Limitations and Methodology

Purpose

These tools provide a unified control catalogue and audit questionnaire that consolidates req
multiple frameworks, including NIST SP 800-53, ISO/IEC 27001:2022, ISO/IEC 42001:2023, ISC
HIPAA, HITRUST CSF, CAIQ/CCM, CIS Controls v8, NIST AI RMF 1.0, the EU AI Act, and SIG 202
written in plain language, then cross-mapped to these source frameworks based on professic
interpretive guidance, rather than being copied from any single standard. Cross-mappings are
gap analysis, and internal readiness assessments, not to serve as an authoritative or exhaustiv
applicability and sufficiency against the latest official publications and, where necessary, obta
on these tools for certification, regulatory submissions, or opinions of compliance. EU AI Act r
consolidated Regulation text dated 27 July 2026; applicability varies by operator role, system

Insertion note

This sheet was added to preserve the original structure and formulas of the workbook while c
or mapped content.

quirements and good-practice guidance from
O 31000:2018, SOC 2, GDPR, NIS2, DORA, PCI DSS v4,
1. Control statements and audit questions are
onal judgement, publicly available cross-walks, and
e indicative: they are designed to support scoping,
ve legal mapping. Users must always validate
ain formal legal or regulatory advice before relying
references in this version were reviewed against the
classification, and phased application date.

clearly separating explanatory language from scored

AI AUDIT QUESTION

Comprehensive AI/ML Systems Audit Tool — Applic

PURPOSE

This workbook provides a structured, framework-aligned questionnaire for auditing AI and ma
It covers the full AI lifecycle from governance through deployment, monitoring, and retirement
party AI risk, incident response, regulatory compliance, and generative AI.

HOW TO USE THIS WORKBOOK

1. Each tab represents an audit domain. Work through each domain tab sequentially or pri

2. For each question, assess the organization's current state and assign a Maturity Rating
below.

3. Record evidence references, auditor observations, and identified gaps in the designated

4. The Scoring Dashboard tab automatically aggregates maturity scores by domain, provid

5. Framework mappings are embedded in each domain tab across the NIST AI RMF, ISO/
columns.

MATURITY RATING SCALE

1 — Initial	Ad hoc or absent. No formal AI-specific policies, processes, or managed.
2 — Developing	Awareness exists and some informal practices are emerging specific teams. Key gaps remain.
3 — Defined	Formal policies, processes, and controls are documented an responsibilities are assigned. Compliance is monitored.
4 — Managed	AI controls are measured, monitored with metrics, and subje are active. Lessons learned are incorporated.
5 — Optimizing	Industry-leading practices. AI governance is fully integrated i emerging risks, regulations, and technologies.

AUDIT DOMAINS

1. AI Governance & Strategy	Governance program, accountability, policies, risk appetite,
2. AI Risk Management	Risk framework alignment, risk assessment, AI system class
3. Data Governance	Training data quality, provenance, bias in data, PII handling,
4. Model Lifecycle	Development, testing, validation, documentation, model carc
5. AI Security	Adversarial robustness, model protection, access controls, r

6. Privacy & Data Protection	PIAs for AI, consent, inference risks, de-identification, indivic
7. Transparency & Ethics	Explainability, human oversight, fairness, responsible AI, prc
8. Third-Party AI Risk	Vendor AI assessment, contracts, SBOMs, API risk, concent
9. Incident Response	AI-specific incident plans, model rollback, failure notification,
10. Regulatory Compliance	EU AI Act, state laws, sector rules (FDA, SR 11-7, EEOC), c
11. Generative AI	LLM controls, prompt security, hallucination, content safety,

FRAMEWORKS REFERENCED

NIST	AI Risk Management Framework — Govern, Map, Measure, Manage functions
ISO/I	AI Management System (AIMS) — Annex A controls and organizational requirements
EU A	Risk-based regulation — Prohibited practices, high-risk obligations, transparency, gener
NIST	Security and Privacy Controls — mapped to relevant AI-adjacent control families
Sect	FDA AI/ML guidance, OCC SR 11-7 (Model Risk), EEOC AI hiring guidance, FTC AI enf

NAIRE

able to Any Environment

chine learning systems in any organizational environment.
:, with dedicated sections for security, privacy, ethics, third-

oritize based on your risk assessment.

from 1 (Initial) to 5 (Optimizing) using the scale defined

l columns.

ling an at-a-glance view of AI risk posture.

IEC 42001, EU AI Act, SP 800-53, and Other Standards

or controls in place. AI risks are not systematically identified

g, but they are inconsistent, undocumented, or limited to

ıd implemented across the organization. Roles and

ct to regular review. Continuous improvement processes

into enterprise risk management. Proactive adaptation to

board oversight

sification, risk appetite

data lifecycle

ds, change management

ed-teaming

dual rights

ohibited uses

tration risk

post-incident review

compliance monitoring

data leakage

al-purpose AI

forcement

e | *2026*

Domain: 1. Governance

7 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
GOV-01	Does the organization have a formal AI governance program with defined roles, responsibilities, and executive-level accountability?
GOV-02	Has the organization defined and documented its risk appetite and tolerance levels specifically for AI/ML systems?
GOV-03	Are AI governance policies reviewed and updated on a defined schedule, and do they reflect changes in technology, regulations, and organizational risk?
GOV-04	Does the organization provide AI-specific training and awareness programs for staff involved in developing, deploying, and overseeing AI systems?
GOV-05	Is there a defined process for AI use case approval that requires risk assessment, ethical review, and sign-off before AI systems are developed or deployed?
GOV-06	Does the organization maintain a current, comprehensive inventory of all AI/ML systems, including their purpose, risk classification, data dependencies, and deployment status?
GOV-07	Has the organization designated a senior leader (e.g., Chief AI Officer, AI Ethics Lead) with explicit accountability for AI risk management outcomes?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: AI governance charter, designated AI governance committee or board, named AI ethics officer or equivalent, defined escalation paths. Evidence: policy documents, org charts, committee meeting minutes.	GOVERN 1.1, 1.2	A.2, A.4.1, A.5.1
Look for: documented AI risk appetite statements, risk tolerance thresholds by AI use case type, board-approved risk parameters. Evidence: risk appetite framework, AI risk policy.	GOVERN 1.1, 1.5	A.5.2, A.6.1
Look for: policy review cadence (at minimum annual), version control, change log, evidence of regulatory monitoring feeding into updates. Evidence: policy revision history, regulatory tracking process.	GOVERN 1.3, 1.4	A.5.2, A.9.3
Look for: role-based AI training curriculum (developers, users, executives, auditors), completion tracking, refresher cadence. Evidence: training materials, LMS records, attendance logs.	GOVERN 2.1, 2.2	A.4.2, A.7.2
Look for: AI use case intake form, stage-gate review process, approval authority matrix, documented rejection criteria. Evidence: approval records, review board minutes.	GOVERN 1.3, MAP 1.1	A.6.1, A.8.2
Look for: centralized AI system register, fields for model type/purpose/owner/risk tier/status/data sources, regular reconciliation. Evidence: system inventory, CMDB entries.	GOVERN 1.6, MAP 1.1	A.5.4, A.8.1
Look for: named individual with AI oversight in job description, reporting line to board or C-suite, budget authority. Evidence: role description, organizational announcement, reporting structure.	GOVERN 1.2	A.5.1, A.5.3

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 9(1), Art. 26	PM-1, PM-2		
Art. 9(2)	PM-9, RA-3		
Art. 9(9)	PM-1, PL-2		
Art. 4	AT-2, AT-3		
Art. 9(1), Art. 26(1)	PL-2, RA-3, CA-6		
Art. 49 (registration, where applicable); Art. 71 (EU database)	CM-8, PM-5		
Art. 26(2)	PM-2		

Evidence / Findings / Gaps

Domain: 2. Risk Management

6 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
RISK-01	Has the organization adopted or mapped its AI risk management practices to a recognized framework (e.g., NIST AI RMF, ISO/IEC 42001)?
RISK-02	Does the organization classify AI systems by risk level, and are controls applied proportionate to each system's risk tier?
RISK-03	Are AI-specific risk assessments conducted prior to deployment and periodically thereafter, covering technical, ethical, legal, and reputational risks?
RISK-04	Does the organization assess the potential for AI systems to cause harm to individuals, groups, communities, or the environment?
RISK-05	Are AI risk assessment results formally communicated to senior leadership and integrated into enterprise risk reporting?
RISK-06	Does the organization maintain documented risk treatment plans with owners, timelines, and acceptance criteria for residual AI risks?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: explicit framework adoption statement, gap analysis against chosen framework, roadmap for full alignment. Evidence: framework mapping document, gap analysis report.	GOVERN 1.1, All functions	A.5.1, A.6.1
Look for: risk classification taxonomy (e.g., minimal/limited/high/unacceptable), defined control baselines per tier, evidence of proportionate control application. Evidence: classification criteria, system risk register.	MAP 1.5, MAP 2.1	A.6.1, A.8.2
Look for: pre-deployment risk assessment template covering all four dimensions, periodic reassessment schedule, trigger-based reassessment criteria. Evidence: completed risk assessments, review cadence documentation.	MAP 2.1, MAP 2.2, MEASURE 2.1	A.6.1, A.8.2
Look for: impact assessment methodology addressing individual rights, group fairness, societal effects, and environmental costs (e.g., energy consumption). Evidence: impact assessments, harm taxonomy.	MAP 2.2, MAP 5.1	A.6.1.2, A.8.4
Look for: AI risk dashboard or reporting template, inclusion in enterprise risk register, board/committee reporting cadence. Evidence: risk committee presentations, board minutes.	GOVERN 1.5, MANAGE 4.1	A.5.3, A.9.3
Look for: risk treatment register with named owners, target dates, residual risk acceptance authority. Evidence: risk treatment plans, risk acceptance sign-offs.	MANAGE 1.1, MANAGE 2.1	A.6.1, A.8.3

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 9	PM-9, RA-3		
Art. 6, Art. 7, Annex III	RA-2, RA-3	EU AI Act risk tiers	
Art. 9(2), Art. 9(9)	RA-3, RA-5, CA-2		
Art. 9(2)(a), Recital 47	RA-3, RA-8		
Art. 9(9)	PM-9, PM-28		
Art. 9(2)	PM-4, RA-3		

Evidence / Findings / Gaps

Domain: 3. Data Governance

7 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
DATA-01	Does the organization maintain documented policies and procedures for governing AI/ML training, validation, and test data?
DATA-02	Are data quality checks systematically performed on training data, including completeness, accuracy, consistency, timeliness, and representativeness?
DATA-03	Does the organization assess training data for bias, including underrepresentation, historical bias, and label bias, with documented remediation?
DATA-04	Is data provenance (lineage and sourcing) documented for all training, validation, and test datasets, including third-party data?
DATA-05	Are there controls ensuring that personally identifiable information (PII) in training data is handled in compliance with applicable privacy laws and organizational policy?
DATA-06	Does the organization enforce data retention and deletion policies specific to AI training data and model artifacts?
DATA-07	Are there controls to prevent unauthorized use of copyrighted, licensed, or restricted data in AI model training?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: data governance policy specific to AI/ML, data quality standards, documented data lifecycle processes. Evidence: data governance framework, data management procedures.	MAP 2.3, MANAGE 1.3	A.8.5, B.6.3
Look for: automated data quality pipelines, defined quality metrics and thresholds, remediation procedures for quality failures. Evidence: data quality reports, pipeline configurations.	MAP 2.3, MEASURE 2.6	A.8.5, B.6.3
Look for: bias assessment methodology, statistical analysis of protected attribute distributions, documented remediation actions (e.g., resampling, re-labeling). Evidence: bias audit reports, fairness metrics.	MAP 2.3, MEASURE 2.6, MEASURE 2.11	A.8.4, B.6.3
Look for: data lineage tracking tool or register, documentation of data sources, transformations, and chain of custody. Evidence: data lineage diagrams, provenance logs.	MAP 2.3	A.8.5, B.6.3
Look for: PII scanning/detection in datasets, consent verification, purpose limitation enforcement, data minimization practices. Evidence: PII scan reports, data processing agreements.	MAP 2.3, GOVERN 1.1	A.8.5, B.6.4
Look for: AI-specific retention schedules, automated deletion workflows, evidence of enforcement. Evidence: retention policy, deletion logs, storage audits.	MANAGE 2.3	A.8.5, B.6.4
Look for: data licensing review process, IP compliance checks before training, approved data source register. Evidence: license inventory, legal review records.	MAP 2.3, GOVERN 1.1	A.8.5

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 10(1)	PM-24, SI-12		
Art. 10(2)(f)	SI-7, PM-24		
Art. 10(2)(f), Art. 10(2)(g)	RA-3, SI-4	EEOC AI guidance	
Art. 10(2)(b)	SR-4, SA-12		
Art. 10(5)	PT-2, PT-3, SI-19	GDPR Art. 6, 9	
Art. 10(5), Art. 12(4)	SI-12, MP-6		
Art. 53(1)(c) (GPAI providers, where applicable)	SA-4, PM-24	Copyright Act, DMCA	

Evidence / Findings / Gaps

Domain: 4. Model Lifecycle

7 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
LIFE-01	Does the organization follow a documented AI/ML model development lifecycle (MDLC) with defined stages, quality gates, and required documentation?
LIFE-02	Are model design decisions documented, including architecture choices, feature selection rationale, training approach, and known limitations?
LIFE-03	Are AI/ML models validated by individuals or teams independent of the development team prior to production deployment?
LIFE-04	Does the organization maintain model cards or equivalent documentation for each deployed AI/ML model, including intended use, performance metrics, limitations, and ethical considerations?
LIFE-05	Is there a formal change management process for AI/ML models, including version control, impact assessment for changes, and rollback procedures?
LIFE-06	Does the organization have a defined process for model retirement, including criteria for decommissioning, data disposal, and stakeholder notification?
LIFE-07	Are AI/ML models tested for performance, accuracy, robustness, and fairness against defined benchmarks before deployment, and are test results documented?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: MDLC framework document, stage-gate criteria (design, develop, validate, deploy, monitor, retire), required artifacts per stage. Evidence: MDLC policy, project records.	MAP 1.1, MANAGE 1.1	A.8.2, A.8.4
Look for: model design documents, architecture decision records, feature engineering rationale, documented constraints and assumptions. Evidence: design docs, model cards.	MAP 1.5, MAP 3.1	A.8.2, B.6.2
Look for: independent validation function (separate from development), validation methodology, sign-off authority. Evidence: validation reports, organizational separation documentation.	MEASURE 2.1, MEASURE 2.5	A.8.4, A.9.2
Look for: standardized model card template, completed cards for all production models, inclusion of fairness metrics and known failure modes. Evidence: model card repository.	MAP 1.1, MAP 1.5, MEASURE 2.5	A.8.2, B.6.2
Look for: model versioning system (e.g., MLflow, DVC), change impact assessment template, documented rollback procedure, approval workflow for model updates. Evidence: version control logs, change records.	MANAGE 2.2, MANAGE 2.4	A.8.2, A.8.3
Look for: model retirement criteria (e.g., sustained performance below threshold, regulatory change), disposal procedures for model artifacts and training data, communication plan. Evidence: retirement policy, decommission records.	MANAGE 2.3, MANAGE 2.4	A.8.2, A.8.5
Look for: test plans with defined metrics and thresholds, benchmark datasets, test execution records, pass/fail criteria. Evidence: test reports, benchmark results.	MEASURE 2.5, MEASURE 2.6	A.8.4, B.6.5

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 9(1), Art. 17	SA-3, SA-15	SR 11-7 (OCC)	
Art. 11, Art. 13	SA-15(1), SA-8		
Art. 43 (conformity assessment, where applicable); no general requirement for independent internal validation	SA-11, SA-11(3)	SR 11-7 (OCC)	
Art. 11, Art. 13	CM-8, SA-15		
Art. 9(9), Art. 12	CM-3, CM-9, SA-10		
Art. 12(4)	SA-15(11), SI-12		
Art. 9(5), Art. 10(4)	SA-11, CA-2	SR 11-7	

	Evidence / Findings / Gaps

Domain: 5. Security

6 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
SEC-01	Does the organization assess and mitigate adversarial threats specific to AI/ML systems, including data poisoning, evasion attacks, model extraction, and model inversion?
SEC-02	Are AI/ML model artifacts (weights, parameters, training data, configuration) protected with appropriate access controls, encryption, and integrity verification?
SEC-03	Does the organization conduct adversarial testing (red-teaming) of AI/ML systems prior to deployment and on an ongoing basis?
SEC-04	Are input validation and output filtering controls implemented for AI/ML systems to detect and prevent adversarial or anomalous inputs and harmful outputs?
SEC-05	Are AI/ML inference endpoints and APIs secured against unauthorized access, rate-limited to prevent model extraction, and monitored for anomalous query patterns?
SEC-06	Does the organization's vulnerability management program include AI-specific vulnerabilities (e.g., supply chain risks in ML libraries, known model weaknesses)?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: AI-specific threat model, adversarial attack taxonomy, countermeasures mapped to each threat. Evidence: threat assessment, penetration test reports, red-team findings.	MANAGE 1.3, MEASURE 2.7	A.8.4, B.6.5
Look for: role-based access to model repositories, encryption at rest and in transit for model artifacts, integrity checksums. Evidence: access control lists, encryption configurations, audit logs.	MANAGE 1.3	A.8.4, B.6.5
Look for: AI red-team program, defined scope and methodology, regular cadence, findings tracked to remediation. Evidence: red-team reports, remediation tracking.	MEASURE 2.7, MEASURE 2.8	A.8.4, B.6.5
Look for: input sanitization pipelines, anomaly detection on inputs, output content filters, guardrails. Evidence: pipeline configurations, filter rule sets, test results.	MANAGE 1.3, MEASURE 2.7	A.8.4
Look for: authentication/authorization on all AI endpoints, rate limiting, query anomaly detection, logging. Evidence: API gateway configs, monitoring dashboards, incident logs.	MANAGE 1.3	A.8.4, B.6.5
Look for: AI/ML libraries in vulnerability scanning scope, tracking of CVEs in ML frameworks (TensorFlow, PyTorch, etc.), patching cadence. Evidence: vulnerability scan reports, patching records.	MANAGE 1.3	A.8.4

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 9(2)(d)	SI-3, SI-7, SA-11	MITRE ATLAS	
Art. 15(3)	AC-3, SC-28, SI-7		
Art. 9(6)	CA-8, SA-11(5)	MITRE ATLAS	
Art. 9(2)(d), Art. 15(4)	SI-10, AC-4, SI-3		
Art. 15(3)	AC-3, AC-17, SI-4, AU-12		
Art. 15(1)	RA-5, SI-2, SR-3		

Evidence / Findings / Gaps

Domain: 6. Privacy

6 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
PRIV-01	Does the organization conduct privacy impact assessments (PIAs) specifically tailored to AI/ML systems, addressing inference risks, profiling, and emergent data uses?
PRIV-02	Are data minimization principles enforced in AI/ML training, ensuring only necessary personal data is collected and retained?
PRIV-03	Does the organization assess and mitigate the risk that AI/ML models could memorize, reconstruct, or leak personal data from training sets?
PRIV-04	Are individuals informed when AI/ML systems are used to make decisions about them, and are they provided with meaningful information about the logic involved?
PRIV-05	Do individuals have the right to contest or request human review of decisions made solely by AI/ML systems, and is this right operationalized?
PRIV-06	Does the organization enforce purpose limitation for personal data used in AI training, ensuring it is not repurposed beyond the original consent or legal basis?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: AI-specific PIA template, coverage of inference/profiling/re-identification risks, completed PIAs for all AI systems processing personal data. Evidence: PIA reports.	MAP 2.2, MAP 5.1	A.8.4, B.6.4
Look for: data minimization reviews during model design, documentation of necessity for each data element, anonymization/pseudonymization where possible. Evidence: data review records, anonymization reports.	MAP 2.3, GOVERN 1.1	A.8.5, B.6.4
Look for: memorization testing (e.g., membership inference attacks as part of validation), differential privacy or other privacy-preserving techniques, canary testing. Evidence: privacy attack test reports.	MEASURE 2.6, MEASURE 2.7	A.8.4, B.6.4
Look for: AI-specific privacy notices, layered disclosures, individual notification mechanisms. Evidence: privacy notices, UI disclosures, communication templates.	GOVERN 1.4, MAP 5.2	A.8.4, B.6.7
Look for: documented contestation process, accessible mechanism for individuals to request review, SLA for human review, tracking and outcomes reporting. Evidence: process documentation, complaint logs.	GOVERN 1.4, MAP 5.2	A.8.4, B.6.7
Look for: purpose limitation controls in data pipelines, consent tracking, legal basis documentation per dataset, prohibition on unauthorized repurposing. Evidence: data use agreements, consent records.	MAP 2.3, GOVERN 1.1	A.8.5, B.6.4

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 26(9) (high-risk deployers, where applicable); GDPR Art. 35	RA-8, PL-5, PT-2	GDPR Art. 35, 36	
Art. 10(5)	PT-2, PT-3, SI-12	GDPR Art. 5(1)(c)	
Art. 10(5), Art. 15(4)	SI-19, SC-28, SI-7		
Art. 13, Art. 86(1)	PT-4, PT-5	GDPR Art. 13(2)(f), 14(2)(g)	
Art. 86 (right to explanation, where applicable); GDPR Art. 22 may also apply	PT-4, PT-8	GDPR Art. 22	
Art. 10(5)	PT-2, PT-3	GDPR Art. 5(1)(b)	

Evidence / Findings / Gaps

Domain: 7. Transparency & Ethics

6 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
TRANS-01	Does the organization provide appropriate levels of explainability for AI/ML system outputs, proportionate to the risk and impact of decisions?
TRANS-02	Does the organization conduct regular bias and fairness assessments on AI/ML models, particularly those affecting individuals, using recognized fairness metrics?
TRANS-03	Does the organization maintain and enforce a responsible AI/ethical AI use policy that defines prohibited applications and high-risk review requirements?
TRANS-04	Are there documented policies and technical controls ensuring meaningful human oversight of AI-driven decisions with significant consequences for individuals?
TRANS-05	Does the organization publicly disclose or make available information about its high-risk AI systems, including their purpose, capabilities, and limitations?
TRANS-06	Does the organization have a process for employees, stakeholders, or affected individuals to raise ethical concerns about AI systems without fear of retaliation?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: explainability requirements by risk tier, implemented techniques (e.g., SHAP, LIME, counterfactual), user-facing explanations for high-impact decisions. Evidence: explainability standards, example explanations.	MAP 1.5, MEASURE 2.11	A.8.4, B.6.7
Look for: fairness metrics defined per use case (demographic parity, equalized odds, etc.), regular assessment cadence, documented remediation. Evidence: fairness audit reports.	MEASURE 2.6, MEASURE 2.11	A.8.4, B.6.5
Look for: responsible AI policy, prohibited use list (e.g., manipulative AI, mass surveillance, social scoring), mandatory review for high-risk uses, enforcement mechanism. Evidence: policy document, review records.	GOVERN 1.3, GOVERN 1.4	A.5.2, A.8.2
Look for: human-in-the-loop/on-the-loop requirements by risk tier, ability to override AI decisions, reviewer training, audit trail of human-AI interactions. Evidence: oversight policy, override logs.	GOVERN 1.4, MAP 3.3, MANAGE 1.2	A.8.4, B.6.7
Look for: public AI transparency report, AI system registry (internal or external), published model cards for high-risk systems. Evidence: transparency reports, published documentation.	GOVERN 1.4, MAP 1.5	A.8.2, B.6.7
Look for: AI ethics reporting channel (hotline, form), whistleblower protections, documented investigation process, tracking and outcomes. Evidence: reporting mechanism, case log.	GOVERN 1.4	A.5.2

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 13, Art. 86(1)	PT-4, PT-5		
Art. 9(2)(a), Art. 10(2)(f)	RA-3, SI-4, CA-2	EEOC AI guidance	
Art. 5 (Prohibited), Art. 6-7 (High-risk)	PL-4, PM-9		
Art. 14, Art. 26(2)	AC-3, PT-8, AU-12		
Art. 49, Art. 71; Art. 53(1)(d) (GPAI providers, where applicable)	PL-4, PT-5		
No direct EU AI Act mapping	PM-9, PL-4		

Evidence / Findings / Gaps

Domain: 8. Third-Party AI

6 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
TPAI-01	Does the organization conduct AI-specific risk assessments of third-party vendors before integrating their AI models, APIs, or AI-enabled services?
TPAI-02	Do vendor contracts include AI-specific terms covering model governance, data usage restrictions, performance guarantees, change notification, audit rights, and liability?
TPAI-03	Does the organization maintain an inventory of all third-party AI components, including foundation models, APIs, embedded ML, and AI SaaS services?
TPAI-04	Does the organization assess concentration risk arising from dependency on a small number of AI providers, foundation models, or AI infrastructure providers?
TPAI-05	Does the organization require and verify AI model transparency from vendors, including model cards, data sheets, or equivalent documentation for integrated AI systems?
TPAI-06	Are third-party AI systems subject to the same bias, fairness, and performance testing requirements as internally developed models?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: AI-specific vendor risk assessment questionnaire, pre-integration evaluation criteria, documented approval process. Evidence: completed assessments, approval records.	GOVERN 1.6, MAP 1.1	A.8.2, A.8.5
Look for: AI-specific contract clauses/addenda, restrictions on using customer data for training, model change notification SLAs, right-to-audit provisions. Evidence: contract templates, executed agreements.	GOVERN 1.6	A.8.5
Look for: third-party AI register, fields for provider/model/version/data flow/risk tier, regular reconciliation. Evidence: inventory, procurement integration.	MAP 1.1, GOVERN 1.6	A.8.1, A.8.5
Look for: AI vendor concentration analysis, single-point-of-failure assessment, contingency plans for provider disruption. Evidence: concentration risk report, contingency plans.	GOVERN 1.6, MANAGE 2.3	A.6.1
Look for: vendor transparency requirements in RFPs and contracts, received model documentation, verification process. Evidence: vendor model cards, data sheets, evaluation records.	MAP 1.5, GOVERN 1.6	A.8.5, B.6.2
Look for: uniform testing standards regardless of source, third-party model validation process, ongoing monitoring of vendor model performance. Evidence: test reports for vendor models.	MEASURE 2.5, MEASURE 2.6	A.8.4, A.8.5

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 25(4) (high-risk value-chain agreements, where applicable)	SA-4, SA-9, SR-6		
Art. 25(4); Art. 26 (deployer obligations, where applicable)	SA-4, SA-9		
Art. 25 (value-chain responsibilities); Art. 49 (registration, where applicable)	CM-8, SA-9, SR-4		
No direct EU AI Act concentration-risk requirement; Art. 25 is relevant to value-chain dependencies	SA-9, SR-3(1)		
Art. 13; Art. 25(2), Art. 25(4) (where applicable)	SA-4(2), SA-15		
Art. 9, Art. 15; Art. 25 (where applicable)	SA-11, CA-2		

Evidence / Findings / Gaps

Domain: 9. Incident Response

5 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
IR-01	Does the organization's incident response plan include AI/ML-specific scenarios such as model failure, adversarial attack, biased outputs, data poisoning, and unintended autonomous actions?
IR-02	Does the organization have model rollback capabilities allowing rapid reversion to a previous known-good model version in the event of an AI incident?
IR-03	Are AI-related incidents tracked, analyzed for root cause, and fed back into model improvement and governance processes?
IR-04	Does the organization have defined notification procedures for stakeholders, regulators, and affected individuals when AI incidents cause or may cause harm?
IR-05	Are AI incident response procedures tested through tabletop exercises or simulations at least annually?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: AI-specific incident categories in IR plan, defined severity levels, response procedures per scenario type. Evidence: IR plan AI sections, tabletop exercise records.	MANAGE 3.1, MANAGE 3.2	A.8.3, A.6.1.3
Look for: model versioning with rollback capability, tested rollback procedures, defined rollback triggers, RTO for model rollback. Evidence: rollback test records, version control system.	MANAGE 2.2, MANAGE 3.2	A.8.3
Look for: AI incident register, root cause analysis methodology, linkage to model improvement backlog, governance reporting on incident trends. Evidence: incident log, RCA reports, improvement records.	MANAGE 3.1, MANAGE 4.1	A.8.3, A.9.2, A.10.1
Look for: AI incident notification policy, stakeholder/regulator notification thresholds, individual notification templates, timeline requirements. Evidence: notification procedures, communication templates.	MANAGE 3.2	A.8.3, A.6.1.3
Look for: AI-specific tabletop exercise schedule, scenario library, post-exercise improvement actions. Evidence: exercise reports, lessons learned, action item tracking.	MANAGE 3.2	A.8.3

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 9; Art. 72-73 (high-risk systems, where applicable)	IR-4, IR-8		
Art. 15(5)	CM-3, IR-4		
Art. 9(9), Art. 72-73	IR-5, IR-6, PM-4		
Art. 26(5), Art. 73 (high-risk systems, where applicable)	IR-6, IR-6(3)	GDPR Art. 33, 34	
Art. 9(9)	IR-3, CP-4		

Evidence / Findings / Gaps

Domain: 10. Regulatory

6 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
REG-01	Does the organization maintain a regulatory monitoring process that tracks emerging AI-specific laws, regulations, standards, and enforcement actions across all applicable jurisdictions?
REG-02	If subject to the EU AI Act, has the organization classified its AI systems according to the Act's risk tiers and implemented corresponding obligations?
REG-03	Does the organization comply with sector-specific AI requirements (e.g., FDA AI/ML guidance for medical devices, OCC SR 11-7 for financial model risk, EEOC guidance for AI in hiring)?
REG-04	For high-risk AI systems, does the organization maintain technical documentation sufficient to demonstrate compliance with applicable regulatory requirements?
REG-05	Does the organization have a process for conducting conformity assessments or independent audits of high-risk AI systems?
REG-06	Are AI-generated outputs appropriately labeled or disclosed as AI-generated where required by regulation or organizational policy?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: regulatory tracking mechanism, assigned responsibility, cadence of review, documented gap assessments when new regulations emerge. Evidence: regulatory tracker, gap analysis reports.	GOVERN 1.1, GOVERN 1.3	A.5.2, A.6.1
Look for: EU AI Act risk classification for all applicable systems, conformity assessment evidence for high-risk systems, prohibited practice screening. Evidence: classification register, conformity documentation.	MAP 1.5, GOVERN 1.1	A.6.1, A.8.2
Look for: sector-specific compliance mapping, evidence of adherence to relevant guidance, regulatory submissions or filings. Evidence: compliance checklists, regulatory correspondence.	GOVERN 1.1	A.5.2, A.6.1
Look for: comprehensive technical documentation package per high-risk system, version control, accessibility for regulators. Evidence: documentation repository, completeness checklist.	MAP 1.5, MEASURE 2.5	A.8.2, B.6.2
Look for: conformity assessment procedures, internal or third-party audit program for AI, auditor qualifications, findings tracking. Evidence: audit reports, conformity certificates.	MEASURE 2.5	A.9.2, A.9.3
Look for: AI content labeling policy, technical implementation of labeling/watermarking, compliance monitoring. Evidence: policy, labeled output examples, monitoring reports.	GOVERN 1.4	A.8.4, B.6.7

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 9(1)	PM-1, CA-2		
Art. 5-7, Art. 9-15, Annex III	RA-2, CA-2	EU AI Act	
Art. 9(1)	CA-2, PM-1	FDA, SR 11-7, EEOC	
Art. 11, Annex IV	SA-15, PL-2		
Art. 43, Art. 44	CA-2, CA-2(3)		
Art. 50	PT-4, PT-5		

Evidence / Findings / Gaps

Domain: 11. Generative AI

7 questions | Rate each 1-5 (Initial → Optimizing)

Ref #	Audit Question
GEN-01	Does the organization have a specific policy governing the use of generative AI and large language models (LLMs), both internally and in customer-facing applications?
GEN-02	Are controls in place to prevent prompt injection, jailbreak, and other adversarial manipulation of generative AI systems?
GEN-03	Does the organization implement controls to detect and mitigate hallucinations, fabricated content, and factual inaccuracies in generative AI outputs?
GEN-04	Are there controls preventing sensitive data (PII, trade secrets, confidential information) from being included in prompts sent to external generative AI services?
GEN-05	Does the organization clearly label or disclose AI-generated content to recipients, particularly in customer-facing or public communications?
GEN-06	Does the organization assess and manage intellectual property risks associated with generative AI, including copyright infringement in outputs and ownership of AI-generated works?
GEN-07	Does the organization monitor and control the use of shadow or unauthorized generative AI tools by employees?

Guidance / Expected Evidence	NIST AI RMF	ISO/IEC 42001
Look for: generative AI acceptable use policy, approved and prohibited use cases, employee guidance, customer-facing deployment standards. Evidence: policy document, communication records.	GOVERN 1.1, GOVERN 1.3	A.5.2, A.8.2
Look for: input sanitization, system prompt protection, adversarial testing for prompt attacks, monitoring for jailbreak attempts. Evidence: security architecture, red-team reports, monitoring dashboards.	MANAGE 1.3, MEASURE 2.7	A.8.4
Look for: grounding mechanisms (RAG, knowledge bases), output verification processes, confidence scoring, human review for high-stakes outputs. Evidence: architecture documentation, accuracy testing results.	MEASURE 2.5, MEASURE 2.6	A.8.4, B.6.5
Look for: DLP controls on AI prompts, approved vs. restricted data classifications for AI use, technical enforcement (e.g., proxy, API gateway). Evidence: DLP policies, technical controls, scan reports.	MANAGE 1.3, GOVERN 1.1	A.8.4, A.8.5, B.6.4
Look for: AI content labeling standards, technical implementation (metadata, watermarks, disclosures), compliance monitoring. Evidence: labeling policy, implementation examples.	GOVERN 1.4	A.8.4, B.6.7
Look for: IP risk assessment for generative AI, legal review process for AI-generated content, terms of service analysis for AI providers. Evidence: legal opinions, IP policy, provider ToS reviews.	GOVERN 1.1, MAP 5.1	A.6.1
Look for: approved AI tool list, technical controls to detect unauthorized AI tool usage (network monitoring, endpoint DLP), employee acknowledgment. Evidence: approved tool register, monitoring reports.	GOVERN 1.1, MANAGE 1.3	A.5.2, A.8.4

EU AI Act	SP 800-53	Other Standards	Maturity Rating (1-5)
Art. 50; Art. 53 (GPAI providers, where applicable)	PL-4, PM-9		
Art. 9(2)(d), Art. 15(4)	SI-3, SI-10, AC-4	OWASP LLM Top 10	
Art. 15(1)-(2) (high-risk systems, where applicable)	SI-7, SI-4		
No direct EU AI Act mapping; GDPR/data-protection requirements may apply	AC-4, PT-2, SC-7		
Art. 50	PT-4, PT-5		
Art. 53(1)(c) (GPAI providers, where applicable)	SA-4, PM-9	Copyright Act	
Art. 4	CM-7, CM-10, SI-4		

Evidence / Findings / Gaps

AI AUDIT SCORING DASHE

Automated summary of maturity ratings across all audit domains

Domain	# Questions	Avg Maturity	Min Rating	Max Rating
1. Governance	7			
2. Risk Management	6			
3. Data Governance	7			
4. Model Lifecycle	7			
5. Security	6			
6. Privacy	6			
7. Transparency & Ethics	6			
8. Third-Party AI	6			
9. Incident Response	5			
10. Regulatory	6			
11. Generative AI	7			
OVERALL	69			

MATURITY RATING INTERPRETATION

Critical (Avg < 2.0)	Significant deficiencies. Immediate remediation
Developing (2.0 - 2.9)	Controls are emerging but inconsistent. Remedi
Adequate (3.0 - 3.9)	Formal controls in place. Monitor for continuous
Strong (4.0 - 5.0)	Mature, measured controls. Industry-leading pra

BOARD

Questions Rated	Completion %	Domain Status
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**
0	0%	**Not Started**

required.
iation plan needed.
improvement.
actices.