Securing Your AI Ecosystem

Strengthening Your AI Journey from Risk Identification to Governance

As AI becomes integral to business operations, organizations encounter new security and compliance risks that extend beyond traditional cybersecurity measures. Accorian's AI Security delivers expert advisory, guidance, tailored assessments and audits to address unique threats, compliance gaps, and operational risks, ensuring responsible and secure AI deployment .
This applies whether you've home grown your AI capability or, leverage a 3rd party AI tool or, open source LLM.

COMMON MYTHS ABOUT APPLICABILITY

AI SECURITY DOES NOT APPLY TO ME AS I USE A 3RD PARTY AI TOOL OR, LLM

Organizations forget about their shared responsibility with the AI service provider and are still responsible for numerous security elements like access controls, data security, monitoring, logging etc. Just like hosting on the cloud.

WE ONLY HAVE 1 APPROVED AI TOOL WHICH IS COPILOT

Most organizations are plagued by shadow AI and the inability to detect leakage of sensitive data on 3rd party AI tools that their teams are using. It's important to track, review, inventory and manage all AI tools & utilities.

SECURITY CAN WAIT TILL WE HAVE FULLY OPERATIONALIZED AI INTERNALLY

Old adage of stitch in time saves nine, it's essential to keep security at it's core. Data was initially confinded to endpoints, servers then networks and then cloud which was managed by 3rd parties and today is accessible by AI tools which are learning from your data, utilizing it for further tweaking their models and could also lead to possible leakage of your sensitive data through effective prompting. Hence, it's important to factor for securing your AI implementation in the design phase to include the necessary controls & guard rails.

RISKS OF UNSECURED AI SYSTEMS

1. **Data Leakage from AI Systems**

   AI models require large volumes of data. This could include your IP, sensitive data, client information etc. Without strong encryption, access controls, and secure processing, these systems expose critical business or customer information to breaches.

2. **Embedded Bias in AI Decision-Making**

   Poorly trained or unmonitored models reinforce societal biases, leading to unfair or discriminatory outcomes, posing legal, ethical, and reputational risks.

3. **Security Vulnerabilities in Third-Party Vendor Systems**

   AI tools rely on complex supply chains involving third-party datasets, cloud services, and open-source code. Each component introduces potential attack vectors that must be independently validated.

4. **Regulatory Non-Compliance and Oversight Gaps**

   With AI-specific regulations evolving globally, organizations face increasing pressure to meet transparency, accountability, and auditability requirements. Failing to do so results in penalties or loss of stakeholder trust.

ACCORIAN'S AI SECURITY SERVICE LINE DELIVERS EXPERT ADVISORY

1

AI SECURITY STRATEGY & ADVISORY

We enable organizations to align their business objectives with their security strategy.

1. AI Security & Risk Assessment

Evaluate your current AI security and risk posture through in-depth review of your current AI inventory including homegrown models, third-party services, open-source LLMs, etc. and assess attributes like usage mapping, and data flow. The inventory helps in identifying current & potential risk exposure.

Additionally, the AI-specific risk assessments help uncover model flaws, bias, and regulatory gaps, helping build trust and meet compliance expectations.

2. AI Security Strategy Development

Design a framework and strategy for secure AI use.

3. AI Threat Modeling

Identify your current threats to your AI/ML stack. We will leverage our past experience of threat profiling AI systems along with referencing the MITRE ATLAS framework.

4. Executive Reporting and Guidance on AI Risk

Simplify complex AI risks into clear, actionable insights to support informed decision-making and governance.

2

AI SECURITY COMPLIANCE & AUDIT

We aid organizations with

Readiness | Advisory | Assessment | Audit | Monitoring

We help organizations meet and maintain the compliance standard through our tailored end to end program, from scoping to readiness to remediation advisory to pre-audit to assessment/audit.

1. HITRUST AI Risk Management Framework & Certification

Provide a structured approach to embed privacy, security, and risk controls into AI systems, with certification validating effective implementation. Strengthens health data security by aligning AI systems with industry trusted HITRUST standards, offering assurance to regulators, partners, and patients in healthcare and other sensitive data environments.

2. NIST AI Risk Management Framework (AI RMF)

Align AI lifecycle with NIST's AI RMF to ensure governance, data integrity, transparency, and resilience while managing evolving AI risks.

3. ISO 42001 - AI Management Systems

Adopt ISO 42001 to enable responsible AI development, secure deployment, and governance throughout the AI lifecycle in line with global standards and EU AI Act.

4. ISO 23894 - AI Risk Management

Apply ISO 23894 to manage AI risks using ISO 31000 principles, enabling structured documentation and flexible mitigation of AI-specific threats.

5. U.S. State-Level AI Compliance

Ensure alignment with emerging AI regulations such as Colorado's AI Act and New York's RAISE Act, focusing on high-risk AI system governance, discrimination prevention, and safety reporting.

6. OWASP Top 10 for LLM

Address the most critical security vulnerabilities in LLM and generative AI systems such as prompt injection, data leakage, and model poisoning by implementing OWASP's secure coding and risk mitigation best practices.

7. ISO/IEC 42005:2025 Information Technology - Artificial Intelligence (AI) - AI System Impact Assessment

The ISO/IEC has published 42005:2025 Information Technology Artificial Intelligence (AI) - AI System Impact Assessment. ISO/IEC 42005 guides organizations conducting AI system impact assessments. These assessments focus on understanding how AI systems and their foreseeable applications may affect individuals, groups, or society at large. The standard supports transparency, accountability and trust in AI by helping organizations identify, evaluate and document potential Impacts throughout the AI system lifecycle.

Key components of an AI Impact Assessment include:

01 DOCUMENTING THE PROCESS

02 INTEGRATING WITH ORGANIZATIONAL MANAGEMENT

03 DETERMINING TIMING AND SCOPE

04 ALLOCATING RESPONSIBILITIES

05 ESTABLISHING THRESHOLDS

06 RECORDING AND REPORTING

07 ESTABLISHING AN APPROVAL PROCESS

08 CONDUCTING MONITORING AND REVIEW

09 PERFORMING THE ASSESSMENT

10 ANALYZING RESULTS

This standard empowers organization to:

- Assess and manage the real-world impacts of AI systems.
- Embed fairness, safety, and transparency into your operations.
- Navigate regulatory expectations with confidence.
- Show users and stakeholders that you take responsible.

3

AI SECURITY GOVERNANCE

We aid organizations with implementing strong AI governance that addresses bias, model manipulation, and transparency, aligning with regulatory demands and reducing operational risks.

1. Creation of AI Security Governance program

Establish a governance structure for AI and securing it while aligning with AI security regulatory landscape – MITRE ATLAS, NIST AI RMF, ISO/IEC 42001 and other security standards to enable a structured and well monitored environment.

2. Creation of AI Security Policies & Procedures

Develop AI security policies and procedures, define acceptable AI use cases, onboard third-party tools, set access control requirements, ensure human-in-the-loop oversight, manage data ingestion, monitor systems, and handle exceptions.

3. Third Party Risk Assessment of your AI utilities

Creation of a baseline for a third-party risk assessment for all new AI utilities that you plan to adopt. Subsequently, we can aid in performing an independent validation of external AI systems to assess security, governance, and operations across the entire AI vendor ecosystem.

4. AI Security Awareness

Driving a culture of secure usage of AI tools whether internal or, 3rd party utilities along with education on threats, risks, bias, compliance issues etc.

4

AI SECURITY TESTING & ASSURANCE

1. Red Team Assessment of AI Systems

Adversarial-style assessments to identify vulnerabilities such as data leakage, access control bypass, and injection attacks across the AI stack, including homegrown models, open-source frameworks, and third-party integrations.

2. Chatbot Penetration Testing

Security testing focused on conversational flows, user interactions, and the complexities of language models. Includes assessment of web interfaces, chatbot-specific logic, underlying LLM components, and associated APIs for comprehensive coverage.

3. Third-Party AI Tool Assessment

Thoroughly test your third-party models, commercial or open sources to ensure no compromise and leakage of data through backdoors, injection etc.

4. Secure AI Development Lifecycle

Understanding how AI plays into your product and it's lifecycle at each stage from dev to UAT to prod. This would include architecture analysis, code reviews, dependency scanning etc to understand how models are trained, what guard rails exists and how everything is being secured.

WHY DO YOU NEED AI SECURITY & COMPLIANCE?

AI systems create vulnerabilities that didn't exist in traditional IT environments. AI Systems learn, evolve and process vast amounts of sensitive data, and making autonomous decisions that can be difficult to predict or explain. Without proper security and compliance measures, organizations risk data breaches, regulatory penalties, and reputational damage from biased AI decisions. As regulators implement new AI-specific requirements worldwide, proactive AI security and compliance has become a business necessity.

ACCORIAN'S PROVEN APPROACH

01 HOLISTIC AI EVALUATION
Detailed assessments conducted to evaluate third-party AI solutions and LLMs across the AI lifecycle, offering a complete view of organizational AI security posture.

02 STAKEHOLDER ENGAGEMENT
Facilitated discussions with cross-functional teams to uncover operational gaps and inefficiencies in AI development, deployment, and oversight processes.

03 TECHNICAL EVIDENCE REVIEW
Validation of supporting documentation, training datasets, evaluation logs, and bias mitigation controls to assess the effectiveness of implemented safeguards and ongoing monitoring.

04 AI GOVERNANCE AUDIT
Evaluation of enterprise AI governance structures, including risk management protocols, accountability frameworks, incident response readiness, and third-party oversight mechanisms.

05 AI RISK POSTURE REPORTING
Delivery of an in-depth report outlining security and compliance scores, domain-specific risk ratings, and benchmarking against industry standards and peers.

06 PRIORITIZED REMEDIATION & STRATEGIC GUIDANCE
A structured, prioritized remediation roadmap accompanied by expert advisory to enhance organizational AI security and align with best practices.

07 MULTI-FRAMEWORK COMPLIANCE INTEGRATION
Adding AI security frameworks and standards to your existing security framework. They would range from frameworks like HITRUST AI, ISO/IEC 42001, and EU AI Act to support current and future regulatory compliance requirements.

WHY CHOOSE ACCORIAN?

Accorian differentiates itself by its in-depth knowledge of AI's distinct security and regulatory challenges, providing niche services that go beyond conventional cybersecurity models. Our end-to-end approach rigorously assesses the full AI lifecycle, utilizing top-tier governance frameworks to guarantee across-the-board compliance with changing international regulations. By delivering rich, actionable insights and continuous remediation support, Accorian enables organizations to actively monitor and manage AI-specific risks, drive algorithmic fairness, and safeguard against advanced AI-targeted attacks, ultimately providing a secure and compliant AI journey.

LET ACCORIAN TAKE CARE OF YOUR SECURITY WHILE YOU FOCUS ON YOUR BUSINESS

info@accorian.com +1 732 443 3468 www.accorian.com