QOS MSP
Managed Services

HITRUST COMPLIANCE
STRATEGY GUIDE

The CSF, e1 vs i1 vs r2, real timelines and costs — what IT leaders should know before committing to certification.

+1 (877) 800-7672

www.qosmsp.com

The HITRUST Compliance Strategy Guide

Somewhere in your pipeline, a customer has asked for your HITRUST certification — or is about to. Before you commit six figures and six months, you should know what HITRUST actually involves, which assessment you really need, and where the costs hide.

This guide is the plain-English version: what the framework is, how the three assessment types differ, the readiness roadmap we use with clients, and honest answers on timeline and budget.

1. What HITRUST Actually Is — and Who Demands It

HITRUST maintains the CSF (Common Security Framework) — a certifiable framework that harmonizes HIPAA, NIST, ISO 27001, PCI DSS, GDPR, and dozens of other standards into one control set. Unlike HIPAA, which has no official certification, HITRUST certification is a formal, externally validated credential: an authorized assessor firm tests your controls, and HITRUST itself reviews the results and issues the certification.

Who demands it: hospitals and health systems of their vendors, payers and TPAs of their partners, and increasingly any enterprise vendor-risk program that touches health data. For many deals it has quietly moved from “nice to have” to a condition of the contract.

The Rule:

HITRUST is usually bought to win and keep contracts — treat it as a revenue project with a security dividend, and scope it around what your customers actually require.

2. e1 vs i1 vs r2 — Choosing the Right Assessment

- **e1 (Essentials)** — a streamlined annual assessment of foundational cyber-hygiene controls (a few dozen requirements). Fastest and least expensive; good entry-level assurance, and often enough for smaller vendors.
- **i1 (Implemented)** — moderate assurance across a substantially larger, threat-adaptive control set, assessed annually. The middle path for vendors whose customers want more than essentials.
- **r2 (Risk-based)** — the comprehensive option: controls tailored to your scope, regulatory obligations, and risk factors, typically hundreds of requirements, on a two-year cycle with an interim review. When a large health system says "HITRUST certified," this is usually what they mean.

The Rule:

Buy the assurance level your customer contract actually names. Ask them — don't default to r2 because it sounds safest; the jump in cost and effort is large.

3. The Readiness Roadmap

1. **Scope it** — which systems, locations, and vendors touch the sensitive data. Tight scoping is the biggest cost lever you control.
2. **Readiness assessment** — measure your controls against the CSF and get a risk-ranked gap list.
3. **Remediate by risk** — close the gaps in priority order; this is where most of the calendar goes.
4. **Build evidence discipline** — collect proof as controls operate, not in a panic before the assessor arrives.
5. **Validated assessment** — your authorized assessor firm tests; HITRUST reviews and certifies.

The Red Flag:

Booking a validated assessment before a readiness assessment. Failing controls in front of your assessor is the most expensive way to discover a gap.

4. Timelines and Cost Drivers, Honestly

Timeline: an e1 can move in a few months; most first-time i1 and r2 certifications run six months to a year or more — remediation dominates, not paperwork.

Where the money goes:

- **Assessment type and scope** — the levers behind every other number
- **Assessor firm fees** — the external validation engagement
- **HITRUST's own platform and certification fees**
- **Remediation work** — the largest and most variable line
- **Internal time** — evidence, coordination, and control ownership
- **Program management** — keeping all of it moving

The Rule:

The certificate's fixed costs are quotable up front; remediation is where budgets blow up. A readiness assessment prices the whole journey before you commit to any of it.

5. Keeping Certification After Year One

Certification is not a trophy; it's a cycle. i1 recertifies annually; r2 requires an interim assessment at year one and full recertification at year two. Meanwhile controls drift, staff turn over, vendors change, and evidence has to keep accumulating.

What keeps it: quarterly control checks, evidence collected as you go, vendor reviews on a schedule, and one owner for the program.

The Red Flag:

A compliance binder that only gets opened the month before an assessment.

6. How QOS MSP Helps

We carry organizations through the full journey — readiness assessment, risk-ranked remediation, documentation, validated-assessment preparation, and the ongoing program management that keeps certification alive — at flat Compliance-plan rates, founder-led since 2007. One honest boundary: validated assessments must come from an authorized HITRUST assessor firm. We don't replace them — we make sure they find what they expect to find.

The Final Word

The organizations that struggle with HITRUST treat it as an audit event. The ones that sail through treat it as a program that happens to produce a certificate.

Next Step:

Ask your customer which assessment they require, then get a readiness assessment scoped. QOS MSP will do that scoping call at no cost: call +1 (877) 800-7672 or visit www.qosmsp.com.