ACCORIAN

AI SECURITY STRATEGY, ADVISORY & ASSURANCE

HITRUST Authorized External Assessor

Inc. 5000 America's Fastest-Growing Private Companies

PCI Security Standards Council Approved Scanning Vendor

ISO

AICPA SOC aicpa.org/soc4so

PCI Security Standards Council Qualified Security Assessor

CREST PEN TEST

NIST

Forbes India D Globalist Accelerating eXtrepreneurs™

ACCORIAN'S AI SERVICES

AI Strategy & Advisory Services

Fractional AI Security Team to aid with

- Advisory – Rollout, tools, implementation
- Secure AI Deployment Advisory
- Setup of AI Governance Framework
- Secure AI Architecture Design review
- AI Threat Modelling Workshops
- Data Access & Permission Assessment
- AI Control Advisory & Security Tool Selection
- AI Security Training

Assessment & Compliance

- AI Security Maturity Assessment
- AI Risk Assessment
- AI Impact Assessment
- Readiness & Assessment - ISO 42001, NIST AI RMF, EU AI Act, HITRUST AI, US State AI laws etc

Offensive/Testing

- AI Chatbot Testing/Prompt Injection
- AI Red Team Assessment
- Shadow AI Discovery
- AI Supply Chain Security Review
- API Penetration Testing
- AI Chatbot vulnerability scanning
- AI Evals Testing

Accorian can facilitate the Phase I of your AI journey with it's AI Strategy & Advisory Services
For Phase 2, steady AI operations, we will be your partner for assessments, compliance & testing

KEY QUESTIONS

- **What's your current AI stack or, what are your AI rollout plans?**
- Are you conducting a security due diligence of your current vendors who have AI capabilities or, new vendors you plan to onboard?
- **How are you securing your current AI implementation like vibe coding tools, chatbots etc?**
- Do you have an AI security policy in place?
- **Are you aware of your shadow AI?**
- Do your customers except AI capabilities from you? If yes, what's that feature?
- Who owns AI risk?
- Do you have the ability to assess and monitor your AI implementation?

It would be apt to go beyond your security contact to the CTO, CIO or, Chief Strategy Officer or, Chief AI Officer who is likely in charge of rolling out AI in the org

AI RUSH & CURRENT AI IMPLEMENTATIONS

2025 was all about AI adoption, with more than **88%** of executives and board members pushing for it across their teams.

HOW HAVE MOST COMPANIES ROLLED OUT AI IN THEIR ENTERPRISES?

76% of all teams are utilizing existing AI models and tools

CO-PILOTS OR, READY TO USE AI TOOL SPRAWL

Enterprise licenses were provided to teams for their day-to-day operations.

DOWNSIDE

An inability to demonstrate efficiency gains and ROI, combined with a lack of alignment to specific workflows and use cases, resulted in reduced effectiveness.

AI WRAPPERS

By utilizing a popular AI model through API calls to leverage its general intelligence, organizations can implement RAG systems with contextual grounding and training.

DOWNSIDE

Expenses can escalate quickly, insufficient context or training can lead to hallucinations, and substantial time investment is often required for fine-tuning.

GOING AGENTIC OR, MCP - BREWING

AI agents handle complex, end-to-end tasks with human oversight and reviews, RAG systems in place.

DOWNSIDE

High implementation complexity. Success depends on a strong AI team, robust review framework, and significant time dedicated to refinement and validation.

RAG systems are expensive & need clean data infrastructure - sorting, labelling, vector DBs

AI RISKS & THREATS

LOSS OF CUSTOMER TRUST

OPERATIONAL DISRUPTION, DEPENDENCY RISKS

BIAS, **HALLUCINATIONS** & UNFAIR OUTCOMES, TRAINING DATA POISONING, & UNAUTHORIZATION DATA RETRIEVAL

SECURITY AWARENESS & PROTECTION AGAINST **AI-POWERED SCAMS**, SOCIAL ENGINEERING ATTACKS

LEAKAGE OF DATA ON 3RD PARTY TOOLS, CHATBOTS, & SHADOW AI

SUPPLY CHAIN SECURITY - THIRD-PARTY VENDOR SYSTEMS, MODELS, OR TOOLS

REGULATORY **NON-COMPLIANCE** AND OVERSIGHT GAPS

CODE QUALITY, MODEL PERFORMANCE & RELIABILITY RISKS

TOP RISKS & MITIGATION FOCUS AREAS

SHADOW AI

Easy for any employee to often use unlicensed and unmanaged tools or access to 3rd party AI tools, chatbots, leading to leakage of the company

MITIGATION

Setup of AI Security Governance Program, selection of an Advanced robust DLP for blocking browser-based leakage and endpoints

VIBE CODING

Rapid coding has introduced security vulnerabilities through unreviewed code, outdated libraries, technical debt, and licensing issues

MITIGATION

IMPLEMENTATION OF REVAMPED DEVSECOPS PROGRAM

Mandatory code scans before deployment, post-release testing, third-party library security assessments, chatbot testing, and open-source code reviews with human validation and tracking

LOSS OF CUSTOMER TRUST

Your AI-powered rebranding raises concerns about data protection and requires demonstrable assurance, as unexplainable AI decisions, hallucinations, or data breaches could erode client trust

MITIGATION

Conduct an AI Posture Assessment (Phase 1) followed by ISO 42001 Certification (Phase 2) to establish trust

3rd PARTY SECURITY & DEPENDENCY RISK

It is essential to protect organizational and client data from AI-related risks and third-party data leakage, while ensuring uninterrupted critical operations

MITIGATION

REVAMPED VENDOR RISK PROGRAM

Assessing all current & new vendors who support the AI operations along with all vendors who are AI powered (like SaaS) along with gauging dependency risk and SLAs

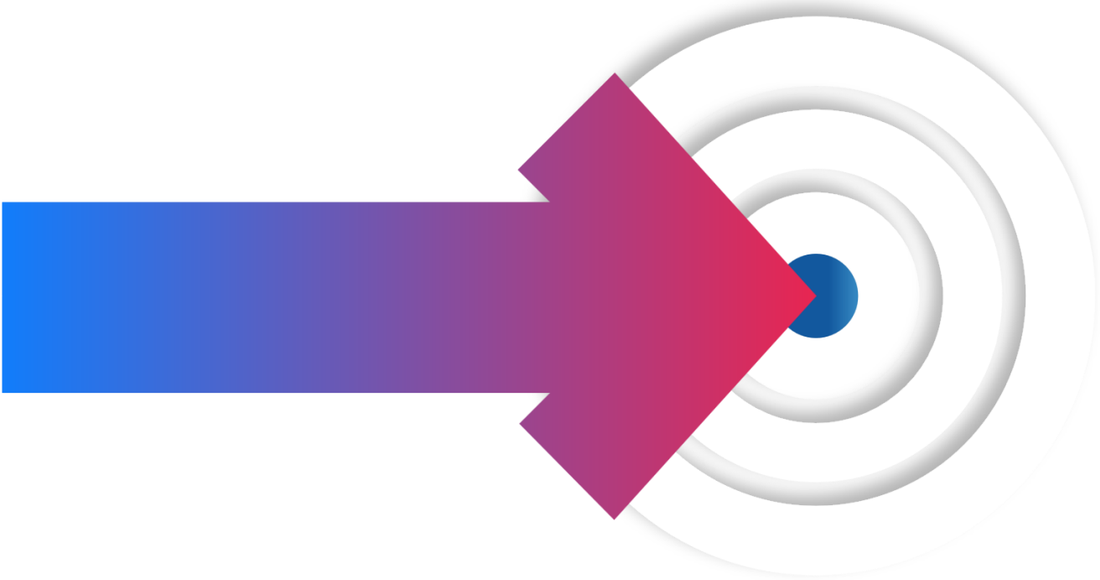
EMPLOYEE SECURITY AWARENESS

There has been a surge in AI-powered scams, including deepfakes and social engineering attacks conducted through email, video, chat, and other digital channels

MITIGATION

Quarterly or semi-annual testing of employee awareness, along with email gateway reviews and enhancements to O365 security controls

ACCORIAN'S AI SECURITY & ASSURANCE ADVISORY



HOW EFFECTIVELY & SECURELY HAVE ORGS ROLLED OUT AI?

- Accorian's AI tiger team has been working with clients to aid them through their AI implementation journey.
- Current clients have found the most value of bringing on our experts during the roadmap, planning and build out phase to review, assess and advise on how to achieve a secure AI implementation.

AI Advisory Services

Phase I Coverage : Day 1 to Day 90

Operationalizing AI to aid efficiency and relevance

AI Strategy and Planning -

Internal Ops:

a) Current AI usage
b) Use case identification and prioritization
c) Build vs Buy
d) Rollout strategies
e) Change management and adoption

Product:

a) Use case identification and prioritization
b) Build vs Buy vs Embed
c) Rollout strategies
d) Agentic workflow design

Securing your current bases

Current Usage:

a) Inventory of current AI tools and shadow AI detection
b) Perimeter check
c) Data flow

Measures:

a) Drafting of AI Security policies & procedures
b) Bolstering your first line of defense for AI risks, threats – SWG, 24*7, DLP, O365 etc
c) Employee awareness
d) Security due diligence of your AI tools
e) Secure rollout of your critical AI tools with guardrails, policies, hardening, processes, testing, reporting – Enterprise chatbot, dev tool, knowledge base etc.
f) Monitoring
g) First pass review of your custom AI implementation

SECURITY FLAWS FOR THE 3 POPULAR AI APPROACHES

1

CO-PILOTS OR, READY TO USE AI TOOL SPRAWL

- Data oversharing & leakage if popular tools used & controls aren't in place
- Permission sprawl
- Zero click vulnerabilities
- Regulatory & compliance issues

2

AI WRAPPERS

- Same as #1
- Prompt injection
- Data exfiltration
- API driven attacks
- System compromise
- API key & credential exposure
- Fine-tuning risks
- Supply chain risks

3

GOING AGENTIC

- Autonomous decision making without oversight
- Identity based attacks
- Untraceable data leakage
- Memory poisoning & data corruption
- Tool misuse & privilege escalation

INDICATIVE NEXT STEPS

CURRENT STATE AI SECURITY / POSTURE ASSESSMENT

- Workshops with all entities to understand current AI usage and security measures
- Inventory of all AI tools + SaaS tools with AI to aid with identifying shadow AI
- Assessing the risk of current AI tools, SaaS, utilities & 3rd parties
- Review of current AI policies & procedures and assessing employee awareness
- Perimeter check to assess if your data is present on popular AI tools*
- Assessing current AI coding practices and its security

AI GOVERNANCE FRAMEWORK – POLICIES & CONTROLS

- Rolling out AI security policies as part of setting up a governance framework
- Identification & rollout of a robust DLP to block data leakage on 3rd party AI tools & browser
- Blocking 3rd party AI tools that are not approved
- Review of O365 configuration to ensure strengthened AI spam protection

ISO 42001/HITRUST AI/NIST RMF - Readiness and certification audit

- Readiness Assessment
- Policy & Procedure writing & Implementation Advisory
- Pre-assessment
- Audit

VIBE CODING

- Securing the current configuration of your vibe coding utility
- Revamping of the current DevSecOps and vulnerability management program
- Mandatory code scan and check before each sprint push on production, along with testing after each major release
- 3rd party library for security vulnerabilities and open-source code checks

AI SECURITY AWARENESS TRAININGS

- To be rolled out among all employees

AI TESTING

- Chatbot / Prompt Testing
- Evals to check for performance, bias, safety, accuracy if models are hosted

REVAMPED AI VENDOR RISK AND DEPENDENCY ASSESSMENT

- Identify all 3rd parties - vendors, 3rd parties, tools
- Update questionnaires with questions on AI risk, dependency risk, and revisit all the 3rd parties

CASE STUDY

AUDITING RESPONSIBLE AI GOVERNANCE WITH ISO 42001 AIMS CERTIFICATION

100%	Enterprise-Wide AIMS Implementation	5-Phase
AI Systems Scoped		Certification Cycle

THE CLIENT

A California-based enterprise AI platform provider serving highly regulated industries sought to formalize responsible AI governance by achieving ISO 42001 certification. The organization aimed to strengthen transparency, accountability, and ethical AI deployment across autonomous intelligence solutions operating in Financial Services, Insurance, Healthcare, and High-Tech sectors.

OUR APPROACH

- Defined AI system boundaries and governance ownership under the Artificial Intelligence Management System (AIMS).
- Performed a structured gap assessment across AI lifecycle and governance controls against ISO 42001 requirements.
- Developed governance policies, bias and fairness measurement criteria, and risk assessment frameworks.
- Supported remediation and conducted an internal audit to prepare for certification readiness.

THE RESULT

The organization established a formal Artificial Intelligence Management System aligned with ISO 42001 requirements across its AI lifecycle within 4 months. Governance maturity improved through defined AI objectives, structured bias monitoring, strengthened documentation controls, and formal accountability mechanisms. Certification readiness enhanced stakeholder trust and reinforced the organization’s commitment to transparent and responsible AI practices.

BEFORE	AFTER
Informal AI Governance	ISO 42001-Aligned AIMS
Limited Bias Metrics	Defined AI Objectives
Fragmented Documentation	Structured Governance Controls
No Certified AI Framework	Certified AI Security Framework

ACCORIAN

CASE STUDY

STRENGTHENING CHATBOT SECURITY AGAINST ADVANCED THREATS

100%	24-Hour	100%	200%
Test Coverage	Risk Reporting	Remediation in 30 days	Security Improvement

THE CLIENT

A fast-growing U.S.-based FinTech organization offered an AI-driven, multi-tenant chatbot for financial support and guidance. Due to the chatbot's access to sensitive financial data, the application had a high-risk profile requiring rigorous security validation.

OUR APPROACH

- Conducted AI chatbot penetration testing across APIs, interfaces, and infrastructure.
- Assessed for prompt injection, model manipulation, data leakage, and LLM-specific threats.
- Simulated attacks (XSS, SQLi, command injection) to identify vulnerabilities.
- Delivered tailored remediation plans and best practice documentation.

THE RESULT

- We detected 4 issues and the critical and high vulnerabilities were remediated within **30 days**.
- Security posture improved with a continuous testing strategy and threat advisory support.

BEFORE	AFTER
No formal security assessment	Full chatbot penetration testing completed
Unknown exposure to LLM-specific threats	Prompt injection and model risks mitigated
Critical vulnerabilities unaddressed	All Critical & High issues fixed within 30 days
No testing cadence or advisory framework	Ongoing test calendar & threat advisories

CASE STUDY

STRENGTHENING AI RISK MANAGEMENT AND REGULATORY READINESS

2 High	5 Medium	5-Phase	ISO/IEC 42001
Risks Identified	Risks Identified	Remediation Roadmap Delivered	Readiness Path Defined

THE CLIENT

A FinTech organization leveraging AI-assisted development tools and customer-facing AI features sought clarity on its AI security posture. The board and executive team required visibility into regulatory exposure, data leakage risks, and unmanaged (“shadow”) AI usage across the enterprise.

OUR APPROACH

- Conducted workshops and stakeholder interviews to map AI usage, workflows, and existing security controls.
- Performed an inventory of AI tools and AI-enabled SaaS to identify shadow AI exposure.
- Executed risk assessments across AI applications, development tools, and third-party integrations.
- Tested potential data leakage pathways and reviewed AI coding practices, governance policies, and security awareness coverage.

THE RESULT

Accorian delivered an executive-ready report with prioritized findings and a five-phase remediation roadmap. The assessment identified 2 high-risk and 5 medium-risk issues, enabling targeted corrective action.

The roadmap established structured AI governance controls, strengthened developer and DLP oversight, formalized vendor risk management, and positioned the organization for ISO/IEC 42001 readiness.

BEFORE	AFTER
Limited AI Security Visibility	Board-Level Risk Transparency
Unmanaged Shadow AI Usage	Structured AI Governance Framework
Informal AI Governance Controls	Defined Developer & DLP Controls
Unclear Data Leakage Exposure	ISO 42001 Readiness Path

ACCORIAN

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

info@accorian.com

+1 732 443 3468

HITRUST Authorized External Assessor

Inc. 5000 America's Fastest-Growing Private Companies

PCI Security Standards Council — Approved Scanning Vendor

ISO

AICPA SOC

PCI Security Standards Council — Qualified Security Assessor

CREST PEN TEST

NIST

Forbes India D Globalist Accelerating eXtrepreneurs™