AI Security Assessment and Certification for AI System Vendors

HITRUST

Turn AI security uncertainty into confidence, speed, and ecosystem trust for your business.

Accelerate and Scale AI Adoption

For AI system vendors, securing the technology is only half the challenge. Proving it's secure is equally important.

As AI systems expand across foundation models, APIs, agentic capabilities, and third-parties vendors face growing scrutiny around:

- Data Protection and Privacy
- Model Security
- AI Infrastructure Security
- AI Supply Chain Transparency
- Emerging Threats, like breaches through AI agents

61% **YoY increase in AI-related breaches**

– IBM Cost of a Data Breach Report 2026

Security, trust, sales, and product leaders must navigate evolving third-party risk management (TPRM), inconsistent industry standards, buyer skepticism, and increasingly complex security reviews, while also maintaining innovation speed and trying to reduce friction in the sales process.

But customers increasingly expect clear, proven assurance that AI systems are secured against AI threats before they adopt them.

HITRUST AI Security Assessment and Certification helps vendors demonstrate confidence through AI-specific threat adaptive controls, independent assessments, validation, and certification

Outcomes Achieved

Build Buyer Trust Faster

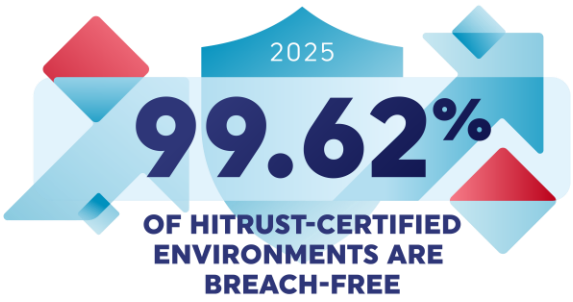
Enterprise buyers are asking tough questions about AI system security, including how customer data is protected, what third-party models and datasets are used, and how emerging threats are mitigated. HITRUST AI Security provides independent validation that helps vendors answer those questions with confidence and build trust faster.

Reduce Security Review Friction

Replace repetitive questionnaires and lengthy explanations with defensible, reusable assurance. HITRUST AI Security helps vendors address customer security concerns more efficiently, accelerating procurement and sales cycles.

Demonstrate Protection Against Real AI Threats

Security teams need more than broad governance claims, they need proof that AI systems are protected against relevant threats. HITRUST AI Security uses AI-specific, threat-adaptive controls mapped to relevant security threats, helping vendors demonstrate safeguards against current and emerging threats. The result? Proven results with a **99.62% breach-free rate** of HITRUST-certified environments.



Why HITRUST AI Security

Proactive Threat Defense

Addresses AI-specific threats through the Cyber Threat Adaptive Process

Testable, AI-Specific Controls

Control requirements designed specifically for AI systems and platforms

Harmonized Framework

Consolidates requirements from multiple authoritative sources into a single framework

Independent Validation & Certification

Converts AI security from a self-attested claim into validated assurance

Shared Responsibility & Control Inheritance

Supports control inheritance from cloud service providers and AI platforms

Complements AI Governance

Works in tandem with AI governance assurance frameworks

How HITRUST Compares to Other AI Security Assurance Approaches

	ISO/IEC 42001	HITRUST AI Security	AIUC-1
Framework Type	AI management system	AI system security assurance	Agentic AI security assurance
Purpose	Establish and operate an AI governance program	Prove AI systems and underlying infrastructure are secure	Prove agentic AI security and governance
What's Assessed	AI policies, procedures, and management practices	AI system security controls	Agentic AI security controls and governance
Governance vs. Security	Governance-focused, limited security depth	Security-first, controls depth, governance supported	Both, but only for agentic AI
Risk Reduction Focus	Designed to manage AI security responsibly, not secure systems	Designed to measure and reduce AI system risk	Designed to secure and manage agentic AI only
Control Relevance and Rigor	Broad AI guidance with principle-based, non-prescriptive requirements	Prescriptive, testable AI-specific security controls	A mix of prescriptive, testable security controls and non-prescriptive requirements specific to agentic AI
Assessor Options	< 30 globally	Over 100 authorized assurance partners globally	< 5 assessors
Assurance Strength	Assurance via independent testing, selective testing, variable rigor	Validated assurance via independent testing and centralized QA	Assurance via independent testing and centralized QA
Certifiable	Yes	Yes	Yes
Reporting and Evidence	Scoping and summary of implemented governance controls	Standardized reporting	Standardized reporting

HITRUST AI Security is the gold standard in AI security assurance.
Learn more at https://hitrustalliance.net/AI-security

HITRUST