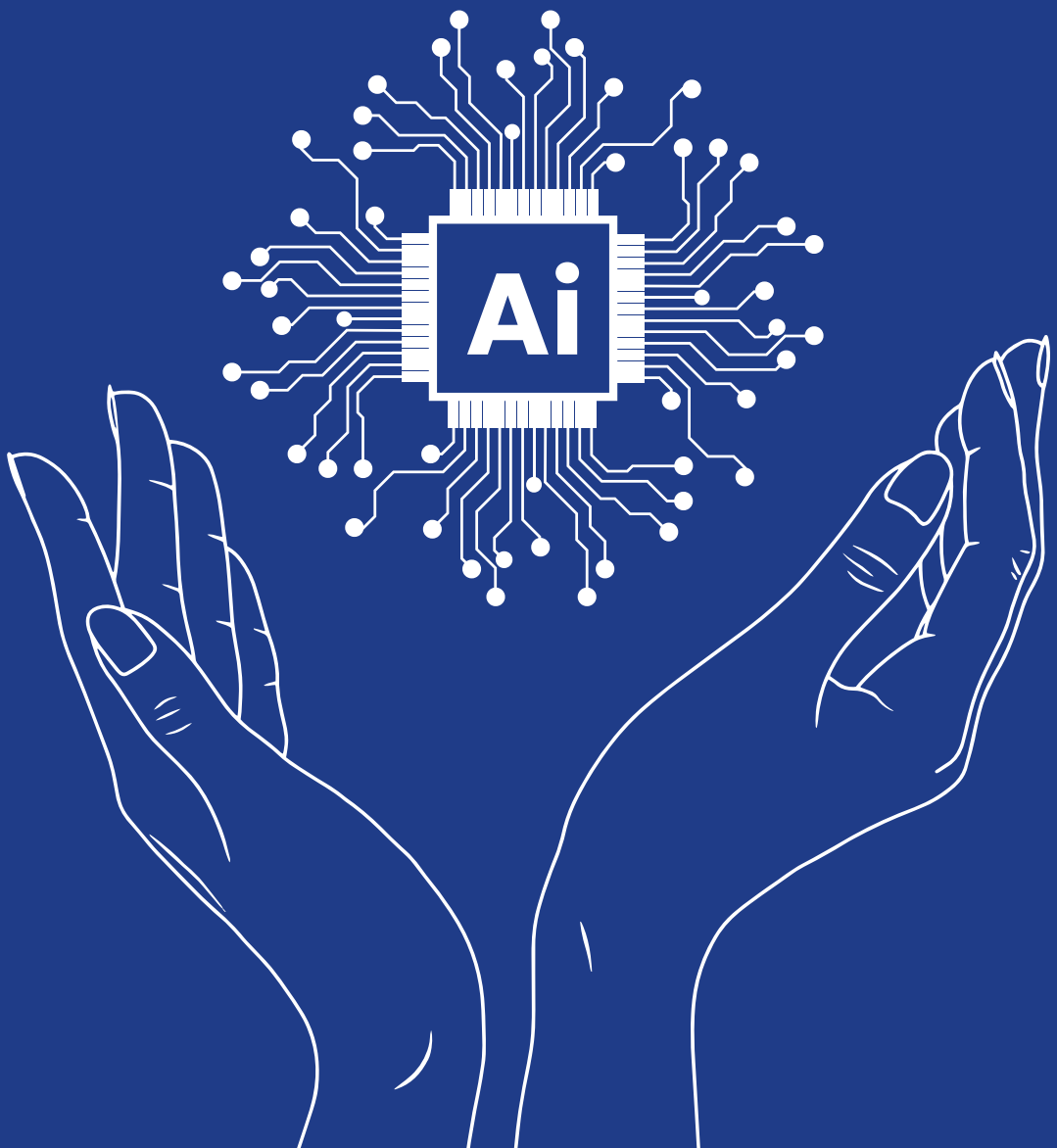
CTC

Certified Trainers
and Consultants

AI

Audit Checklist

By: Kamran Iqbal



AI Governance & Compliance Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Governance Policies	Does the organization have a documented AI governance framework?	Review governance documents, policies, and roles related to AI governance.	
AI Governance Policies	Are AI risk management processes aligned with ISO 42001, NIST AI RMF, and GDPR?	Assess AI risk management documentation and compare against ISO, NIST, and GDPR standards.	
AI Governance Policies	Is there an AI ethics committee overseeing AI governance?	Check meeting minutes, structure, and decision-making authority of the AI ethics committee.	
Regulatory Compliance	Does the AI system comply with GDPR, ISO 42001, CCPA, or sector-specific regulations?	Review legal compliance documentation and regulatory audit reports.	
Regulatory Compliance	Are AI data processing activities documented and legally justified?	Examine data processing policies, logs, and legal bases for AI data use.	
Regulatory Compliance	Are AI models designed to ensure transparency, explainability, and accountability?	Review AI system documentation, model explanations, and accountability mechanisms.	
AI Risk Management & Auditing	Is there a risk assessment framework for AI deployment?	Evaluate risk assessment frameworks, methodologies, and past risk reports.	
AI Risk Management & Auditing	Are AI risks monitored and reported regularly?	Check AI risk reports, monitoring dashboards, and periodic risk assessments.	
AI Risk Management & Auditing	Does the organization have a formal AI audit plan?	Review AI audit policies, past audit reports, and compliance review schedules.	

AI Bias Detection & Fairness Auditing Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Training Data Bias Assessment	Is AI training data diverse and representative of different demographics?	Review dataset composition, demographic distributions, and data collection sources.	
AI Training Data Bias Assessment	Has the AI model been tested for racial, gender, or socioeconomic biases?	Analyze bias testing reports, fairness analysis results, and past bias mitigation efforts.	
AI Training Data Bias Assessment	Are fairness metrics such as Equalized Odds, Disparate Impact, and Statistical Parity applied?	Check if fairness metrics are calculated and if disparities are flagged for corrective action.	
AI Training Data Bias Assessment	Are data preprocessing techniques used to remove historical biases?	Review preprocessing methodologies like data balancing, re-weighting, or adversarial debiasing.	
AI Model Fairness & Transparency	Does the AI model undergo regular bias audits and fairness testing?	Examine AI audit reports and fairness testing logs for evidence of regular monitoring.	
AI Model Fairness & Transparency	Are fairness results documented and reviewed by compliance teams?	Review fairness documentation, compliance reports, and stakeholder reviews.	
AI Model Fairness & Transparency	Does AI have explainability tools (SHAP, LIME) to clarify decisions?	Assess whether AI models are equipped with SHAP, LIME, or other explainability tools.	
AI Model Fairness & Transparency	Is AI fairness validated using external tools like IBM AI Fairness 360, Fairlearn?	Check if AI models have been tested with IBM AI Fairness 360, Fairlearn, or similar frameworks.	
AI Decision Review & Human Oversight	Are AI-generated decisions audited for fairness before deployment?	Review AI decision audit logs and pre-deployment validation reports.	
AI Decision Review & Human Oversight	Is there a human-in-the-loop process to monitor AI decisions?	Examine human oversight mechanisms, workflows, and monitoring procedures.	
AI Decision Review & Human Oversight	Are users given the ability to challenge AI decisions in high-risk applications (e.g., hiring, lending, law enforcement)?	Verify if appeal mechanisms exist for AI-generated decisions in high-risk areas.	

AI Security & Adversarial Attack Protection Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Model Security & Access Controls	Are AI models protected with role-based access control (RBAC)?	Review access control policies and verify implementation of RBAC.	
AI Model Security & Access Controls	Does the AI system require multi-factor authentication (MFA) for access?	Check authentication configurations and system logs for MFA enforcement.	
AI Model Security & Access Controls	Are AI models encrypted at rest and in transit (e.g., AES-256, TLS 1.3)?	Review encryption policies and test encryption of stored and transmitted AI data.	
AI Model Security & Access Controls	Is there logging and monitoring of AI access attempts?	Examine AI system access logs and monitoring dashboards.	
Adversarial Attack & AI Model Tampering Protection	Are AI models tested against adversarial attacks (evasion, poisoning, model inversion, etc.)?	Analyze adversarial robustness testing reports and security evaluations.	
Adversarial Attack & AI Model Tampering Protection	Are AI training datasets protected against data poisoning attacks?	Review dataset protection measures and security policies against poisoning attacks.	
Adversarial Attack & AI Model Tampering Protection	Has AI undergone penetration testing using adversarial AI security tools (e.g., Microsoft Counterfit, CleverHans)?	Examine penetration testing reports and security assessments.	
Adversarial Attack & AI Model Tampering Protection	Is AI output monitored for unexpected behavior caused by adversarial inputs?	Monitor AI model behavior logs and validate unexpected output detection mechanisms.	
AI API & Cloud Security Measures	Are AI APIs secured with OAuth 2.0 authentication and rate limiting?	Review API authentication mechanisms, security tokens, and rate-limiting configurations.	
AI API & Cloud Security Measures	Does AI use API monitoring and anomaly detection to prevent unauthorized queries?	Analyze API monitoring reports and anomaly detection logs.	
AI API & Cloud Security Measures	Are AI model weights and datasets secured in cloud environments (AWS, Azure, Google Cloud) with encryption and restricted access?	Check cloud security configurations, encryption settings, and access control policies.	
AI API & Cloud Security Measures	Does AI security comply with ISO 27001, SOC 2, and NIST Cybersecurity Framework?	Review cybersecurity audit reports and compliance documentation.	

AI Explainability & Transparency Auditing Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Model Interpretability & Documentation	Is AI model documentation comprehensive and accessible for auditors?	Review AI model documentation, system design, and training logs.	
AI Model Interpretability & Documentation	Does AI provide clear explanations for decision-making processes?	Analyze model explainability reports and decision-making justifications.	
AI Model Interpretability & Documentation	Are AI model parameters, assumptions, and feature importance well-documented?	Check documentation of model parameters, key assumptions, and feature importance analysis.	
AI Model Interpretability & Documentation	Are explainability frameworks (e.g., SHAP, LIME, Integrated Gradients) used?	Examine whether SHAP, LIME, or similar frameworks are used for interpretability.	
User & Regulatory Explainability Requirements	Does the AI system comply with GDPRâ€™s 'Right to Explanation'?	Review compliance policies, GDPR documentation, and 'Right to Explanation' implementation.	
User & Regulatory Explainability Requirements	Can end-users understand AI-generated decisions (e.g., loan approvals, hiring)?	Conduct user surveys or tests to evaluate the understandability of AI decisions.	
User & Regulatory Explainability Requirements	Is there an explainability dashboard for auditors and compliance teams?	Assess the presence and functionality of an explainability dashboard.	
User & Regulatory Explainability Requirements	Are AI-generated justifications consistent, unbiased, and reproducible?	Review AI justification logs, decision consistency tests, and bias assessments.	
AI Transparency & Ethical Compliance	Is AI trained on open-source, legally obtained, and ethically sourced data?	Examine dataset licenses, sourcing records, and ethical data acquisition reports.	
AI Transparency & Ethical Compliance	Are AI decision pathways logged and traceable for compliance audits?	Check audit logs and traceability mechanisms for AI decision pathways.	

AI Transparency & Ethical Compliance	Does AI disclose when a decision is AI-generated vs. human-generated?	Review disclosures in user interfaces and decision reports regarding AI-generated outcomes.	
AI Transparency & Ethical Compliance	Are transparency guidelines aligned with ISO 42001, EU AI Act, and OECD AI Principles?	Analyze AI transparency documentation and alignment with regulatory guidelines.	

AI Model Performance & Drift Monitoring Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Model Accuracy & Stability Checks	Does AI undergo regular accuracy testing using precision, recall, F1-score, and AUC-ROC?	Review AI testing reports, confusion matrices, and performance metric calculations.	
AI Model Accuracy & Stability Checks	Are AI models validated against real-world datasets to prevent overfitting?	Analyze AI validation reports using real-world datasets to detect overfitting risks.	
AI Model Accuracy & Stability Checks	Is AI performance tracked over time using trend analysis and performance metrics?	Check AI performance dashboards and statistical trend analysis reports.	
AI Model Accuracy & Stability Checks	Are AI models tested under different conditions and edge cases?	Examine test cases, adversarial scenarios, and edge case testing results.	
Model Drift & Continuous Monitoring	Does AI have automated drift detection to identify model performance degradation?	Review AI drift detection logs and automated monitoring alerts.	
Model Drift & Continuous Monitoring	Are AI predictions compared to real-world outcomes to detect drift?	Compare AI predictions against real-world outcomes and historical benchmarks.	
Model Drift & Continuous Monitoring	Is there a retraining schedule to update AI models with fresh data?	Examine AI retraining logs and schedule adherence.	
Model Drift & Continuous Monitoring	Are AI monitoring tools (e.g., Evidently AI, AWS Model Monitor, Azure ML Monitoring) used?	Verify implementation of AI monitoring tools and their alert configurations.	
AI Model Retraining & Governance	Is there a formal AI model retraining and validation policy?	Review AI model retraining policies, guidelines, and governance documentation.	
AI Model Retraining & Governance	Are AI updates and retraining logged and reviewed by compliance teams?	Assess AI update logs, compliance team meeting records, and retraining validation reports.	
AI Model Retraining & Governance	Are auditors provided with historical AI performance reports for assessment?	Check if auditors have unrestricted access to AI performance logs and reports.	
AI Model Retraining & Governance	Does AI comply with ISO 42001 and NIST AI RMF guidelines on model lifecycle management?	Review compliance documentation for adherence to ISO 42001 and NIST AI RMF requirements.	

AI Deployment & Post-Implementation Risk Auditing Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Deployment Security & Governance	Are AI deployment environments protected against unauthorized modifications?	Review AI deployment security policies and access logs.	
AI Deployment Security & Governance	Are role-based access controls (RBAC) implemented to restrict AI model changes?	Assess RBAC policies and user role configurations for AI system changes.	
AI Deployment Security & Governance	Is AI deployment aligned with cloud security standards (ISO 27001, SOC 2, NIST CSF)?	Check compliance documentation and audit reports for cloud security adherence.	
AI Deployment Security & Governance	Are AI models encrypted at rest and in transit to prevent data leaks?	Analyze encryption policies and validate implementation in AI deployment.	
AI Model Post-Implementation Monitoring	Is AI performance tracked using real-time monitoring dashboards?	Inspect AI monitoring dashboards, logs, and performance tracking systems.	
AI Model Post-Implementation Monitoring	Are AI-generated decisions logged and reviewed for anomalies?	Review AI decision logs for unusual patterns and conduct anomaly detection tests.	
AI Model Post-Implementation Monitoring	Is AI monitored for bias reintroduction or model drift over time?	Analyze AI bias monitoring reports and model drift analysis logs.	

AI Model Post-Implementation Monitoring	Are AI post-deployment reports regularly submitted to auditors and compliance teams?	Check AI audit submission records and compliance team reviews.	
AI Incident Response & Fail-Safe Mechanisms	Are there predefined AI failure response protocols in case of system errors?	Examine AI incident response plans and failure protocol documents.	
AI Incident Response & Fail-Safe Mechanisms	Is there a rollback mechanism to revert AI models to previous stable versions?	Review rollback process documentation and conduct rollback testing if feasible.	
AI Incident Response & Fail-Safe Mechanisms	Are AI alerts integrated into security teams for real-time anomaly detection?	Verify AI security alert configurations and integration with SOC/SIEM tools.	
AI Incident Response & Fail-Safe Mechanisms	Does AI have a 'human-in-the-loop' intervention system for high-risk applications?	Evaluate human intervention mechanisms and case studies for AI-assisted decision-making.	

AI Ethical Compliance & Responsible AI Auditing Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Ethical Guidelines & Compliance	Does the organization follow responsible AI frameworks (OECD AI Principles, UNESCO AI Ethics, ISO 42001, EU AI Act)?	Review AI governance policies and adherence to responsible AI frameworks.	
AI Ethical Guidelines & Compliance	Are AI models designed with fairness, accountability, and transparency (FAT) principles?	Examine AI model design documentation for fairness, accountability, and transparency principles.	
AI Ethical Guidelines & Compliance	Is AI decision-making aligned with corporate ethics and human rights guidelines?	Analyze AI decision-making policies and ethical compliance guidelines.	
AI Ethical Guidelines & Compliance	Are AI-generated outcomes reviewed for unintended negative consequences?	Review impact assessments and audits of AI-generated outcomes for unintended harm.	
Human Oversight & AI Accountability	Is there a human-in-the-loop (HITL) or human-on-the-loop (HOTL) mechanism for AI decisions?	Check documentation on human oversight mechanisms and HITL/HOTL implementations.	
Human Oversight & AI Accountability	Can end-users challenge and appeal AI-generated decisions?	Verify user appeal processes and mechanisms for challenging AI decisions.	
Human Oversight & AI Accountability	Are AI risks communicated to stakeholders and regulators?	Assess stakeholder communication reports and AI risk disclosure statements.	
Human Oversight & AI Accountability	Is there a clear escalation process for AI failures or ethical concerns?	Examine AI failure escalation workflows and historical incident reports.	
AI Bias, Inclusivity, and Fairness Audits	Does AI undergo bias and fairness testing before deployment?	Review AI bias and fairness testing reports and validation processes.	
AI Bias, Inclusivity, and Fairness Audits	Are AI datasets diverse and representative of all user groups?	Analyze AI dataset composition and diversity assessment reports.	
AI Bias, Inclusivity, and Fairness Audits	Is there external third-party auditing of AI fairness and inclusivity?	Check external audit reports and fairness compliance certifications.	
AI Bias, Inclusivity, and Fairness Audits	Does AI comply with GDPR's Right to Explanation, AI Act risk classification, and anti-discrimination laws?	Evaluate GDPR, AI Act, and anti-discrimination compliance documentation.	

AI Continuous Monitoring & Automated Risk Detection Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Real-Time Monitoring & Alert Systems	Is AI performance tracked using real-time dashboards and anomaly detection tools?	Inspect AI monitoring dashboards and logs for real-time performance tracking.	
AI Real-Time Monitoring & Alert Systems	Are AI risks automatically flagged using machine learning-based auditing systems?	Review AI risk detection reports and logs from automated auditing systems.	
AI Real-Time Monitoring & Alert Systems	Are AI models integrated with SIEM (Security Information and Event Management) tools for security monitoring?	Check AI security integration with SIEM platforms and security monitoring logs.	
AI Real-Time Monitoring & Alert Systems	Are automated alerts sent to compliance and security teams for quick remediation?	Analyze AI security alert configurations and response protocols.	
AI Bias & Drift Detection Automation	Are AI bias detection tools (e.g., IBM AI Fairness 360, Fairlearn) integrated for continuous auditing?	Assess AI bias monitoring tool integration and review bias detection reports.	

AI Bias & Drift Detection Automation	Does AI automatically flag model drift and degradation for retraining?	Review AI drift detection mechanisms and retraining triggers.	
AI Bias & Drift Detection Automation	Are fairness checks performed regularly with automated reports?	Examine automated fairness audit reports and compliance tracking logs.	
AI Bias & Drift Detection Automation	Are baseline fairness metrics defined for AI compliance tracking?	Review baseline fairness metric definitions and implementation evidence.	
AI Security & Adversarial Attack Detection	Does AI monitoring include intrusion detection for adversarial attacks?	Analyze AI security logs and verify intrusion detection effectiveness.	
AI Security & Adversarial Attack Detection	Are AI-generated logs reviewed for anomalies that may indicate cyber threats?	Review AI system logs and identify anomalies that may indicate security risks.	
AI Security & Adversarial Attack Detection	Are adversarial attack detection tools (e.g., Microsoft Counterfit, CleverHans) integrated into AI security frameworks?	Check AI security policies and adversarial attack defense mechanisms.	
AI Security & Adversarial Attack Detection	Is there an automated rollback or shutdown mechanism in case of AI failures?	Verify AI rollback mechanisms and assess past rollback or shutdown cases.	
AI Continuous Compliance Monitoring	Does AI undergo automated compliance checks against GDPR, ISO 42001, EU AI Act, NIST AI RMF?	Review AI compliance automation reports and audit history for GDPR, ISO, and AI Act alignment.	
AI Continuous Compliance Monitoring	Are AI-generated decisions automatically logged and audited for transparency?	Inspect AI-generated decision logs and confirm they meet transparency requirements.	
AI Continuous Compliance Monitoring	Are AI compliance reports generated in real-time for regulatory audits?	Assess AI compliance report generation frequency and content.	
AI Continuous Compliance Monitoring	Does AI alert governance teams if compliance thresholds are breached?	Check AI governance alert mechanisms and review past compliance alerts.	

AI Audit Report Writing & Documentation Best Practices Checklist

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Audit Report Structure & Documentation	Does the report include a clear executive summary with key findings?	Review AI audit reports for completeness and clarity of the executive summary.	
AI Audit Report Structure & Documentation	Are AI risks categorized based on impact level (low, medium, high, critical)?	Analyze risk categorization methodologies in AI audit reports.	
AI Audit Report Structure & Documentation	Are all audit findings supported with data, evidence, and analysis?	Validate if audit findings include supporting data, evidence, and in-depth analysis.	
AI Audit Report Structure & Documentation	Is there a recommendation section outlining corrective actions?	Check the presence and structure of the corrective action recommendations section.	
AI Governance & Compliance Documentation	Does the audit report include AI model compliance status (GDPR, ISO 42001, NIST AI RMF, AI Act)?	Examine AI audit documentation for compliance status across major regulatory standards.	
AI Governance & Compliance Documentation	Are AI governance policies and procedures properly documented?	Assess AI governance documentation for completeness and policy adherence.	
AI Governance & Compliance Documentation	Is AI decision-making transparency clearly explained with logs and model justifications?	Review AI decision-making transparency logs and justifications included in the report.	
AI Governance & Compliance Documentation	Are compliance gaps and regulatory concerns highlighted with mitigation plans?	Inspect compliance reports for regulatory gaps and proposed mitigation strategies.	
AI Bias, Fairness, and Performance Reporting	Does the report include bias and fairness assessment results?	Analyze bias and fairness testing documentation included in the audit report.	
AI Bias, Fairness, and Performance Reporting	Are AI performance metrics compared against baseline standards?	Compare AI performance benchmarks to established baseline standards.	
AI Bias, Fairness, and Performance Reporting	Is AI drift detection documented with trend analysis and remediation steps?	Review AI drift detection logs and trend analysis data.	
AI Bias, Fairness, and Performance Reporting	Are fairness audit results visualized using charts and statistical summaries?	Inspect audit reports for fairness results visualized with statistical summaries.	
AI Security & Risk Management Reporting	Does the report include security vulnerabilities, adversarial risks, and attack simulations?	Assess security audit logs for vulnerability testing, adversarial risk analysis, and simulations.	
AI Security & Risk Management Reporting	Are AI security incidents logged and analyzed for impact assessment?	Review AI security incident logs and impact analysis reports.	

Audit Area	Audit Question	How to Check	Compliance Status (Yes/No) & Remarks
AI Security & Risk Management Reporting	Are security and compliance gaps mapped to regulatory frameworks?	Check if AI security and compliance gaps are mapped to relevant frameworks.	
AI Security & Risk Management Reporting	Are recommendations for security improvements clearly outlined with action plans?	Validate the security recommendations section for clear and actionable remediation steps.	
AI Continuous Monitoring & Post-Audit Follow-Up	Is there a post-audit follow-up plan for reviewing AI improvements?	Examine follow-up plans for tracking AI improvements post-audit.	
AI Continuous Monitoring & Post-Audit Follow-Up	Are AI audit results tracked over time to monitor governance improvements?	Assess AI governance monitoring records to ensure long-term tracking of audit results.	
AI Continuous Monitoring & Post-Audit Follow-Up	Are continuous AI compliance assessments scheduled with automated tracking?	Review automated compliance tracking tools for AI risk assessment.	
AI Continuous Monitoring & Post-Audit Follow-Up	Are AI audit stakeholders provided with regular reports on AI risks and governance updates?	Check if AI risk and governance reports are distributed regularly to stakeholders.	

Author:

Kamran Iqbal - CIA, CISA, CFE, CICA, CMA, MBA, LLB, FMVA
Founder & Lead Trainer
CTC Global
Certified Trainers and Consultants
https://www.linkedin.com/in/acmakamran

CTC **Certified Trainers and Consultants**

Author's Profile:

KAMRAN IQBAL

CIA, CFE, CISA, CMA, CICA, FMVA, MBA, LLB

Kamran is the Founder and Lead Trainer at CTC Global, a premier training and consultancy firm with a global footprint.

With over a decade of extensive experience as a professional trainer, he has delivered impactful and engaging training sessions for various Certification Programs and in other key areas such as IT Auditing, Fraud Investigations, Internal Audit, Risk Assessment, Internal Controls, Power BI, and Microsoft Excel, consistently empowering professionals to enhance their skills and drive organizational success.

Our Socials:

ctc-global.com

@Certified Trainers and Consultants

@Certified Trainers and Consultants

FOLLOW US FOR MORE INSIGHTS, UPDATES AND TEMPLATES!