HITRUST

Using the Work of Others in a HITRUST CSF Assessment

FAQs

FAQs are specific to this webinar. Visit our General FAQs here.

Q: How does relying on Internal Assessors' work affect the need to perform all testing within 90 days of submission? Does testing have to be less than 90 days old at the time of submission, or at the time of review by the External Assessor?

A: There are two separate 90-day windows: The HITRUST CSF® Internal Assessor's (Internal Assessor) testing window, and the HITRUST CSF External Assessor's (External Assessor) testing window (the former immediately precedes the latter).

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:

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

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

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

All testing performed by the External Assessor in support of the validated assessment must be conducted within 90 days of the submission date to HITRUST®.

Q: Do Internal Assessors have to be HITRUST Certified CSF Practitioners (CCSFPs) ?

A: All Internal Assessors must hold an active CCSFP credential in order 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). Where this 100% hours threshold is not met, the External Assessor should not rely on the Internal Assessor function's testing.

Q: What about a Cybersecurity team that conducts the annual risk assessment? Will they accept any certification? CISA? CISSP? Can a Risk function or Security function be the Internal Assessor as well?

A: Without knowing the specifics of the Cybersecurity team or the annual risk assessment in question, we're unable to provide a definitive response. However, consider the following three points:

1. Through an application process, HITRUST reviews each team seeking to attain the status of Authorized Internal Assessor Function. HITRUST reviews applications to ensure that the following team composition, expertise, and objectivity requirements are met:

   - Team Composition: The Internal Assessor must be competent with respect to the HITRUST CSF, the HITRUST CSF Assurance Program Requirements, and the overall HITRUST CSF Validated Assessment process. To that end, Authorized Internal Assessor Functions must consist of at least two members who are CCSFPs or have a plan in place to become CCSFPs prior to the start of their internal HITRUST CSF Assessment procedures.

   - Expertise Requirements: Each team member must have, at a minimum, two years of information security and/or technical assessment expertise (e.g., security and privacy policy development/implementation, IT audit, risk management, risk assessment/analysis/mitigation). College/university degrees are not considered substitutes for the requirement of at least two years of professional experience.

- Objectivity Verification: The Internal Assessor function must be positioned to reasonably ensure its members are objective of the controls and processes being assessed. "Objectivity" refers to a lack of bias, judgment, or prejudice. Example situations where objectivity is not considered to exist include: a) When the Internal Assessor function and the function being assessed (e.g., IT) roll up to the same executive, and b) When the Internal Assessors are involved in the design, implementation, or operation of the controls being tested.

2. Further, testing performed by Authorized Internal Assessor Functions must meet certain criteria in order to be relied upon by the External Assessor. Specifically, the Internal Assessor's testing must:

- Adhere to HITRUST's Assessment Methodology
- Adhere to HITRUST's documentation requirements
- Be documented within MyCSF® (evidence and scores)
- Be less than 90 days old
- Focus on same scope as External Assessor
- Cover all PRISMA levels for tested requirement statements

3. If all of the above Internal Assessor function and Internal Assessor testing requirements are met, the External Assessor can--at their discretion--rely upon the work of the Internal Assessor function.

Q: Can the External Assessor and Internal Assessor be from the same firm, as long as they are different individuals?

A: Please refer to the "Segregation of Assessor Duties" section of this document:
https://hitrustalliance.net/content/uploads/ExternalAssessorRequirements.pdf

Q: Is it the External Assessors' responsibility to evaluate if the Internal Assessor functions meet all criteria (e.g., be an CCSFP, be non-biased, be qualified to perform assessment, and be licensed to use the CSF commercially)? If so, would there be a checklist?

A: By requiring potential Internal Assessor functions to apply to HITRUST in order to become an Authorized Internal Assessor Function, HITRUST will play a role in ensuring that Authorized Internal Assessors are licensed to use the CSF commercially, CCSFPs, objective from assessed areas, and qualified to perform HITRUST CSF Assessments. However, External Assessors have a role to play as well. Because Authorized External Assessors (not HITRUST) are involved in performing walkthroughs, interviewing control owners, meeting with Internal Assessors, and reviewing Internal Assessor testing, External Assessors are positioned to identify circumstances which do not comply with HITRUST's requirements over using the work of others. When such issues arise, the Internal Assessor and External Assessor teams should discuss the matter and the External Assessors should adjust their work-of-others reliance strategy accordingly.

Q: Does "be documented in MyCSF" refer to "Assessor Notes"?

A: Internal Assessors are held to the same documentation expectations placed upon External Assessors. All assessors are required to document the results of their testing in MyCSF and must either upload or reference supporting evidence in MyCSF. Text areas/comment fields are available in MyCSF for the purpose of communicating testing narratives, test results, and other information helpful to subsequent reviewers of assessment procedures. Testing narratives and other contextual information about an assessor's testing can also be attached within MyCSF as a stand-alone lead sheet, test summary, or testing narrative.

Q: If External Assessors are responsible for the test plans, do the Internal Assessors have to follow our test plans?

A: Internal and External Assessors should work closely in the planning phase of the engagement to clearly define what Internal Assessors will be testing, which should correspond to items on the External Assessor's test plan. Testing that is not on the External Assessor's test plan may not be useful for the External Assessor team.

Q: Should the External Assessors always have to be external to the organization or just external to the areas being assessed, but within the organization?

A: External Assessors must be external to the organization. Internal Assessors may be internal personnel or external personnel.

Q: Could a SOC team that reports up to the same director as the HITRUST team be the Internal Assessor function?

A: (This answer assumes that the acronym "SOC" used in this question stands for "Service Organization Controls" and not "Security Operations Center." Yes, professionals employed by a CPA firm and engaged by a client to perform testing in support of a SOC engagement can also act as members of an organization's Internal Assessor function. However:

- The organization is still required to go through the Authorized Internal Assessor Function application process.
- These professionals cannot also be that organization's External Assessors.

Q: Are External Assessors required to accept Internal Assessor work? Or could the External Assessor choose to only rely on the External Assessor work?

A: No, External Assessors are not required to accept any Internal Assessor work; this is up to the External Assessor's sole discretion.

Q: When will the mapping for using third-party audit reports be required?

A: Such mappings are required for all objects submitted and accepted on or after 12/31/2019.

Q: For "Relying on 3rd Party Reports," are we able to utilize official HITRUST-AICPA mappings for SOC2® Type II (with reference to the mapping step, number 7)?

A: When relying on a SOC2 Type II, the HITRUST CSF to AICPA Trust Services Criteria mappings available at https://hitrustalliance.net/soc2/ can be used as only a *starting point* for the required mapping back to the applicable HITRUST CSF elements included in the scope of the HITRUST CSF Assessment. Because this mapping stops at the HITRUST CSF control reference level (e.g., 01.a Access Control Policy) and at the trust services criteria level (e.g., CC3.2 Risk Identification), it is not alone detailed enough for assessors to identify which of the organization's control activities tested in the SOC2 inspection provide coverage against the HITRUST CSF requirement statements and CSF elements included in the HITRUST CSF Assessment.

Q: Is inheritance materially different than looking at a HITRUST report and typing our procedures into the assessor comments box? Or is this just a streamlined way to rely on HITRUST reports?

A: Inheritance simplifies the process of relying on another HITRUST CSF Report since the scores and subscriber comments are automatically imported into MyCSF. Also, in some cases a customer may only provide the letter of certification rather than the full report--inheritance is likely the only option to obtain the information required to score a particular requirement statement.

Q: Is approving a request for inheritance at the control level, where the parent must accept each one, or can the parent just blanket-approve all requests based on the valid business relationship?

A: An entity approving an inheritance request can approve all requirement statements grouped under the request based upon the validity of the business relationship with the entity requesting inheritance.

Q: If I have a client utilizing a large cloud service provider (CSP) that wants to inherit a control from their CSP's HITRUST assessment, the CSP has to explicitly approve that request to inherit? Won't this heavily slow testing given the size of the large cloud providers with thousands of customers?

A: The CSP must approve each request from tenants. Currently most large CSPs who participate in the program have teams to check the business relationships and approve the inheritance requests, which has not significantly slowed the inheritance process. The HITRUST Shared Responsibilities Working Group, compromised of leading CSPs, is also looking at this issue as well to see if it can be further automated.

Q: Why require 2 CCSFP's for the Internal Assessor function? Does one have to be a Certified HITRUST Quality Professional (CHQP) - or can we leave that to the External Assessor organization?

A: Two is a minimum, not a recommendation or a maximum. All Internal Assessors must be competent with respect to the HITRUST CSF, the HITRUST CSF Assurance Program Requirements, and the overall HITRUST CSF Validated Assessment process. To that end, Authorized Internal Assessor Functions must consist of at least two members who are CCSFPs or have a plan in place to become CCSFPs prior to the start of their internal HITRUST CSF Assessment procedures. The Internal Assessor function is not required to have any CHQPs on staff, as the External Assessor placing reliance on their work in essence performs quality assurance checks on their work during reperformance of their tests.

Q: Is an External Assessor firm automatically an Authorized Internal Assessor Function?

A: No. While outside professionals may serve their clients in the role of Internal Assessors, they would still need to operate within an Authorized Internal Assessor Function in order to have an External Assessor place reliance on their testing. To achieve the Authorized Internal Assessor Function designation, an application process must be completed on a per-client basis.

Q: Is reperformance of Internal Assessor's work by the External Assessor up to the External Assessor's discretion, or does HITRUST have minimum expectations around this?

A: When an External Assessor relies on an Internal Assessor's sample-based test, the External Assessor must reperform 20% of the samples tested by the Internal Assessor (rounding up to the nearest integer).

Q: May we place reliance on Internal Assessors for assessments submitted before 12/31? Even if there's no button in MyCSF, we can add comments describing the Internal Assessor's tests and External Assessor's tests.

A: Please contact HITRUST for any requests to early adopt.

Q: Can you give some examples of mapping for other certifications, i.e. ISO 27001, SOC II?

A: https://www.nist.gov/cyberframework/informative-references/informative-reference-catalog/hitrust-csf-v92-nist-csf-v11
https://hitrustalliance.net/content/uploads/Mapping-of-2017-SOC-2-Trust-Services-Criteria-to-HITRUST-CSF-v9-9.1-and-9.2.xlsx

Q: What are the high-level requirements for registering an Authorized Internal Assessor Function?

A: Application Process: HITRUST performs a review of each Authorized Internal Assessor Function application to ensure that the following team composition, expertise, and objectivity requirements are met:

- Team Composition: The Internal Assessor must be competent with respect to the HITRUST CSF, the HITRUST CSF Assurance Program Requirements, and the overall HITRUST CSF Validated Assessment process. To that end, Authorized Internal Assessor Functions must consist of at least two members who are CCSFPs or have a plan in place to become CCSFPs prior to the start of their internal HITRUST CSF Assessment procedures.
- Expertise Requirements: Each team member must have, at a minimum, two years of information security and/or technical assessment expertise (e.g., security and privacy policy development/implementation, IT audit, risk management, risk assessment/analysis/mitigation). College/university degrees are not considered substitutes for the requirement of at least two years of professional experience.
- Objectivity Verification: The Internal Assessor function must be positioned to reasonably ensure its members are objective of the controls and processes being assessed. "Objectivity" refers to a lack of bias, judgment, or prejudice. Example situations where objectivity is not considered to exist include: a) When the Internal Assessor function and the function being assessed (e.g., IT) roll up to the same executive, and b) When the Internal Assessors are involved in the design, implementation, or operation of the controls being tested.

Items that must be included in an Authorized Internal Assessor Function application:

1. Application Fee of $500, due at the time of application
2. Application Form
3. Resume/bio for each applicant
4. An organizational chart which clearly shows where the proposed Internal Assessment function resides within the organization (e.g., within IT, within the Internal Audit Department which rolls directly up to a subcommittee of the board)

Q: Is this the same process PCI uses for Internal Security Assessors (ISAs)?

A: There are similarities between the HITRUST Internal Assessor Program and the PCI SSC Internal Security Assessor (ISA) Program.

Q: Can an Internal Assessor be objective of certain requirements but not others? For example, someone within the Security team is objective of requirements related to things like storage, privacy, etc., but not requirements related to security tools.

A: Yes. Based upon their reporting relationships to various aspects of the business and based on any non-assessment operational duties they have, an Internal Assessor may not be objective from certain HITRUST CSF areas. As employees of their respective organizations, internal assessment personnel have the purview to assess their organizations against any subject matter they choose (regardless of whether objectivity is met). However, in order for an Internal Assessor's testing to be relied upon by an External Assessor, objectivity must be in place (i.e., the Internal Assessor must be sufficiently objective of the area being assessed).

Where known conflicts exist, these conditions should be communicated to HITRUST in the Authorized Internal Assessor Function application for consideration by HITRUST. If the application is approved despite the identified conflicts, the approval would be provisional--specifically excluding any testing performed by Internal Assessors in those specific areas from being relied upon by an External Assessor. Known conflicts should also be communicated to the External Assessor.

Q: Can External Assessors/External Assessor organizations act as an Internal Assessor for another organization that then uses a separate External Assessor firm to do the assessment?

A: Any firm that is an Authorized External Assessor Organization can serve in the Internal Assessor role for an organization which they are not the External Assessor. However, the Authorized Internal Assessor Function application process must still be performed.

Q: One of the requirements for relying on a third-party audit report is that HITRUST and the External Assessor must be authorized recipients of the report, but does this need to be specified in a contract or letter?

A: Under normal circumstances this could be specified in the report itself, specifically in the section that addresses restrictions on use or authorized users of the report. If necessary or desired, a contractual clause or letter that the report could be shared with HITRUST and the External Assessor would also be acceptable.

Q: If an Internal Assessor is used, do they need to be included on the Assessor Timesheet?

A: Internal Assessors will have their own timesheet within MyCSF separate from the External Assessors' timesheet.

Q: When calculating the percentage of work performed by CCSFPs, do Internal Assessors need to be taken into account?

A: All work performed by Internal Assessors must be performed by CCSFPs. External Assessors continue to need 50% of their hours performed by CCSFPs and do not receive any credit for hours performed by Internal Assessors.

Q: If we detail our test results in our test plan, will the page number in the SOC report that we are mapping the requirement statement to along with highlighting the control in the SOC report be sufficient?

A: HITRUST did not release prescriptive guidance on what the mapping documents should look like; however, keep in mind that there could be multiple test procedures mapped to a control in a SOC 2. Combined with five PRISMA attributes for a requirement statement and the illustrative procedures that support a requirement statement, a mapping at the SOC 2 control level may not contain enough information to show appropriate reliance on the SOC 2.

Q: With inheritance, it states in the requirement statements' inherited assessment must be less than 2 years old, and a HITRUST CSF Interim Assessment must have been completed if required. Based on this comment, does the assessment framework version matter? I.e., can a v9.3 inherit from a v9.2?

A: Inheritance is based upon the requirement statement. If the requirement statement appeared in a particular version and was scored by the other entity, it is eligible for inheritance.