

HITRUST Certification Levels

Choosing the right HITRUST Certification for Your Organization

HITRUST enables organizations to select the level of assurance that aligns with their current needs, whether establishing a foundational security baseline, demonstrating implemented best practices, or achieving comprehensive, risk-based validation.

As your organization grows, your certification can evolve with you.

With the addition of AI-focused assurance, HITRUST also supports organizations navigating emerging risks, ensuring your certification strategy not only reflects where you are today, but where your organization is headed.

e1 Certification

- Fixed set of foundational controls
- No tailoring or extensive risk analysis
- Rapid assessment timeline

Best Fit:

- Early-stage companies
- Organizations beginning compliance journey
- Vendors with minimal data exposure

r2 Certification

- Fully tailored control requirements
- Incorporates organizational risk factors
- Most rigorous validation and testing

Best Fit:

- Enterprises
- Large healthcare organizations
- Highly regulated industries (financial services, gov contractors)

i1 Certification

- Expanded control set
- Focus on operational maturity
- No extensive risk tailoring

Best Fit:

- SaaS companies
- Organizations handling sensitive but not highly regulated data
- Mid-market organizations scaling compliance



Certification Levels at a Glance

Certification Level	Assurance Level	Ideal For	Assessment Rigor	Validity Period
e1 (Essential)	Foundational	Low-risk organizations or startups	Low	1 year
i1 (Implemented)	Moderate	Organizations with moderate risk exposure	Moderate	1 year
r2 (Risk-based)	High	High-risk or highly regulated environments	High	2 years (with interim)

HITRUST AI Certification

The HITRUST AI certification extends traditional security and compliance principles to artificial intelligence systems, addressing emerging risks tied to AI development, deployment, and governance.

Key Focus Areas:

- AI governance and accountability
- Model risk management
- Data integrity and bias mitigation
- Secure AI lifecycle (development - deployment - monitoring)
- Third-party AI risk

Why It Matters:

- Aligns AI usage with regulatory expectations
- Builds trust in AI-driven products
- Supports emerging standards like ISO/IEC 42001 and NIST AI RMF

Best Fit:

- Organizations building AI into products/services
- Companies using generative AI or ML models
- Enterprises with AI governance requirements



*Sample image shown. Final certificate badge design may vary.

Which Level is Right for You?

Feature	e1	i1	r2	AI Certification
Risk-Based Controls	No	Limited	Yes	Yes (AI-specific)
Control Customization	No	No	Yes	Yes
Assessment Depth	Low	Medium	High	High
Focus Area	Basic hygiene	Operational maturity	Full risk posture	AI systems & governance
Ideal Use Case	Entry-level	Growing orgs	Mature compliance	AI-enabled orgs

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization’s organizations, people, and assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization’s unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and—year after year—apply our cumulative learnings to continually strengthen the company’s digital defenses.

ACHIEVED ACCREDITATIONS



ACHIEVED ASSESSOR

