CLOUD SECURITY AUDIT CHECKLIST



By: Dr. Nath Alagbe

Disclaimer and Copyright

This Cloud Security Audit Checklist and Audit Guide is produced for professional educational and internal audit purposes. The content is intended as a practitioner reference and does not constitute legal, regulatory, or compliance advice. Organizations should adapt audit procedures to their specific environments, risk profiles, applicable regulations, and cloud configurations.

Framework references including NIST, ISO/IEC, CIS, CSA CCM, COBIT, PCI DSS, HIPAA, GDPR, and FedRAMP are cited for informational and mapping purposes. Readers should consult official framework publications for authoritative guidance.

© 2026 Dr. Nath Alagbe. All rights reserved. Reproduction for commercial distribution requires written permission. Internal use within audit engagements and professional development is permitted.

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



1. Introduction to Cloud Security Audit

Definition

A cloud security audit is a systematic, evidence-based examination of an organization's cloud computing environment to evaluate the effectiveness of security controls, governance structures, configuration management practices, and compliance posture. Unlike traditional IT audits focused on on-premises infrastructure, cloud security audits must account for shared responsibility models, dynamic resource provisioning, API-driven architectures, and the involvement of one or more cloud service providers.

Purpose and Key Objectives

Cloud security audits serve to identify control deficiencies before they result in breaches, validate regulatory compliance, assure leadership and regulators, and drive continuous improvement in cloud security posture. Core objectives include:

- Evaluate the adequacy and effectiveness of cloud security controls across IaaS, PaaS, and SaaS environments
- Assess compliance with applicable regulatory frameworks including PCI DSS, HIPAA, GDPR, FedRAMP, and SOX
- Identify misconfigurations, excessive permissions, unencrypted data, and monitoring gaps
- Validate the shared responsibility model implementation between cloud providers and the organization
- Provide management and the board with independent assurance on cloud security risk
- Support continuous improvement through actionable, risk-rated findings and recommendations

Business Risks Addressed

Cloud security audits directly address material business risks including data breaches from exposed storage and misconfigured services, regulatory fines from non-compliance with privacy and financial regulations, service outages from inadequate resilience controls, reputational damage from publicly disclosed cloud incidents, and financial losses from insider threats or external attacks exploiting cloud vulnerabilities.

2. Overview of Cloud Computing

Service Models

Infrastructure as a Service (IaaS) provides virtualized compute, storage, and networking resources. The cloud customer manages the operating system, middleware, and applications. Examples include Amazon EC2, Azure Virtual Machines, and Google Compute Engine. PaaS provides a platform for application development without infrastructure management. The provider manages the runtime, middleware, and operating system. Examples include AWS Elastic Beanstalk, Azure App Service, and Google App Engine. SaaS delivers fully managed software applications over the internet. The provider manages the entire stack. Examples include Microsoft 365, Salesforce, and Google Workspace.

Deployment Models

Public cloud resources are owned and operated by a cloud service provider and shared among multiple customers with logical isolation. Private cloud infrastructure is dedicated to a single organization, either on-premises or hosted by a provider. Hybrid cloud combines public and private cloud environments with orchestration allowing workload portability. Multi-cloud uses services from two or more cloud providers to avoid vendor lock-in and optimize for cost, capability, or resilience.

3. Cloud Shared Responsibility Model

The shared responsibility model defines the division of security obligations between the cloud provider and the cloud customer. Misunderstanding this boundary is one of the leading causes of cloud security failures.

AWS Shared Responsibility

AWS is responsible for security 'of' the cloud: physical facilities, hypervisor, managed service infrastructure, and network controls. Customers are responsible for security 'in' the cloud: operating system configuration, IAM, application security, data encryption, network access controls, and regulatory compliance.

Microsoft Azure

Azure's model mirrors AWS with provider responsibility for physical infrastructure, fabric, and some platform services. Customer responsibilities scale with service type: maximum responsibility under IaaS, reduced under PaaS, minimal under SaaS - though data classification, access management, and client endpoint security always remain the customer's obligation.

Google Cloud Platform

GCP shares the same tiered model. Google manages hardware, storage encryption at rest by default, and the network infrastructure. Customers own identity configuration, application security, data governance, and access policies.

4. Common Cloud Security Risks

The following risks are the primary drivers for conducting cloud security audits. They represent the most common failure patterns observed across enterprise cloud environments.

- Misconfiguration: Publicly accessible storage buckets, open security groups, disabled logging, and unenforced MFA account for the majority of cloud breach root causes
- Excessive permissions: IAM roles granting administrator access to users and service accounts beyond operational need create catastrophic breach potential
- Insecure APIs: APIs without authentication, rate limiting, or input validation expose cloud services to injection, enumeration, and denial-of-service attacks
- Shadow IT: Business units adopting unsanctioned cloud services create data governance gaps and bypass security controls
- Data leakage: Sensitive data stored in unencrypted or publicly accessible cloud storage is exfiltrated by external attackers and insider threats
- Poor monitoring: Disabled audit logs and absent SIEM integration leave organizations blind to attacks occurring in their cloud environments
- Third-party risks: Vendor integrations with cloud access introduce supply chain vulnerabilities and data sharing risks
- Container and Kubernetes risks: Privileged pods, exposed API servers, and unscanned images enable cluster-level compromise
- AI and automation risks: LLM prompt injection, model poisoning, and uncontrolled automation actions introduce novel attack vectors in cloud-hosted AI systems

5. Cloud Security Audit Methodology

Planning

Define audit objectives, scope boundaries, and regulatory framework applicability. Identify cloud service providers, accounts, subscriptions, and projects in scope. Review prior audit findings and management action plans. Engage cloud operations, security, and compliance stakeholders for planning input.

Scoping

Determine which cloud deployment models (IaaS, PaaS, SaaS), environments (production, staging, development), and geographic regions are in scope. Apply a risk-based approach to prioritize higher-risk environments and data types.

Risk Assessment

Identify cloud-specific risks using threat modeling, prior incident data, vulnerability reports, and regulatory requirements. Rate risks by likelihood and impact to prioritize audit focus areas. Document the risk assessment in the audit planning memorandum.

Evidence Gathering and Technical Validation

Collect evidence through configuration exports, IAM reports, log samples, architecture diagrams, policy documents, and stakeholder interviews. Use cloud provider native tools (AWS Config, Azure Policy, GCP Security Command Center) and third-party CSPM tools for automated evidence collection. Apply sampling methodology for high-volume controls.

Reporting

Document findings with clear condition, criteria, cause, and effect (4Cs). Rate findings by risk level (Critical, High, Medium, Low, Informational). Develop actionable recommendations with responsible owners and target remediation dates. Present results in an executive summary and detailed audit report.

6. Cloud Security Audit Best Practices

- Apply a risk-based approach to focus audit effort on highest-risk cloud environments and data types
- Use cloud-native and third-party CSPM tools to automate evidence collection and configuration analysis
- Implement continuous auditing capabilities alongside periodic audits to detect control drift between formal audit cycles
- Apply Zero Trust audit lens: verify that every user, device, and service is authenticated and authorized regardless of location
- Validate the shared responsibility boundary for each cloud service in scope before assigning control ownership
- Ensure audit procedures cover all three major cloud providers (AWS, Azure, GCP) when multi-cloud environments are in scope
- Engage technical cloud architects and engineers during audit fieldwork to accurately interpret configuration evidence
- Maintain an evidence chain of custody and version-control all workpapers for audit quality and litigation readiness
- Issue findings with quantified business impact to drive management prioritization and remediation urgency
- Follow up on prior audit findings before closing the current audit cycle to track remediation effectiveness

7. Comprehensive Cloud Security Audit Checklist

The following checklist is organized by 15 mandatory audit domains. Each domain contains detailed control areas with associated risks, control objectives, audit test steps, evidence requirements, and framework references. Auditors should adapt procedures to the specific cloud environment, applicable regulations, and organizational risk profile.

1. Cloud Governance and Risk Management

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Cloud Security Policy Framework	Absence of documented policies leads to inconsistent security controls and regulatory gaps	Ensure a formal, board-approved cloud security policy exists and is reviewed annually	Review policy documentation; confirm last review date; interview CISO and cloud owner; verify policy covers all deployment models (IaaS, PaaS, SaaS)	Cloud security policy document; Board approval minutes; Policy review logs	NIST CSF GV.OC-01; ISO 27001 A.5.1; COBIT APO01; CSA CCM GRC-01
Cloud Risk Register	Untracked cloud risks lead to unmitigated exposures and audit surprises	Verify a current cloud-specific risk register exists and is actively maintained	Inspect risk register; confirm risks are rated by likelihood and impact; verify owner assignments and review cadence	Risk register export; Risk treatment plans; Review meeting minutes	NIST SP 800-53 RA-3; ISO 27001 Clause 6.1; COBIT APO12; CSA CCM GRC-04
Cloud Security Roles and Responsibilities	Role ambiguity results in control gaps and accountability failures	Confirm cloud security roles (CISO, Cloud Architect, Cloud Owner) are formally defined and assigned	Review RACI matrix; interview stakeholders; inspect job descriptions; verify escalation paths	RACI or responsibility matrix; Org chart; Job descriptions	ISO 27001 A.6.1; COBIT APO01.02; NIST CSF GV.RR-01
Third-Party Cloud Risk Assessments	Unvetted third-party cloud vendors introduce supply chain and data breach risks	Ensure third-party cloud providers are assessed before onboarding and reviewed annually	Review vendor risk assessments; inspect SOC 2 reports; confirm due diligence procedures; verify contract security clauses	Vendor risk assessment reports; SOC 2 Type II reports; Contracts with security SLAs	ISO 27001 A.5.19; NIST SP 800-53 SA-9; CSA CCM STA-01; PCI DSS Req. 12.8
Cloud Compliance Obligations Inventory	Missing compliance mapping results in regulatory violations and audit findings	Confirm all applicable regulatory and contractual obligations are mapped to cloud controls	Review compliance inventory; inspect control mapping documents; verify ownership and monitoring schedules	Compliance inventory document; Control mapping matrix; Regulatory tracking logs	NIST CSF GV.OC-03; COBIT MEA03; ISO 27001 Clause 4.2
Cloud Security Budget and Resource Planning	Insufficient resources for cloud security lead to control gaps and tool deficiencies	Verify cloud security budget is formally allocated and aligned with identified risks	Review security budget approvals; interview CISO; inspect resource allocation for cloud security tools and training	Approved budget documents; Security tool subscription records; Staffing plans	COBIT APO06; NIST CSF GV.OC-02
Cloud Security Awareness and Training Program	Untrained staff make misconfigurations and fall for phishing attacks targeting cloud credentials	Confirm cloud security training is delivered to all staff with cloud access roles	Review training completion records; inspect curriculum for cloud-specific content; verify annual refresh requirements	LMS training completion reports; Training curriculum; Role-based training matrices	ISO 27001 A.6.3; NIST SP 800-53 AT-2; CSA CCM HRS-09
Cloud Governance Committee	Lack of governance oversight leads to unauthorized cloud adoption and policy drift	Verify a cloud governance body meets regularly and reviews cloud risk and compliance posture	Review committee charter; inspect meeting minutes; confirm escalation procedures and reporting to board	Governance committee charter; Meeting minutes; Board reporting artifacts	COBIT APO01.08; ISO 27001 Clause 5.1; NIST CSF GV.OC-01
Cloud Security Strategy Alignment	Cloud security strategy misaligned with business objectives	Confirm cloud security strategy supports business goals and is reviewed with leadership	Interview CISO and executives; review strategy documents; verify alignment with enterprise risk appetite	Cloud security strategy document; Executive sign-off; Risk appetite statement	NIST CSF GV.OC-02; COBIT APO02; ISO 27001 Clause 5.2

	creates risk blind spots				
Cloud Incident Reporting to Regulators	Failure to report cloud incidents within required timeframes triggers regulatory penalties	Verify incident escalation and regulatory reporting procedures are documented and tested	Review incident response plan; inspect regulatory notification thresholds; test tabletop exercise records	Incident response plan; Regulatory notification procedures; Tabletop exercise reports	NIST SP 800-61; GDPR Art. 33; HIPAA Breach Notification; PCI DSS Req. 12.10

2. Identity and Access Management (IAM)

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Multi-Factor Authentication (MFA) Enforcement	Compromised credentials without MFA enable unauthorized cloud access and data breaches	Verify MFA is enforced for all users accessing cloud management consoles and privileged accounts	Pull IAM reports from AWS IAM, Azure AD, or GCP IAM; filter for users without MFA; review conditional access policies; confirm no exceptions without compensating controls	AWS IAM Credential Report; Azure AD MFA status report; GCP Cloud Identity audit log	NIST SP 800-63B; CIS CSC 6; ISO 27001 A.8.5; PCI DSS Req. 8.4
Least Privilege and Role Assignment	Over-privileged accounts increase blast radius of compromise and enable insider threats	Ensure IAM roles follow least privilege principles and are reviewed quarterly	Export IAM role assignments; identify users with admin or wildcard permissions; compare against job function requirements; inspect last-used data	IAM role assignment export; AWS Access Analyzer findings; Azure AD Privileged Identity Management report	NIST SP 800-53 AC-6; CIS CSC 5; ISO 27001 A.8.2; FedRAMP AC-6
Privileged Access Management (PAM)	Uncontrolled privileged access creates catastrophic breach potential and audit trail gaps	Confirm privileged accounts are managed through a PAM solution with session recording and approval workflows	Review PAM tool configuration; inspect privileged session logs; verify just-in-time access controls; confirm break-glass procedures	PAM session recordings; Privileged access request tickets; Break-glass access logs	NIST SP 800-53 AC-17; CIS CSC 4; ISO 27001 A.8.2; SOC 2 CC6.3
Service Account and API Key Management	Hardcoded or unrotated service account keys enable persistent unauthorized access	Verify service accounts use short-lived credentials and API keys are rotated on schedule	List all service accounts; check key age; inspect secrets management configuration; verify no hardcoded credentials in source code or configs	AWS IAM key rotation report; GCP service account key inventory; Azure Managed Identity configuration	NIST SP 800-53 IA-5; CIS CSC 5; CSA CCM IAM-09
Federated Identity and SSO Integration	Weak SSO configurations allow unauthorized access through identity provider vulnerabilities	Confirm SSO is properly configured with a trusted IdP and SAML or OIDC protocols	Inspect IdP configuration (Okta, Azure AD, Ping); review SAML assertions; verify session timeout settings; confirm fallback access controls	IdP configuration export; SAML trace logs; SSO policy documentation	NIST SP 800-53 IA-8; ISO 27001 A.5.17; CSA CCM IAM-04
Access Review and Recertification	Stale access accumulates over time creating excessive privilege and audit exposure	Verify user access reviews are performed at least quarterly with documented recertification	Pull access review completion records; inspect certification workflow logs; verify terminated employees are deprovisioned within SLA	Access recertification reports; Offboarding logs; HR termination records with IAM disable timestamps	ISO 27001 A.8.2; NIST SP 800-53 AC-2; SOC 2 CC6.2; PCI DSS Req. 8.3
Root and Break-Glass Account Controls	Uncontrolled root accounts can bypass all controls and cause irreversible damage	Confirm root/break-glass accounts are locked, stored securely, and never used for routine operations	Inspect root account last-used logs; verify MFA on root; confirm credentials stored in approved vault; review CloudTrail for root activity	Root account MFA status; CloudTrail root usage events; Vault access logs	CIS Benchmark AWS 1.4; NIST SP 800-53 AC-6(9); FedRAMP AC-2
Identity Lifecycle Management	Failure to deprovision leavers creates orphaned accounts exploitable by threat actors	Verify joiner, mover, leaver processes are automated and audited across cloud environments	Interview HR and IT; inspect provisioning/deprovisioning workflows; check for active accounts belonging to terminated employees	HRIS data vs. IAM account comparison; Provisioning workflow logs; Deprovisioning SLA reports	ISO 27001 A.5.18; NIST SP 800-53 AC-2; SOC 2 CC6.2
Cross-Account and Cross-	Misconfigured trust relationships	Ensure cross-account role	Inspect AWS STS assume-role policies; review Azure	IAM trust policy exports; Cross-	NIST SP 800-53 AC-4; CSA CCM

Cloud Trust Relationships	allow lateral movement across cloud accounts and tenants	assumptions and trust policies are minimal and reviewed regularly	resource delegation; audit GCP project IAM bindings for external accounts	account access logs; STS usage reports	IAM-14; CIS Benchmark AWS 1.21
Identity Threat Detection and Anomaly Monitoring	Undetected credential abuse and identity-based attacks persist unnoticed without behavioral monitoring	Confirm identity threat detection tools monitor for anomalous login patterns and privilege escalation	Review SIEM/SOAR integration for identity events; inspect AWS GuardDuty IAM findings; check Azure Identity Protection alerts; verify escalation playbooks	SIEM identity alert reports; GuardDuty findings; Azure Identity Protection risk events	NIST SP 800-53 AU-6; ISO 27001 A.8.16; CSA CCM TVM-09

3. Network Security

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Virtual Network Segmentation	Flat network architectures allow lateral movement after initial compromise	Verify cloud networks use proper segmentation with VPCs, subnets, and routing controls	Inspect VPC/VNET architecture; review subnet routing tables; verify workload separation between production, development, and DMZ environments	VPC configuration export; Subnet routing table documentation; Network architecture diagrams	NIST SP 800-53 SC-7; CIS Benchmark AWS 5.1; ISO 27001 A.8.22; CSA CCM NET-01
Security Group and Firewall Rule Review	Overly permissive security groups expose cloud resources to unauthorized network access	Ensure security group rules follow least-privilege and deny all inbound traffic by default	Export all security group rules; identify rules with 0.0.0.0/0 source for inbound; inspect port exposures; review unused rules	Security group export; AWS Config evaluation reports; Azure NSG flow logs; GCP VPC firewall rules	NIST SP 800-53 SC-7; CIS Benchmark AWS 5.2-5.4; PCI DSS Req. 1.3
Network Access Control Lists (NACLs)	Misconfigured NACLs create bypass paths around security group controls	Verify NACLs are configured as a defense-in-depth layer aligned with security group rules	Inspect NACL configurations; verify stateless rule ordering; check for overly permissive allow rules that contradict security groups	NACL configuration export; Traffic flow analysis; AWS Config compliance report	NIST SP 800-53 SC-7(5); CIS Benchmark AWS 5.5; CSA CCM NET-07
VPN and Private Connectivity Controls	Unencrypted or improperly authenticated VPNs expose corporate-to-cloud traffic	Confirm all administrative access to cloud environments traverses approved VPN or private links	Review VPN gateway configurations; inspect Direct Connect/ExpressRoute settings; verify certificate-based authentication; confirm split-tunneling policies	VPN configuration documentation; VPN gateway logs; Direct Connect topology diagrams	NIST SP 800-53 SC-8; ISO 27001 A.6.7; FedRAMP SC-28
DDoS Protection Controls	Unprotected cloud endpoints are vulnerable to volumetric DDoS attacks causing availability disruptions	Verify DDoS protection is enabled for internet-facing cloud resources	Inspect AWS Shield configuration; review Azure DDoS Protection plan; check GCP Cloud Armor policies; verify WAF rules complement DDoS mitigations	AWS Shield Advanced dashboard; Azure DDoS Protection reports; WAF rule configuration export	NIST SP 800-53 SC-5; CSA CCM NET-09; ISO 27001 A.8.22
DNS Security Controls	Unprotected DNS allows data exfiltration, DNS hijacking, and phishing via cloud domains	Ensure DNS security controls (DNSSEC, DNS logging, private zones) are properly configured	Inspect Route 53/Azure DNS/Cloud DNS configurations; verify DNSSEC signing where applicable; review DNS query logging; check for public vs. private zone separation	DNS configuration exports; DNS query logs; DNSSEC signing status reports	NIST SP 800-53 SC-20; CIS Benchmark; ISO 27001 A.8.22
Zero Trust Network Access (ZTNA)	Traditional perimeter-based access fails in cloud environments with distributed workforces	Confirm ZTNA principles are implemented with continuous verification and micro-segmentation	Review ZTNA tool deployment (Zscaler, Netskope, etc.); inspect access policies; verify device compliance checks; confirm application-level segmentation	ZTNA policy documentation; Access decision logs; Device compliance reports	NIST SP 800-207; ISO 27001 A.8.22; CSA CCM IAM-08
Network Traffic Monitoring and Inspection	Lack of network visibility allows threat actors to move laterally and exfiltrate data undetected	Ensure network flow logs and deep packet inspection are enabled for all critical cloud networks	Inspect VPC Flow Log configuration; review Azure Network Watcher; check GCP VPC flow logging; verify logs are sent to SIEM	VPC Flow Log configuration; Network monitoring dashboard; SIEM ingestion confirmation	NIST SP 800-53 SI-4; ISO 27001 A.8.16; CIS Benchmark AWS 3.9

API Gateway and Edge Security	Unprotected API gateways expose backend cloud services to injection, DoS, and authentication attacks	Verify API gateways enforce authentication, rate limiting, and input validation	Inspect API Gateway configurations; review throttling policies; check OAuth/JWT enforcement; inspect WAF integration with API endpoints	API Gateway configuration export; API access logs; WAF rule reports	NIST SP 800-53 SC-7; OWASP API Security Top 10; CSA CCM AIS-05
Network Encryption in Transit	Unencrypted network traffic enables interception of sensitive data crossing cloud boundaries	Confirm TLS 1.2 or higher is enforced for all data in transit within and between cloud services	Inspect load balancer SSL/TLS policies; review API endpoint encryption settings; verify inter-service communication encryption; check for deprecated protocols (TLS 1.0, 1.1, SSL)	SSL/TLS configuration reports; Load balancer listener settings; Certificate inventory	NIST SP 800-53 SC-8; PCI DSS Req. 4.2; HIPAA Security Rule; ISO 27001 A.8.24

4. Data Protection and Encryption

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Data Classification and Inventory	Unclassified data is inadequately protected, increasing breach risk and compliance exposure	Verify a data classification policy exists and cloud-stored data is classified and inventoried	Review data classification policy; inspect data discovery tool outputs; confirm classification tags on S3 buckets, Azure Blob, or GCS; interview data owners	Data classification policy; Data discovery reports; Storage resource tagging inventory	ISO 27001 A.5.12; NIST SP 800-53 RA-2; GDPR Art. 30; CSA CCM DSP-01
Encryption at Rest	Unencrypted data at rest is fully readable to anyone with storage access, including insider threats	Confirm all sensitive data stored in cloud is encrypted using approved algorithms (AES-256 or stronger)	Inspect S3 bucket encryption settings; review Azure Storage encryption; check GCP encryption configuration; verify customer-managed keys (CMK) where required	S3 encryption status report; Azure Policy compliance report; GCP CMEK configuration	NIST SP 800-53 SC-28; PCI DSS Req. 3.5; HIPAA Security Rule; ISO 27001 A.8.24
Encryption Key Management (KMS)	Poor key management leads to key exposure, rotation failures, and compliance violations	Verify encryption keys are managed through an approved KMS with rotation, access control, and audit logging	Inspect AWS KMS, Azure Key Vault, or GCP Cloud KMS configuration; verify key rotation schedules; check key access policies; review KMS audit logs	KMS key rotation audit; Key access policy exports; KMS CloudTrail logs	NIST SP 800-53 SC-12; CIS Benchmark AWS 3.7; ISO 27001 A.8.24; FedRAMP SC-12
Data Loss Prevention (DLP) Controls	Undetected data exfiltration results in regulatory breaches and reputational damage	Confirm DLP tools monitor and block unauthorized data movement from cloud environments	Review DLP policy configuration; inspect policy rule coverage (PII, PHI, PCI data); check DLP alert logs and incident history; verify endpoint-to-cloud coverage	DLP policy configuration; DLP alert and incident reports; Data movement analytics	ISO 27001 A.8.12; NIST SP 800-53 SI-12; GDPR Art. 25; PCI DSS Req. 3
Secrets and Credentials Management	Exposed secrets in code repositories or config files enable unauthorized access to cloud resources	Verify secrets (API keys, passwords, tokens) are stored in vaults and never hardcoded	Scan source code repositories with secrets detection tools; inspect Secrets Manager/Key Vault usage; verify rotation policies; check CI/CD pipeline for exposed secrets	Secrets detection scan report; Secrets Manager inventory; Rotation schedule records	NIST SP 800-53 IA-5; CIS Benchmark; CSA CCM IAM-09
Data Residency and Sovereignty Controls	Data stored in unapproved geographic regions violates regulatory requirements and contractual obligations	Confirm cloud data is stored only in approved geographic regions per regulatory and business requirements	Inspect cloud region configurations; review storage account location settings; verify data residency policies; check for cross-region replication settings	Cloud region configuration export; Data residency policy; Cross-region replication audit	GDPR Art. 44-49; ISO 27001 A.5.33; CSA CCM DSP-17
Database Encryption and Access Controls	Unencrypted or improperly secured databases are primary targets for exfiltration attacks	Ensure cloud databases use encryption at rest and in transit with access restricted to authorized services	Inspect RDS/Azure SQL/Cloud SQL encryption settings; review database IAM/access policies; check transparent data encryption; verify no public database endpoints	Database encryption audit; DB access policy exports; Public endpoint scan results	NIST SP 800-53 SC-28; PCI DSS Req. 3.4; HIPAA Security Rule; ISO 27001 A.8.24

Data Backup Encryption	Unencrypted backups represent a secondary attack vector for sensitive data exfiltration	Verify all cloud backups are encrypted with keys separate from production encryption keys	Inspect backup configuration in AWS Backup, Azure Backup, or GCP Backup; verify encryption key separation; review backup access controls	Backup policy configuration; Encryption audit for backup vaults; Access control reports	NIST SP 800-53 CP-9; ISO 27001 A.8.13; PCI DSS Req. 3.5
Data Masking and Tokenization	Full sensitive data values in non-production environments increase breach impact and compliance risk	Confirm sensitive data is masked or tokenized in development, testing, and analytics environments	Review data masking configuration; inspect test environment data; verify PII/PCI data is not present in raw form in non-production	Data masking tool configuration; Test environment data samples review; DLP scan of non-production systems	PCI DSS Req. 3.3; HIPAA; ISO 27001 A.8.11; GDPR Art. 25
Secure Data Deletion and Disposal	Residual data on decommissioned cloud storage creates unauthorized access risks and compliance violations	Verify data destruction procedures comply with policy when cloud resources are decommissioned	Inspect decommissioning runbooks; review crypto-shredding or data wipe procedures; verify logs of resource deletion; confirm key destruction for CMK-protected data	Decommissioning procedure documentation; Key deletion logs; Resource termination audit trails	NIST SP 800-53 MP-6; ISO 27001 A.8.10; GDPR Art. 17; CSA CCM DSP-07

5. Logging and Monitoring

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Cloud Audit Log Enablement	Disabled audit logs prevent detection of attacks and create evidence gaps during incident investigations	Verify audit logging is enabled across all cloud accounts and services	Check AWS CloudTrail status (all regions); inspect Azure Monitor Diagnostic Settings; review GCP Cloud Audit Logs configuration; verify log coverage for management, data, and activity events	CloudTrail configuration screenshot; Azure Diagnostic Settings export; GCP Audit Logs status	CIS Benchmark AWS 3.1-3.14; NIST SP 800-53 AU-2; PCI DSS Req. 10.2; ISO 27001 A.8.15
Log Integrity and Tamper Protection	Tampered logs prevent forensic investigation and undermine audit evidence reliability	Confirm cloud logs are protected from modification with integrity checks enabled	Inspect CloudTrail log file validation; review Azure Immutable Storage for logs; check GCP log sink configurations; verify WORM storage for log archives	CloudTrail log integrity validation report; Azure Immutable Blob configuration; Log hash verification records	NIST SP 800-53 AU-9; PCI DSS Req. 10.5; ISO 27001 A.8.15; FedRAMP AU-9
SIEM Integration and Log Centralization	Siloed logs in individual cloud accounts prevent correlation of cross-account attack patterns	Verify all cloud logs are centralized in a SIEM for correlation and retention	Review log export configurations to SIEM; inspect SIEM dashboards for cloud log ingestion; verify log volume and completeness; confirm alerting rules are configured	SIEM ingestion report; Log source inventory; SIEM cloud dashboard screenshot	NIST SP 800-53 SI-4; ISO 27001 A.8.16; SOC 2 CC7.2; CSA CCM LOG-05
Log Retention Policy Compliance	Insufficient log retention prevents forensic investigations and violates regulatory requirements	Ensure cloud logs are retained for the minimum period required by policy and regulation	Review log retention configuration in CloudWatch, Azure Monitor, and GCP; compare retention periods against regulatory minimums (PCI: 12 months, HIPAA: 6 years); verify archive policies	Log retention configuration exports; Retention policy documentation; Regulatory mapping document	PCI DSS Req. 10.7; HIPAA 45 CFR 164.312; NIST SP 800-53 AU-11; ISO 27001 A.8.15
Real-Time Alerting and Threshold Monitoring	Delayed detection of security events allows attackers extended dwell time to cause damage	Confirm real-time alerting is configured for critical cloud security events	Review CloudWatch Alarms and metric filters; inspect Azure Alerts; check GCP Alerting Policies; verify alert routing to SOC and on-call personnel	Alert rule configuration export; Alert history reports; On-call escalation procedures	NIST SP 800-53 SI-4; CIS Benchmark AWS 3.1-3.14; ISO 27001 A.8.16
User Activity and Behavioral Analytics (UEBA)	Subtle insider threats and compromised accounts evade signature-based detection without behavioral baselines	Verify UEBA tools monitor cloud user behavior and generate risk scores for anomalous activity	Inspect UEBA tool configuration (Microsoft Sentinel UEBA, Splunk UEBA); review baseline establishment; check risk score alerts; verify SOC review procedures	UEBA risk score reports; Anomaly detection alerts; SOC investigation tickets	NIST SP 800-53 AU-6; ISO 27001 A.8.16; CSA CCM LOG-09

Cloud-Native Security Service Monitoring	Disabling cloud-native security services creates detection blind spots for platform-level threats	Confirm AWS GuardDuty, Azure Defender, and GCP Security Command Center are enabled and tuned	Inspect GuardDuty enablement across all accounts and regions; review Azure Defender plans; check GCP SCC findings; verify finding suppression and tuning procedures	GuardDuty finding summary; Azure Defender coverage report; GCP SCC findings dashboard	NIST SP 800-53 SI-3; CIS Benchmark; ISO 27001 A.8.16
Privileged Activity Monitoring	Unmonitored privileged actions create accountability gaps and enable undetected insider threats	Ensure all privileged and administrative actions are logged with sufficient detail	Review privileged session recording configuration; inspect management console audit trails; verify API call logging for admin-level operations; check PAM tool logs	PAM session logs; CloudTrail admin event filters; Privileged action summary reports	NIST SP 800-53 AC-2(4); ISO 27001 A.8.15; SOC 2 CC6.8; PCI DSS Req. 10.2
Network Traffic Log Analysis	Absence of network log analysis allows data exfiltration and lateral movement to go undetected	Verify VPC flow logs and network logs are analyzed for anomalous traffic patterns	Inspect VPC Flow Log configuration; verify log delivery to SIEM or analytics platform; check for threat hunting procedures using network logs	VPC Flow Log samples; Network anomaly detection reports; Threat hunting runbooks	NIST SP 800-53 SI-4; CIS Benchmark AWS 3.9; ISO 27001 A.8.15
Log Access Controls	Unauthorized access to security logs enables an attacker to cover tracks after a breach	Confirm log access is restricted to authorized security personnel with audit trails of log access	Review IAM policies governing log bucket/storage access; inspect access logs for the log repositories themselves; verify MFA for log access	Log storage bucket access policy; Log access audit trail; IAM policy for log readers	NIST SP 800-53 AU-9; ISO 27001 A.8.15; PCI DSS Req. 10.5; FedRAMP AU-9

6. Incident Response and Recovery

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Cloud Incident Response Plan	Absence of a cloud-specific incident response plan increases breach containment time and regulatory exposure	Verify a documented, tested cloud incident response plan exists covering all major cloud providers in scope	Review incident response plan; confirm it covers cloud-specific scenarios (data breach, ransomware, account takeover); verify escalation paths; check last review date	Cloud IR plan document; Plan review approval records; Tabletop exercise reports	NIST SP 800-61; ISO 27001 A.5.26; SOC 2 CC7.3; PCI DSS Req. 12.10
Incident Detection and Triage Procedures	Inefficient triage procedures delay response and increase breach impact	Confirm incident detection sources are integrated and triage procedures are clearly documented	Inspect triage runbooks; review alert-to-ticket workflow; verify SIEM rule mappings to incident categories; confirm on-call rotation	Triage runbook; Alert-to-ticket workflow documentation; On-call schedule	NIST SP 800-61 Rev. 3; ISO 27001 A.5.25; SOC 2 CC7.4
Cloud Forensic Capability	Inability to conduct cloud forensics leads to evidence loss and failed root cause analysis	Ensure forensic procedures address cloud-specific evidence collection (snapshots, logs, memory)	Review cloud forensic runbooks; inspect evidence collection procedures for AWS, Azure, GCP; verify chain of custody procedures; check forensic tool access	Cloud forensic runbooks; Evidence collection checklists; Forensic tool access approvals	NIST SP 800-86; ISO 27001 A.5.28; CSA CCM SEF-05
Incident Communication Procedures	Poor communication during incidents leads to regulatory notification failures and reputational damage	Verify internal and external incident communication templates and contacts are current	Review communication templates; inspect regulatory notification contacts; confirm PR and legal involvement procedures; check notification timelines vs. regulatory requirements	Communication plan; Regulatory notification templates; Legal and PR escalation list	GDPR Art. 33-34; NIST SP 800-61; ISO 27001 A.5.26
Post-Incident Review Process	Without structured lessons learned, organizations repeat the same incidents	Confirm post-incident reviews are conducted after all significant cloud security incidents	Review post-incident review (PIR) reports; inspect corrective action tracking; verify RCA procedures; check implementation status of prior PIR action items	PIR reports; Corrective action tracking logs; Remediation evidence	NIST SP 800-61; ISO 27001 A.5.27; SOC 2 CC7.5
Cloud Account Isolation and Quarantine	Inability to isolate compromised cloud accounts allows	Verify procedures exist to isolate a compromised	Review account isolation runbooks; inspect IAM permission revocation	Account isolation runbook; Network quarantine	NIST SP 800-53 IR-4; ISO 27001

	attackers to persist and escalate	cloud account or resource within defined time targets	procedures; verify VPC isolation procedures; test quarantine time objectives in tabletop	procedure; Tabletop exercise results	A.5.26; CSA CCM SEF-03
Backup and Snapshot Availability for Recovery	Corrupted or missing backups prevent recovery from ransomware and data destruction attacks	Confirm cloud resource snapshots and backups are available and tested for incident recovery	Inspect backup configuration; verify backup frequency against RPO requirements; review recent restoration test results; check backup immutability settings	Backup configuration reports; Restoration test results; Immutable storage configuration	NIST SP 800-53 CP-9; ISO 27001 A.8.13; SOC 2 A1.3; PCI DSS Req. 9.4
Third-Party IR Support Retainer	Lack of pre-established IR retainer delays expert engagement during high-severity cloud incidents	Verify an IR retainer agreement with a qualified cloud security firm is in place and accessible	Review retainer agreement; inspect scope coverage for cloud environments; verify contact procedures and SLA commitments; confirm retainer is not expired	IR retainer agreement; Vendor contact list; SLA terms review	NIST SP 800-61; ISO 27001 A.6.8; SOC 2 CC7.3
Regulatory Breach Notification Compliance	Late or missing regulatory breach notifications trigger fines and enforcement actions	Confirm breach notification timelines (72-hour GDPR, state laws) are documented and tested	Review notification procedures; inspect regulatory timeline tracking; verify legal review process; check notification log for prior incidents	Notification procedure document; Regulatory timeline matrix; Prior breach notification records	GDPR Art. 33; HIPAA Breach Notification Rule; NIST SP 800-53 IR-6
Cloud IR Tabletop Exercises	Untested IR plans fail during actual incidents when time pressure is highest	Verify cloud-specific tabletop exercises are conducted at least annually with documented outcomes	Review tabletop exercise plans and reports; confirm cloud scenarios are included; check action item tracking from prior exercises; interview IR team	Tabletop exercise agendas and reports; Action item tracking log; Participant sign-off records	NIST SP 800-53 IR-3; ISO 27001 A.5.26; SOC 2 CC7.3; PCI DSS Req. 12.10

7. Vulnerability and Patch Management

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Cloud Vulnerability Scanning Program	Unscanned cloud workloads harbor known vulnerabilities exploitable by automated attack tools	Confirm vulnerability scanning is performed on all cloud workloads at least weekly	Review scanning tool configuration (Amazon Inspector, Tenable, Qualys); verify scan frequency; check scan coverage across all accounts and regions; inspect exception management	Vulnerability scan reports; Scan coverage dashboard; Exception register	NIST SP 800-53 RA-5; CIS CSC 7; PCI DSS Req. 11.3; ISO 27001 A.8.8
Patch SLA and Prioritization Process	Unprioritized patching leaves critical vulnerabilities open beyond acceptable risk thresholds	Verify a patch prioritization process exists with defined SLAs by severity (Critical: 24-72h, High: 7-14 days)	Review patch policy and SLA definitions; inspect patch compliance reports; check for critical vulnerabilities exceeding SLA; verify CVSS-based prioritization	Patch compliance dashboard; SLA tracking report; Overdue patch list	NIST SP 800-53 SI-2; CIS CSC 7; PCI DSS Req. 6.3; ISO 27001 A.8.8
Container Image Vulnerability Management	Vulnerable container images are deployed into production without detection in high-velocity environments	Ensure container images are scanned before deployment and base images are updated regularly	Inspect container registry scanning configuration (ECR, ACR, Artifact Registry); review CI/CD pipeline image scan gates; check for critical vulnerabilities in running images	Container image scan reports; CI/CD scan gate configuration; Registry scanning policy	NIST SP 800-190; CIS Docker Benchmark; ISO 27001 A.8.8; CSA CCM CCC-06
Cloud Provider Security Advisory Monitoring	Organizations miss critical cloud platform security advisories without a formal monitoring process	Confirm cloud provider security bulletins and advisories are monitored and actioned within defined SLAs	Review cloud security advisory subscription; inspect advisory tracking logs; verify responsible team for actioning advisories; check for overdue advisory responses	Security advisory subscription confirmation; Advisory tracking log; Remediation records	NIST SP 800-53 SI-5; ISO 27001 A.8.8; CSA CCM TVM-07
AMI and Base Image Hardening	Poorly hardened base images propagate security weaknesses to	Verify that approved, hardened base images are used for all cloud	Inspect approved AMI/image catalog; review CIS Benchmark hardening validation; verify drift detection	Approved image catalog; CIS hardening validation report;	CIS Benchmark; NIST SP 800-53 CM-6; NIST SP 800-190; ISO 27001 A.8.9

	every workload built from them	compute instances	from baseline; check image build pipeline controls	Drift detection alerts	
Serverless Function Dependency Scanning	Vulnerable third-party libraries in serverless functions introduce supply chain risk	Confirm Lambda and other serverless functions have their dependencies scanned for known vulnerabilities	Review serverless function dependency manifests; inspect automated dependency scanning configuration; check for known CVEs in function packages	Dependency scan reports; SBOM (Software Bill of Materials) inventory; Lambda function code scan reports	NIST SP 800-53 RA-5; CSA CCM CCC-09; OWASP Dependency-Check
Penetration Testing Program	Internal scanning alone fails to identify complex attack chains that simulate real adversary techniques	Verify cloud environments are included in the annual penetration testing program	Review penetration testing scope documentation; confirm cloud environments are in scope; inspect most recent pen test report; verify finding remediation tracking	Penetration test scope; Pen test reports; Remediation tracking report	PCI DSS Req. 11.4; ISO 27001 A.8.8; NIST SP 800-53 CA-8; SOC 2 CC4.1
Vulnerability Risk Acceptance Process	Vulnerabilities accepted without proper authorization and risk assessment increase residual risk	Confirm a formal risk acceptance process exists for vulnerabilities that cannot be patched immediately	Review risk acceptance policy; inspect existing risk acceptance records; verify appropriate authority approval; check expiration dates on accepted risks	Risk acceptance policy; Risk acceptance register; Approver authorization evidence	NIST SP 800-53 RA-3; ISO 27001 Clause 6.1.3; SOC 2 CC9.1
SBOM Management	Unknown third-party components in cloud applications create hidden vulnerability exposure	Verify software bill of materials is maintained for all cloud applications and reviewed against known CVEs	Inspect SBOM generation process; review SBOM tool integration with CI/CD; verify CVE correlation against SBOM components	SBOM inventory; CVE correlation reports; CI/CD SBOM pipeline configuration	NIST SP 800-53 SR-3; Executive Order 14028; CSA CCM CCC-09
Cloud Configuration Drift and Hardening Validation	Configuration drift from secure baselines reintroduces vulnerabilities over time	Ensure cloud configuration is continuously validated against CIS or vendor security benchmarks	Inspect AWS Security Hub Config rules; review Azure Policy compliance; check GCP Security Command Center; verify drift alerts trigger remediation workflows	Security Hub compliance report; Azure Policy compliance dashboard; Remediation workflow logs	CIS Benchmark; NIST SP 800-53 CM-6; ISO 27001 A.8.9; FedRAMP CM-6

8. Cloud Configuration Management

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Infrastructure as Code (IaC) Security Controls	Insecure IaC templates deploy misconfigured resources at scale and speed	Verify IaC templates are scanned for misconfigurations before deployment	Inspect Terraform/CloudFormation/Bicep security scanning integration; review scan gate configuration in CI/CD; check for policy-as-code enforcement; inspect rejected deployment history	IaC scan reports; Policy-as-code configuration; Rejected deployment logs	NIST SP 800-53 CM-3; ISO 27001 A.8.9; CSA CCM CCC-07
Cloud Security Posture Management (CSPM)	Manual configuration review cannot keep pace with cloud resource creation velocity	Confirm a CSPM tool continuously monitors cloud configurations against security benchmarks	Inspect CSPM tool configuration (Wiz, Prisma Cloud, Defender for Cloud); review finding dashboard; verify alert routing; check benchmark coverage (CIS, PCI, HIPAA)	CSPM dashboard report; Benchmark compliance scores; Alert routing configuration	NIST SP 800-53 CM-6; CIS Benchmark; ISO 27001 A.8.9; CSA CCM CCC-01
Change Management for Cloud Resources	Unauthorized cloud configuration changes introduce security risks and create audit trail gaps	Ensure all cloud infrastructure changes go through an approved change management process	Review change management policy; inspect cloud change tickets; verify production changes correlate with approved CRs; check for unauthorized changes via CloudTrail	Change management policy; Change tickets with approvals; CloudTrail change event correlation	NIST SP 800-53 CM-3; ISO 27001 A.8.32; COBIT BAI06; SOC 2 CC8.1
S3 Bucket and Storage Public Access Controls	Publicly accessible storage buckets are among the most common	Verify no storage buckets or containers are publicly accessible unless	Run AWS Trusted Advisor public bucket check; review Azure Storage Account public access settings; inspect GCP IAM for allUsers/allAuthenticatedUsers;	Public bucket report; AWS Config S3 rules evaluation; Azure	CIS Benchmark AWS 2.1; NIST SP 800-53 AC-3; CSA CCM DSP-06

	causes of cloud data breaches	explicitly required and approved	verify S3 Block Public Access is enabled org-wide	Policy public access report	
Resource Tagging and Asset Inventory	Untagged cloud resources evade security monitoring and create shadow asset risks	Confirm all cloud resources are tagged with owner, classification, environment, and cost center	Inspect tagging policy; run untagged resource reports across AWS, Azure, GCP; verify tagging compliance enforcement through policy; check asset inventory completeness	Tagging policy; Untagged resource audit report; CMDB/asset inventory export	NIST SP 800-53 CM-8; ISO 27001 A.5.9; COBIT APO09
Default Credential and Service Configuration Review	Unchanged default credentials and configurations are among the easiest attack vectors	Verify all cloud service defaults (passwords, open ports, sample data) have been changed from vendor defaults	Inspect new service deployment checklist; review default password change procedures; check for default admin accounts in cloud services; verify default security groups are not used	Deployment security checklist; Default configuration change records; Security group audit	CIS Benchmark; NIST SP 800-53 IA-5; PCI DSS Req. 2.1; ISO 27001 A.8.9
Cloud Resource Deletion Protection	Accidental or malicious deletion of critical cloud resources causes outages and data loss	Confirm deletion protection is enabled on critical cloud resources (databases, S3 buckets, key vaults)	Inspect deletion protection settings on RDS, S3 versioning, Azure Resource Locks; verify Key Vault soft-delete and purge protection; check Terraform state locking	Deletion protection configuration export; Resource lock audit; Versioning status report	NIST SP 800-53 CP-10; ISO 27001 A.8.13; AWS Well-Architected Reliability Pillar
Cloud Account Structure and Landing Zone	Poorly structured cloud accounts create blast radius exposure and governance gaps	Verify cloud account structure follows a multi-account strategy with proper organizational units (OUs)	Review AWS Organizations structure; inspect Azure Management Group hierarchy; check GCP Folder structure; verify SCPs/Azure Policies at OU level enforce guardrails	AWS Organizations structure diagram; SCP policy exports; Management Group hierarchy	AWS Well-Architected Framework; NIST SP 800-53 CM-2; CSA CCM GRC-01
Immutable Infrastructure Practices	Long-running, mutated cloud instances accumulate unpatched vulnerabilities and configuration drift	Confirm critical cloud workloads follow immutable infrastructure principles with regular replacement cycles	Review image build pipeline; inspect instance replacement policies; verify no direct SSH/RDP patching of production instances; check Auto Scaling group configurations	Image build pipeline documentation; Instance replacement schedule; Auto Scaling group config	NIST SP 800-53 SI-7; AWS Well-Architected Security Pillar; CIS Benchmark
Cloud Security Benchmark Compliance Scoring	Without baseline compliance scoring, security posture improvement cannot be measured or demonstrated	Confirm cloud environments are benchmarked against CIS or cloud provider benchmarks with tracked scores over time	Inspect benchmark scoring in Security Hub, Defender for Cloud, or CSPM; review score trends; verify remediation tracking for failed controls; confirm reporting to leadership	Benchmark compliance score history; Failed control remediation log; Leadership reporting artifacts	CIS Benchmark; NIST SP 800-53 CA-7; ISO 27001 A.8.9

9. DevSecOps and CI/CD Security

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Security Gate Integration in CI/CD Pipelines	Code with known vulnerabilities and misconfigurations is deployed to production without detection	Verify security scanning gates (SAST, DAST, SCA, IaC scanning) are integrated into CI/CD pipelines	Inspect pipeline configuration (Jenkins, GitHub Actions, Azure DevOps); verify mandatory security scan steps; confirm pipeline fails on critical findings; inspect scan tool configuration	Pipeline configuration exports; Security scan reports; Build failure logs	NIST SP 800-53 SA-11; ISO 27001 A.8.25; CSA CCM CCC-02; OWASP DevSecOps
Static Application Security Testing (SAST)	Insecure code patterns such as injection vulnerabilities are introduced undetected without source code analysis	Confirm SAST is run on every pull request with findings tracked and remediated	Review SAST tool configuration (SonarQube, Checkmarx, Semgrep); inspect finding severity thresholds; verify PR blocking for critical/high findings; review false positive management	SAST scan reports; PR gate configuration; Finding remediation tracking	NIST SP 800-53 SA-11(1); ISO 27001 A.8.25; OWASP SAMM
Dynamic Application	Runtime vulnerabilities in deployed cloud	Verify DAST is performed against deployed cloud	Inspect DAST tool configuration (OWASP ZAP, Burp Suite Enterprise); review scan	DAST scan reports; Scan schedule	NIST SP 800-53 SA-11(2); ISO

Security Testing (DAST)	applications go undetected without active exploitation testing	applications in staging and production	schedules; check production DAST procedures; inspect finding remediation timelines	configuration; Remediation tracking log	27001 A.8.29; OWASP SAMM
Software Composition Analysis (SCA)	Vulnerable open-source libraries are included in production code without awareness or remediation	Confirm SCA is integrated in CI/CD to identify vulnerable third-party dependencies	Inspect SCA tool configuration (Snyk, Black Duck, Dependabot); review dependency vulnerability reports; verify automated PR creation for dependency updates; check license compliance	SCA reports; Dependency vulnerability inventory; License compliance report	NIST SP 800-53 SA-12; Executive Order 14028; ISO 27001 A.8.25
Secure Code Review Process	Manual code reviews lacking security focus allow security vulnerabilities to be merged	Verify security-focused code review is required for changes to security-sensitive code components	Review code review policy; confirm security team reviewer requirements for sensitive components; inspect PR approval workflows; check code review completeness on recent deployments	Code review policy; PR approval history; Security reviewer sign-off records	NIST SP 800-53 SA-11; ISO 27001 A.8.28; OWASP SAMM
Pipeline Access Controls and Privilege Separation	Overly privileged CI/CD pipelines can be abused to deploy malicious code or access production secrets	Confirm CI/CD pipeline accounts follow least privilege and deploy with environment-specific credentials	Inspect pipeline service account permissions; verify environment-specific secrets management; check for production-access separation in lower environment pipelines; review pipeline RBAC	Pipeline IAM permission export; Secrets management configuration; RBAC policy for pipelines	NIST SP 800-53 AC-6; ISO 27001 A.8.25; CIS CSC 5; CSA CCM CCC-04
Artifact Signing and Supply Chain Integrity	Unsigned build artifacts enable supply chain attacks via tampered binaries or packages	Verify build artifacts are cryptographically signed and signatures are validated before deployment	Inspect artifact signing configuration; review signature validation in deployment pipeline; check container image signing (Cosign, Notary); verify registry admission control	Artifact signing policy; Signature validation logs; Registry admission controller config	NIST SP 800-53 SI-7; Executive Order 14028; SLSA Framework; ISO 27001 A.8.25
Environment Separation (Dev/Staging/Prod)	Shared environments allow a development or testing compromise to escalate into production impact	Confirm development, staging, and production environments are fully separated with distinct credentials and accounts	Inspect cloud account/subscription separation; verify no shared credentials across environments; check network isolation between environments; review deployment promotion controls	Environment architecture diagram; IAM credential audit; Network segmentation review	NIST SP 800-53 CM-2; ISO 27001 A.8.31; SOC 2 CC8.1
Dependency and Package Registry Controls	Dependency confusion and typosquatting attacks introduce malicious packages into builds	Verify approved package registries are enforced and dependency pinning is used in build configurations	Inspect package manager configurations (npm, pip, Maven); review private registry enforcement; verify dependency pinning (exact versions); check for dependency confusion controls	Package registry configuration; Build dependency lock files; Private registry enforcement logs	NIST SP 800-53 SA-12; CSA CCM CCC-09; OWASP Top 10 (A06)
Security Champions Program	Development teams without embedded security knowledge propagate the same security defects across products	Confirm a Security Champions program exists to embed security expertise within development teams	Review Security Champions program charter; inspect training completion records for champions; verify champion involvement in code reviews and security assessments	Security Champions program documentation; Training records; Champion activity logs	ISO 27001 A.6.3; NIST CSF PR.AT; OWASP SAMM

10. Container and Kubernetes Security

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Kubernetes RBAC Configuration	Overly permissive Kubernetes RBAC allows	Verify Kubernetes RBAC is configured with least privilege for all service	Export Kubernetes ClusterRoleBindings and RoleBindings; identify principals with cluster-admin	kubectl get clusterrolebindings output; RBAC audit report;	NIST SP 800-53 AC-6; CIS Kubernetes Benchmark 5.1;

	privilege escalation and lateral movement within clusters	accounts, users, and groups	or wildcard permissions; compare against job function requirements; inspect service account permissions	Service account review	ISO 27001 A.8.2; CSA CCM CCC-06
Container Image Security Scanning	Vulnerable container images introduce known CVEs directly into production workloads	Ensure all container images are scanned for vulnerabilities before admission to production clusters	Inspect image scanning configuration in ECR, ACR, or Artifact Registry; verify admission controller blocking high/critical images; review base image update frequency	Container scan reports; Admission controller configuration; Base image currency report	NIST SP 800-190; CIS Docker Benchmark 4.1-4.6; ISO 27001 A.8.8; PCI DSS Req. 6.3
Pod Security Standards/Admission Control	Privileged pods and host namespace access enable container escape and cluster-level compromise	Confirm Pod Security Standards (or equivalent) are enforced to prevent privileged container execution	Review Pod Security Admission configuration; inspect OPA Gatekeeper or Kyverno policies; check for running privileged pods; verify host path mount restrictions	Pod Security Admission config; OPA/Kyverno policy exports; Privileged pod audit	CIS Kubernetes Benchmark 5.2; NIST SP 800-190; ISO 27001 A.8.9; NSA Kubernetes Hardening Guide
Secrets Management in Kubernetes	Kubernetes Secrets stored as base64 in etcd without encryption are trivially decoded by unauthorized users	Verify Kubernetes Secrets are encrypted at rest and managed through an external secrets manager	Inspect etcd encryption configuration; review External Secrets Operator or Vault integration; check for hardcoded secrets in Pod specs or ConfigMaps; verify secret rotation procedures	etcd encryption configuration; Secret management tool config; ConfigMap audit for secrets	NIST SP 800-53 SC-28; CIS Kubernetes Benchmark 1.2; ISO 27001 A.8.24
Network Policies in Kubernetes	Kubernetes pods without network policies have unrestricted east-west communication enabling lateral movement	Confirm Kubernetes Network Policies enforce micro-segmentation between namespaces and workloads	Inspect applied Network Policies; verify default-deny policies exist in each namespace; check service mesh configuration (Istio, Linkerd); review inter-namespace communication rules	Network Policy YAML exports; Default-deny policy audit; Service mesh configuration	NIST SP 800-53 SC-7; CIS Kubernetes Benchmark 5.3; NSA Kubernetes Hardening Guide
Kubernetes Control Plane Security	Exposed or improperly secured control plane components enable full cluster takeover	Verify Kubernetes API server, etcd, and controller manager are hardened and access-restricted	Inspect API server flags for anonymous authentication disable; verify etcd access restrictions; check audit logging configuration; review API server audit policies	API server configuration audit; etcd access controls; Kubernetes audit log configuration	CIS Kubernetes Benchmark 1.1-1.4; NIST SP 800-53 AC-17; NSA Kubernetes Hardening Guide
Container Runtime Security	Unmonitored container runtime behavior allows malicious processes to execute undetected	Confirm runtime security tools (Falco, Sysdig, eBPF-based) monitor container behavior for anomalies	Inspect Falco rule configuration; review runtime alert history; check for behavioral anomaly rules (shell spawning, file system writes); verify alert routing to SIEM	Falco rule configuration; Runtime alert report; SIEM integration confirmation	NIST SP 800-190; ISO 27001 A.8.16; CIS Kubernetes Benchmark; CSA CCM CCC-06
Kubernetes Cluster Update and Patch Management	Running end-of-life Kubernetes versions exposes clusters to known CVEs with public exploits	Verify Kubernetes clusters are running supported versions and are patched within defined SLAs	Check cluster version against supported release matrix; inspect node pool update configurations; review upgrade history; verify auto-upgrade policies for managed clusters (EKS, AKS, GKE)	Cluster version report; Node pool configuration; Upgrade history	NIST SP 800-53 SI-2; CIS Kubernetes Benchmark; NIST SP 800-190
Namespace Isolation and Multi-Tenancy Controls	Insufficient namespace isolation allows workloads from different tenants or sensitivity levels to interfere	Confirm namespace-level isolation controls are implemented for multi-tenant or mixed-sensitivity clusters	Inspect namespace Resource Quotas and LimitRanges; review namespace-level RBAC; check for cross-namespace secret access; verify tenant isolation documentation	Namespace configuration audit; Resource Quota exports; RBAC namespace bindings	NIST SP 800-53 SC-2; CIS Kubernetes Benchmark; ISO 27001 A.8.22

Supply Chain Security for Container Builds	Compromised container build pipelines inject malicious code into production container images	Verify container build pipelines are secured and images are signed and verified before deployment	Review container build pipeline security; inspect image signing configuration (Cosign); verify signature validation at deployment; check for reproducible build practices	Build pipeline security review; Image signing configuration; Cosign verification logs	NIST SP 800-53 SI-7; Executive Order 14028; SLSA Framework; ISO 27001 A.8.25

11. API and Application Security

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
API Authentication and Authorization	Unauthenticated or improperly authorized APIs expose cloud resources to unauthorized access and abuse	Verify all APIs enforce authentication (OAuth 2.0, API keys) and authorization with least privilege	Review API Gateway authentication configuration; inspect OAuth 2.0/OIDC implementation; verify scope-based authorization; check for unauthenticated endpoints	API Gateway configuration export; OAuth scope documentation; API access logs	NIST SP 800-53 AC-3; OWASP API Security Top 10 (API1, API5); ISO 27001 A.8.5
API Rate Limiting and Throttling	Unrestricted API access enables denial-of-service attacks and credential stuffing at scale	Confirm API rate limiting and throttling are enforced on all public and partner APIs	Inspect API Gateway rate limit configuration; review throttling policies by consumer tier; test rate limiting effectiveness; verify 429 response handling	API Gateway throttling policy export; Rate limit test results; API access analytics	NIST SP 800-53 SC-5; OWASP API Security Top 10 (API4); CSA CCM AIS-05
Web Application Firewall (WAF) Protection	Applications without WAF protection are exposed to OWASP Top 10 attacks including SQL injection and XSS	Verify WAF is deployed and tuned for all public-facing cloud applications	Inspect WAF rule configuration (AWS WAF, Azure WAF, Cloud Armor); review OWASP core rule set activation; check WAF logging and alerting; inspect custom rule coverage	WAF rule configuration export; WAF block event logs; OWASP rule set audit	NIST SP 800-53 SI-3; PCI DSS Req. 6.4; OWASP Top 10; ISO 27001 A.8.29
API Inventory and Discovery	Shadow APIs not in the official inventory are unmonitored and unprotected	Confirm a complete API inventory exists and is reconciled with deployed APIs	Review API catalog completeness; inspect API discovery tool output; compare discovered APIs against approved inventory; verify decommissioned API removal	API inventory/catalog; API discovery scan report; Reconciliation report	OWASP API Security Top 10 (API9); NIST SP 800-53 CM-8; ISO 27001 A.5.9
Sensitive Data Exposure in API Responses	APIs returning excessive data expose PII, credentials, or business-sensitive information	Verify APIs return only the minimum data required and do not expose sensitive fields unnecessarily	Review API response schemas; conduct sample API calls and inspect responses for PII, secrets, or internal IDs; verify data masking in non-production API endpoints	API response schema review; Sample API response documentation; DLP scan of API outputs	OWASP API Security Top 10 (API3); GDPR Art. 25; NIST SP 800-53 SC-28
API Security Testing	APIs are deployed without security validation, exposing them to OWASP API vulnerabilities	Confirm API security testing is performed before production deployment and periodically thereafter	Review API security test scope; inspect DAST reports for APIs; verify OWASP API Top 10 coverage; check testing frequency against API change cadence	API security test reports; DAST reports with API coverage; Test schedule documentation	OWASP API Security Top 10; NIST SP 800-53 SA-11; ISO 27001 A.8.29
mTLS and Service-to-Service Authentication	Unverified service-to-service communication enables man-in-the-middle attacks within cloud environments	Verify mutual TLS (mTLS) is implemented for service-to-service communication in microservices architectures	Inspect service mesh mTLS configuration (Istio, Linkerd); verify certificate issuance and rotation; check for services bypassing mTLS; review certificate management	Service mesh mTLS configuration; Certificate inventory; mTLS enforcement report	NIST SP 800-53 SC-8; ISO 27001 A.8.24; CSA CCM NET-10
Application Secret and Configuration Management	Hardcoded secrets in application code or config files create persistent	Confirm applications retrieve secrets from centralized vaults rather than configuration files	Inspect application deployment configurations; check for secrets in environment variables; review Secrets Manager/Key Vault integration; scan recent	Application deployment config review; Secrets Manager integration audit;	NIST SP 800-53 IA-5; ISO 27001 A.8.24; CIS Benchmark;

	unauthorized access risks	or environment variables	deployments for hardcoded credentials	Secrets scan report	CSA CCM IAM-09
CORS Policy Configuration	Misconfigured CORS policies enable cross-origin attacks on cloud-hosted applications	Verify CORS policies are restrictively configured to allow only trusted origins	Inspect CORS configurations on API Gateways and web applications; check for wildcard (*) origins; review allowed methods and headers; test CORS enforcement	CORS configuration export; CORS test results; Web application CORS audit	OWASP Top 10; NIST SP 800-53 AC-4; ISO 27001 A.8.29
Input Validation and Output Encoding	Missing input validation and output encoding enable injection attacks against cloud applications	Confirm application input validation and output encoding controls are implemented and tested	Review application security design documentation; inspect SAST reports for injection findings; verify server-side validation (not client-side only); check output encoding practices	SAST injection finding reports; Application security design review; Code review evidence	OWASP Top 10 (A03, A07); NIST SP 800-53 SI-10; ISO 27001 A.8.28

12. Third-Party and Vendor Management

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Vendor Risk Assessment Program	Unassessed third-party cloud vendors introduce hidden security risks into the supply chain	Verify a formal vendor risk assessment process exists for all cloud service providers and integrations	Review vendor risk assessment procedures; inspect completed assessments for key vendors; verify risk tiers and assessment frequency; check for unapproved vendors in use	Vendor risk assessment reports; Vendor register; Risk tier classification	ISO 27001 A.5.19; NIST SP 800-53 SA-9; PCI DSS Req. 12.8; SOC 2 CC9.2
Cloud Provider SOC Report Review	Organizations relying on cloud providers without reviewing SOC reports lack assurance of inherited controls	Confirm SOC 2 Type II reports from key cloud providers are reviewed annually and findings noted	Request and review AWS, Azure, GCP SOC 2 reports; inspect user entity control considerations; verify complementary user entity controls (CUECs) are implemented; document review evidence	SOC 2 Type II reports; CUEC implementation evidence; Report review documentation	SOC 2 Trust Services Criteria; ISO 27001 A.5.19; PCI DSS Req. 12.8
Third-Party API and Integration Security	Third-party integrations with cloud data access create data exfiltration and credential exposure risks	Verify all third-party API integrations are reviewed for security and granted minimal access	Inspect OAuth application permissions; review API key scope for third-party tools; verify third-party access is logged; check for dormant integrations with excessive permissions	Third-party API permission audit; OAuth application review; Dormant integration report	ISO 27001 A.5.19; NIST SP 800-53 SA-9; OWASP API Security Top 10
Vendor Contract Security Clauses	Contracts without security provisions leave the organization without recourse when vendors cause breaches	Confirm all cloud vendor contracts include security, privacy, breach notification, and audit rights clauses	Review key vendor contracts; inspect data processing agreements (DPAs); verify breach notification requirements; check audit rights provisions; confirm data return/deletion on termination	Contract security clause review; DPA inventory; Audit rights documentation	GDPR Art. 28; ISO 27001 A.5.20; PCI DSS Req. 12.8
Vendor Access Management	Unmonitored vendor access to cloud environments enables unauthorized data access and configuration changes	Verify vendor access to cloud environments is time-limited, monitored, and revoked after engagement	Inspect vendor IAM accounts; verify just-in-time access provisioning; review session recording for vendor sessions; confirm access revocation after project completion	Vendor IAM account audit; PAM session logs for vendor accounts; Access revocation records	ISO 27001 A.6.6; NIST SP 800-53 AC-17; SOC 2 CC6.3
SaaS Security Assessment	Approved SaaS applications with cloud data access are often underassessed, creating data protection gaps	Confirm SaaS applications with access to sensitive data are assessed and approved before adoption	Review SaaS approval process; inspect SaaS inventory; verify security assessments for SaaS with data integration; check CSA STAR registry for SaaS providers	SaaS inventory; SaaS security assessment reports; CSA STAR attestations	ISO 27001 A.5.19; CSA CCM STA-01; NIST SP 800-53 SA-9
Vendor Incident Notification Requirements	Vendor breaches affecting cloud data go unreported, delaying	Verify vendor contracts require incident notification	Review contract breach notification clauses; confirm notification timelines meet regulatory requirements;	Contract notification clause review; Vendor incident	GDPR Art. 28(3); ISO 27001 A.6.8;

	organizational response	within defined timeframes	inspect notification tracking for prior vendor incidents	notification log; Regulatory timeline mapping	PCI DSS Req. 12.8
Fourth-Party Risk Management	Vendors' vendors (fourth parties) with cloud access create indirect supply chain risks	Confirm the organization has visibility into critical fourth-party dependencies of key cloud vendors	Review vendor questionnaire responses on subcontractor use; inspect AWS, Azure, GCP supply chain disclosures; verify critical fourth-party mapping	Vendor subcontractor disclosures; Fourth-party mapping documentation; Supply chain risk assessment	ISO 27001 A.5.19; NIST SP 800-53 SA-12; SOC 2 CC9.2
Vendor Offboarding Procedures	Improper vendor offboarding leaves vendor credentials and data access active after contract termination	Verify formal offboarding procedures ensure data return, access revocation, and credential rotation	Review vendor offboarding checklist; inspect access revocation records for terminated vendors; verify data return/destruction certificates; check for orphaned vendor accounts	Offboarding checklist; Access revocation logs; Data return/destruction certificates	ISO 27001 A.5.20; NIST SP 800-53 AC-2; SOC 2 CC6.2
Third-Party Penetration Testing Results Review	Vendor security assessment scores without reviewing penetration testing evidence provide false assurance	Confirm security assessments of critical vendors include penetration testing evidence review	Request pen test reports from critical vendors; inspect scope and recency; verify critical findings are remediated; check for NDA or report sharing agreements	Vendor pen test reports; Finding remediation tracking; Report sharing agreements	ISO 27001 A.8.8; PCI DSS Req. 12.8; SOC 2 CC4.1

13. Compliance and Regulatory Management

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Regulatory Obligation Mapping	Unmapped regulatory requirements result in compliance gaps and audit findings	Confirm all applicable regulations are mapped to specific cloud controls	Review compliance inventory; inspect control mapping matrix; verify coverage of applicable regulations (PCI, HIPAA, GDPR, SOX); check update frequency as regulations evolve	Compliance inventory; Control mapping matrix; Regulatory tracking log	NIST CSF GV.OC-03; ISO 27001 Clause 4.2; COBIT MEA03
PCI DSS Cloud Compliance Controls	Non-compliance with PCI DSS for cloud-hosted cardholder data environments triggers assessor findings and fines	Verify PCI DSS requirements are met for all cloud environments in scope for cardholder data	Identify CDE scope in cloud; inspect network segmentation between CDE and non-CDE; review PCI DSS control mapping; check QSA assessment documentation	PCI DSS SAQ or ROC; Network segmentation evidence; QSA assessment report	PCI DSS v4.0 Requirements 1-12; ISO 27001; CSA CCM
HIPAA Security Rule Controls in Cloud	HIPAA violations for cloud-hosted PHI result in significant civil monetary penalties	Confirm technical safeguards under the HIPAA Security Rule are implemented in cloud environments hosting PHI	Review Business Associate Agreements with cloud providers; inspect access controls for PHI; verify audit logging for PHI access; check encryption of PHI at rest and in transit	BAA documents; PHI access control configuration; Audit log samples; Encryption certificates	HIPAA Security Rule 45 CFR Part 164; HITECH; NIST SP 800-66
GDPR Data Protection Controls	GDPR violations for cloud-processed personal data of EU residents result in fines up to 4% of global revenue	Verify GDPR technical controls are implemented for personal data processed in cloud environments	Review DPAs with cloud providers; inspect data subject rights procedures; verify data residency controls; check breach notification procedures; review DPIA for high-risk processing	DPA inventory; DPIA documentation; Data subject rights procedure; Breach notification procedure	GDPR Arts. 25, 28, 32-34; ISO 27001 A.5.34; CSA CCM DSP-17
FedRAMP Authorization Management	Use of unauthorized cloud services for federal data violates FedRAMP requirements and federal contracts	For federal environments, verify cloud services in use have appropriate FedRAMP authorization	Review FedRAMP authorization status of cloud services; inspect continuous monitoring deliverables; verify POA&M items are tracked and remediated; check ATO documentation	FedRAMP authorization letters; Continuous monitoring reports; POA&M tracking	FedRAMP; NIST SP 800-53; FISMA
SOX IT General Controls for Cloud	Cloud-hosted financial applications without	Verify SOX ITGCs are implemented for	Inspect logical access controls for financial systems in cloud; review change management for	SOX ITGC control matrix; Access control evidence;	SOX Section 302 and 404;

	adequate ITGCs expose the organization to SOX audit findings	cloud environments hosting financial reporting systems	financial applications; verify audit trail completeness; check backup and recovery	Change management records; Audit trail samples	COBIT; COSO; ISO 27001
Data Retention and Legal Hold Procedures	Failure to retain required data or preserve legal hold subjects results in legal and regulatory sanctions	Confirm cloud data retention policies comply with legal minimums and legal hold procedures are operational	Review data retention policy; inspect retention configurations in S3, Azure Storage, GCS; verify legal hold procedures; test legal hold application on a sample data set	Data retention policy; Retention configuration export; Legal hold procedure; Legal hold test evidence	GDPR Art. 5(1)(e); ISO 27001 A.5.33; SOX; Federal Rules of Civil Procedure
Privacy by Design Implementation	Privacy requirements not built into cloud architectures result in costly rework and compliance failures	Verify privacy by design principles are applied in cloud application and data architecture	Review privacy impact assessments; inspect data minimization practices in cloud applications; verify consent management for data collection; check anonymization/pseudonymization implementations	DPIA reports; Privacy review records; Consent management configuration; Anonymization design documentation	GDPR Art. 25; ISO 27701; NIST Privacy Framework; CSA CCM DSP-02
Cloud Compliance Continuous Monitoring	Point-in-time compliance assessments fail to detect compliance drift between audit cycles	Confirm continuous compliance monitoring is implemented with automated evidence collection	Inspect CSPM compliance dashboards; review automated control testing configuration; verify continuous monitoring reporting cadence; check compliance drift alerts	CSPM compliance reports; Automated test results; Compliance trend reports	NIST CSF DE.CM; FedRAMP Continuous Monitoring; ISO 27001 Clause 9.1
Cross-Border Data Transfer Compliance	Unauthorized cross-border data transfers of personal data violate GDPR, APPI, and other privacy laws	Verify cross-border data transfer mechanisms are documented and compliant with applicable regulations	Review cross-border transfer mechanisms (SCCs, BCRs, adequacy decisions); inspect cloud region configurations for data residency; verify DPAs address transfer restrictions	SCCs/BCRs documentation; Data residency configuration; DPA transfer restriction clauses	GDPR Arts. 44-49; ISO 27001 A.5.33; CSA CCM DSP-17

14. Backup, Business Continuity, and Disaster Recovery

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
Cloud Backup Configuration and Coverage	Incomplete backup coverage means critical cloud data cannot be recovered after loss events	Verify backup policies cover all critical cloud workloads with defined RPO and RTO targets	Inspect backup policy scope; verify all critical systems are included; review RPO/RTO documentation; check backup job success rates; inspect backup coverage across regions	Backup policy; Backup job success reports; RPO/RTO documentation; Coverage audit	NIST SP 800-53 CP-9; ISO 27001 A.8.13; SOC 2 A1.2; PCI DSS Req. 9.4
Backup Restoration Testing	Untested backups frequently fail during actual recovery events when the organization needs them most	Confirm backup restoration tests are conducted at least quarterly with documented results	Review restoration test schedule; inspect test results documentation; verify full and partial restoration tests; check RTO achievement against documented targets	Restoration test reports; RTO achievement records; Test schedule	NIST SP 800-53 CP-4; ISO 27001 A.8.13; SOC 2 A1.3
Geographic Redundancy and Multi-Region Architecture	Single-region cloud deployments cannot recover from regional cloud provider outages	Verify critical cloud workloads use multi-region deployment or have documented multi-region failover capability	Inspect cloud architecture diagrams; review multi-region replication configuration; verify failover procedures; check DNS failover configuration	Architecture diagrams; Replication configuration; Failover procedure documentation	NIST SP 800-53 CP-7; ISO 27001 A.17.2; AWS Well-Architected Reliability Pillar
Business Continuity Plan (BCP) for Cloud	BCP that doesn't address cloud provider outages fails to address one of the highest-	Confirm the BCP explicitly addresses cloud provider outage scenarios and	Review BCP documentation; confirm cloud provider outage scenarios are included; inspect alternative processing	BCP document; Cloud outage scenario coverage; BCP test reports	ISO 22301; NIST SP 800-53 CP-2; FFIEC BCP; SOC 2 A1.2

	probability disruption scenarios	alternative processing	procedures; verify BCP is tested with cloud outage simulation		
RPO and RTO Target Validation	Undefined or untested RPO/RTO targets leave the organization without clear recovery expectations	Verify RPO and RTO targets are defined for all critical cloud systems and tested annually	Review BCP/DR documentation for RPO/RTO targets; compare targets against business requirements; inspect test results to confirm target achievement; check for gaps	RPO/RTO documentation; Business impact analysis; DR test results vs. targets	ISO 22301; NIST SP 800-53 CP-2; SOC 2 A1.2
Cloud Backup Security and Immutability	Ransomware attacks specifically target and encrypt or delete backups to prevent recovery	Confirm cloud backups are immutable and stored in an isolated, access-controlled location	Inspect S3 Object Lock configuration; review Azure Immutable Blob Storage settings; verify backup access is restricted to dedicated backup administrators; check for air-gapped backup copies	S3 Object Lock configuration; Immutable storage audit; Backup access control policy	NIST SP 800-53 CP-9; ISO 27001 A.8.13; CIS Benchmark
DR Runbook Currency and Completeness	Outdated or incomplete DR runbooks cause failures during high-pressure recovery events	Verify DR runbooks are current, tested, and accessible to recovery teams without dependency on production systems	Review DR runbook update dates; inspect runbook completeness for critical systems; confirm runbooks are stored offline or in a separate system; verify version control	DR runbooks; Last review dates; Runbook storage location audit; Version control records	NIST SP 800-53 CP-10; ISO 22301; SOC 2 A1.3
DR Tabletop Exercises and Full Failover Tests	Organizations that never test full failover discover critical gaps only during actual disasters	Confirm DR tabletop exercises are conducted annually and full failover tests are performed at defined intervals	Review tabletop and failover test reports; confirm cloud failover scenarios are covered; inspect action item tracking; verify leadership sign-off on test results	Tabletop exercise reports; Full failover test reports; Action item tracking log	NIST SP 800-53 CP-4; ISO 22301; SOC 2 A1.3; FFIEC BCP
Cloud Provider SLA Monitoring	Failure to monitor cloud provider SLAs results in undetected SLA breaches and missed credit claims	Verify cloud provider SLA availability commitments are monitored and breaches are tracked	Review cloud provider SLA documentation; inspect availability monitoring dashboards; check SLA breach notification procedures; review credit claim history	Cloud provider SLA documentation; Availability monitoring dashboards; SLA breach records	ISO 22301; SOC 2 A1.1; AWS/Azure/GCP SLA documents
Dependency Mapping for DR	Unknown system dependencies cause DR failures when dependent systems are not recovered in the correct sequence	Confirm cloud application dependency maps are maintained and inform DR recovery sequencing	Review dependency mapping documentation; verify maps are updated with infrastructure changes; check recovery sequencing against dependency maps; inspect CMDB for cloud dependencies	Dependency mapping documentation; CMDB export; Recovery sequencing procedure	NIST SP 800-53 CP-2; ISO 22301; COBIT DSS04

15. AI and Automation Security in Cloud

Control Area	Risk	Control Objective	Audit Test Steps	Evidence Required	Framework Reference
AI/ML Model Access Controls	Unauthorized access to AI/ML models and training data enables intellectual property theft and model poisoning	Verify AI/ML models and their associated data are access-controlled with least privilege	Inspect IAM permissions for ML services (SageMaker, Azure ML, Vertex AI); review model access policies; verify training data access controls; check for public exposure of model endpoints	ML service IAM configuration; Model access policy exports; Endpoint access audit	NIST AI RMF Govern 1; ISO/IEC 42001 A.6; EU AI Act Art. 13; NIST SP 800-53 AC-3
AI Model Supply Chain Security	Untrusted pre-trained models or datasets may contain backdoors or poisoned data	Confirm AI models sourced from external repositories are validated and tested before production use	Review model procurement procedures; inspect model validation testing documentation; verify model provenance tracking; check for adversarial testing prior to production deployment	Model procurement policy; Validation test reports; Provenance documentation	NIST AI RMF Govern 2; ISO/IEC 42001 A.7; ; NIST SP 800-53 SA-12

Automated Remediation Controls	Security automation without human oversight can cause outages or incorrect remediation actions	Verify automated cloud security remediation has appropriate guardrails and approval workflows for high-risk actions	Review automation runbook configurations; inspect approval workflows for high-risk remediation actions; verify rollback capabilities; check automation audit logs	Automation runbook configuration; Approval workflow logs; Rollback procedure documentation	NIST AI RMF Manage 1; ISO/IEC 42001 A.10; NIST SP 800-53 SI-7
AI Training Data Protection	Exposure of sensitive training data violates privacy regulations and enables data poisoning	Confirm AI training datasets are classified, access-controlled, and protected per data classification requirements	Inspect training dataset storage controls; verify access logging for training data; check for PII in training data; review data anonymization for sensitive training sets	Training data access control configuration; PII scan of training datasets; Data anonymization records	GDPR Art. 25; ISO/IEC 42001 A.8; NIST AI RMF Map 1; NIST SP 800-53 SC-28
AI Security and Bias Testing	Biased or adversarially vulnerable AI systems make incorrect security decisions leading to breaches or discrimination	Verify AI systems used for security decisions are tested for bias, adversarial robustness, and accuracy	Review AI model evaluation reports; inspect adversarial testing procedures; verify bias assessment documentation; check fairness metrics for decision models	AI model evaluation reports; Adversarial test results; Bias assessment documentation	NIST AI RMF Measure 1; ISO/IEC 42001 A.9; EU AI Act Art. 9; NIST SP 800-53 SA-11
LLM and Generative AI Security Controls	Generative AI systems processing sensitive data may leak information or be manipulated via prompt injection	Confirm LLM deployments in cloud have guardrails against prompt injection, data leakage, and jailbreaking	Inspect LLM deployment configuration; review input/output filtering controls; verify data isolation for each tenant in shared LLM deployments; check for prompt injection testing	LLM security configuration; Input/output filtering policy; Prompt injection test results	OWASP LLM Top 10; NIST AI RMF; ISO/IEC 42001; EU AI Act
RPA and Automation Security	RPA bots with excessive permissions can be used to exfiltrate data or perform unauthorized transactions	Verify RPA and automation bots follow least privilege and their activities are monitored	Inspect RPA bot IAM permissions; review activity logs for automation accounts; verify bot credential management; check for approval workflows on high-risk automated actions	RPA bot permission audit; Automation activity logs; Credential management documentation	NIST SP 800-53 AC-6; ISO 27001 A.8.2; CSA CCM IAM-09
AI Incident Response Procedures	AI-related incidents (model failures, adversarial attacks, data poisoning) are not covered in standard IR procedures	Confirm the incident response plan includes AI-specific scenarios and escalation procedures	Review IR plan for AI incident coverage; inspect AI incident history; verify AI-specific escalation paths; check for model rollback procedures	IR plan AI section; AI incident register; Model rollback procedure documentation	NIST AI RMF Manage 4; ISO/IEC 42001 A.10; NIST SP 800-61
AI Governance and Accountability Framework	Absent AI governance allows deployment of high-risk AI systems without oversight or accountability	Verify an AI governance framework assigns accountability for AI systems and requires risk assessments before deployment	Review AI governance policy; inspect AI system risk assessment process; verify board-level AI risk oversight; check AI register for all systems in use	AI governance policy; AI risk assessment reports; AI system register; Board reporting evidence	NIST AI RMF Govern 1-6; ISO/IEC 42001 Clause 6; EU AI Act Arts. 9, 17; COBIT APO12
Cloud Infrastructure Automation Security (Terraform, Ansible)	Insecure IaC automation scripts can expose credentials, create permissive configurations, or be tampered with	Confirm IaC automation tools are secured with code scanning, version control, and secret management	Inspect Terraform/Ansible repository access controls; review IaC scanning integration; verify secrets are not hardcoded in automation scripts; check state file security for Terraform	IaC repository access controls; Automation scan reports; State file security configuration	NIST SP 800-53 CM-3; ISO 27001 A.8.25; CIS Benchmark; CSA CCM CCC-07

8. Conclusion

Cloud security auditing is no longer a specialized niche within IT audit - it is a core competency required to provide credible assurance in any organization that operates in cloud environments. The controls, procedures, and framework references in this guide reflect current leading practices drawn from NIST, ISO/IEC, CIS, CSA CCM, and regulatory requirements applicable to financial services, healthcare, retail, and federal environments.

Effective cloud security audits require a combination of technical depth, regulatory knowledge, and professional judgment. Auditors who invest in cloud platform fluency, continuous learning on emerging threats, and collaborative relationships with cloud engineering and security teams will deliver the highest-value assurance to their organizations.

This guide should be reviewed and updated at least annually to reflect changes in cloud technology, emerging risks, and evolving regulatory requirements.



9. References

- NIST Cybersecurity Framework (CSF) 2.0 - https://www.nist.gov/cyberframework
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-190 - Application Container Security Guide
- NIST SP 800-61 Rev. 3 - Computer Security Incident Handling Guide
- NIST SP 800-207 - Zero Trust Architecture
- NIST AI Risk Management Framework (AI RMF 1.0)
- CSA Cloud Controls Matrix (CCM) v4.0 - https://cloudsecurityalliance.org
- ISO/IEC 27001:2022 - Information Security Management Systems
- ISO/IEC 27017:2015 - Cloud Services Security Controls
- ISO/IEC 27018:2019 - Protection of PII in Public Clouds
- ISO/IEC 42001:2023 - AI Management Systems
- CIS Benchmarks for AWS, Azure, GCP, Docker, and Kubernetes - https://www.cisecurity.org
- COBIT 2019 - ISACA IT Governance Framework
- SOC 2 Trust Services Criteria - AICPA
- PCI DSS v4.0 - PCI Security Standards Council
- HIPAA Security Rule - 45 CFR Part 164
- GDPR - Regulation (EU) 2016/679
- FedRAMP Program - https://www.fedramp.gov
- AWS Well-Architected Framework - https://aws.amazon.com/architecture/well-architected
- Microsoft Azure Security Benchmark v3 - Microsoft
- Google Cloud Security Best Practices - https://cloud.google.com/security/best-practices
- OWASP API Security Top 10 - https://owasp.org/www-project-api-security
- NSA Kubernetes Hardening Guide - National Security Agency, 2022
- EU AI Act - Regulation (EU) 2024/1689
- NIST SP 800-66 - HIPAA Security Rule Implementation Guide