

# AI Security and Risk Management Assurance

# HITRUST®

HITRUST helps you go from AI uncertainty to AI deployment with confidence, speed, and ecosystem trust.

## From Experiment to Everyday Use

AI has moved from an experiment to being embedded in everyday use across organizations large and small, and executives, boards, customers, and regulators are all converging on the same question: "Is AI being adopted securely and well-governed?"

# 92%

Share of organizations that reported an AI-related breach and lacked proper AI access controls

*IBM Cost of a Data Breach Report 2026.pdf*

## What Makes AI Different

- **Data protection is more demanding**  
New exposure through data leakage, re-identification, and data-extraction attacks that legacy controls can miss.
- **AI supply chain transparency**  
Organizations expect to know which models, datasets, tools, APIs, and retrieval sources shape a system.
- **Assurance must keep pace with change**  
Probabilistic behavior and frequent model updates make a one-time, pass/fail assessment go stale fast.
- **Governance and security are connected, but distinct**  
Managing AI risk and protecting AI systems are different disciplines, and stakeholders expect both.

## The HITRUST Advantage

HITRUST addresses both AI security and risk concerns with two complementary assessments - AI Security Assessment and Certification and AI Risk Management Assessment - giving you a clear path to secure and manage AI systems.

## The Benefits of HITRUST AI Assurance

### Proven assurance against today's threats

AI-specific controls for relevant AI threats, so risk management and assurance reflect the real threat and regulatory landscapes. Cyber Threat Adaptive is an intel-driven approach that updates prescriptive controls as new AI threats emerge, keeping your certification relevant.

### Adopt AI faster with less friction

A standardized security and risk assessment approach for AI systems streamlines procurement processes and reduces adoption barriers. HITRUST enables a consistent, evidence-backed way to answer the question everyone is asking: "Is the AI system secure?"

### Trust you can put in front of anyone

Independent, third-party validation and formal certification demonstrate the trust you can put in front of anyone. HITRUST is built on rigorous, independent testing and is backed by measurable, proven results. HITRUST has a 99.62% breach-free rate across certified environments, so the trust signal is grounded in proof, not theory.



# Choosing Your AI Assurance Path

|              | AI Security Assessment & Certification                                                            | AI Risk Management Assessment                                         |
|--------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Purpose      | Formal validation of AI system security                                                           | Targeted evaluation of AI risk management practices                   |
| Deliverables | AI Security Readiness Assessment and validated Certification                                      | AI Risk Management Readiness Assessment and validated Insights Report |
| Controls     | Prescriptive, testable AI-specific security controls covering over a dozen AI security threats    | AI-specific risk management controls harmonized to ISO and NIST       |
| Validation   | Independent testing by a HITRUST External Assessor plus centralized HITRUST QA review and scoring | Self-assessment, or engage a HITRUST External Assessor                |
| Adaptability | Standalone, or paired with HITRUST e1/i1 (ai1) or r2 (ai2) assessment and certifications          | Standalone or add onto existing HITRUST e1, i1, r2, and AI Security   |
| Best for     | AI system vendors needing standardized, shareable assurance                                       | Organizations building or maturing an AI risk program                 |

99.62%

breach-free rate among HITRUST-certified environments in 2025

75%

of the Fortune 20  
rely on HITRUST CSF

19

years of championing and  
leading cybersecurity and  
cyber risk assurance

“HITRUST r2 certification proves our overall security and compliance posture, while the HITRUST AI Security Certification proves we’ve hardened our AI systems against unique threats... Both show that our platform and AI usage are validated to a high bar.”

**Vivian Lee**  
Security Analyst, Notable Health

HITRUST is the gold standard for AI security and risk assurance.  
Learn more at: [hitrustalliance.net/ai-hub](https://hitrustalliance.net/ai-hub)

HITRUST®