BARR
ADVISORY

2024 Whitepaper

HITRUST AI Security Certification

Revolutionizing Security Assurance for AI Providers

Table of Contents

2 | Introduction

3 | A Trusted Framework Tailored to AI Risk

4 | Integration with Compliance Frameworks

5 | Key Benefits for Organizations

6 | FAQs: The HITRUST AI Security Assessment

7 | About BARR Advisory

Introduction

As artificial intelligence (AI) reshapes industries, organizations must ensure their AI systems are not only innovative but also secure.

Introduction

Recognizing this critical need, HITRUST has announced the HITRUST AI Security Assessment and Certification—a practical, prescriptive, and tailored solution to address AI risks. Developed in collaboration with leading AI industry participants, this framework offers organizations a rigorous mechanism to secure their AI systems and build trust with stakeholders.

Scheduled for release in December 2024, the HITRUST AI Security Assessment builds on HITRUST's trusted compliance methodologies, addressing the unique challenges posed by AI technologies. Here's everything you need to know.

A Trusted Framework Tailored to AI Risk

A Comprehensive Control Set

The HITRUST AI Security Assessment is based on up to 44 prescriptive controls, addressing a broad spectrum of risks specific to AI platforms and deployed systems. These controls span:

- **AI Security Threat Management:** Mitigating vulnerabilities unique to AI systems.
- **Governance and Oversight:** Establishing accountability for AI security.
- **Secure AI Development:** Promoting safe development practices.
- **Access and Data Controls:** Securing AI system access and sanitizing inputs and outputs.
- **System Logging and Resilience:** Ensuring AI systems are monitored, resilient, and prepared for recovery.

These controls can be tailored to fit various deployment scenarios, aligning with organizational risk profiles and assurance needs.

A Rigorous Assurance Mechanism

HITRUST brings its hallmark independent testing, centralized review, and certification process to the AI Security Assessment. This ensures organizations can proactively address evolving threats with quarterly updates to controls and leverage shared responsibility and inheritance, ultimately increasing efficiency. Additionally, the assessment and certification demonstrate dependability—in the event of an AI security incident, the assessment provides robust evidence of a secure program.

Integration with Compliance Frameworks

How it Works

The HITRUST AI Security Assessment is not a standalone certification—it must be added to a HITRUST e1, i1, or r2 certification. Depending on the foundation, AI Security Certifications are labeled:

- **ai1:** Built on e1 or i1 for moderate assurance needs.
- **ai2:** Built on r2 for the highest level of assurance.

This layered approach ensures comprehensive coverage of both AI-specific and broader security requirements.

Complementing ISO 42001

ISO 42001 establishes frameworks for AI management systems. The HITRUST AI Security Assessment complements ISO 42001 by offering *specificity, practical implementation, and consistency:*

- **Specificity:** Detailed, actionable controls.
- **Practical Implementation:** Harmonized with NIST, ISO, and OWASP, ensuring relevance and applicability.
- **Consistency:** Centralized reviews and certification processes create uniformity and reliability.

Together, these frameworks address the full spectrum of AI risk management, from governance to cybersecurity.

Did you know?

Only 0.6% of organizations that have HITRUST certifications reported a breach to HITRUST in 2022 and 2023.

Key Benefits

Why Choose HITRUST AI Security Assessment?

The HITRUST AI Security Assessment is more than a certification—it's a comprehensive framework for achieving AI security excellence. Organizations deploying or providing AI technologies benefit from tailored controls, proactive adaption, enhanced trust, and efficiency gains.

Tailored Controls

With up to 44 prescriptive controls, the framework addresses the unique risks of AI systems, such as secure access, data sanitization, and system resilience, ensuring a customized solution for various deployment scenarios. This adaptability enables organizations to mitigate threats effectively without overburdening resources.

Proactive Adaption

One of the most significant advantages of the HITRUST AI Security Assessment is its proactive nature. With quarterly updates, the framework evolves alongside emerging threats and regulatory changes, ensuring that organizations remain secure and compliant as the AI industry advances. By aligning with established standards like NIST, ISO, and OWASP, the framework provides relevant, future-ready assurance while addressing gaps left by traditional compliance mechanisms.

Enhanced Trust and Efficiency

Achieving HITRUST AI certification also builds trust with customers, partners, and regulators. Certification demonstrates a commitment to top-tier security and robust risk management, making it easier to expand into new markets and establish partnerships. The ability to inherit controls from pre-certified systems further streamlines the process, reducing complexity and resource requirements. This combination of efficiency, adaptability, and trust makes the HITRUST AI Security Assessment an indispensable tool for organizations looking to innovate securely in the AI space.

> ***"The HITRUST AI Security Assessment takes a deep look at the security of the AI in an organizations environment to ensure you maintain trust for your stakeholders while preparing for the future."***
>
> Steve Ryan, HITRUST Manager

FAQs: The HITRUST Security Assessment

What is the HITRUST AI Security Assessment?

A comprehensive solution addressing AI system risks, built on up to 44 tailored controls, integrated into HITRUST e1, i1, or r2 certifications.

Who is it for?

Providers of AI systems, including AI application and platform providers. It is not intended for organizations using third-party AI systems.

Why do organizations need it?

Existing frameworks lack specificity for AI security. HITRUST bridges this gap with a practical, implementable model for demonstrating AI security.

How does certification work?

AI Security Certification is valid for the same period as the base HITRUST certification (one year for e1/i1, two years for r2 with interim review). Customers can leverage existing certifications to streamline the AI assessment process.

HITRUST AI Security Assessment vs. Other Frameworks

Feature	HITRUST AI Security Assessment	ISO 42001	SOC 2
AI-Specific Controls	Yes	Limited	No
Prescriptive Directives	Yes	No	No
Comprehensive AI Focus	Yes	Broad AI System Management Scope	No

About BARR Advisory

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about the HITRUST Security AI Assessment? Contact us today.