SCHNEIDER DOWNS

Big Thinking. Personal Focus.

The HITRUST Journey:

7 Steps to Expect Before You Certify

TABLE OF **contents**

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

The HITRUST Journey: 7 Steps to Expect Before You Certify

HITRUST isn't just a compliance checkbox. It is proof that your organization meets a high standard of security and risk management. Certification requires a rigorous, evidence-based process that requires planning, cross-functional coordination, and genuine readiness. Certification isn't simply given. It's earned.

Here are the 7 key steps in your journey to certification.

Step 1: Procure an Experienced Translator

HITRUST has its own language, and if you don't speak it, you're traveling abroad without a reliable translator. You wouldn't want to be stuck in a foreign country without a card showing your hotel address in different languages, and you wouldn't want to get caught roaming the vast lands of the HITRUST CSF without a HITRUST Authorized External Assessor. After all, they're the one who ultimately submits validated assessments to HITRUST for quality review. That means they know the answers to the test that you will have to pass to obtain certification. Engaging an external assessor firm early on in your journey will save you and your team days of wandering unfamiliar areas for a semblance of familiarity.

Step 2: Define Scope and Objectives

To define your scope and objectives, you will need to answer the following questions:

- What systems, data, and services are in scope? While this is a seemingly simple first question, it is everything. In fact, for experienced external assessors, it's only the first instance in which this question will be asked. It continues to be revisited time and time again throughout your HITRUST journey to ensure you're doing the right amount of assurance – not too little nor too much.
- Is certification motivation driven by prospective or current customer demands, market positioning and enablement, or internal maturity factors?
- What level of assurance do you need? Minimal, moderate, or high?
- What assessment type should you choose (e1, i1, r2, etc.)? Check out our more detailed breakdown of the assessment types here. Know that many organizations treat the e1, i1, r2 certifications like a maturity ladder. It benefits your organization to do so, as with each step in the ladder you will experience more. More controls, more attributes, more associated fees – with the same rigor. So, start small if you can and get good at the basics like anything else.
- Are any additional scoping factors applicable (HIPAA, State-level regulations, AI Risk Management, etc.)? If you end up choosing the r2 path, you will be subject to a more elaborate scoping process where a handful of additional scoping factors (Organizational, Technical, Regulatory, etc.) are necessary to tailor your assessment.

How Long Does This Phase Take?

This phase is generally completed in a matter of weeks but does require some technical validation of your infrastructure and systems.

Step 3: Readiness Assessment

Before a validated assessment (certification), most organizations complete a readiness phase to:

- Perform a gap analysis against HITRUST CSF controls and identify missing policies, procedures, and technical proof. This is where you'll work through the questions on the test to explain how you'll answer it come validated assessment time. It's a full walkthrough of your game plan, packed with a playbook on how to handle inevitable audibles in the thick of auditor testing.
- Prioritize remediation tasks by effort and risk. Controls are required to be "implemented" for 60-90 days, depending on the type of control, prior to initiating a validated assessment period. That is what HITRUST refers to as the "Incubation Period." Therefore, it's important to prioritize gap remediation to ensure your roadmap can be accomplished as efficiently as possible. Assessors should also be able to identify required gaps vs optional enhancements. The enhancement are things that are nice to have in the future, but not necessary to achieve compliance and certification now.

How Long Does This Phase Take?

This phase generally takes anywhere from one to three months, depending on the complexities of your infrastructure and systems.

Remediate and Align

This is where the heavy lifting happens. You're now armed with the honey-do list of gaps to close, along with a prioritized roadmap. This phase is about executing the plan and checking back with your audit partner to ensure you did it the right way. In this phase, you will:

- Update or develop formal documentation – policies, procedures, standards, etc. Templates go a long way and good audit partner firms will have a library to get you started.
- Implement technical safeguards (MFA, logging & monitoring, encryption, etc.). This is a wide-ranging task, based on the number and type(s) of gaps previously identified. It could be as simple as enabling a dormant configuration to be as extensive as implementing a new SDLC process and supporting systems.
- Assign control owners, prepare evidence for each control, and align with your external assessor firm on its completeness and accuracy. Consider this an extension of the gap assessment that was previously completed to further validate that your newly remediated gaps are indeed remediated in the manner they'll be tested.
- Develop testing efficiencies to allow for automated evidence collection and evaluation. Consider how you can integrate compliance and security operations in a continuous, systematic way, moving beyond point-in-time assessments to a model of continuous monitoring and risk mitigation. Good external assessor firms will be able to realize these efficiencies and relay discounts based on their own reduced audit efforts.

Step 4: 90-day Incubation Period

Once all your readiness gaps have been closed and “implemented” (Congrats, you get a free 90-day vacation!) Well, sort of…HITRUST requires a 90-day “incubation period” for controls to be implemented (or 60 days for policies/procedures), before you can officially start your 90-day examination. In practice, you can begin that 90-day incubation clock as soon as the last gap is closed.

During this period of peace, it’s the perfect opportunity to book that HITRUST QA reservation. Once your assessment is scoped and loaded into MyCSF, you’ll be able to reserve a date on the HITRUST QA Team’s calendar, much like that of an online dinner reservation (the kind of one that takes your credit card preauthorization). This is a key step to ensure you meet your timeline as the HITRUST QA Team’s availability fluctuates based on demand. You don’t want to overpromise your delivery date if the QA team can’t meet your needs.

Additionally, the assessed entity can begin to work with the external assessor to preload MyCSF. While most of the controls will require time-stamped evidence from within your 90-day examination period, there’s still plenty your teams can do ahead of time to make the examination period run more smoothly. This includes tasks like:

- Answering all pre-assessment questions, organization information, assessment options, assessment scope, scoping factor
- Drafting all requirement statements and completing the validated report agreement
- Validating your internal documentation paths to ensure smooth and possibly automated evidence collection

Step 5: The Validated Assessment

At this stage, the External Assessor performs fieldwork and tests whether your claims survive contact with scrutiny.

- **Performing Validation:** The assessor validates pre-assessment scores, links required documents, executes the test plan, and completes the QA checklist. This is where most of the hours are spent. Performing validation is the most grueling part of the campaign: assessors spend days and weeks combing through evidence, re-scoring pre-assessment judgments, and linking every screenshot, configuration, and attestation to the framework. The test plan drives hundreds of small exchanges, including requests for logs, clarification emails, system demos, and each one consumes time from both the assessment team and internal staff.
- **Assessment Results Review:** Once the bulk of validation is complete, the work shifts to the assessment results review. The entity and assessor sit shoulder-to-shoulder to acknowledge findings, accept wins and record errors.
- **Inputting Corrective Action Plans (CAPS) & Signing Rep Letter:** CAPS are carved into the record, a pledge that gaps will not be left unguarded. The management representation letter is signed.
- **Reviewing CAPs:** The assessor validates these commitments, ensuring every promise is backed by real action.

This is no longer theory on paper. It is proof standing under fire. The validated assessment reveals not just the state of your controls, but the strength of your coordination under pressure.

Step 6: HITRUST Quality Assurance Review

With the assessment complete, the campaign now passes to final judgment. Your file advances to HITRUST, where a tribunal dissects *a sample of* every word, every score, every justification. This is the trial by fire, a distant but unyielding review where survival depends on precision.

- **Performing Check-In:** HITRUST performs automated quality assurance (QA) checks, scanning for inconsistencies in documents and evidence.
- **Addressing Check-In Tasks:** If issues arise, new tasks are assigned, and the entity and assessor must respond timely.
- **Reviewing Pending Check-In Tasks:** HITRUST evaluates the fixes. If gaps remain, the engagement loops again until resolution.

Only when the defenses hold does the assessment move forward:

- **Pending QA:** The assessment sits in waiting, queued for its reserved QA block.
- **Performing QA:** The QA Analyst begins the full, impartial review of ratings, citations, and evidence under the microscope. This includes a review of a sample of control requirements in a live screen-sharing session with the External Assessor team. In this live session, the control references are randomly selected immediately before the call, and the External Assessor team shares their screen and walks the HITRUST QA Analyst through each evaluative element and the associated evidence for each sampled control requirement.
- **Escalated QA:** If numerous and/or severe concerns are identified during QA, the Escalated QA phase will be triggered. This warrants an additional, internal review conducted by the HITRUST quality team and is more intensive than the standard QA process. Common reasons for Escalated QA include significant scoring inaccuracies, insufficient evidence to prove implementation, lack of rigor or testing inaccuracies, or extensive gaps.
- **Addressing QA Tasks:** More tasks may follow; remediation and clarification continue under fire. Only when every task is closed does the review advance.

But the journey is not finished. Reports must be drafted, revised, and approved:

- HITRUST prepares and executives review the draft deliverables; the entity approves or requests revisions.
- Additional drafts, revisions, and reporting tasks cycle through until every open question is resolved.

This quality assurance review is relentless, and impartial. It demands not just accuracy, but endurance. The patience to close loop after loop until applicable weaknesses are fully understood.

Step 7: Certification & Beyond – The Standard of Trust

Finally, the verdict: certification is granted… or… not. *Regardless*, a validated assessment report is published, with its certifying decision one way or the other. On the one hand, The Standard of Trust earned. On the other, Trust may cease to exist for now.

But the journey does not end here, it changes form. Certification is not a trophy to display; it is a banner raised over your organization, a signal to the market that you have endured and can be trusted.

- **Validity:** 1 year for e1 and i1 and two for the r2. Interim reviews and recertifications loom on the horizon.
- **Continuous Vigilance:** New controls, new threats, new regulations will arise. Certification is not the end but the beginning of stewardship.
- **Sustained Discipline:** Prepare for each cycle as if it were your first; remediate continuously; embed resilience into the daily rhythm of operations.

Those who treat certification as a finish line often falter; those who treat it as a campaign standard to uphold lead their industries forward with credibility and strength. Certification is a call to remain vigilant, to adapt as threats evolve, and to prove, again and again, that trust is not a point in time, but a posture of resilience.

How Can Schneider Downs Help?

As an Authorized HITRUST External Assessor Firm, Schneider Downs has a strong track record with HITRUST protocols, providing trusted guidance and support throughout the certification process. For more information, contact our HITRUST team at **contactsd@schneiderdowns.com**.

About 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.