Information Systems Audit Checklist



The Nexus of Digital Assurance

By: Dr. Nath Alagbe

Information Systems Audit Checklist

By: **Dr. Nath Alagbe**; CISA, CISM, CISSP, CRISC, CCAK, AAIA, CCEP, CFE, FCA, FCTI, FFAR, MBA, PhD

This checklist provides a comprehensive framework for auditing information systems across 14 critical domains. Each domain includes at least 6 audit areas with detailed objectives, questions, validation steps, and references.

Domain 1: IT Governance and Strategy

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
IT Strategic Alignment	Ensure IT strategy supports business goals.	Is there a documented IT strategy aligned with the business plan?	Review IT and Business strategic plans for alignment.	IT Strategic Plan, Business Plan, Alignment Matrix.	IT investments may not deliver business value.	COBIT 2019 APO02
IT Steering Committee	Verify effective oversight of IT activities.	Does an IT Steering Committee meet regularly with senior management?	Review committee charters and meeting minutes.	Committee Charter, Meeting Minutes, and Attendance Logs.	Lack of executive direction and oversight.	COBIT 2019 EDM01
IT Policies & Procedures	Ensure formal guidance for IT operations.	Are IT policies documented, approved, and communicated?	Inspect the policy repository and evidence of communication.	IT Policy Manual, Approval Records, Employee Handbook.	Inconsistent practices and compliance gaps.	ISO 27001 Clause 5.2
Resource Management	Optimize use of IT human and tech resources.	Is there a process for IT resource planning and allocation?	Review resource plans and utilization reports.	Resource Plan, Skills Matrix, and Utilization Reports.	Project delays and operational inefficiencies.	COBIT 2019 APO07
Performance Measurement	Monitor IT performance against targets.	Are IT Key Performance Indicators (KPIs) defined and reported?	Review KPI reports and management dashboards.	KPI Reports, Dashboards, Performance Reviews.	Inability to identify and correct performance issues.	COBIT 2019 MEA01
Value Delivery	Ensure IT projects deliver expected benefits.	Is there a process to track benefits realization for IT projects?	Review post-implementation reviews and business cases.	Business Cases, Post-Implementation Reviews.	Wasted investment on non-beneficial projects.	COBIT 2019 EDM02

Domain 2: Risk Management

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Risk Management Framework	Establish a consistent risk approach.	Is there a formal IT risk management framework in place?	Review the Risk Management Policy and Framework.	Risk Management Policy, Framework Document.	Inconsistent risk identification and treatment.	ISO 31000, COBIT APO12
Risk Assessment Process	Identify and evaluate IT risks.	Are periodic IT risk assessments conducted?	Review recent risk assessment reports.	Risk Assessment Reports, Methodology Document.	Critical risks may remain unidentified.	NIST SP 800-30
Risk Treatment Plan	Mitigate identified risks effectively.	Are risk treatment plans developed for high-risk areas?	Inspect the Risk Register for treatment actions.	Risk Register, Action Plans, Remediation Logs.	Risks may exceed organizational appetite.	ISO 27001 Clause 6.1.3
Risk Monitoring	Track risk status over time.	Is there a process for ongoing monitoring of IT risks?	Review risk reporting to the Board/Management.	Risk Dashboards, Quarterly Risk Reports.	Failure to detect changes in risk landscape.	COBIT 2019 APO12.06
Risk Appetite	Define acceptable risk levels.	Has the Board defined IT risk appetite and tolerance?	Review Board minutes or Risk Appetite Statement.	Risk Appetite Statement, Board Minutes.	Over or under-investment in security controls.	COBIT 2019 EDM03
Emerging Risk ID	Prepare for future threats.	Is there a process to identify emerging technology risks?	Review industry research or threat intelligence logs.	Threat Intel Reports, Emerging Risk Logs.	Organization may be blindsided by new threats.	NIST CSF (ID.RA)

Domain 3: IT General Controls (ITGC)

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Logical Access	Prevent unauthorized system access.	Is access granted based on the principle of least privilege?	Test a sample of user access rights against job roles.	User Access Lists, HR Role Descriptions.	Unauthorized data access or modification.	NIST SP 800-53 AC-2
Physical Security	Protect IT assets from physical threats.	Are data centers and server rooms secured?	Conduct a walkthrough and review access logs.	Physical Access Logs, CCTV Records, Badge Reports.	Theft or physical damage to critical hardware.	ISO 27002 Control 7
Change Management	Ensure controlled system changes.	Are all changes authorized, tested, and approved?	Review a sample of change	Change Request Forms, UAT Results, CAB Minutes.	System instability or unauthorized changes.	ITIL Change Enablement

			requests and approvals.			
Backup and Recovery	Ensure data availability.	Are backups performed regularly and tested?	Review backup logs and recent restoration test results.	Backup Logs, Restoration Test Reports.	Permanent data loss during a disaster.	NIST SP 800-53 CP-9
Job Scheduling	Ensure reliable batch processing.	Are automated jobs monitored for success/failure?	Review job schedules and failure alerts.	Job Schedules, Alert Logs, Resolution Records.	Business process delays due to failed jobs.	COBIT 2019 DSS01
Problem Management	Resolve root causes of IT issues.	Is there a process for root cause analysis of major incidents?	Review a sample of Problem Records.	Problem Logs, Root Cause Analysis Reports.	Recurring incidents impacting productivity.	ITIL Problem Management

---

Domain 4: Identity and Access Management (IAM)

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
User Provisioning	Ensure authorized access creation.	Is there a formal process for granting new user access?	Review access request forms and approval records.	Access Request Forms, Approval Emails.	Unauthorized users gaining system access.	CIS Control 5
User Termination	Prevent access by former employees.	Is access revoked immediately upon termination?	Compare HR termination lists with IT access logs.	HR Termination List, Access Revocation Logs.	Malicious actions by disgruntled ex-employees.	NIST SP 800-53 PS-4
Multi-Factor Auth	Strengthen authentication security.	Is MFA required for remote and privileged access?	Inspect system configurations for MFA enforcement.	System Config Screenshots, MFA Policy.	Credential theft leading to account takeover.	CIS Control 6
Privileged Access	Control high-level system rights.	Are administrative accounts strictly controlled and monitored?	Review the list of privileged users and their activity.	Privileged User List, Admin Activity Logs.	Widespread system compromise via admin accounts.	ISO 27002 Control 9.4.4
Periodic Access Review	Validate ongoing access necessity.	Are user access rights reviewed by managers periodically?	Review evidence of the most recent access review.	Access Review Sign-off, Manager Approvals.	"Privilege creep" where users retain unneeded rights.	SOC 2 CC6.3
Password Policy	Enforce strong authentication.	Does the password policy meet industry standards?	Inspect Group Policy Objects (GPO) for password settings.	GPO Screenshots, Password Policy Document.	Weak passwords susceptible to brute-force attacks.	NIST SP 800-63B

Domain 5: Infrastructure and Network Security

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Firewall Management	Protect network boundaries.	Are firewall rules reviewed and optimized regularly?	Review firewall rule base and review logs.	Firewall Config, Rule Review Records.	Unauthorized network traffic entering the perimeter.	CIS Control 4
Network Segmentation	Limit the lateral movement of threats.	Is the network segmented to isolate sensitive data?	Review network diagrams and VLAN configurations.	Network Diagrams, VLAN Configs.	A single breach spreading across the entire network.	NIST SP 800-53 SC-7
IDS/IPS Monitoring	Detect and prevent intrusions.	Are IDS/IPS systems active and monitored?	Review IDS/IPS logs and alert response records.	IDS/IPS Logs, Incident Tickets.	Undetected malicious activity on the network.	ISO 27002 Control 13
Wireless Security	Secure wireless access points.	Is wireless traffic encrypted using strong protocols (WPA3)?	Inspect wireless controller configurations.	Wireless Config Screenshots, Encryption Policy.	Eavesdropping or unauthorized wireless access.	CIS Control 12
Vulnerability Scanning	Identify technical weaknesses.	Are regular vulnerability scans performed on the network?	Review recent vulnerability scan reports and remediation.	Scan Reports, Remediation Logs.	Exploitation of known unpatched vulnerabilities.	NIST SP 800-53 RA-5
Patch Management	Keep systems updated.	Is there a formal process for deploying security patches?	Review patch compliance reports for servers/workstations.	Patch Reports, WSUS/SCCM Logs.	System compromise via old vulnerabilities.	CIS Control 7

— Dr. Nath Alagbe —

Domain 6: Application Controls

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Input Validation	Ensure data accuracy at entry.	Does the application validate data format and range?	Perform "negative testing" or review code validation logic.	Test Scripts, Code Snippets, Error Logs.	Invalid data causing system errors or fraud.	OWASP ASVS
Processing Integrity	Ensure correct data processing.	Are there controls to detect processing errors or duplicates?	Review reconciliation reports and error handling logs.	Reconciliation Reports, Error Logs.	Financial inaccuracies or data corruption.	COBIT 2019 DSS06
Output Reconciliation	Verify output accuracy.	Is application output reconciled to source data?	Inspect evidence of output reviews and sign-offs.	Output Reports, Reconciliation Sign-offs.	Decisions made based on incorrect reports.	SOC 2 PI1.1

Interface Controls	Secure data transfers between systems.	Are data transfers between applications encrypted and logged?	Review interface specifications and transfer logs.	Interface Specs, SFTP Logs, Encryption Config.	Data leakage or tampering during transit.	ISO 27002 Control 14
Audit Trails	Maintain accountability.	Does the application log all critical user actions?	Inspect application log settings and sample logs.	Application Logs, Logging Policy.	Inability to reconstruct events after an incident.	NIST SP 800-53 AU-2
Error Handling	Manage system failures gracefully.	Do error messages avoid disclosing sensitive info?	Review sample error messages and exception handling.	Error Message Screenshots, Exception Logs.	Information disclosure to potential attackers.	OWASP Top 10

Domain 7: Change Management

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Change Authorization	Prevent unauthorized changes.	Are all changes formally requested and authorized?	Review a sample of Change Request (CR) forms.	CR Forms, Approval Records.	Unauthorized changes causing outages.	ITIL Change Enablement
Testing and QA	Ensure change quality.	Are changes tested in a non-production environment?	Review User Acceptance Testing (UAT) results.	UAT Sign-offs, Test Plans.	Bugs or performance issues in production.	COBIT 2019 BAI06
Separation of Duties	Prevent conflict of interest.	Are developers restricted from deploying to production?	Review access rights for Dev vs. Prod environments.	Access Matrix, Deployment Logs.	Unauthorized or malicious code deployment.	NIST SP 800-53 AC-5
Rollback Procedures	Enable recovery from failed changes.	Do all change plans include a documented rollback strategy?	Inspect change plans for back-out procedures.	Change Plans, Rollback Scripts.	Extended downtime if a change fails.	ISO 27002 Control 12.1.2
Emergency Changes	Control urgent fixes.	Is there a formal process for emergency changes?	Review the emergency change log and post-approvals.	Emergency Change Logs, Retroactive Approvals.	Bypassing controls under the guise of urgency.	ITIL Service Transition
Post-Implementation	Verify change success.	Are post-implementation reviews (PIR) conducted?	Review PIR reports for major changes.	PIR Reports, Incident Logs.	Unresolved issues persisting after deployment.	COBIT 2019 BAI06.01

Domain 8: Data Governance and Privacy

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference

Data Classification	Categorize data by sensitivity.	Is there a data classification policy and schema?	Review the policy and inspect data labels.	Data Classification Policy, Labeled Data.	Inadequate protection for sensitive data.	ISO 27001 Clause 8.2
Data Retention	Manage data lifecycle.	Is data retained and disposed of per policy?	Review retention schedules and disposal certificates.	Retention Policy, Disposal Records.	Legal non-compliance or excessive storage costs.	NIST Privacy Framework
Privacy Impact (PIA)	Assess privacy risks.	Are PIAs conducted for new systems handling PII?	Review recent PIA reports.	PIA Reports, Privacy Policy.	Regulatory fines (GDPR/CCPA) for privacy breaches.	ISO 27701
Data Encryption	Protect data at rest.	Is sensitive data encrypted on servers and backups?	Inspect encryption configurations and key management.	Encryption Configs, Key Management Policy.	Data breach leading to clear-text exposure.	NIST SP 800-53 SC-28
Data Quality	Ensure data reliability.	Are there processes to ensure data accuracy and completeness?	Review data quality reports or cleansing logs.	Data Quality Metrics, Cleansing Logs.	Poor business decisions based on "dirty" data.	COBIT 2019 APO14
Data Ownership	Assign accountability.	Are data owners identified for all critical datasets?	Review the Data Inventory or Asset Register.	Data Asset Register, Owner List.	Lack of accountability for data protection.	ISO 27002 Control 8.1.1

Domain 9: Incident Management

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Incident Response Plan	Prepare for security events.	Is there a documented Incident Response Plan (IRP)?	Review the IRP and verify it is updated.	Incident Response Plan, Update Logs.	Chaotic and ineffective response to breaches.	NIST SP 800-61
Detection & Reporting	Ensure timely awareness.	Are incidents detected and reported promptly?	Review monitoring alerts and incident logs.	Monitoring Logs, Incident Tickets.	Prolonged attacker dwell time.	CIS Control 17
Incident Categorization	Prioritize response efforts.	Are incidents categorized by severity and impact?	Inspect the incident management system.	Incident Logs, Priority Matrix.	Misallocation of resources during a crisis.	ITIL Incident Management
Root Cause Analysis	Prevent recurrence.	Is a Root Cause Analysis (RCA) performed for major incidents?	Review a sample of RCA reports.	RCA Reports, Problem Records.	Recurring incidents causing repeated downtime.	ISO 27002 Control 16
Post-Incident Review	Improve future response.	Are "Lessons Learned" sessions held after incidents?	Review meeting minutes from post-incident reviews.	Lessons Learned Reports, Action Items.	Failure to improve security posture after a breach.	NIST SP 800-61

Communication Plan	Manage stakeholder info.	Is there a plan for communicating during an incident?	Review the communication protocols in the IRP.	Communication Plan, Contact Lists.	Reputational damage due to poor communication.	SOC 2 CC7.3

Domain 10: Business Continuity and Disaster Recovery (BCDR)

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Business Impact (BIA)	Identify critical processes.	Has a BIA been conducted to determine RTO/RPO?	Review the BIA report and methodology.	BIA Report, RTO/RPO Table.	Recovery priorities not aligned with business needs.	ISO 22301
Disaster Recovery Plan	Ensure technical recovery.	Is there a documented and approved DR Plan?	Review the DRP for technical completeness.	Disaster Recovery Plan, Approval.	Inability to restore IT services after a disaster.	NIST SP 800-34
DR Testing	Validate recovery capability.	Are DR tests (simulations/failovers) conducted annually?	Review the most recent DR test report.	DR Test Results, Action Plans.	The DR plan fails when actually needed.	ISO 27002 Control 17
Offsite Storage	Protect backups from local disasters.	Are backups stored in a geographically separate location?	Verify off-site storage location and security.	Offsite Storage Contract, Transfer Logs.	Local disaster destroying both primary and backup data.	NIST SP 800-53 CP-6
Crisis Management	Coordinate emergency response.	Is there a crisis management team with defined roles?	Review the Crisis Management Plan and Org Chart.	Crisis Plan, Team Contact List.	Lack of leadership during a major disruption.	COBIT 2019 DSS04
Plan Maintenance	Keep BCDR plans current.	Are BCDR plans reviewed and updated regularly?	Check version history and review dates on plans.	Updated BCDR Plans, Review Logs.	Outdated plans that don't reflect current IT environment.	ISO 22301 Clause 9

Domain 11: Third-Party Risk Management (TPRM)

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Vendor Due Diligence	Assess vendor security.	Is security due diligence performed before hiring vendors?	Review completed vendor security questionnaires.	Security Questionnaires, Audit Reports.	Onboarding high-risk or insecure vendors.	NIST SP 800-161

Right to Audit	Ensure oversight rights.	Do contracts include a "Right to Audit" clause?	Review a sample of vendor contracts.	Vendor Contracts, Legal Templates.	Inability to verify vendor security claims.	ISO 27002 Control 15
SLA Monitoring	Ensure service quality.	Are vendor Service Level Agreements (SLAs) monitored?	Review vendor performance reports against SLAs.	SLA Reports, Performance Dashboards.	Poor service impacting business operations.	COBIT 2019 APO10
Data Processing Agmt	Protect data shared with vendors.	Are DPAs in place for vendors handling PII?	Inspect signed Data Processing Agreements.	Signed DPAs, Privacy Clauses.	Legal liability for vendor data breaches.	GDPR Article 28
Vendor Termination	Securely end relationships.	Is there a process to revoke vendor access upon termination?	Review the vendor offboarding checklist.	Offboarding Logs, Access Revocation.	Former vendors retaining access to systems/data.	SOC 2 CC9.2
Supply Chain Risk	Manage Nth-party risks.	Does the organization assess risks from vendors' vendors?	Review supply chain risk assessment reports.	Supply Chain Maps, Risk Reports.	Hidden risks in the extended supply chain.	NIST CSF (ID.SC)

Domain 12: Cloud Governance and Security

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Shared Responsibility	Define security duties.	Is the shared responsibility model understood and documented?	Review the cloud security strategy or RACI matrix.	RACI Matrix, Cloud Strategy.	Security gaps where neither party takes ownership.	CSA CCM
Cloud Config Mgmt	Prevent misconfigurations.	Are cloud resources configured securely (e.g., no public S3)?	Use cloud security posture management (CSPM) tools.	CSPM Reports, Config Screenshots.	Data exposure due to simple config errors.	CIS Cloud Benchmarks
Cloud IAM	Secure cloud access.	Is MFA enforced for all cloud console access?	Inspect IAM settings in the cloud portal (AWS/Azure/GCP).	IAM Policy, MFA Status Report.	Full cloud environment takeover via stolen creds.	NIST SP 800-210
Data Residency	Control data location.	Is cloud data stored in approved geographic regions?	Inspect cloud resource location settings.	Region Configs, Compliance Reports.	Violation of data sovereignty laws.	ISO 27017
Shadow IT Monitoring	Detect unauthorized cloud use.	Is there a process to detect "Shadow IT"	Review CASB logs or network egress reports.	CASB Reports, Egress Logs.	Unmanaged data sprawl in insecure cloud apps.	COBIT 2019 APO01

		cloud services?				
CSP Compliance	Verify provider security.	Are SOC 2 or ISO reports reviewed for cloud providers?	Review the most recent CSP audit reports.	CSP SOC 2 Reports, Review Notes.	Relying on an insecure cloud infrastructure.	SOC 2 CC9.1

Domain 13: Logging, Monitoring, and SOC Operations

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Log Management	Ensure log availability.	Are logs from critical systems centralized and protected?	Inspect SIEM configuration and log retention settings.	SIEM Config, Log Retention Policy.	Inability to investigate security incidents.	NIST SP 800-92
SIEM Alerting	Detect threats in real-time.	Are SIEM alerts tuned to reduce false positives?	Review alert logic and recent alert history.	Alert Rules, False Positive Logs.	"Alert fatigue" leading to missed real threats.	CIS Control 8
24/7 Monitoring	Ensure continuous oversight.	Is there 24/7 monitoring of security events?	Review SOC shift schedules or MSSP contract.	SOC Schedule, MSSP SLA.	Attacks occurring during "off-hours" go undetected.	ISO 27002 Control 12.4
Incident Escalation	Ensure timely response.	Is there a clear escalation path for security alerts?	Review the SOC Playbooks or Escalation Matrix.	SOC Playbooks, Contact Matrix.	Critical alerts not reaching the right decision-makers.	COBIT 2019 DSS02
Threat Hunting	Proactively find threats.	Does the SOC perform proactive threat hunting?	Review threat hunting reports and findings.	Threat Hunt Logs, IOC Lists.	Advanced persistent threats (APTs) staying hidden.	NIST CSF (DE.AE)
SOC Metrics	Measure SOC effectiveness.	Are SOC metrics (MTTD/MTTR) tracked and reported?	Review SOC monthly performance reports.	SOC Dashboards, MTTR Reports.	Inefficient SOC operations and slow response.	CIS Control 17

Domain 14: Compliance and Regulatory Alignment

Audit Area	Audit Objective	Audit Questions	How to Validate	Evidence Required	Risk if Deficient	Reference
Regulatory Mapping	Identify legal obligations.	Are all relevant IT laws and regulations identified?	Review the Compliance Register or Legal Matrix.	Compliance Register, Legal Matrix.	Legal penalties and loss of license to operate.	COBIT 2019 MEA03

Compliance Monitoring	Ensure ongoing adherence.	Is there a process for regular compliance self-assessments?	Review self-assessment reports and workpapers.	Self-Assessment Reports, Checklists.	Undetected non-compliance until an external audit.	ISO 27001 Clause 9.1
Internal Audit Program	Provide independent assurance.	Is there an annual IT internal audit plan?	Review the Internal Audit Charter and Annual Plan.	Audit Charter, Annual Audit Plan.	Lack of independent oversight on IT controls.	IIA Standards
External Audit Coord	Manage external reviews.	Is there a process to coordinate with external auditors?	Review external audit reports and management responses.	External Audit Reports, Responses.	Inefficient audits and unaddressed external findings.	COBIT 2019 MEA01
Policy Alignment	Ensure internal rules meet laws.	Do internal IT policies align with regulatory requirements?	Perform a gap analysis between policies and laws.	Gap Analysis Report, Policy Map.	Policies that fail to meet legal minimums.	NIST SP 800-53 PL-2
Ethics and Conduct	Promote professional behavior.	Is there an IT code of ethics or conduct?	Review the Code of Conduct and training records.	Code of Ethics, Training Logs.	Insider threats and unethical IT practices.	COBIT 2019 APO01.06

Follow me on:

📌 Click 👉 ***here*** for my LinkedIn Profile.

📌 Click 👉 ***here*** for CyberVerge's LinkedIn Page

📌 Click 👉 ***here*** & 👉 ***here*** for X Accounts

— Dr. Nath Alagbe —