observation and/or inspection must be uploaded into MyCSF.” to clarify QA expectations. (not a change for current expected

Evidence	process)
11.3 Working Papers & Evidence	Added section at the end of 11.3 titled “Evidence Generated by Intermediate Software Platforms” which includes additional criteria 11.3.17 through 11.3.26. This is new criteria providing guidance to External Assessors on the procedures which must be performed on evidence when it is generated and provided directly into MyCSF by the intermediate software platform.
11.4 Population & Sampling	In paragraph above 11.4.7, changed ‘collection’ to ‘generation’.
11.4 Population & Sampling	11.4.7: Modified the criteria to avoid the use of only older evidence to validate operation of the control. Changes include: The minimum 90 day population must be consecutive days. Additional criteria to cover 180 days if entire population used is older than 180 days. Added example scenarios to further clarify.
11.4 Population & Sampling	11.4.7: Added a sentence to clarify and confirm that External Assessors may test “time-based” controls meeting this evidence criteria prior to the start of the fieldwork period. (not a change from current process)
12.2 Reliance on Assessment Results Using Inheritance	12.2.1: Updated wording to align the use of inheritance with the new status designations in a certification.
12.2 Reliance on Assessment Results Using Inheritance	12.2.4: New criteria restricting the use of internal inheritance on an expiring assessment without HITRUST approval.
12.2 Reliance on Assessment Results Using Inheritance	12.2.5: New criteria restricting the use of inheritance on identical assessment scopes and types to avoid continually extending a certification using inheritance.
12.2 Reliance on Assessment Results Using Inheritance	12.2.22: New criteria requiring an inheritance provider to use the latest HITRUST certification for inheritance (when there is more than one certification of an identical scope and assessment type).
12.3 Reliance on Audits and/or Assessments Performed by a Third-Party	12.3.4: Added a NOTE on the HITRUST expectation for relying on a third-party report when the report has not yet been issued but the audit has been completed.
12.3 Reliance on Audits and/or Assessments	12.3.8: Added an example.

Performed by a Third-Party	
12.3 Reliance on Audits and/or Assessments Performed by a Third-Party	12.3.10: Added ‘publicly available’ since HITRUST’s expectation of a professional standard is that it is widely available for the general public to review and/or utilize.
12.3 Reliance on Audits and/or Assessments Performed by a Third-Party	12.3.11: Added this new criteria to reflect that HITRUST may reject certain third-party reports if there are quality concerns on the performance of its auditors.
13.9 CAPs and Gaps	13.9.3: Removed the prior workflow diagram and added two new diagrams to reflect the two separate workflows for ai1 and ai2. (not a change from current workflow, prior diagram was incomplete)
13.9 CAPs and Gaps	13.9.9: Added this criteria to clarify the expectations when inheriting service provider scores resulting in CAPs. (not a change from current process)
14.1 Quality Assurance Process	Updated ‘reviews’ to ‘re-performs’ in this chapter to reflect that a QA Analyst re-performs the work done by an External Assessor.
15.1 HITRUST Reporting	Added a section titled “Certification Status” which includes new criteria 15.1.6 through 15.1.8. This describes each of the statuses which a certification may hold, and the expectations for each status.
15.1 HITRUST Reporting	Under “HITRUST AI Security Assessment with Certification (ai1 or ai2)” section, included a link to the HITRUST AI certification help website.
15.3 Security Events & Fraud	15.3.1: Added a sentence with the notification process for a security event.
15.3 Security Events & Fraud	15.3.5: Added this criteria to describe what should be included when reporting a security event to HITRUST.
15.4 Interim Assessment	15.4.6: Added this criteria to require the External Assessor to notify and discuss with HITRUST when control degradation has been confirmed in an interim assessment.
15.4 Interim Assessment	15.4.12: Added this criteria to indicate that External Assessors may not submit interim assessments where testing of the sampled requirements has not been completed.
15.4 Interim Assessment	15.4.24: Added this criteria to reflect that Assessed Entity’s may perform an e1 or i1 assessment in lieu of an interim assessment (if it covers the same scope).
15.5 Rapid Assessments	15.5.10: Added this criteria to clarify when rapid assessments may be generated. (not a change in current process)

15.6 Significant Changes	15.6.3: Added additional wording to this criteria on information to consider and disclose to HITRUST to make the determination of a significant change.
15.6 Significant Changes	15.6.4: Added this criteria to confirm that Assessed Entities may immediately inherit from service providers rather than wait for the 90 day incubation period.
A-20: Never N/A Registry	An appendix which includes a list of core HITRUST requirement statements that are expected to never be scored as Not Applicable (N/A).