cycore

FREE DOWNLOAD

2026 EDITION

HITRUST CSF

# HITRUST Readiness Guide

Cycore's guide to the three HITRUST assessment types. Compare e1, i1, and r2, settle version and scope first, and take the right questions to your assessor.

PREPARED BY

Cycore

ONLINE

cycoresecure.com

Cycore wrote this guide for health care and technology teams weighing a HITRUST assessment, usually because a customer or contract asked for one. HITRUST has three assessment types: e1, i1, and r2. Which one you need depends on what your customers and contracts require, which systems and data are in scope, and how much assurance you have to show. Settle those before anyone creates an assessment in MyCSF, HITRUST's assessment platform, and confirm the CSF version first.

## Check the CSF version first

As of 2026-09-01, HITRUST CSF v11.8 is the current release for newly created e1 and i1 assessments. HITRUST transition rules can affect an assessment already created under v11.7. Confirm the version and deadline in MyCSF and the current HITRUST advisories before relying on this guide.

HITRUST announced CSF v11.8.0 on 2026-05-07 and changed the e1 and i1 baselines with it (HITRUST advisory HAA 2026-002, CSF v11.8.0 release). From that day, every new e1 and i1 assessment has to be created on v11.8.0. An e1 or i1 assessment already created on v11.7.0 can still be submitted. HITRUST has said it will announce the v11.7.0 submission deadline at least 90 days in advance (HITRUST advisory HAA 2026-003, v11.7 creation deadline for e1 and i1 assessments). If you already have an assessment object open, ask your assessor which version it's on and what that deadline means for your submission date.

## The three assessment types

The descriptions and counts below are HITRUST's, from its 2026 Trust Report. They move with CSF releases, so read them with the version note above.

| | e1 | i1 | r2 |
|---|---|---|---|
| Intended assurance depth | Entry-level. Shows that essential cybersecurity hygiene is in place. | Moderate. Covers a broader range of active cyber threats than e1. | HITRUST's highest level of assurance. |

| | e1 | i1 | r2 |
|---|---|---|---|
| Scope | 43 requirement statements (2026 Trust Report). | 182 requirement statements (2026 Trust Report). | Tailored to your environment. There's no fixed total. |
| Validation | Tested by an authorized HITRUST External Assessor, then reviewed by HITRUST's QA team before certification. | Tested by an authorized HITRUST External Assessor, then reviewed by HITRUST's QA team before certification. | Tested by an authorized HITRUST External Assessor, reviewed by HITRUST's QA team before certification, with an interim assessment at the one-year mark. |
| Certification period | One year. | One year. | Two years. |
| Tailoring | A predefined set. HITRUST changed it in the v11.8.0 release. | A predefined set. HITRUST changed it in the v11.8.0 release. | Your risk analysis sets the requirement statements from data volumes, regulatory requirements, and other risk factors. |

Source for the table: the HITRUST 2026 Trust Report for the descriptions, the counts, the QA review, and the interim assessment, and HAA 2026-002 for the baseline changes by release.

In 2025, an r2 validated assessment averaged 387 requirement statements (HITRUST 2026 Trust Report). That's an average across 2025's r2 validated assessments, and it's context only. Your own r2 count comes out of your risk analysis in MyCSF.

## How to choose

Start with what your customers and contracts require. Ask the person who raised HITRUST which assessment type they'll accept, and get the answer in writing. If nobody has named r2, i1 gives you a fixed scope and a moderate level of assurance, and e1 fits a first HITRUST assessment or a small, well-defined environment. An r2 fits complex environments, large volumes of PHI, or a customer who wrote r2 into the contract. No assessment type automatically

satisfies every regulator, customer, or contract, so the requirement has to come from whoever is asking.

## Where the requirement statements come from

The HITRUST CSF is a certifiable control framework that HITRUST builds from other standards, best-practice frameworks, and regulations, which it calls authoritative sources. As of 2026-09-01, the CSF incorporates more than 60 authoritative sources (HITRUST 2026 Trust Report). The report's own examples: NIST Cybersecurity Framework v1.1 and 2.0, NIST SP 800-53 Revisions 4 and 5, CIS Critical Security Controls v7.1, ISO/IEC 27001:2022 and 27002:2022, HIPAA at 45 CFR Part 164 Subparts C, D, and E, and the AICPA Trust Services Criteria for Security, Confidentiality, and Availability. You can select one or more of those sources into your assessment, which adds that source's requirements to what gets tested. The number of sources changes with releases, so check the current CSF before you quote it to anyone.

## Version and scope questions to settle first

Settle these with your team before you create the assessment object. Each one changes the scope, the count, or the deadline. A GRC platform tracks evidence against the scope you set in MyCSF, so make these decisions before you turn on its HITRUST module.

- **CSF version.** Confirm in MyCSF which version your object uses. New e1 and i1 objects are created on v11.8.0, and an existing v11.7.0 object has a submission deadline that HITRUST will announce at least 90 days ahead.
- **Assessment type.** Get the type the customer or contract requires in writing before you pick one.
- **Systems, facilities, and third parties.** List every system, location, and service provider that creates, receives, maintains, or transmits the data in question. For an r2, this list feeds the risk analysis that sets the count.

- **Risk factors.** For an r2, work out the data volumes, regulatory requirements, and other risk factors you'll enter, because the risk analysis sets your requirement statements from them.
- **Authoritative sources.** Decide whether to select a source such as HIPAA or NIST into the assessment, and check whether the customer expects one.
- **Inheritance.** List the controls you can inherit from your cloud provider, vendors, or a prior HITRUST assessment, and the ones that stay yours. Inheritance runs through a request and approval process and covers only what the provider's own validated assessment covers (HITRUST 2026 Trust Report).
- **Evidence owners.** Put a name on the evidence for each domain now, so the readiness assessment has someone to ask. HITRUST's 2026 Trust Report says Access Control was the lowest-scoring e1 domain for the third year in a row. It also says i1 and r2 organizations have struggled with Data Protection and Privacy over the same three years. Those two domains are where we'd start.

## Common mistakes we see

- **Choosing r2 when nobody asked for it.** Unless a customer or contract names r2, an i1 may give you the assurance level your buyers accept, with a fixed 182-statement scope (2026 Trust Report). Check the requirement before you commit to a two-year, tailored assessment.
- **Underestimating the evidence.** Every requirement statement in scope needs artifacts: policies, procedures, configuration exports, screenshots, logs. Teams that leave evidence collection to the end are the ones that stall. Start collecting when you set the scope, and give every artifact an owner.
- **Getting inheritance wrong in either direction.** Skipping inheritance means testing controls your cloud provider already had validated. Assuming inheritance covers more than it does leaves gaps for the assessor to find. Ask your assessor to confirm what each provider's validated assessment covers before you plan your testing.

- **Treating HITRUST as your HIPAA program.** A HITRUST certification maps to HIPAA and doesn't replace it. You still owe the HIPAA risk analysis, business associate agreements, and the rest of your HIPAA program.
- **Skipping the readiness assessment.** Going straight to the validated assessment means the assessor finds your gaps during testing. A readiness assessment, run against the same requirement statements before the validated assessment starts, finds them first and gives each one an owner.

## Questions to bring to your assessor

Take these into your first conversation with an authorized HITRUST External Assessor, along with your answers to the seven decisions above.

- Which CSF version will our assessment be created on, and what happens to an object we already created on v11.7.0?
- Given the assessment type our customers and contracts name, would an e1 or i1 be accepted where we assumed r2?
- Which systems, facilities, and third parties belong in scope, and for an r2, how does each one change the requirement statement count?
- For an r2, which data volumes, regulatory factors, and other risk factors will the risk analysis use, and can we see the resulting requirement statements before we commit?
- Which authoritative sources should we select into the assessment, and what does each one add to the testing?
- Which controls can we inherit from our cloud provider or vendors, and what does inheritance leave with us?
- What evidence will you test for each requirement statement, and in what form?
- If we choose an r2, what does the interim assessment at the one-year mark involve?

- If a domain falls short of the certification threshold, what happens, and how do corrective action plans work?
- When should we reserve our QA slot with HITRUST, and what does the reservation commit us to?
- If HITRUST releases a new CSF version while our assessment is open, what changes for us?

> ### Anterior's result
>
> *Cycore reports that Anterior became HITRUST-ready within seven weeks.*
>
> Read the case study

## More Cycore guides and checklists

- SOC 2 Readiness Checklist
- ISO 27001 Gap Assessment
- HIPAA Compliance Checklist
- AI Governance Starter Kit

## Next step

**Talk to Cycore about your HITRUST assessment**