AI Audit

– Checklist

TechEd Academy

Learn | Certify | Succeed

AI Audit Checklist – a practical, step-by-step tool designed to help teams evaluate and improve the transparency, fairness, safety, and governance of their AI systems.

Why this matters: AI systems are powerful, but they're not infallible. Whether you're deploying a recommendation engine, an LLM-based chatbot, or an internal automation tool, you must be able to answer key questions:

- Is the model fair and unbiased?
- Are we using the right data, and is it protected?
- Can we explain our outputs?
- Who is accountable for the outcomes?
- Are we aligned with emerging regulations and best practices?

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Governance & Compliance	AI Governance Policies	Does the organization have a documented AI governance framework?	Lack of governance can lead to misaligned AI practices, reputational damage, and regulatory non-compliance.	Review governance documents, policies, and roles related to AI governance.
AI Governance & Compliance	AI Governance Policies	Are AI risk management processes aligned with ISO 42001, NIST AI RMF, and GDPR?	Lack of governance can lead to misaligned AI practices, reputational damage, and regulatory non-compliance.	Assess AI risk management documentation and compare against ISO, NIST, and GDPR standards.
AI Governance & Compliance	AI Governance Policies	Is there an AI ethics committee overseeing AI governance?	Lack of governance can lead to misaligned AI practices, reputational damage, and regulatory non-compliance.	Check meeting minutes, structure, and decision-making authority of the AI ethics committee.
AI Governance & Compliance	Regulatory Compliance	Does the AI system comply with GDPR, ISO 42001, CCPA, or sector-specific regulations?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Review legal compliance documentation and regulatory audit reports.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Governance & Compliance	Regulatory Compliance	Are AI data processing activities documented and legally justified?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Examine data processing policies, logs, and legal bases for AI data use.
AI Governance & Compliance	Regulatory Compliance	Are AI models designed to ensure transparency, explainability, and accountability?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Review AI system documentation, model explanations, and accountability mechanisms.
AI Governance & Compliance	AI Risk Management & Auditing	Is there a risk assessment framework for AI deployment?	Control weakness may expose the organization to operational, legal, or reputational risks.	Evaluate risk assessment frameworks, methodologies, and past risk reports.
AI Governance & Compliance	AI Risk Management & Auditing	Are AI risks monitored and reported regularly?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check AI risk reports, monitoring dashboards, and periodic risk assessments.
AI Governance & Compliance	AI Risk Management & Auditing	Does the organization have a formal AI audit plan?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI audit policies, past audit reports, and compliance review schedules.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Bias Detection & Fairness	AI Training Data Bias Assessment	Is AI training data diverse and representative of different demographics?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review dataset composition, demographic distributions, and data collection sources.
AI Bias Detection & Fairness	AI Training Data Bias Assessment	Has the AI model been tested for racial, gender, or socioeconomic biases?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze bias testing reports, fairness analysis results, and past bias mitigation efforts.
AI Bias Detection & Fairness	AI Training Data Bias Assessment	Are fairness metrics such as Equalized Odds, Disparate Impact, and Statistical Parity applied?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check if fairness metrics are calculated and if disparities are flagged for corrective action.
AI Bias Detection & Fairness	AI Training Data Bias Assessment	Are data preprocessing techniques used to remove historical biases?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review preprocessing methodologies like data balancing, re-weighting, or adversarial debiasing.
AI Bias Detection & Fairness	AI Model Fairness & Transparency	Does the AI model undergo regular bias audits and fairness testing?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine AI audit reports and fairness testing logs for evidence of regular monitoring.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Bias Detection & Fairness	AI Model Fairness & Transparency	Are fairness results documented and reviewed by compliance teams?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review fairness documentation, compliance reports, and stakeholder reviews.
AI Bias Detection & Fairness	AI Model Fairness & Transparency	Does AI have explainability tools (SHAP, LIME) to clarify decisions?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess whether AI models are equipped with SHAP,LIME, or other explainability tools.
AI Bias Detection & Fairness	AI Model Fairness & Transparency	Is AI fairness validated using external tools like IBM AI Fairness 360, Fair learn?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check if AI models have been tested with IBM AI Fairness 360, Fair learn, or similar frameworks.
AI Bias Detection & Fairness	AI Decision Review & Human Oversight	Are AI-generated decisions audited for fairness before deployment?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI decision audit logs and pre-deployment validation reports.
AI Bias Detection & Fairness	AI Decision Review & Human Oversight	Is there a human-in-the-loop process to monitor AI decisions?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine human oversight mechanisms, workflows, and monitoring procedures.
AI Bias Detection & Fairness	AI Decision Review &	Are users given the ability to challenge AI decisions in high-	Control weakness may expose the organization	Verify if appeal mechanisms exist for AI-generated decisions in high-risk areas.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
	Human Oversight	risk applications (e.g., hiring, lending, law enforcement)?	to operational, legal, or reputational risks.	
AI Bias Detection & Fairness	AI Model Security & Access Controls	Are AI models protected with role-based access control (RBAC)?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review access control policies and verify the implementation of RBAC.
AI Bias Detection & Fairness	AI Model Security & Access Controls	Does the AI system require multi-factor authentication (MFA) for access?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check authentication configurations and system logs for MFA enforcement.
AI Bias Detection & Fairness	AI Model Security & Access Controls	Are AI models encrypted at rest and in transit (e.g., AES-256, TLS 1.3)?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review encryption policies and test encryption of stored and transmitted AI data.
AI Bias Detection & Fairness	AI Model Security & Access Controls	Is there logging and monitoring of AI access attempts?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine AI system access logs and monitoring dashboards.
AI Bias Detection & Fairness	Adversarial Attack & AI Model	Are AI models tested against adversarial attacks (evasion, poisoning, model inversion,etc)?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze adversarial robustness testing reports and security evaluations.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
	Tampering Protection			
AI Bias Detection & Fairness	Adversarial Attack & AI Model Tampering Protection	Are AI training datasets protected against data poisoning attacks?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review dataset protection measures and security policies against poisoning attacks.
AI Bias Detection & Fairness	Adversarial Attack & AI Model Tampering Protection	Has AI undergone penetration testing using adversarial AI security tools (e.g., Microsoft Counter fit, Clever Hans)?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine penetration testing reports and security assessments.
AI Bias Detection & Fairness	Adversarial Attack & AI Model Tampering Protection	Is AI output monitored for unexpected behavior caused by adversarial inputs?	Control weakness may expose the organization to operational, legal, or reputational risks.	Monitor AI model behavior logs and validate unexpected output detection mechanisms.
AI Bias Detection & Fairness	AI API & Cloud Security Measures	Are AI APIs secured with OAuth 2.0 authentication and rate limiting?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review API authentication mechanisms, security tokens, and rate-limiting configurations.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Bias Detection & Fairness	AI API & Cloud Security Measures	Does AI use API monitoring and anomaly detection to prevent unauthorized queries?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze API monitoring reports and anomaly detection logs.
AI Bias Detection & Fairness	AI API & Cloud Security Measures	Are AI model weights and datasets secured in cloud environments (AWS, Azure, Google Cloud) with encryption and restricted access?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check cloud security configurations, encryption settings, and access control policies.
AI Bias Detection & Fairness	AI API & Cloud Security Measures	Does AI security comply with ISO 27001, SOC 2, and NIST Cybersecurity Framework?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review cybersecurity audit reports and compliance documentation.
AI Explainability & Transparency	AI Model Interpretability & Documentation	Is AI model documentation comprehensive and accessible for auditors?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI model documentation, system design, and training logs.
AI Explainability & Transparency	AI Model Interpretability & Documentation	Does AI provide clear explanations decision-making processes?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze model explainability reports and decision-making justifications.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Explainability & Transparency	AI Model Interpretability & Documentation	Are AI model parameters, assumptions, and feature importance well-documented?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check documentation of model parameters, key assumptions, and feature importance analysis.
AI Explainability & Transparency	AI Model Interpretability & Documentation	Are explainability frameworks (e.g., SHAP,LIME, Integrated Gradients) used?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine whether SHAP,LIME, or similar frameworks are used for interpretability.
AI Explainability & Transparency	User & Regulatory Explainability Requirements	Does the AI system comply with GDPR 'Right to Explanation'?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Review compliance policies, GDPR documentation, and 'Right to Explanation ' implementation.
AI Explainability & Transparency	User & Regulatory Explainability Requirements	Can end-users understand AI-generated decisions (e.g., loan approvals, hiring)?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Conduct user surveys or tests to evaluate the understandability of AI decisions.
AI Explainability & Transparency	User & Regulatory Explainability Requirements	Is there an explainability dashboard for auditors and compliance teams?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Assess the presence and functionality of an explainability dashboard.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Explainability & Transparency	User & Regulatory Explainability Requirements	Are AI-generated justifications consistent, unbiased, and reproducible?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Review AI justification logs, decision consistency tests, and bias assessments.
AI Explainability & Transparency	AI Transparency & Ethical Compliance	Is AI trained on open-source, legally obtained, and ethically sourced data?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine dataset licenses, sourcing records, and ethical data acquisition reports.
AI Explainability & Transparency	AI Transparency & Ethical Compliance	Are AI decision pathways logged and traceable for compliance audits?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check audit logs and traceability mechanisms for AI decision pathways.
AI Explainability & Transparency	AI Transparency & Ethical Compliance	Does AI disclose when a decision is AI-generated vs. human-generated?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review disclosures in user interfaces and decision reports regarding AI-generated outcomes.
AI Explainability & Transparency	AI Transparency & Ethical Compliance	Are transparency guidelines aligned with ISO 42001, EU AI Act, and OECD AI Principles?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze AI transparency documentation and alignment with regulatory guidelines.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Model Performance & Drift Monitoring	AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks	Does AI undergo regular accuracy testing using precision, recall, F1-score,and AUC-ROC?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI testing reports, confusion matrices, and performance metric calculations.
AI Model Performance & Drift Monitoring	AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model	Are AI models validated against real-world datasets to prevent overfitting?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze AI validation reports using real-world datasets to detect overfitting risks.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
	Accuracy & Stability Checks			
AI Model Performance & Drift Monitoring	AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks	Is AI performance tracked over time using trend analysis and performance metrics?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check AI performance dashboards and statistical trend analysis reports.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Model Performance & Drift Monitoring	AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks AI Model Accuracy & Stability Checks	Are AI models tested under different conditions and edge cases?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine test cases, adversarial scenarios, and edge case testing results.
AI Model Performance & Drift Monitoring	Model Drift & Continuous Monitoring	Does AI have automated drift detection to identify model performance degradation?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI drift detection logs and automated monitoring alerts.
AI Model Performance & Drift Monitoring	Model Drift & Continuous Monitoring	Are AI predictions compared to real-world outcomes to detect drift?	Control weakness may expose the organization to operational, legal, or reputational risks.	Compare AI predictions against real-world outcomes and historical benchmarks.
AI Model Performance &	Model Drift & Continuous Monitoring	Is there a retraining schedule to update AI models with fresh data?	Control weakness may expose the organization	Examine AI retraining logs and schedule adherence.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
Drift Monitoring			to operational, legal, or reputational risks.	
AI Model Performance & Drift Monitoring	Model Drift & Continuous Monitoring	Are AI monitoring tools (e.g., Evidently AI, AWS Model Monitor, Azure ML Monitoring) used?	Control weakness may expose the organization to operational, legal, or reputational risks.	Verify implementation of AI monitoring tools and their alert configurations.
AI Model Performance & Drift Monitoring	AI Model Retraining & Governance	Is there a formal AI model retraining and validation policy?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI model retraining policies, guidelines, and governance documentation.
AI Model Performance & Drift Monitoring	AI Model Retraining & Governance	Are AI updates and retraining logged and reviewed by compliance teams?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess AI update logs, compliance team meeting records, and retraining validation reports.
AI Model Performance & Drift Monitoring	AI Model Retraining & Governance	Are auditors provided with historical AI performance reports for assessment?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check if auditors have unrestricted access to AI performance logs and reports.
AI Model Performance & Drift Monitoring	AI Model Retraining & Governance	Does AI comply with ISO 42001 and NIST AI RMF guidelines on model lifecycle management?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review compliance documentation for adherence to ISO 42001 and NIST AI RMF requirements.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Deployment & Post-Implementation Risk	AI Deployment Security & Governance	Are AI deployment environments protected against unauthorized modifications?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI deploymentsecurity policies and access logs.
AI Deployment & Post-Implementation Risk	AI Deployment Security & Governance	Are role-based access controls (RBAC)implemented to restrict AI model changes?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess RBAC policies and user role configurations for AI system changes.
AI Deployment & Post-Implementation Risk	AI Deployment Security & Governance	Is AI deployment aligned with cloud security standards (ISO 27001, SOC 2,NIST CSF)?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check compliance documentation and audit reports for cloud security adherence.
AI Deployment & Post-Implementation Risk	AI Deployment Security & Governance	Are AI models encrypted atrest and in transit to prevent data leaks?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze encryption policies and validate implementation in AI deployment.
AI Deployment & Post-Implementation Risk	AI Model Post-Implementation Monitoring	Is AI performance tracked using real-time monitoring dashboards?	Control weakness may expose the organization to operational, legal, or reputational risks.	Inspect AI monitoring dashboards, logs, and performance tracking systems.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Deployment & Post-Implementation Risk	AI Model Post-Implementation Monitoring	Are AI-generated decisions logged and reviewed for anomalies?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI decision logs for unusual patterns and conduct anomaly detection tests.
AI Deployment & Post-Implementation Risk	AI Model Post-Implementation Monitoring	Is AI monitored for bias reintroduction or model drift over time?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze AI bias monitoring reports and model drift analysis logs.
AI Deployment & Post-Implementation Risk	AI Model Post-Implementation Monitoring	Are AI post-deployment reports regularly submitted to auditors and compliance teams?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Check AI audit submission records and compliance team reviews.
AI Deployment & Post-Implementation Risk	AI Incident Response & Fail- Safe Mechanisms AI Incident Response & Fail- Safe Mechanisms	Are there predefined AI failure response protocols in case of system errors?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine AI incident response plans and failure protocol documents.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Deployment & Post-Implementation Risk	AI Incident Response & Fail- Safe Mechanisms AI Incident Response & Fail- Safe Mechanisms	Is there a rollback mechanism to revert AI models to previous stable versions?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review rollback process documentation and conduct rollback testing if feasible.
AI Deployment & Post-Implementation Risk	AI Incident Response & Fail- Safe Mechanisms AI Incident Response & Fail- Safe Mechanisms	Are AI alerts integrated into security teams for real-time anomaly detection?	Control weakness may expose the organization to operational, legal, or reputational risks.	Verify AI security alert configurations and integration with SOC/SIEM tools.
AI Deployment & Post-Implementation Risk	AI Incident Response & Fail- Safe Mechanisms AI Incident Response &	Does AI have a 'human-in-the-loop' intervention system for high-risk applications?	Control weakness may expose the organization to operational, legal, or reputational risks.	Evaluate human intervention mechanisms and case studies for AI-assisted decision-making.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
	Fail- Safe Mechanisms			
AI Ethical Compliance & Responsible AI Auditing Checklist	AI Ethical Guidelines & Compliance	Does the organization follow responsible AI frameworks (OECD AI Principles, UNESCO AI Ethics, ISO 42001, EU AI Act)?	Absence of an ethics committee may result in unchecked biases and ethical misconduct in AI systems.	Review AI governance policies and adherence to responsible AI frameworks.
AI Ethical Compliance & Responsible AI Auditing Checklist	AI Ethical Guidelines & Compliance	Are AI models designed with fairness, accountability, and transparency (FAT)principles?	Absence of an ethics committee may result in unchecked biases and ethical misconduct in AI systems.	Examine AI model design documentation for fairness, accountability, and transparency principles.
AI Ethical Compliance & Responsible AI	AI Ethical Guidelines & Compliance	Is AI decision-making aligned with corporate ethics and human rights guidelines?	Absence of an ethics committee may result in unchecked biases and ethical misconduct in AI systems.	Analyze AI decision-making policies and ethical compliance guidelines.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Ethical Compliance & Responsible AI	AI Ethical Guidelines & Compliance	Are AI-generated outcomes reviewed for unintended negative consequences?	Absence of an ethics committee may result in unchecked biases and ethical misconduct in AI systems.	Review impact assessments and audits of AI-generated outcomes for unintended harm.
AI Ethical Compliance & Responsible AI	Human Oversight & AI Accountability	Is there a human-in-the-loop (HITL) or human-on-the-loop (HOTL) mechanism for AI decisions?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check documentation on human oversight mechanisms and HITL/HOTL implementations.
AI Ethical Compliance & Responsible AI	Human Oversight & AI Accountability	Can end-users challenge and appeal AI generated decisions?	Control weakness may expose the organization to operational, legal, or reputational risks.	Verify user appeal processes and mechanisms for challenging AI decisions.
AI Ethical Compliance & Responsible AI	Human Oversight & AI Accountability	Are AI risks communicated to stakeholders and regulators?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess stakeholder communication reports and AI risk disclosure statements.
AI Ethical Compliance & Responsible AI	Human Oversight & AI Accountability	Is there a clear escalation process for AI failures or ethical concerns?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine AI failure escalation workflows and historical incident reports.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Ethical Compliance & Responsible AI	AI Bias, Inclusivity, and Fairness Audits	Does AI undergo bias and fairness testing before deployment?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI bias and fairness testing reports and validation processes.
AI Ethical Compliance & Responsible AI	AI Bias, Inclusivity, and Fairness Audits	Are AI datasets diverse and representative of all user groups?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze AI dataset composition and diversity assessment reports.
AI Ethical Compliance & Responsible AI	AI Bias, Inclusivity, and Fairness Audits	Is there external third-party auditing of AI fairness and inclusivity?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check external audit reports and fairness compliance certifications.
AI Ethical Compliance & Responsible AI	AI Bias, Inclusivity, and Fairness Audits	Does AI comply with GDPR's Right to Explanation, AI Act risk classification, and anti-discrimination laws?	Control weakness may expose the organization to operational, legal, or reputational risks.	Evaluate GDPR, AI Act, and anti-discrimination compliance documentation.
AI Continuous Monitoring & Automated Risk Detection	AI Real-Time Monitoring & Alert Systems	Is AI performance tracked using real-time dashboards and anomaly detection tools?	Control weakness may expose the organization to operational, legal, or reputational risks.	Inspect AI monitoring dashboards and logs for real-time performance tracking.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Continuous Monitoring & Automated Risk Detection	AI Real-Time Monitoring & Alert Systems	Are AI risks automatically flagged using machine learning-based auditing systems?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI risk detection reports and logs from automated auditing systems.
AI Continuous Monitoring & Automated Risk Detection	AI Real-Time Monitoring & Alert Systems	Are AI models integrated with SIEM (Security Information and Event Management) tools for security monitoring?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check AI security integration with SIEM platforms and security monitoring logs.
AI Continuous Monitoring & Automated Risk Detection	AI Real-Time Monitoring & Alert Systems	Are automated alerts sent to compliance and security teams for quick remediation?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze AI security alert configurations and response protocols.
AI Continuous Monitoring & Automated Risk Detection	AI Bias & Drift Detection Automation	Are AI bias detection tools (e.g., IBM AI Fairness 360, Fairlearn) integrated for continuous auditing?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess AI bias monitoring tool integration and review bias detection reports.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Continuous Monitoring & Automated Risk Detection	AI Bias & Drift Detection Automation	Does AI automatically flag model drift and degradation for retraining?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI drift detection mechanisms and retraining triggers.
AI Continuous Monitoring & Automated Risk Detection	AI Bias & Drift Detection Automation	Are fairness checks performed regularly with automated reports?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine automated fairness audit reports and compliance tracking logs.
AI Continuous Monitoring & Automated Risk Detection	AI Bias & Drift Detection Automation	Are baseline fairness metrics defined for AI compliance tracking?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review baseline fairness metric definitions and implementation evidence.
AI Continuous Monitoring & Automated Risk Detection	AI Security & Adversarial Attack Detection	Does AI monitoring include intrusion detection for adversarial attacks?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze AI security logs and verify intrusion detection effectiveness.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Continuous Monitoring & Automated Risk Detection	AI Security & Adversarial Attack Detection	Are AI-generated logs reviewed for anomalies that may indicate cyber threats?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI system logs and identify anomalies that may indicate security risks.
AI Continuous Monitoring & Automated Risk Detection	AI Security & Adversarial Attack Detection	Are adversarial attack detection tools (e.g., Microsoft Counterfit, CleverHans) integrated intoAI security frameworks?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check AI security policies and adversarial attack defense mechanisms.
AI Continuous Monitoring & Automated Risk Detection	AI Security & Adversarial Attack Detection	Is there an automated rollback or shutdown mechanism in case of failures?	Control weakness may expose the organization to operational, legal, or reputational risks.	Verify AI rollback mechanisms and assess past rollback or shutdown cases.
AI Continuous Monitoring & Automated Risk Detection	AI Continuous Compliance Monitoring	Does AI undergo automated compliance checks against GDPR, ISO 42001, EU AI Act, NIST AI RMF?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Review AI compliance automation reports and audit history for GDPR, ISO, and AI Act alignment.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Continuous Monitoring & Automated Risk Detection	AI Continuous Compliance Monitoring	Are AI-generated decisions automatically logged and audited for transparency?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Inspect AI-generated decision logs and confirm they meet transparency requirements.
AI Continuous Monitoring & Automated Risk Detection	AI Continuous Compliance Monitoring	Are AI compliance reports generated in real-time for regulatory audits?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Assess AI compliance report generation frequency and content.
AI Continuous Monitoring & Automated Risk Detection	AI Continuous Compliance Monitoring	Does AI alert governance teams if compliance thresholds are breached?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Check AI governance alert mechanisms and review past compliance alerts.
AI Audit Report Writing & Documentation Best Practices	AI Audit Report Structure & Documentation	Does the report include a clear executive summary with key findings?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI audit reports for completeness and clarity of the executive summary.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Audit Report Writing & Documentation Best Practices	AI Audit Report Structure & Documentation	Are AI risks categorized based on impact level (low, medium, high, critical)?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze risk categorization methodologies in AI audit reports.
AI Audit Report Writing & Documentation Best Practices	AI Audit Report Structure & Documentation	Are all audit findings supported with data, evidence, and analysis?	Control weakness may expose the organization to operational, legal, or reputational risks.	Validate if audit findings include supporting data, evidence, and in-depth analysis.
AI Audit Report Writing & Documentation Best Practices	AI Audit Report Structure & Documentation	Is there a recommendation section outlining corrective actions?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check the presence and structure of the corrective action recommendations section.
AI Audit Report Writing & Documentation Best Practices	AI Governance & Compliance Documentation	Does the audit report include AI model compliance status (GDPR, ISO 42001,NIST AI RMF, AI Act)?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Examine AI audit documentation for compliance status across major regulatory standards.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Audit Report Writing & Documentation Best Practices	AI Governance & Compliance Documentation	Are AI governance policies and procedures properly documented?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Assess AI governance documentation for completeness and policy adherence.
AI Audit Report Writing & Documentation Best Practices	AI Governance & Compliance Documentation	Is AI decision-making transparency clearly explained with logs and model justifications?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Review AI decision-making transparency logs and justifications included in the report.
AI Audit Report Writing & Documentation Best Practices	AI Governance & Compliance Documentation	Are compliance gaps and regulatory concerns highlighted with mitigation plans?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Inspect compliance reports for regulatory gaps and proposed mitigation strategies.
AI Audit Report Writing & Documentation Best Practices	AI Bias, Fairness, and Performance Reporting	Does the report include bias and fairness assessment results?	Control weakness may expose the organization to operational, legal, or reputational risks.	Analyze bias and fairness testing documentation included in the audit report.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Audit Report Writing & Documentation Best Practices	AI Bias, Fairness, and Performance Reporting	Are AI performance metrics compared against baseline standards?	Control weakness may expose the organization to operational, legal, or reputational risks.	Compare AI performance benchmarks to established baseline standards.
AI Audit Report Writing & Documentation Best Practices	AI Bias, Fairness, and Performance Reporting	Is AI drift detection documented with trend analysis and remediation steps?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI drift detection logs and trend analysis data.
AI Audit Report Writing & Documentation Best Practices	AI Bias, Fairness, and Performance Reporting	Are fairness audit results visualized using charts and statistical summaries?	Control weakness may expose the organization to operational, legal, or reputational risks.	Inspect audit reports for fairness results visualized with statistical summaries.
AI Audit Report Writing & Documentation Best Practices	AI Security & Risk Management Reporting	Does the report include security vulnerabilities, adversarial risks, and attack simulations?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess security audit logs for vulnerability testing, adversarial risk analysis, and simulations.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Audit Report Writing & Documentation Best Practices	AI Security & Risk Management Reporting	Are AI security incidents logged and analyzed for impact assessment?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review AI security incident logs and impact analysis reports.
AI Audit Report Writing & Documentation Best Practices	AI Security & Risk Management Reporting	Are security and compliance gaps mapped to regulatory frameworks?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Check if AI security and compliance gaps are mapped to relevant frameworks.
AI Audit Report Writing & Documentation Best Practices	AI Security & Risk Management Reporting	Are recommendations for security improvements clearly outlined with action plans?	Non-compliance with legal standards may lead to fines, lawsuits, or operational restrictions.	Validate the security recommendations section for clear and actionable remediation steps.
AI Audit Report Writing & Documentation Best Practices	AI Continuous Monitoring & Post-Audit Follow-Up	Is there a post-audit follow-up plan for reviewing AI improvements?	Control weakness may expose the organization to operational, legal, or reputational risks.	Examine follow-up plans for tracking AI improvements post-audit.

Process	Sub-Process	Audit Question	Risk	Detailed Audit Test Procedure
AI Audit Report Writing & Documentation Best Practices	AI Continuous Monitoring & Post-Audit Follow-Up	Are AI audit results tracked over time to monitor governance improvements?	Control weakness may expose the organization to operational, legal, or reputational risks.	Assess AI governance monitoring records to ensure long-term tracking of audit results.
AI Audit Report Writing & Documentation Best Practices	AI Continuous Monitoring & Post-Audit Follow-Up	Are continuous AI compliance assessments scheduled with automated tracking?	Control weakness may expose the organization to operational, legal, or reputational risks.	Review automated compliance tracking tools for AI risk assessment.
AI Audit Report Writing & Documentation Best Practices	AI Continuous Monitoring & Post-Audit Follow-Up	Are AI audit stakeholders provided with regular reports on AI risks and governance updates?	Control weakness may expose the organization to operational, legal, or reputational risks.	Check if AI risk and governance reports are distributed regularly to stakeholders.

Thank You

Follow us for More such Audit Checklist

TechEd Academy
Learn | Certify | Succeed