SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Evaluating HITRUST Certifications: e1, i1 and r2

What are the pros and cons of each HITRUST Certification?

When it comes to properly navigating the post **HITRUST** version 11 certification types, understanding the pros and cons of each assessment type enables your organization to select the assessment that best fits your needs. Let us take a closer look at the e1, i1, and r2 assessments.

e1 Assessment (Essential 1-Year)

The **e1 assessment** is the simplest of the three assessments. With 44 control requirements, the e1 assessment lets organizations quickly and efficiently receive a HITRUST certification. The e1 assessment confirms whether the control requirement statements have been implemented. The control requirements for the e1 demonstrate that your organization has reasonably achieved essential cybersecurity hygiene.

For the e1 assessment, both readiness and validated assessment options are possible. Many organizations think of the readiness assessment as a stepping-stone for the validated assessment. While there is no certification granted for the readiness assessment, we still generate a report that helps organizations identify and remediate gaps before performing a validated assessment. Upon completion of a validated assessment, a HITRUST certification is received.

Given the smaller scope of the e1 assessment, there is limited flexibility for the assessed entity. This is most evident when considering the fact that the certification only lasts 1 year. The assessed entity must also select the most current version of the e1 assessment that is available. Further, the assessed entity does not have the option to tailor the control requirements to cover privacy, information protection regulations (e.g., Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS)), or the National institute of Standards and Technology (NIST) Cybersecurity Framework). The e1 assessment lets your organization carve out service providers from testing.

Pros and Cons of the HITRUST e1 Assessment Summary

Pros

✓ Only 44 control requirements, allowing for a quick and efficient certification process
✓ Readiness and validated assessment options possible
✓ HITRUST certification granted through the validated assessment
✓ Third party service providers can be carved out

Cons

x Certification lasts for 1 year
x Limited flexibility in tailoring control requirements
x Shows only essential cybersecurity practices are in place
x The maturity level tested only shows whether the control requirements have been implemented

i1 Assessment (Implemented 1-Year)

The i1 assessment is an expansion of the e1 assessment. Covering 182 requirements, the i1 assessment includes the same 44 e1 control requirements, plus another 138. The i1 assessment provides a moderate level of assurance that your organization has implemented leading cybersecurity practices against a broader range of cyber threats when compared to the e1 assessment. Again, both readiness and validated assessment options are possible for the i1 assessment.

The **i1 assessment** offers some further flexibility than the e1 but share many of the same limitations. Like the e1, service providers can be carved out, and control requirements cannot be tailored to cover privacy, information protection regulations, or the NIST Cybersecurity Framework. Further, the certification for the validated assessment only lasts for 1 year.

Where the i1 offers greater flexibility is in the rapid recertification process. After your organization obtains the i1 certification, for the following year, you can be evaluated based on a selection of i1 requirement statements instead of being tested against all requirement statements again. This reduces the amount of testing required to complete the assessment.

The rapid recertification results in the same i1 assessment reports and i1 certification that is valid for one year. To use the rapid recertification process, there must not have been any significant changes to your organization's control environment since the last i1 assessment. HITRUST defines a significant change as any of the following: The i1 assessment is an expansion of the e1 assessment. Covering 182 requirements, the i1 assessment includes the same 44 e1 control requirements, plus another 138. The i1 assessment provides a moderate level of assurance that your organization has implemented leading cybersecurity practices against a broader range of cyber threats when compared to the e1 assessment. Again, both readiness and validated assessment options are possible for the i1 assessment.

The i1 assessment offers some further flexibility than the e1 but share many of the same limitations. Like the e1, service providers can be carved out, and control requirements cannot be tailored to cover privacy, information protection regulations, or the NIST Cybersecurity Framework. Further, the certification for the validated assessment only lasts for 1 year.

Where the i1 offers greater flexibility is in the rapid recertification process. After your organization obtains the i1 certification, for the following year, you can be evaluated based on a selection of i1 requirement statements instead of being tested against all requirement statements again. This reduces the amount of testing required to complete the assessment.

The rapid recertification results in the same i1 assessment reports and i1 certification that is valid for one year. To use the rapid recertification process, there must not have been any significant changes to your organization's control environment since the last i1 assessment. HITRUST defines a significant change as any of the following:

1. Moving an on-premises data center to a public cloud environment
2. Moving an in-scope facility to a different physical location
3. Decommissioning a data center and moving all assets to a different data center
4. Replacing any of the in-scope platforms that were included in the previous i1 report
5. Changing an in-scope system to use a different back-end system
6. Moving away from an outsourced IT model by standing up an internal IT function
7. Changes in responsibility for performance or oversight of the in-scope control activities (outsourcing, insourcing, or change in service providers)
8. New functionality in an in-scope platform enabling it to be accessed from a public location
9. Acquisitions, divestures, mergers, or other changes in control of an Assessed Entity where controls over in-scope systems are no longer being operated bt the Assessed Entity who originally obtained the certified report
10. Changes in a "Factor" question response within the validated assessment

Pros and Cons of the HITRUST i1 Assessment Summary

Pros

✓ More expansive than the e1 assessment
✓ Readiness and validated assessment options possible
✓ HITRUST certification granted through the validated assessment
✓ Third party service providers can be carved out
✓ Rapid Certification process is available after your organization obtains the i1 certification

Cons

x More extensive than the e1 assessment
x Certification lasts for 1 year
x Limited flexibility in tailoring control requirements
x Must use the most current version of the assessment at the time of creation
x The maturity level tested only shows whether the control requirements have been implemented

r2 Assessment (Risk-based 2-year)

The **r2 assessment** is the most comprehensive of the three assessment types and offers the most flexibility. The r2 assessment encompasses the same control requirements as the e1 and i1 assessments, while also incorporating additional controls based on data volumes handled by your organization, applicable regulatory compliance, and other risk factors relevant to your organization.

Further, not only does the r2 assessment test the control requirement implementation status, but it also tests whether a policy or standard is in place for the control and whether the process supports the policy. There are 2 additional maturity levels that can be added as part of a r2 Assessment.

The first is “measured,” which looks at whether the control requirement is being tracked and tested by management to ensure the control is operating. The second is “managed,” which looks to see whether necessary corrective actions are being performed on the measured results. The r2 assessment provides a high level of assurance on the design and implementation of the leading cybersecurity practices and additional risk-based controls.

As a part of the further flexibility offered by the r2 assessment, the control requirements for the assessment can be tailored to cover privacy and information protection regulations. Upon receiving the r2 certification of a validated assessment, HITRUST will also issue your organization a certification over the NIST Cybersecurity Framework. Where flexibility is limited for an r2 assessment is that third party service providers cannot be carved out of testing.

Like the e1 and i1 assessments, the r2 offers both a readiness and validated assessment option type. It is not required for your organization to select the most current version of the r2 assessment at the time of assessment creation.

Due to the r2 being the most extensive assessment, the certification for the validated assessment lasts for 2 years, but an interim assessment is required after 1 year. The interim assessment takes 1 randomly selected requirement statement from each domain to be fully retested and rescored to ensure that certification requirements are maintained. The interim assessment also reviews any corrective action plans that were identified during the initial testing to ensure that issues were either remediated or that satisfactory progress has occurred.

Pros and Cons of the HITRUST r2 Assessment Summary

Pros

- ✓ Provides the highest level of assurance when compared to the other assessment types
- ✓ Certification lasts for 2 years
- ✓ Interim testing reduces the amount of testing needed for year 2
- ✓ HITRUST issued certification is provided over the NIST Cyber Security Framework
- ✓ Readiness and validated assessment options possible
- ✓ HITRUST certification granted through the validated assessment
- ✓ The r2 assessment offers 5 levels of maturity to test in policy, process, implementation, measured, and managed (measured and managed are optional)
- ✓ Assessment can be tailored to include privacy and information protection regulations

Cons

- x Most extensive testing
- x Third party service providers cannot be carved out

If your organization is considering obtaining a HITRUST certification, Schneider Downs can assist you at any point through the process. We can help further discussions to determine which assessment is best for your organization, guide you through a readiness to gain the confidence in obtaining a certification, as well as perform the validated assessment itself for your organization. To learn more, visit our **HITRUST** services page.

About Schneider Downs IT Risk Advisory

Schneider Downs' team of experienced risk advisory professionals focus on collaborating with your organization to identify and effectively mitigate risks. Our goal is to understand not only the risks related to potential loss to the organization, but to drive solutions that add value to your organization and advise on opportunities to ensure minimal disruption to your business

To learn more, visit our dedicated **Risk Advisory Service** page or contact the team at **contactsd@schneiderdowns.com**.

Pittsburgh
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

Columbus
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

Metropolitan Washington
1660 International Drive
Suite 600
McLean, VA 21102
P 571.380.9003

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

HITRUST Assessment Types

CHARACTERISTIC	HITRUST ESSENTIALS, 1-YEAR (E1) ASSESSMENT FOUNDATIONAL CYBER-SECURITY	HITRUST IMPLEMENT-ED,1-YEAR (I1) ASSESS-MENT LEADING PRAC-TICES	HITRUST RISK-BASED,2-YEAR (R2) ASSESSMENT EXPANDED PRACTICES
HIGH-LEVEL			
Purpose	Provides entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place	Provides a moderate level of assurance that addresses cybersecurity leading practices and a broader range of active cyber threats than the e1 assessment	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
Number of HITRUST CSF Requirements on a 2-Year Basis	44 (Year 1), 44 (Year 2)	182 (Year 1), ~60 (Year 2 with Rapid Recertification)	~375 Average (Year 1), ~40 Average (Year 2 Interim Assessment)
Readiness assessments and validated assessments (certifications) can be performed	Yes		
Length of certification	1 year	1 year, 2 years with Rapid Recertification	2 years, with Interim Assessment
Maturity Levels Considered	Implemented	Implemented	Policy, Procedure, and Implemented
Policy and Procedure Consideration	Minimal	Minimal	Thorough
Level of Security Assurance	Low	Moderate	High
Flexibility of Control Selection (Can be tailored to optionally convey assurances over dozens of information protection regulations and standards (e.g., HIPAA, NIST CSF, PCI DSS).	No Tailoring	No Tailoring	Tailoring
Evaluation Approach	1x5: Implementation control maturity level	1x5: Implementation control maturity level	3x5 or 5x5: Control maturity assessment against either 3 or 5 maturity levels
HITRUST CSF requirements performed by the assessed entity's third party service providers (such as cloud service providers) on behalf of the organization can be carved out / excluded from consideration	Yes	Yes	No
Requires an Authorized HITRUST External Assessor Organization to inspect documented evidence to validate control implementation	Yes		
Leverages the HITRUST Control Maturity Scoring Rubric	Yes		
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 (RDS)	Yes		
Can result in a HITRUST-issued certification over the NIST Cybersecurity Framework	No	No	Yes
Can be bridged through a HITRUST bridge certificate	No	No	Yes
Threat-adaptive assessment	Yes		
Assessor's validated assessment fieldwork window (maximum)	90 days		
Alignment with Authoritative Sources	CISA Cyber Essentials, Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations, NIST 171's Basic Requirements, NIST IR 7621	NIST SP 800-171 (Basic and Derived Requirements), HIPAA Security Rule, and HICP for Medium-Sized Organizations	NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, PCI DSS, GDPR, and Dozens of Others
Must use the most current version of the CSF available at time of assessment creation.	Yes	Yes	No