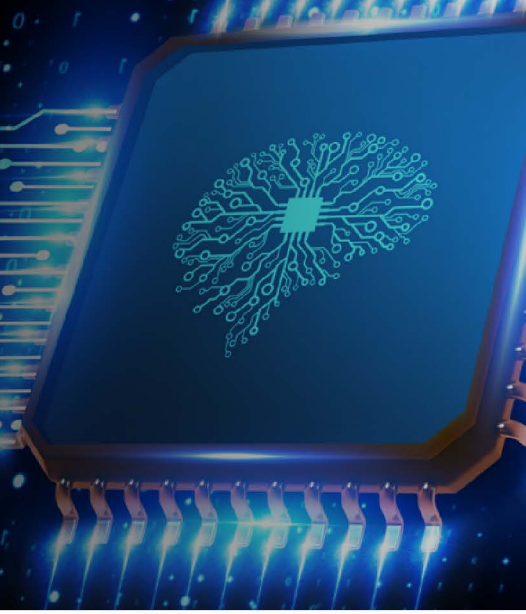
ACCORIAN

THE IDEAL AI SECURITY FRAMEWORK FOR YOU

As artificial intelligence (AI) and machine learning (ML) systems, including Generative AI (GenAI), become integral to business operations, maintaining robust security and ethical standards is becoming critical too. Organizations face unique AI challenges—from safeguarding data and ensuring privacy to mitigating potential biases. **This is where AI security frameworks and standards provide structured guidelines to manage these risks effectively while ensuring fairness, non-discrimination, transparency, explainability, and accountability.**



Applies to all organizations that have an AI capability through a 3rd Party or, home grown AI/LLM

WHY DO YOU NEED AN AI SECURITY STANDARD?

AI systems, including GenAI, introduce new challenges in cybersecurity, privacy, and compliance. As capabilities grow, so do risks like data leakage and bias. Trust depends on secure, reliable AI. Security standards guide organizations in managing these risks and adopting responsible, compliant practices.

1. **ENHANCED RISK MANAGEMENT:** AI frameworks help identify, assess, and mitigate risks unique to AI systems, addressing data integrity, model robustness, and access controls. They also promote fairness and reduce bias.
2. **CONTINUOUS MONITORING AND REASSESSMENT:** AI systems need ongoing monitoring due to constant learning. Security frameworks ensure that updates don't compromise safety or integrity and support transparency for stakeholder trust.
3. **REGULATORY COMPLIANCE AND ACCOUNTABILITY:** Evolving laws like the EU AI Act push for AI compliance. Security standards help meet legal, ethical, and fairness requirements, reducing the risk of penalties.
4. **CLIENT TRUST AND TRANSPARENCY:** Adhering to AI security standards shows commitment to safe, fair, and reliable systems, boosting stakeholder trust and enhancing market credibility.

CHOOSING THE RIGHT STANDARD?

01

AI IMPLEMENTATION FOCUS

In-house developed AI: NIST AI Risk Management Framework or, HITRUST AI Risk Management Assessment are ideal security frameworks followed by the below certifications. For 3rd Party LLM deployment: ISO 42001 is an industry agnostic standard, and if you are in health, then HITRUST AI Certification.

02

INDUSTRY AND COMPLIANCE FOCUS

Sectors with specific regulations (e.g., healthcare) may benefit from HITRUST AI or NIST AI RMF for compliance, while the ISO 42001 standard is broadly applicable across multiple industries.

03

RISK AND VULNERABILITY FOCUS

For thorough risk management, NIST AI RMF is ideal, and the OWASP Top 10 outlines the key risks and critical controls for securing LLMs and Gen AI.

04

CLIENT ASSURANCE FOCUS

Organizations needing third-party validation should consider ISO 42001 or HITRUST AI Certification to demonstrate security transparency and gain client trust.

LEADING AI SECURITY STANDARDS

1 HITRUST AI RISK MANAGEMENT CONTROLS

Purpose: HITRUST offers a set of **AI-specific risk management controls** designed to help organizations identify, manage, and mitigate risks related to the development and use of AI systems. These controls align with leading security, privacy, and risk management frameworks, offering a structured approach for responsible AI use.

Ideal for: Organizations integrating AI into environments with strict data protection requirements, such as healthcare, that want to proactively address AI-related risks while aligning with established compliance expectations.

2 HITRUST AI RISK MANAGEMENT ASSESSMENT & CERTIFICATION

Purpose: While the AI Risk Management (AI RM) controls can be assessed independently, they are not currently eligible for a stand-alone certification. However, organizations can pursue certification that includes AI controls by incorporating them into a broader **HITRUST assessment—such as e1, i1, or r2.**

Ideal for: Organizations seeking formal certification of AI-related risk practices as part of a larger validated HITRUST assessment.

3 ISO 42001 & ISO 23894: AI GOVERNANCE & AI RISK MANAGEMENT

Purpose: ISO 42001 is the first global standard dedicated to AI management, offering a comprehensive framework for organizations to govern AI by setting standards for data security, model governance, and ethical considerations. Whereas, **ISO 23894** offers comprehensive guidance on managing risks associated with AI systems. It integrates risk management principles into AI activities, ensuring alignment with established standards like ISO 31000 and ISO 22989.

Ideal for: Organizations involved in developing, deploying, or managing AI systems that seek to address potential risks and ensure responsible AI practices.

4 NIST AI RISK MANAGEMENT FRAMEWORK (AI RMF)

Purpose: NIST's AI RMF is focused on comprehensive risk management across the AI lifecycle. It covers four essential functions — Prepare, Govern, Manage, and Assess — ensuring organizations can identify, manage, and mitigate risks in AI operations.

Ideal for: Organizations looking for a structured approach to risk management across industries, particularly those needing to align with U.S. federal guidelines.

5 OWASP TOP 10: LLM & GENERATIVE AI SECURITY

Purpose: OWASP Top 10 for LLM and Gen AI framework targets specific vulnerabilities in AI systems with a strong focus on machine learning and large language models (LLMs). It provides guidelines to address the top ten most critical security issues, such as prompt injections, information disclosure, data & model poisoning etc.

Ideal for: Development teams and organizations that build or implement machine learning models, particularly those concerned with secure coding practices and vulnerability management.

AI SECURITY FRAMEWORK COMPARISON TABLE

FRAMEWORK/ STANDARD	ISO 42001	HITRUST AI RISK MANAGEMENT ASSESSMENT	HITRUST AI CERTIFICATION	NIST AI RMF	ISO 23894	OWASP TOP 10 FOR LLM & GEN AI
IDEAL FOR	World's first AIMS standard Establishing a management system for AI, showcasing 3rd party certification and assurance	Establishing a framework to manage AI risks and 3rd party validation and manage AI-related risks, including data privacy, algorithmic bias, and security vulnerabilities, aligning with frameworks like NIST AI RMF and ISO/IEC 23894	The HITRUST Cybersecurity Certification for Deployed AI Systems, launched in November 2024, equips organizations with relevant AI security controls, provides means to assess those controls, and offers reliable reporting that can be shared	Setup of effective Risk management for AI and understanding current posture Needs to be applied in tandem with NIST 800-53 for implementation	Integration and implementation of risk management into AI function	Starting point towards securing home grown or, 3rd party AI systems/LLMs For identifying critical security vulnerabilities. Providing guidelines for secure coding tailored for LLMs.
APPLICABILITY	Any org that develops, provides or, uses AI systems	Any org that develops, provides or, uses AI systems	Providers of AI systems, including AI application, platform providers	Any org that develops, provides or, uses AI systems	Any org that develops, provides or, uses AI systems	Any org that develops, provides or, uses AI systems
CERTIFICATION	Yes	No	Yes* in addition to your regular HITRUST assessment – e1, i1, r2.	No	No	No
CONTROLS	38 controls 10 clauses	51	44	NA 4 key functions, 12 risks, 400+ actions	NA 2 main clauses – #5,#6	NA 10 categories
AREAS OF FOCUS	AI Governance, Risk Mitigation, Trust, Global Standardization	AI Risk Management	AI Governance, Oversight, Development, Legal, Inventory, Supply Chain, Model Robustness, Access to the AI System	Design, Development, Deployment & Use Structured approach to risk management and, ethical AI use	Risk Management and AI System Life Cycle	Top 10 most critical vulnerabilities
ACCEPTANCE	Global - across industries	Health & others - US, Global	Health & others - US, Global	US	Global - across industries	Global - across industries
COVERAGE	Organizational Governance, Risk Management, Compliance & Legal Requirements, Continuous Improvement	Internal & External Controls Across Security Program, Governance, Risk Management, Stakeholder Management, System Life Cycle Alignment	AI Security Governance, Threat Management, Development, Compliance	Prepare, Govern, Manage, Assess	Design, Implementation, Evaluation, Improvement, Risk Assessment, Risk treatment, Monitoring & Review, Recording & Reporting	Design, Development, Maintenance
VALIDITY (UNLESS MAJOR CHANGE)	3 years with an annual surveillance	Annual	Inline with your current assessment's validity – 1 year for e1, i1 & 2 years for r2	Annual	NA	NA

The best AI Security framework to adopt depends on whether you've built your LLM in-house or, use a 3rd party, need to showcase assurance to your clients, which industry you work in etc. But, in the end it will boil down to what reduces your risk while meeting regulatory & compliance requirements for your industry

STAYING AHEAD WITH REGIONAL COMPLIANCE STANDARD

For organizations operating globally, aligning with regional standards is essential for consistent, compliant AI governance. Each regional framework focuses on unique cultural, legal, and ethical values. Adherence to these standards helps organizations maintain global trust and avoid costly compliance penalties.

EVOLVING STANDARDS AND NEW MANDATES

AI regulations are constantly evolving, with frequent updates, in response to technological advancements and public concerns. Staying current with mandates such as the EU AI Act, Canada's AIDA, and U.S. federal guidelines is critical for organizations to ensure ongoing compliance, maintain data security, and support ethical AI practices.

EU AI ACT

The EU AI Act is one of the most comprehensive frameworks aimed at regulating AI to ensure it's safe, transparent, and respects fundamental rights. The act defines AI systems by risk level (from minimal to high-risk), with strict rules for high-risk applications, such as biometric identification or recruitment tools. Compliance with the EU AI Act is essential for organizations operating in Europe, as it emphasizes risk-based regulation, requiring organizations to implement extensive risk management, transparency, and security controls.

CANADA'S ARTIFICIAL INTELLIGENCE AND DATA ACT (AIDA)

Canada's AIDA sets a legal foundation for the responsible use of AI, promoting transparency, accountability, and fairness. It mandates impact assessments and risk management processes for high-impact systems and requires that organizations provide explanations for decisions made by AI systems. AIDA also emphasizes privacy and ethical considerations, making it a critical compliance requirement for organizations operating in Canada or handling Canadian data.

WHITE HOUSE EXECUTIVE ORDER ON AI IN THE U.S.

The White House Executive Order on AI outlines principles for AI usage in government and encourages private organizations to adopt responsible practices. It focuses on areas like AI safety, privacy, and non-discrimination, urging federal agencies to assess and mitigate AI risks. While not as prescriptive as the EU AI Act, this executive order signifies a commitment to responsible AI development, providing guidance for compliance with U.S. federal standards.