Data Security and Privacy Audit Checklist



By: Dr. Nath Alagbe

Data Security and Privacy Audit Checklist Tables

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

A Data Security and Privacy Audit is a formal, systematic examination of an organization's policies, procedures, and controls related to the protection of sensitive data, particularly Personally Identifiable Information (PII). It is a critical function that assesses the effectiveness of safeguards designed to ensure the confidentiality, integrity, and availability of data, while also verifying adherence to privacy principles and regulatory mandates

This section contains the comprehensive, standards-aligned audit checklist, structured into 14 critical domains. This content is designed for direct use by experienced IT auditors and GRC professionals.

Domain 1: Data Governance and Accountability

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Governance Framework	Is a formal Data Governance Framework (DGF) documented, approved by executive management, and communicated across the organization?	Inspect the DGF document for clear scope, objectives, and alignment with business strategy. Interview the Chief Data Officer (CDO) or equivalent.	DGF document, Executive approval minutes.	ISO 27001 (A.5.1), NIST Privacy Framework (GV.PO-P) [3] [4]
Roles and Responsibilities	Are Data Owners, Data Stewards, and a Data Protection Officer (DPO) formally appointed with clearly defined, documented, and communicated responsibilities?	Review organizational charts and job descriptions. Inspect the DPO appointment letter and reporting structure.	Organizational chart, Role descriptions, DPO appointment letter.	GDPR (Art. 37), ISO 27701 (5.2.1) [2] [5]
Policy Management	Are data security and privacy policies reviewed at least annually, version-controlled, and accessible to all relevant personnel?	Inspect the policy repository. Check the last review date on key policies (e.g., Acceptable Use, Data Protection).	Policy review log, Policy version history.	ISO 27001 (A.5.3) [1]

Domain 2: Data Classification and Handling

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Data Inventory	Is a comprehensive data inventory or asset register maintained, identifying all data types, locations, data owners, and regulatory requirements?	Inspect the data inventory tool/register. Trace a sample of sensitive data assets back to the inventory.	Data Inventory/Asset Register, Data Flow Diagrams (DFDs).	NIST SP 800-53 (MP-6), ISO 27001 (A.8.2) [1] [3]
Classification Schema	Is a formal data classification scheme (e.g., Public, Internal, Confidential, Restricted) defined, documented, and approved?	Review the Data Classification Policy. Verify that the scheme aligns with the organization's risk tolerance.	Data Classification Policy, Classification guidelines.	ISO 27001 (A.8.2.1) [1]

Handling Procedures	Are documented procedures in place for the secure handling, storage, and transmission of data based on its classification level?	Observe personnel handling classified information (e.g., printing, emailing). Inspect physical storage controls.	Data Handling Procedures, Training records on classification.	ISO 27001 (A.8.2.3) [1]

Domain 3: Privacy Governance and Consent Management

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Privacy Notice and Transparency	Is a clear, concise, and easily accessible Privacy Notice provided to data subjects before or at the point of data collection?	Review the organization's website and application interfaces. Check for evidence of version control on the notice.	Current Privacy Notice, Records of notice publication dates.	GDPR (Art. 12, 13, 14), CCPA (1798.110) [5] [6]
Consent Mechanism	Where consent is the lawful basis, is it freely given, specific, informed, and unambiguous (opt-in)? Is consent granular for different processing purposes?	Test the consent mechanism on a public-facing application. Inspect the database schema for consent records.	Consent management platform configuration, Consent log extracts.	GDPR (Art. 7), ISO 27701 (7.2.1) [2] [5]
Withdrawal of Consent	Is there an easy-to-use mechanism for data subjects to withdraw consent, and are procedures in place to honor such requests promptly?	Test the withdrawal process. Inspect the procedure for processing withdrawal requests and the associated log.	Consent Withdrawal Procedure, Log of withdrawal requests and fulfillment.	GDPR (Art. 7(3)) [5]

Domain 4: Data Lifecycle Management

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Data Minimization	Is the collection and processing of personal data limited to what is strictly necessary for the specified, explicit, and legitimate purposes?	Review Data Protection Impact Assessments (DPIAs) or Privacy Threshold Analyses (PTAs) for justification of data elements collected.	DPIA/PTA reports, Data collection forms/fields.	GDPR (Art. 5(1)(c)), NIST Privacy Framework (CT.DP-P) [4] [5]
Use Limitation	Are controls in place to ensure that data is not used for purposes incompatible with those for which it was originally collected?	Inspect system access controls and data use agreements. Interview business process owners.	Data Use Policy, System configuration settings (e.g., data masking in test environments).	HIPAA (Privacy Rule), NIST SP 800-53 (PL-4) [3] [7]
Data Quality and Integrity	Are mechanisms in place to ensure the accuracy, completeness, and up-to-datedness of personal data?	Inspect data validation rules in key systems. Review data cleansing and reconciliation procedures.	Data Quality Policy, Data validation reports.	GDPR (Art. 5(1)(d)) [5]

CyVerge

Domain 5: Access Control and Identity Management

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Provisioning and De-provisioning	Are user accounts provisioned and de-provisioned promptly based on changes in employment or role, following a formal workflow?	Sample new hire and termination records. Trace the provisioning/de-provisioning workflow in the Identity Management System (IMS).	IMS workflow documentation, Sample provisioning/de-provisioning logs.	ISO 27001 (A.9.2), NIST SP 800-53 (AC-2) [1] [3]
Least Privilege and Need-to-Know	Is the principle of least privilege enforced, ensuring users only have the minimum access necessary to perform their job functions?	Review access rights for a sample of users against their job roles. Inspect privileged access management (PAM) tool configuration.	Access Control Matrix, PAM system logs.	ISO 27001 (A.9.4.1), NIST SP 800-53 (AC-6) [1] [3]
Multi-Factor Authentication (MFA)	Is MFA enforced for all remote access and for all privileged access to systems containing sensitive data?	Inspect system configuration settings (e.g., VPN, Cloud Console, Database). Attempt to log in to a sensitive system without MFA.	MFA configuration screenshots, Access logs showing MFA usage.	PCI DSS (Req 8.3), SOC 2 (CC6.1) [8] [9]

Domain 6: Encryption and Key Management

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Encryption at Rest	Is all sensitive data (e.g., PII, PHI, Cardholder Data) encrypted when stored on systems, databases, and backup media?	Inspect database and file system encryption settings (e.g., TDE, full-disk encryption). Review backup media inventory.	Encryption Policy, Database configuration screenshots.	PCI DSS (Req 3.4), HIPAA (Security Rule) [7] [8]
Encryption in Transit	Is strong, current encryption (e.g., TLS 1.2 or higher) used to protect sensitive data transmitted over public and internal networks?	Use network scanning tools to verify TLS versions on public-facing services. Inspect internal network configuration.	Network security configuration, SSL/TLS certificate inventory.	ISO 27001 (A.14.2.5) [1]
Key Management Lifecycle	Are cryptographic keys managed throughout their lifecycle, including secure generation, storage (e.g., HSM/KMS), distribution, rotation, and destruction?	Review the Key Management Policy and procedures. Inspect the configuration of the Key Management System (KMS) or Hardware Security Module (HSM).	Key Management Policy, Key rotation logs, KMS/HSM configuration.	NIST SP 800-57, PCI DSS (Req 3.5) [8]

Domain 7: Data Loss Prevention (DLP)

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
DLP Strategy and Scope	Is a formal DLP strategy defined, covering data at rest, in motion,	Review the DLP strategy document. Verify that	DLP Strategy Document, Data	ISO 27001 (A.12.6) [1]

	and in use, and is it aligned with the data classification scheme?	DLP rules cover all sensitive data classifications.	Classification Policy.	
DLP Rule Effectiveness	Are DLP rules configured to accurately detect and prevent unauthorized transmission of sensitive data (e.g., PII, PHI, credit card numbers)?	Perform a test of DLP rules by attempting to send dummy sensitive data via email or upload to an external site.	DLP rule configuration, Test results and corresponding DLP alerts.	NIST SP 800-53 (SI-4) [3]
Alert Monitoring and Response	Are DLP alerts monitored 24/7, and are documented procedures followed for the investigation and remediation of high-severity incidents?	Inspect the DLP console dashboard and alert logs. Review a sample of high-severity incident tickets.	DLP Alert Logs, Incident investigation reports.	SOC 2 (CC7.1), NIST SP 800-53 (IR-4) [3] [9]

Domain 8: Third-Party and Vendor Data Risk

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Due Diligence	Is a risk-based due diligence process performed on all third parties and vendors who process or store sensitive data before contract execution?	Review vendor onboarding files for a sample of high-risk vendors. Inspect the risk assessment methodology.	Vendor Risk Assessment reports, Due Diligence checklists.	ISO 27001 (A.15.1), NIST SP 800-53 (SA-9) [1] [3]
Contractual Requirements (DPA)	Do all contracts with data processors include mandatory data processing agreements (DPAs) that specify security measures, audit rights, and breach notification terms?	Inspect a sample of vendor contracts and DPAs. Verify compliance with GDPR Art. 28 requirements.	Signed Data Processing Agreements (DPAs), Contract review checklist.	GDPR (Art. 28), CCPA (1798.140(w)) [5] [6]
Ongoing Monitoring	Is there a program for the ongoing monitoring of vendor security and compliance, including periodic re-assessment and review of assurance reports (e.g., SOC 2)?	Review the vendor monitoring schedule. Inspect the latest SOC 2 Type 2 reports or ISO 27001 certificates for critical vendors.	Vendor monitoring log, Vendor assurance reports (SOC 2, ISO certs).	SOC 2 (CC9.1), ISO 27001 (A.15.2) [1] [9]

Domain 9: Cloud and Outsourced Data Processing

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Shared Responsibility Model	Is the organization's understanding and implementation of the Cloud Service Provider's (CSP) Shared Responsibility Model documented and correctly applied?	Review the cloud security policy and compare it against the CSP's model documentation. Interview the cloud security team.	Cloud Security Policy, Shared Responsibility Model documentation.	ISO 27017, NIST SP 800-144
Cloud Security Configuration	Are cloud security configurations (e.g., S3 bucket policies, security groups, network access control lists) regularly audited and hardened against best practices?	Inspect the output of Cloud Security Posture Management (CSPM) tools. Review configuration change management logs.	CSPM reports, Cloud configuration audit logs.	NIST SP 800-53 (SC-7), SOC 2 (CC6.6) [3] [9]
Data Residency and Sovereignty	Is the physical location (residency) of all sensitive data stored in the cloud documented,	Review the cloud architecture diagrams and	Cloud Architecture Diagram, Data	GDPR (Chapter V) [5]

	and does it comply with all applicable legal and regulatory requirements?	data residency settings in the CSP console.	Residency Compliance Matrix.	

Domain 10: Logging, Monitoring, and Audit Trails

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Log Generation and Scope	Are audit logs generated for all security-relevant events, including access to sensitive data, system configuration changes, and failed login attempts?	Inspect system configuration files (e.g., database, OS, application) to verify logging is enabled and configured correctly.	Logging Policy, System configuration settings.	ISO 27001 (A.12.4), NIST SP 800-53 (AU-2) [1] [3]
Log Protection and Retention	Are audit logs protected from unauthorized modification or deletion, and are they retained for a period consistent with legal and regulatory requirements?	Inspect log retention settings in the SIEM/log management system. Attempt to modify or delete a log entry (with permission).	Log Retention Policy, SIEM configuration screenshots.	PCI DSS (Req 10.5), NIST SP 800-53 (AU-9) [3] [8]
Monitoring and Review	Are audit logs and security events reviewed daily/periodically for anomalies, and are documented procedures followed for investigating suspicious activity?	Inspect SIEM/monitoring tool dashboards. Review a sample of log review reports and associated incident tickets.	Log Review Procedure, Daily/Weekly log review reports.	SOC 2 (CC7.1), ISO 27001 (A.12.4.3) [1] [9]

Domain 11: Incident Response and Breach Notification

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Incident Response Plan (IRP)	Is a formal, documented IRP in place that includes roles, responsibilities, communication plans, and procedures for data breach handling?	Review the IRP for completeness and alignment with NIST SP 800-61 (Preparation, Detection & Analysis, Containment, Eradication & Recovery, Post-Incident Activity).	Incident Response Plan (IRP), Communication matrix.	NIST SP 800-61, ISO 27001 (A.16.1) [1] [3]
IRP Testing and Training	Is the IRP tested at least annually via tabletop exercises or simulations, and are all relevant personnel trained on their roles?	Review tabletop exercise reports, including lessons learned and remediation actions. Inspect training records.	Tabletop Exercise Report, IRP Training records.	SOC 2 (CC7.2), NIST SP 800-53 (IR-3) [3] [9]
Breach Notification	Are clear procedures in place to notify supervisory authorities and affected data subjects within the mandatory regulatory timelines (e.g., 72 hours for GDPR)?	Review the breach notification procedure. Inspect a sample of past breach notifications (if any) for timeliness.	Breach Notification Procedure, Notification templates, Log of breach notifications.	GDPR (Art. 33, 34), HIPAA (Breach Notification Rule) [5] [7]

CyVerge

Domain 12: Data Subject Rights Management

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
DSAR Procedure	Is a formal procedure documented for handling Data Subject Access Requests (DSARs) and other privacy rights requests (e.g., erasure, rectification, portability)?	Review the DSAR procedure for compliance with regulatory timelines (e.g., 30 days for GDPR/CCPA).	DSAR Procedure, DSAR Request Form.	GDPR (Art. 15-22), CCPA (1798.100) [5] [6]
Identity Verification	Are robust mechanisms in place to verify the identity of the data subject requesting to disclose or modify personal data?	Inspect the identity verification steps in the DSAR procedure. Review a sample of completed DSAR files.	Identity Verification Procedure, Sample DSAR fulfillment logs.	ISO 27701 (7.3.1) [2]
Request Tracking and Fulfillment	Is a system used to log, track, and manage the fulfillment of all privacy rights requests, ensuring all are met within the required timeframes?	Inspect the DSAR tracking system (e.g., GRC tool, ticketing system). Review reports on average fulfillment time.	DSAR Tracking System reports, Fulfillment log.	GDPR (Art. 12) [5]

Domain 13: Retention, Archival, and Secure Disposal

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Retention Schedule	Is a formal data retention schedule documented, approved by legal counsel, and consistently applied across all data repositories?	Review the Retention Schedule. Trace a sample of data types to the schedule and verify the retention period.	Data Retention Schedule, Legal Counsel approval.	GDPR (Art. 5(1)(e)), ISO 27001 (A.8.3.2) [1] [5]
Secure Archival	Are archived data and backup media stored securely, protected by appropriate access controls, and encrypted?	Inspect the physical and logical security controls of the archival location (e.g., off-site vault, cloud archive).	Archival Security Policy, Encryption configuration for archives.	NIST SP 800-53 (MP-4) [3]
Secure Disposal	Are documented procedures followed for the secure and irreversible disposal (e.g., physical destruction, cryptographic erasure) of data and media when no longer required?	Observe the disposal process (e.g., shredding, degaussing). Inspect disposal logs and certificates.	Secure Disposal Procedure, Disposal logs and certificates (e.g., for hard drives).	NIST SP 800-88, PCI DSS (Req 9.8) [8]

Domain 14: Regulatory Compliance and Assurance

Audit Area	Audit Questions	How to Validate	Evidence Required	Explicit References
Legal and Regulatory Register	Is a current register of all applicable data security and privacy laws, regulations, and contractual requirements maintained and regularly reviewed?	Inspect the Legal and Regulatory Register. Verify that the register is updated following new legislation (e.g., CPRA).	Legal and Regulatory Register, Review log.	ISO 27001 (A.18.1.1) [1]

Compliance Monitoring	Is a formal program in place to monitor compliance with the identified legal and regulatory requirements, including internal and external audits?	Review the annual audit plan. Inspect a sample of internal compliance reports.	Annual Audit Plan, Internal Audit Reports.	ISO 27001 (A.18.1.2) [1]
Management Reporting	Are the results of compliance monitoring and audit activities reported to executive management and the Board regularly?	Review minutes from the Risk Committee or Board meetings where compliance reports were presented.	Board/Committee meeting minutes, Compliance dashboard reports.	SOC 2 (CC9.2) [9]

Follow me on:

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

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

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