AI Compliance Verification Report

Generated: 2026-01-20 22:05:46.518451
Standard: ISO 42001:2023

Executive Summary (Compliance Scores)

Module	Progress	Score
AI_CyberSecurity_Module.xlsx	41/99	41.4%
AI_Governance_Module.xlsx	0/8	0.0%
AI_Management_Module.xlsx	16/33	48.5%
AI_Privacy_Module.xlsx	22/38	57.9%

Audit Proof & Mapping Details

Mapped Requirements (Evidence Linked)

ID	Requirement	Evidence Source (Deep Link)
1.1	The organization shall identify all AI models, dat...	Mapped via Content Match (ID)
1.2	The organization shall define all applicable lifec...	Mapped via Content Match (ID)
1.3	The organization shall define all organizational, ...	Mapped via Content Match (ID)
1.4	The organization shall identify internal and exter...	Mapped via Explicit Metadata Link
1.5	The organization shall identify all relevant inter...	Mapped via Content Match (ID)
2.1	The organization shall define documented AI securi...	Mapped via Content Match (ID)
2.2	The organization shall define CIA requirements spe...	Mapped via Content Match (ID)
2.3	The organization shall define security objectives ...	Mapped via Explicit Metadata Link
2.4	The organization shall ensure that AI security obj...	Mapped via Content Match (ID)
2.5	The organization shall define AI security objectiv...	Mapped via Content Match (ID)
3.1	The organization shall monitor AI security control...	Mapped via Content Match (ID)
3.2	The organization shall define and monitor AI secur...	Mapped via Content Match (ID)
3.3	The organization shall ensure the integrity of AI ...	Mapped via Content Match (ID)
3.4	The organization shall monitor how AI model perfor...	Mapped via Content Match (ID)
4.1	The organization shall identify AI-specific cybers...	Mapped via Content Match (ID)
4.2	The organization shall analyze identified AI cyber...	Mapped via Content Match (ID)
4.3	The organization shall evaluate analyzed AI cybers...	Mapped via Content Match (ID)
4.4	The organization shall select, design, and impleme...	Mapped via Content Match (ID)

4.5	The organization shall formally accept AI cybersec...	Mapped via Content Match (ID)
A.5.1	The organization shall validate training, testing,...	Mapped via Content Match (ID)
A.5.2	The organization shall protect datasets from unaut...	Mapped via Content Match (ID)
A.5.3	The organization shall detect data poisoning attem...	Mapped via Content Match (ID)
A.5.4	Data pipelines must be secured against interceptio...	Mapped via Content Match (ID)
A.6.1	The organization shall implement mechanisms to det...	Mapped via Content Match (ID)
A.6.2	Models shall undergo adversarial robustness traini...	Mapped via Explicit Metadata Link
A.6.3	Models shall be periodically tested to assess resi...	Mapped via Explicit Metadata Link
A.6.4	The organization shall deploy controls to prevent ...	Mapped via Explicit Metadata Link
A.6.5	Model outputs shall be monitored to identify suspi...	Mapped via Explicit Metadata Link
A.7.1	The organization shall ensure that AI models (weig...	Mapped via Content Match (ID)
A.7.2	The organization shall use a secure model registry...	Mapped via Explicit Metadata Link
A.7.3	The organization shall maintain strict version con...	Mapped via Explicit Metadata Link
A.7.4	Deployment pipelines for AI systems must integrate...	Mapped via Content Match (ID)
A.7.5	The organization shall prevent unauthorized modifi...	Mapped via Explicit Metadata Link
A.7.6	AI model weights and training parameters shall be ...	Mapped via Explicit Metadata Link
A.8.1	APIs exposing AI models shall be protected using r...	Mapped via Content Match (ID)
A.8.2	APIs must implement rate limiting, throttling, and...	Mapped via Content Match (ID)
A.8.3	Controls must prevent attackers from reconstructin...	Mapped via Content Match (ID)
A.8.4	All inputs to AI systems (prompts, images, data) m...	Mapped via Explicit Metadata Link
A.8.5	AI outputs must be screened for harmful, biased, u...	Mapped via Content Match (ID)
A.9.1	Access to AI systems, data pipelines, model regist...	Mapped via Policy Name Match
A.9.2	APIs must be protected using authentication, autho...	Mapped via Content Match (ID)
A.2.1	The organization shall maintain a model registry r...	Mapped via Content Match (ID)
A.2.2	Dataset lineage shall be documented, including sou...	Mapped via Explicit Metadata Link
A.2.3	The organization shall log all AI-related training...	Mapped via Explicit Metadata Link
A.5.1	AI models shall be benchmarked against defined per...	Mapped via Content Match (ID)
A.5.2	The organization shall conduct stress and boundary...	Mapped via Content Match (ID)
A.5.3	The organization shall test susceptibility to adve...	Mapped via Content Match (ID)
A.5.4	The organization shall document potential model fa...	Mapped via Content Match (ID)
A.6.1	High-risk or consequential AI decisions shall incl...	Mapped via Content Match (ID)
A.6.2	For autonomous or semi-autonomous AI, operators mu...	Mapped via Explicit Metadata Link
A.6.3	AI systems shall include override, pause, or fallb...	Mapped via Explicit Metadata Link
A.6.4	Individuals overseeing AI must be trained on syste...	Mapped via Explicit Metadata Link
A.7.1	Vendors providing AI systems, datasets, or model c...	Mapped via Content Match (ID)

A.7.2	The organization shall require documentation from ...	Mapped via Explicit Metadata Link
A.7.3	Vendors shall not modify deployed AI models withou...	Mapped via Explicit Metadata Link
A.7.4	Organizations must continuously monitor third-part...	Mapped via Content Match (ID)
A.7.5	Contracts shall require transparency, logging, acc...	Mapped via Explicit Metadata Link
2.1	The organization shall identify and document all A...	Mapped via Content Match (ID)
2.2	The organization shall document all AI-related dat...	Mapped via Content Match (ID)
2.3	The organization shall define all internal functio...	Mapped via Explicit Metadata Link
2.4	The organization shall map applicable privacy laws...	Mapped via Content Match (ID)
2.5	AI privacy controls must be consistently implement...	Mapped via Content Match (ID)
3.1	The organization shall measure and monitor re-iden...	Mapped via Content Match (ID)
3.2	3.2.a: Measure personal data minimization level. 3...	Mapped via Content Match (ID)
3.3	The organization shall track and maintain oversigh...	Mapped via Content Match (ID)
3.4	The organization shall track and maintain transpar...	Mapped via Content Match (ID)
4.1	Identify risks in how personal data is collected f...	Mapped via Content Match (ID)
4.2	Identify risks in labeling, transforming, or de-id...	Mapped via Content Match (ID)
4.3	Identify risks in training that cause memorization...	Mapped via Content Match (ID)
4.4	Identify risks where AI model outputs may directly...	Mapped via Content Match (ID)
4.5	Identify risks where AI-driven profiling or automa...	Mapped via Content Match (ID)
4.9	Identify risks where AI causes privacy harm or inc...	Mapped via Content Match (ID)
4.1	Identify risks related to DSARs, consent, and tran...	Mapped via Content Match (ID)
A.2	Maintain a risk register covering AI-specific priv...	Mapped via Content Match (ID)
A.5	Personal data used for AI must only be processed f...	Mapped via Content Match (ID)
A.6	AI systems shall collect, use, and process only th...	Mapped via Content Match (ID)
A.7	Organizations shall apply de-identification, pseud...	Mapped via Content Match (ID)
A.8	The organization shall proactively assess, monitor...	Mapped via Content Match (ID)
A.9	The organization shall ensure that AI system outpu...	Mapped via Content Match (ID)

Gap Analysis (Unmapped Requirements)

ID	Requirement	Module
2.6	The organization shall ensure that AI security obj...	AI_CyberSecurity_Module.xlsx
3.5	The organization shall ensure that AI security mon...	AI_CyberSecurity_Module.xlsx
3.6	The organization shall maintain documented procedu...	AI_CyberSecurity_Module.xlsx
A.5.5	The organization shall enforce least privilege and...	AI_CyberSecurity_Module.xlsx
A.8.6	The organization shall implement protections again...	AI_CyberSecurity_Module.xlsx

A.9.3	AI infrastructure (VMs, GPUs, containers, cloud se...	AI_CyberSecurity_Module.xlsx
A.9.4	Controls shall prevent unauthorized or excessive u...	AI_CyberSecurity_Module.xlsx
A.9.5	Training and inference environments must be protec...	AI_CyberSecurity_Module.xlsx
A.9.6	The organization shall ensure strict separation be...	AI_CyberSecurity_Module.xlsx
A.10.1	The organization shall evaluate the security, qual...	AI_CyberSecurity_Module.xlsx
A.10.2	All third-party AI libraries, frameworks, datasets...	AI_CyberSecurity_Module.xlsx
A.10.3	All third-party AI models, APIs, datasets, and ser...	AI_CyberSecurity_Module.xlsx
A.10.4	The organization shall maintain an AI-SBOM listing...	AI_CyberSecurity_Module.xlsx
A.10.5	The organization shall continuously track vulnerab...	AI_CyberSecurity_Module.xlsx
A.11.1	The organization shall implement controls to preve...	AI_CyberSecurity_Module.xlsx
A.11.2	The organization shall deploy robust security meas...	AI_CyberSecurity_Module.xlsx
A.11.3	The organization shall implement output filters to...	AI_CyberSecurity_Module.xlsx
A.11.4	LLM input and output must be logged to support tra...	AI_CyberSecurity_Module.xlsx
A.11.5	LLM behavior must be aligned with organizational s...	AI_CyberSecurity_Module.xlsx
A.11.6	A documented content policy must govern what conte...	AI_CyberSecurity_Module.xlsx
A.11.7	Controls shall be implemented to minimize hallucin...	AI_CyberSecurity_Module.xlsx
A.11.8	Fine-tuning or retraining must follow strict safet...	AI_CyberSecurity_Module.xlsx
A.12.1	The organization shall continuously monitor AI sys...	AI_CyberSecurity_Module.xlsx
A.12.2	The organization shall implement automated detecti...	AI_CyberSecurity_Module.xlsx
A.12.3	Logging must capture activity across data ingestio...	AI_CyberSecurity_Module.xlsx
A.12.4	The organization shall implement model drift detec...	AI_CyberSecurity_Module.xlsx
A.12.5	AI incidents must be detected and correlated acros...	AI_CyberSecurity_Module.xlsx
A.12.6	The organization shall maintain forensic readiness...	AI_CyberSecurity_Module.xlsx
A.12.7	After incidents, the organization must analyze aff...	AI_CyberSecurity_Module.xlsx
A.13.1	The organization shall ensure that all AI training...	AI_CyberSecurity_Module.xlsx
A.13.2	The organization shall maintain full provenance an...	AI_CyberSecurity_Module.xlsx
A.13.3	Access to datasets must follow least privilege and...	AI_CyberSecurity_Module.xlsx
A.13.4	The organization shall implement controls to detec...	AI_CyberSecurity_Module.xlsx
A.13.5	All AI datasets must be stored securely with encry...	AI_CyberSecurity_Module.xlsx
A.13.6	The organization shall limit the collection and us...	AI_CyberSecurity_Module.xlsx
A.13.7	The organization shall ensure accuracy, consistenc...	AI_CyberSecurity_Module.xlsx
A.13.8	When synthetic data is used, the organization shal...	AI_CyberSecurity_Module.xlsx
A.14.1	The organization shall protect AI model files, wei...	AI_CyberSecurity_Module.xlsx
A.14.2	AI models, especially proprietary or sensitive one...	AI_CyberSecurity_Module.xlsx
A.14.3	The organization shall maintain controlled version...	AI_CyberSecurity_Module.xlsx

A.14.4	The organization shall implement protections again...	AI_CyberSecurity_Module.xlsx
A.14.5	Controls shall prevent attackers from inferring tr...	AI_CyberSecurity_Module.xlsx
A.14.6	Organizations shall watermark or uniquely tag mode...	AI_CyberSecurity_Module.xlsx
A.14.7	Deployment processes must ensure that only validat...	AI_CyberSecurity_Module.xlsx
A.14.8	Runtime defenses must monitor model performance, d...	AI_CyberSecurity_Module.xlsx
A.14.9	Model files, weights, access tokens, and configura...	AI_CyberSecurity_Module.xlsx
A.14.10	AI model registries must be secured with access co...	AI_CyberSecurity_Module.xlsx
A.15.1	The organization shall conduct routine stress test...	AI_CyberSecurity_Module.xlsx
A.15.2	The organization shall implement fail-safe control...	AI_CyberSecurity_Module.xlsx
A.15.3	The organization shall protect AI systems from ope...	AI_CyberSecurity_Module.xlsx
A.15.4	The organization shall perform periodic red-team e...	AI_CyberSecurity_Module.xlsx
A.15.5	AI systems shall undergo periodic evaluation of re...	AI_CyberSecurity_Module.xlsx
A.16.1	The organization shall classify incidents that spe...	AI_CyberSecurity_Module.xlsx
A.16.2	The organization shall implement response steps ta...	AI_CyberSecurity_Module.xlsx
A.16.3	Organizations must perform AI-specific forensic an...	AI_CyberSecurity_Module.xlsx
A.16.4	The organization shall define and test procedures ...	AI_CyberSecurity_Module.xlsx
A.16.5	The organization shall incorporate AI-system conti...	AI_CyberSecurity_Module.xlsx
A.16.6	After AI incidents, the organization must capture ...	AI_CyberSecurity_Module.xlsx
E1	The governing body shall evaluate proposed and exi...	AI_Governance_Module.xlsx
E2	The governing body shall evaluate risks arising fr...	AI_Governance_Module.xlsx
D1	The governing body shall set clear direction on ac...	AI_Governance_Module.xlsx
D2	The governing body shall ensure that accountabilit...	AI_Governance_Module.xlsx
D3	The governing body shall direct management to impl...	AI_Governance_Module.xlsx
M1	The governing body shall monitor AI systems to ens...	AI_Governance_Module.xlsx
M2	The governing body shall ensure that AI-related in...	AI_Governance_Module.xlsx
M3	The governing body shall monitor the effectiveness...	AI_Governance_Module.xlsx
A.1.1	The organization shall establish an AI governance ...	AI_Management_Module.xlsx
A.1.2	The organization shall define a mandatory approval...	AI_Management_Module.xlsx
A.1.3	The organization shall maintain an inventory of al...	AI_Management_Module.xlsx
A.3.1	Each AI system shall have design documentation des...	AI_Management_Module.xlsx
A.3.2	Data preparation steps (collection, cleansing, lab...	AI_Management_Module.xlsx
A.3.3	Training must be reproducible through documented c...	AI_Management_Module.xlsx
A.3.4	All AI models shall undergo validation to demonstr...	AI_Management_Module.xlsx
A.3.5	Deployment must require documented approval confir...	AI_Management_Module.xlsx
A.3.6	The organization shall continuously monitor AI per...	AI_Management_Module.xlsx

A.3.7	Retirement procedures shall define archival requir...	AI_Management_Module.xlsx
A.4.1	The organization shall implement CI/CD pipelines w...	AI_Management_Module.xlsx
A.4.2	Models shall include rollback procedures and failo...	AI_Management_Module.xlsx
A.4.3	The organization shall maintain strict separation ...	AI_Management_Module.xlsx
A.4.4	Monitoring thresholds for performance, drift, late...	AI_Management_Module.xlsx
A.4.5	AI infrastructure shall be hardened to ensure reli...	AI_Management_Module.xlsx
A.4.6	Real-time and batch-data quality checks shall be i...	AI_Management_Module.xlsx
A.5.5	Where required by risk level, models shall include...	AI_Management_Module.xlsx
2.1.1	AI systems shall be included in scope if they use,...	AI_Privacy_Module.xlsx
2.1.2	The organization shall include third-party AI serv...	AI_Privacy_Module.xlsx
2.1.3	AI systems capable of inferring, predicting, or re...	AI_Privacy_Module.xlsx
2.6	AI systems shall be excluded from the AI privacy s...	AI_Privacy_Module.xlsx
3.5	Track vendor privacy KPI. Log unauthorized vendor ...	AI_Privacy_Module.xlsx
3.6	Measure response time for privacy incidents. Track...	AI_Privacy_Module.xlsx
3.7	Report AI privacy KPIs to management....	AI_Privacy_Module.xlsx
4.6	Identify risks in storing and retaining AI dataset...	AI_Privacy_Module.xlsx
4.7	Identify privacy risks from vendors or external AI...	AI_Privacy_Module.xlsx
4.8	Identify risks from changes in AI behavior over ti...	AI_Privacy_Module.xlsx
A.1	Assign roles and responsibilities for managing AI ...	AI_Privacy_Module.xlsx
A.3	Map applicable global privacy laws to AI data proc...	AI_Privacy_Module.xlsx
A.4	Document lawful grounds for using personal data in...	AI_Privacy_Module.xlsx
A.10	The organization shall identify, assess, and mitig...	AI_Privacy_Module.xlsx
A.11	The organization shall ensure that individuals are...	AI_Privacy_Module.xlsx
A.12	The organization shall continuously monitor AI sys...	AI_Privacy_Module.xlsx