HITRUST AI SECURITY ASSESSMENT AND CERTIFICATION

AI technologies are evolving rapidly. So are the associated security challenges. Traditional security approaches often fall short in addressing AI-specific threats, leaving organizations vulnerable.

The HITRUST AI Security Assessment and Certification brings HITRUST's trusted approach to securing AI systems. The assessment offers a comprehensive set of controls, assurances tailored to the unique risks posed by AI systems and provides a prescriptive approach to mitigate these risks. The result is compliance that builds trust with stakeholders.

Why should organizations trust the HITRUST AI Security Assessment and Certification?

HITRUST is the leader in enterprise risk management, information security, and compliance assurances, offering a certification system for the application and validation of security, privacy, and AI controls, informed by over 50 standards and frameworks.

The company's threat-adaptive approach delivers the most relevant and reliable solution, including multiple selectable and traversable control sets, over 100 independent assessment firms, centralized quality reviews and certification, and a powerful SaaS platform enabling its program and ecosystem. For over 17 years, HITRUST has led the assurance industry and is widely recognized as the most trusted solution to establish, maintain, and demonstrate security capabilities for risks management and compliance. HITRUST provides the only assurance mechanism proven to be reliable against threats. 99.4% of HITRUST certified environments reported no breaches over the past two years. It's the only assessment and certification system that can offer validated, quantifiable assurance — proving your organization's commitment to security.

To develop this first of its kind assurance solution, HITRUST collaborated extensively with leading AI innovators and industry working groups to understand the AI risk landscape and determine how to quantify and mitigate AI risks. HITRUST also reviewed and harmonized AI security-specific threats discussed in nearly two dozen authoritative sources, including ISO, NIST and OWASP and multiple commercial AI security sources and analyzed these requirements against HITRUST's framework, the HITRUST CSF, and the Cyber Threat Adaptive engine to land on a comprehensive, prescriptive control specification.

Organizations that successfully complete the AI Security Assessment and then meet the validation and QA standards for HITRUST AI certification can demonstrate the highest level of AI security, risk management and mitigation in a way that has not previously been possible.

Key Features

- **Comprehensive Control Set -** Up to 44 controls, specifically designed to address the security needs of AI platforms and systems
- **Tailored Control Selection -** Select controls for different AI deployment scenarios, based on inherent risk and the approach needed to provide security and resiliency for different AI models
- **Rigorous Assurance Mechanism -** Independent testing and centralized reviews for robust validation of security measures
- **Proactive Threat Adaptation -** Quarterly updates to HITRUST's controls keep pace with the rapidly evolving threat landscape
- **Practical, Applicable Solution -** HITRUST harmonized comprehensive controls with NIST, ISO, OWASP and other standards, analyzed using our proprietary threat-adaptive engine, and delivered a single framework with prescriptive directives that can be readily understood and implemented

Shared Responsibility and Inheritance

HITRUST recognizes the interdependencies common to organizations within the AI sphere. Partner organizations need to ensure their own security and be able to prove the veracity of their security to each other and the end customer. HITRUST certification ensures consistency, as all certified internal and third party certified implemented systems in a business relationship can share the same controls sets and implementation standards. The AI Security Assessment also enables organizations to inherit AI controls from cloud service providers and others whose systems are already HITRUST certified, greatly increasing efficiency. HITRUST actively and intentionally involved the major cloud providers in the development of this solution.

Who should consider the AI Security Assessment?

The HITRUST AI Security Assessment provides security and trust for AI Application and AI Platform providers of any size and in all industries. Whether you develop, deploy and market AI systems to other professional organizations, or you incorporate AI systems directly into your own products, conducting the AI Security Assessment and achieving HITRUST certification ensures your organization meets the highest standards of AI and cybersecurity risk management. It also demonstrates your organization's commitment to security and trustworthiness to your stakeholders.

Who has an interest in AI Security Assessment and Certification?

- **Security and Risk Management Teams -** Use HITRUST as a blueprint for securing deployed AI systems and as a proof point to demonstrate to stakeholders that these systems are secure.
- **Sales, Marketing, and Product Heads -** Leverage HITRUST certification to assure customers and prospects that AI-powered products and services are secure, thereby removing friction and enabling adoption.
- **Third-Party Risk Management (TPRM) Programs -** Ensure that vendors employing AI are properly securing it to manage vendor security risk effectively.
- **Boards, Owners, CEOs, and Executives -** Gain confidence that the AI systems being used and developed are properly secured, with independent proof of security.
- **Cyber Insurance Industry -** Use HITRUST as a reliable, repeatable instrument to address AI risks and understand the actual residual risks they are underwriting, thereby reducing their risk and enabling them to offer better products at lower costs.
- **Regulators and Government Bodies -** The HITRUST AI Security Assessment and Certification serves as the first comprehensive AI assurance program to address rising concerns about AI security, especially in critical infrastructure sectors.

Why Choose HITRUST?

For over 17 years, HITRUST has developed reliable assurance mechanisms that are measurable, quantifiable, and proven. Our methodologies, built around a harmonized framework of over 50 authoritative sources – including NIST, ISO, and PCI - incorporate relevant, implementable control specifications that provide organizations with the assurance they need to protect their systems. Our flexible offerings are designed to be accessible, scalable, and suitable for organizations of any size, from small startups to large enterprises. With a centralized review process, third-party independent testing, and gold-standard certifications, HITRUST is the only organization that provides the level of reliability, consistency, and thoroughness required to secure AI systems today.

Contact Us

For more information on the HITRUST AI Security Assessment and Certification, visit https://hitrustalliance.net/ai-hub