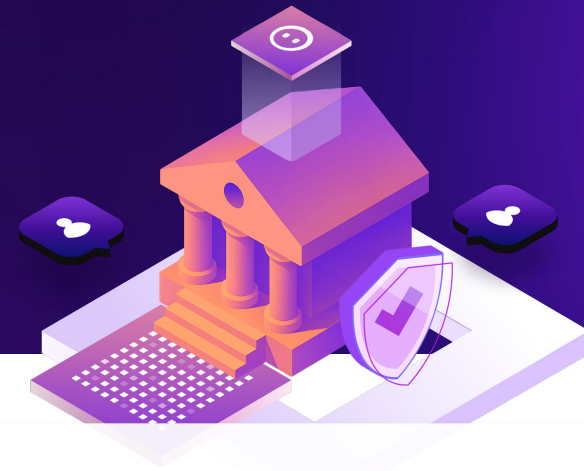


Securonix ISO IEC 42001

GOVERN AI WITH CONFIDENCE EXECUTE WITH CONTROL



Turn AI governance into operational trust

AI is taking on more responsibility in security operations. Governance has to scale with it.

As AI moves from summarizing alerts to performing meaningful security work, CISOs need clear answers: Who is accountable for AI decisions? How are risks assessed? Can actions be explained and audited? Where does human oversight apply?

Securonix has achieved ISO/IEC 42001 certification, the international standard for Artificial Intelligence Management Systems. The independently audited certification provides assurance that Securonix has established a formal system to identify, manage, monitor, and continually improve AI-related risk.

That organizational assurance complements a security AI strategy built around governed execution. Sam, the AI SOC Analyst, accelerates defined Tier 1 and Tier 2 work through Agentic Mesh, while Agentic Guardrails keep activity policy-bound, explainable, auditable, and subject to appropriate human oversight.

Together, these capabilities help enterprises move beyond responsible-AI promises toward governance that can be demonstrated at both the organizational and operational level.



Independent assurance

Use an internationally recognized, independently audited AI management framework to strengthen enterprise trust and vendor due diligence.



Governed execution

Apply policy boundaries, explainability, auditability, approval controls, and human supervision as AI performs security work.



Enterprise accountability

Give security, risk, compliance, procurement, and executive stakeholders clearer evidence of how AI governance is managed.

How Governed AI Works

From organizational governance to controlled execution

STEP 1

Establish AI governance

Define policies, roles, accountability, risk-management processes, and management controls for responsible AI.

STEP 2

Govern operational AI

Coordinate AI-assisted security work within defined policy, permission, approval, and human-oversight boundaries.

STEP 3

Monitor and improve

Review AI-related risks and outcomes, preserve auditability, and improve the management system as requirements evolve.



ISO IEC 42001 Management System Assurance

AI governance and accountability

Establish formal responsibility, policies, objectives, and processes around organizational AI use.

AI risk management

Identify, assess, address, and monitor AI-related risks through a structured management approach.

Lifecycle governance

Apply management discipline to the development, provision, operation, and continual improvement of AI systems.

Transparency and monitoring

Support traceability, review, accountability, and ongoing evaluation rather than isolated policy statements.

Securonix Governed AI in Practice

Sam the AI SOC Analyst

Executes and accelerates defined Tier 1 and Tier 2 work while analysts retain authority over consequential decisions.

Agentic Mesh

Coordinates specialized AI agents, security context, workflows, policies, and approvals through a governed execution layer.

Agentic Guardrails

Apply policies, explanations, approval points, audit trails, and human controls to AI-assisted workflows.

Human in the loop control

Analysts can approve, refine, redirect, or intervene and remain accountable for security outcomes.

💡 CISO OUTCOME

Move faster with AI without surrendering control.

Create additional SOC capacity while maintaining the governance, transparency, and accountability required for enterprise adoption.

Common Enterprise Use Cases

Built for CISOs and security leaders adopting AI across regulated, complex, and high-consequence security environments.

AI SUPPLIER AND VENDOR ASSURANCE

Give procurement, security, and third-party risk teams independently audited evidence of a formal AI management system.

REGULATED AI ADOPTION

Support enterprise governance processes with structured AI risk management, accountability, monitoring, and continual improvement.

AI POWERED SECURITY OPERATIONS

Use Sam to accelerate triage, investigation, enrichment, and response preparation while guardrails maintain policy and human-control boundaries.

BOARD AND AUDIT ASSURANCE

Give executives, boards, auditors, and risk committees a clearer account of how operational AI is controlled.

HUMAN OVERSIGHT OF AI EXECUTION

Define where AI can act, where authorization is required, and how analysts can review or intervene.

AI GOVERNANCE AT SCALE

Apply a repeatable management framework as AI use expands instead of creating isolated controls for every implementation.

Why Organizations Choose Securonix

Certification alone is not an operating model. Securonix combines ISO/IEC 42001-certified organizational AI management with product-level controls designed for AI operating inside the SOC.

- ✓ **Governed AI execution:** AI performs defined security work inside explainable, auditable, policy-controlled workflows.
- ✓ **Human accountability:** Analysts maintain authority over consequential security decisions and outcomes.
- ✓ **Measurable AI capacity:** Sam is designed around operational work performed rather than prompts or opaque AI consumption.
- ✓ **Security-native context:** AI workflows can incorporate security telemetry, identity and behavioral analytics, threat intelligence, and investigation history.
- ✓ **Open security operations:** Securonix is designed for heterogeneous enterprise environments rather than a closed ecosystem.
- ✓ **One connected operating model:** Unified Defense SIEM, Agentic Mesh, Sam, advanced analytics, threat intelligence, and data economics work together.

From AI Innovation to AI You Can Govern

Enterprise AI should deliver more capacity, not more uncertainty. Securonix brings together formal AI governance and security-native operational controls to help organizations scale AI responsibly.

✓ CERTIFIED

ISO IEC 42001 AIMS

Independent assurance of a formal AI management system.

🔒 GOVERNED

Policy bound execution

AI operates through defined permissions, workflows, and approval boundaries.

👥 ACCOUNTABLE

Human supervised outcomes

Explainability and auditability help people remain responsible for consequential decisions.

Governed AI Measurable Security Operations

Customers using Sam have reported

60%

Less investigation time

80%

Less Tier 1 workload

3x

Faster incident resolution

Results vary by environment and implementation. These are not outcomes of ISO/IEC 42001 certification.

Breach Ready. Board Ready.

Securonix combines Unified Defense SIEM, governed AI execution, and outcome-aligned data economics to help enterprises modernize security operations without requiring cost, complexity, and headcount to scale at the same rate.

ISO/IEC 42001 certification strengthens the trust model behind that strategy by adding formal governance, risk management, accountability, and continual improvement.

Execution at Scale. Control by Design.

See governed AI in action. Visit securonix.com or contact sales@securonix.com.

