TEVORA™

HITRUST AI Security Certification

A Certification Built for AI Platform Providers

What is this New Certification?

HITRUST AI Security Certification was released in 2023 to help AI solutions organizations deal with the complex risk landscape posed by new Artificial Intelligence tools. The standard is built by HITRUST in collaboration with trusted industry experts to help address security concerns and vulnerabilities associated with new AI technologies. It focuses specifically on cybersecurity risks to AI systems such as data poisoning, model manipulation, and prompt injection attacks. This certification is not designed to address broader Responsible AI topics like ethics, fairness, or transparency, but rather ensures that the AI system itself is technically secure.

Why Pursue the HITRUST AI Security Certification?

Demonstrate commitment to security in the age of AI

- Third Party Validation: Controls have been independently tested for validation of security measures and follow HITRUST's rigorous and trusted threat-adaptive approach
- Compliance Standard Alignment: Built on NIST SP 800-53, the NIST AI Risk Management Framework (AI RMF), ISO/IEC 27001, ISO/IEC 23894:2023, ISO/IEC 42001:2023, OWASP and others.
- Tailored to AI: Controls apply to unique risks of AI systems (based on model type, architecture, and training data sensitivity)
- Reliable Reporting: Assessor-verified reports that can be shared with executives, regulators, customers, and partners

Who Should Pursue this Certification?

The HITRUST AI Security Certification is available to providers of AI technologies, including:

- Platforms that enable others to deliver AI-integrated products
- Products that provide AI-enabled products directly to end users

Who Should NOT Pursue this Certification?

This certification is not currently intended for organizations that only use AI tools internally or build workflows on third-party AI models. Future updates to HITRUST CSF will include AI usage in standard certifications.

Up to 44 New Requirements

This AI-specific certification must be combined with HITRUST e1, i1, or r2 certification and adds up to 44 new requirements across AI topics such as:

- AI Policies / Governance
- AI Legal / Compliance
- Access to AI systems
- AI Security Threat Management
- AI Supply Chain
- AI System Resilience
- AI Software Development
- Training Data Protections
- Input / Output Data Sanitization

How the Certification Works

The HITRUST AI Security Assessment is not a standalone certification. It must be paired with a concurrent or existing HITRUST assessment to provide a complete picture of organizational and AI-specific security. There are two pathways:

AI1 (Added to e1 or i1)

- Valid for 1 year
- Tests Implementation Only

AI2 (Added to r2)

- Valid for 2 years
- Tests policies, procedures, and implementation, with measured and managed optional

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

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

PCI DSS QSA
PCI PA-DSS QSA
3DS ASSESSOR