

AI Security Assessment and Certification for TPRM

HITRUST®

Go from AI security uncertainty to AI adoption with confidence, speed, and ecosystem trust.

Address AI-specific Threats, Reduce AI Adoption Headaches

AI introduces new cybersecurity threats and risks, expanding an organization's attack surface. The challenge? Traditional risk assessment methods were not designed to address:

- Novel data leakage paths
- Data extraction attacks
- Opaque AI supply chains
- Agentic AI behaviors
- Rapidly changing models

26% of AI-related breaches occurred with third-party deployed SaaS

— IBM Cost of a Data Breach Report 2026

Third-party Risk Management (TPRM) teams are being asked to assess AI systems faster than ever, but many vendors are unprepared to answer detailed AI security questionnaires, controls are inconsistent across the industry, and organizations may lack the expertise needed to evaluate AI system risk with confidence. At the same time, procurement, security, and risk leaders need assurances that can withstand executive, customer, and regulatory scrutiny.

HITRUST AI Security provides a consistent, proven approach to evaluating AI system security through:

- AI-specific, threat-adaptive controls
- Independent assessment
- Rigorous quality review, assurance, and certification

Outcomes Achieved

Assess AI Vendors with Confidence

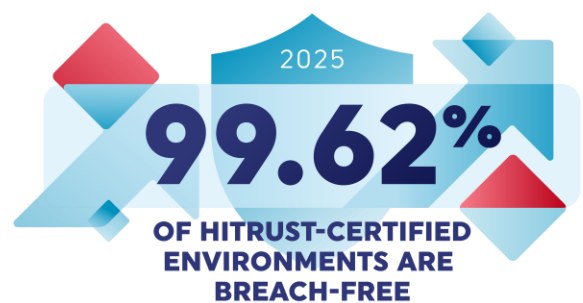
Move beyond inconsistent questionnaires and self-attestations. HITRUST AI Security provides a standardized, independently validated approach to evaluating AI system security, helping TPRM teams make more informed and defensible risk decisions.

Proven Security Against Real AI Threats

Traditional vendor risk assessments often miss AI-specific risks. HITRUST AI Security maps controls to relevant AI threats, enabling TPRM teams to evaluate whether systems are secured against real-world AI security threats, not just broad governance requirements. The result? A **99.62 breach-free rate** of HITRUST certified environments.

Accelerate Procurement and Adoption

Reduce assessment effort, minimize procurement friction, and streamline reviews with a consistent and reusable assurance model. HITRUST AI Security helps organizations evaluate AI system vendors faster while maintaining strong security and risk oversight.



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