CLOUD AUDIT CHECKLIST



By: Dr. Nath Alagbe

Professional Cloud Security Audit Guide & Comprehensive Checklist

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

1. Introduction to Cloud Security Audit

Cloud security auditing is a critical process for evaluating the effectiveness of security controls within a cloud environment. As organizations increasingly migrate sensitive workloads to the cloud, the need for a structured audit methodology becomes paramount. This guide provides a comprehensive framework for IT Audit Managers and Cloud Security professionals to assess risks and verify compliance across ten essential domains.

2. What Cloud Security Audit Entails

A thorough cloud security audit entails a deep dive into the technical configurations, administrative policies, and operational procedures of both the Cloud Service Provider (CSP) and the customer. It focuses on the 'Shared Responsibility Model,' ensuring that all parties are fulfilling their security obligations to protect data and maintain system integrity.

3. Steps to Conducting a Cloud Security Audit

- 1. Define Audit Scope and Objectives: Determine which cloud services (IaaS, PaaS, SaaS) and business units are in scope.
- 2. Review the Shared Responsibility Model: Identify the specific security tasks owned by the CSP versus the customer.
- 3. Conduct a Cloud-Specific Risk Assessment: Evaluate threats such as misconfigurations, insecure APIs, and account hijacking.
- 4. Select Audit Frameworks: Align the audit with industry standards like CSA CCM, NIST 800-53, or ISO 27017.
- 5. Execute Control Testing: Perform technical inspections and interview stakeholders to verify control effectiveness.
- 6. Gather and Document Evidence: Collect screenshots, log exports, and policy documents as proof of compliance or gaps.
- 7. Report Findings and Remediation: Provide a detailed report with prioritized recommendations for closing security gaps.
- 8. Continuous Monitoring: Establish a process for ongoing oversight of cloud security posture.

4. Comprehensive Cloud Security Audit Checklist

This checklist is divided into 10 critical domains, each containing at least 10 control areas to ensure a thorough evaluation of the cloud environment.

1. Governance and Risk Management

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Cloud Security Policy	Lack of direction leading to inconsistent security practices.	Establish a formal cloud security policy approved by management.	1. Review the cloud security policy document. 2. Verify it is reviewed annually.	Approved Cloud Security Policy, meeting minutes.	CSA CCM GRC-01
Shared Responsibility Matrix	Ambiguity in security ownership leading to unmanaged risks.	Clearly define security responsibilities between the organization and CSP.	1. Inspect the shared responsibility matrix. 2. Verify stakeholders understand their roles.	Shared Responsibility Matrix, training records.	CSA CCM GRC-02
Cloud Risk Assessment	Unidentified cloud-specific threats.	Perform regular risk assessments for cloud environments.	1. Review the latest cloud risk assessment report. 2. Verify mitigation plans exist.	Risk Assessment Report, Risk Register.	NIST SP 800-53 RA-3
Compliance Monitoring	Non-compliance with regulatory requirements (GDPR, HIPAA).	Ensure cloud usage complies with relevant laws and regulations.	1. Review compliance reports. 2. Verify automated compliance scanning is active.	Compliance dashboard screenshots, audit reports.	CSA CCM GRC-03
Asset Inventory	Shadow IT and unmanaged cloud resources.	Maintain an accurate inventory of all cloud assets.	1. Compare asset inventory with actual cloud resources. 2. Check for unauthorized accounts.	Cloud Asset Inventory, discovery tool logs.	CIS Control 1
Security Awareness Training	Human error leading to security breaches.	Train employees on cloud-specific security risks.	1. Review training materials. 2. Verify completion rates for cloud security modules.	Training logs, completion certificates.	ISO 27001 A.7.2.2
Cloud Strategy Alignment	Cloud initiatives misaligned with business security goals.	Ensure cloud strategy is integrated with the enterprise security strategy.	1. Review strategic planning documents. 2. Interview IT leadership.	IT Strategy Document, Board reports.	CSA CCM GRC-04
Internal Audit Program	Undetected control failures over time.	Include cloud security in the internal audit schedule.	1. Review the internal audit plan. 2. Inspect previous cloud audit reports.	Internal Audit Plan, Audit Reports.	CSA CCM GRC-05
Policy Exception Management	Unauthorized or unmonitored security exceptions.	Formalize the process for requesting and approving security	1. Review the exception log. 2. Verify approvals and expiration dates.	Exception Log, Approval emails.	NIST SP 800-53 AC-1

		exceptions.			
Cloud Service Provider (CSP) Audit	Reliance on insecure CSP infrastructure.	Review CSP's third-party audit reports (SOC 2, ISO).	1. Obtain and review the CSP's latest SOC 2 Type II report. 2. Verify 'Complementary User Entity Controls' (CUECs) are addressed.	CSP SOC 2 Report, CUEC review document.	CSA CCM GRC-06

2. Identity and Access Management (IAM)

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Multi-Factor Authentication (MFA)	Credential theft leading to account takeover.	Enforce MFA for all cloud console and API access.	1. Check IAM settings for MFA enforcement. 2. Sample users to verify MFA is active.	IAM MFA Status Report.	CSA CCM IAM-02
Least Privilege Access	Excessive permissions leading to data misuse.	Grant users only the minimum access required for their role.	1. Review IAM policies for overly broad permissions (e.g., '*'). 2. Verify RBAC implementation.	IAM Policy JSON, RBAC Role definitions.	NIST SP 800-53 AC-6
Privileged Account Management	Abuse of administrative privileges.	Strictly control and monitor administrative accounts.	1. Identify all admin users. 2. Verify use of dedicated admin accounts (not personal).	Admin User List, Access logs.	CSA CCM IAM-01
Just-In-Time (JIT) Access	Permanent high-level access increasing attack surface.	Implement JIT access for sensitive administrative tasks.	1. Review PIM/PAM configuration. 2. Verify elevation logs.	PIM/PAM logs, elevation requests.	CSA CCM IAM-04
User Access Reviews	Stale access rights for transferred or terminated users.	Perform quarterly reviews of user access rights.	1. Review the latest access review report. 2. Verify revoked access for sampled users.	Access Review Sign-off, Revocation logs.	ISO 27001 A.9.2.5
API Key Management	Hardcoded or leaked API keys.	Securely store and rotate API keys regularly.	1. Check API key age. 2. Verify keys are not in source code.	API Key Metadata, Code scan results.	CSA CCM IAM-06
Service Account Security	Compromised service accounts with high privileges.	Limit service account permissions and monitor their activity.	1. Review service account roles. 2. Check for anomalous service account behavior.	Service Account Role list, CloudTrail logs.	CSA CCM IAM-09
Identity Federation (SSO)	Fragmented identity management across platforms.	Use SSO for centralized identity and access control.	1. Verify integration with corporate IdP. 2. Check for local accounts bypassing SSO.	SSO Config, Local user list.	CSA CCM IAM-08

Root Account Protection	Total environment compromise via root account.	Secure the root account with MFA and avoid daily use.	1. Verify root MFA. 2. Confirm no active API keys for root.	Root account security report.	CIS Benchmark 1.1
Credential Complexity & Rotation	Weak passwords vulnerable to brute force.	Enforce strong password policies and regular rotation.	1. Review IAM password policy settings. 2. Verify rotation requirements.	IAM Password Policy screenshot.	NIST SP 800-53 IA-5

3. Network Security

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Security Group / Firewall Rules	Unrestricted access to internal resources.	Implement 'Deny All' by default and allow only necessary traffic.	1. Review inbound/outbound rules. 2. Check for 0.0.0.0/0 on sensitive ports.	Security Group Rules, Firewall logs.	CSA CCM IVS-06
VPC Segmentation	Lateral movement within the cloud network.	Isolate workloads using subnets and VPCs.	1. Review VPC architecture. 2. Verify routing tables and peering.	Network Diagrams, Routing config.	ISO 27017
Web Application Firewall (WAF)	Exploitation of web vulnerabilities (SQLi, XSS).	Protect public-facing apps with a WAF.	1. Verify WAF association with Load Balancers. 2. Review WAF rules.	WAF Config, Blocked request logs.	CSA CCM IVS-08
DDoS Protection	Service outages due to volumetric attacks.	Enable DDoS mitigation services.	1. Verify DDoS protection status (e.g., AWS Shield). 2. Review incident history.	DDoS service subscription.	CSA CCM IVS-03
Intrusion Detection (IDS/IPS)	Undetected malicious activity within the network.	Monitor network traffic for suspicious patterns.	1. Verify IDS/IPS deployment. 2. Review threat findings.	IDS Config, Threat reports.	CSA CCM IVS-07
Private Connectivity	Traffic exposure to the public internet.	Use Private Links/Endpoints for internal service communication.	1. Check for VPC Endpoints. 2. Verify traffic stays within CSP network.	Endpoint Config, Flow logs.	CSA CCM IVS-04
Network Flow Logging	Lack of visibility into network traffic.	Enable VPC Flow Logs for all active subnets.	1. Verify Flow Logs are active. 2. Check log destination.	Flow Log Config, Sample logs.	CSA CCM IVS-01
VPN / Direct Connect Security	Insecure hybrid cloud connections.	Encrypt and monitor connections between on-prem and cloud.	1. Review VPN tunnel status. 2. Verify encryption protocols.	VPN Config, Connection logs.	NIST SP 800-53 SC-8
Load Balancer Security	Insecure SSL/TLS configurations.	Use secure listeners and modern cipher suites.	1. Review LB listener policies. 2. Check for outdated TLS versions.	LB Config, SSL scan results.	CSA CCM IVS-02
Egress	Malware	Restrict outbound	1. Review outbound	Egress rules, Proxy	CSA CCM IVS-

Filtering	communicating with C2 servers.	traffic to known good destinations.	security group rules. 2. Verify proxy filtering.	logs.	05

4. Data Security and Encryption

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Encryption at Rest	Data exposure if storage is compromised.	Encrypt all sensitive data stored in the cloud.	1. Inspect S3/EBS/RDS encryption settings. 2. Verify use of KMS.	Resource Config reports, KMS key policy.	CSA CCM DSI-01
Encryption in Transit	Data interception during transmission.	Enforce TLS 1.2+ for all data movement.	1. Check LB listener settings. 2. Verify API endpoints require HTTPS.	SSL/TLS certificate config.	CSA CCM DSI-02
Key Management (KMS)	Unauthorized access to encryption keys.	Implement strict access control and rotation for keys.	1. Review KMS key policies. 2. Verify automatic rotation.	KMS Key Policy, Rotation logs.	NIST SP 800-53 SC-12
Data Classification	Inadequate protection for sensitive data.	Identify and label data based on sensitivity.	1. Review data classification policy. 2. Check for resource tags.	Classification Policy, Resource tags.	CSA CCM DSI-03
Data Loss Prevention (DLP)	Exfiltration of sensitive data.	Monitor and prevent unauthorized data transfers.	1. Verify DLP tool configuration. 2. Review DLP alerts.	DLP Config, Alert logs.	CSA CCM DSI-04
Public Bucket Prevention	Accidental public exposure of files.	Block public access to storage buckets by default.	1. Check 'Block Public Access' settings. 2. Scan for public buckets.	S3 Public Access settings.	CIS Benchmark 2.1.1
Database Backups	Data loss due to corruption or ransomware.	Ensure regular, encrypted backups of all databases.	1. Review backup schedules. 2. Verify backup encryption.	Backup logs, Encryption reports.	CSA CCM BCR-02
Data Retention & Disposal	Compliance violations or data lingering.	Enforce data retention policies and secure deletion.	1. Review lifecycle policies. 2. Verify secure wipe procedures.	Lifecycle Policy config.	ISO 27001 A.8.2.3
Snapshot Security	Unauthorized access to volume snapshots.	Restrict snapshot sharing to authorized accounts.	1. Check snapshot permissions. 2. Verify encryption.	Snapshot metadata.	CSA CCM DSI-05
Secrets Management	Hardcoded secrets in code.	Use a dedicated secrets manager for credentials.	1. Verify use of Secrets Manager. 2. Check for secrets in env vars.	Secrets Manager config.	CSA CCM EKM-03

5. Vulnerability and Patch Management

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Vulnerability Scanning	Undetected software vulnerabilities.	Perform regular vulnerability scans on cloud instances.	1. Review scan schedules. 2. Inspect latest scan reports.	Vulnerability Scan Reports.	CSA CCM TVM-01
Patch Management Policy	Exploitation of known vulnerabilities.	Establish a formal process for patching cloud resources.	1. Review the patch management policy. 2. Verify patching timelines.	Patch Management Policy.	NIST SP 800-53 SI-2
Automated Patching	Delayed patching due to manual processes.	Use automated tools for patch deployment.	1. Verify use of Systems Manager or similar tools. 2. Check patch compliance status.	Patch Compliance Dashboard.	CSA CCM TVM-02
Golden Image Management	Deployment of insecure or outdated OS images.	Use hardened and patched 'Golden Images' for deployments.	1. Review the image creation process. 2. Verify images are scanned before use.	Hardened Image List, Scan results.	CIS Control 5
Container Image Scanning	Vulnerabilities in containerized applications.	Scan container images in the registry for vulnerabilities.	1. Review ECR/ACR scan settings. 2. Check for high-severity findings.	Container Scan Reports.	CSA CCM TVM-03
Penetration Testing	Complex attack vectors missed by automated scans.	Conduct annual penetration tests of cloud environments.	1. Review the latest pen test report. 2. Verify remediation of findings.	Penetration Test Report.	PCI DSS 11.3
Third-Party Vulnerability Disclosure	Unaware of vulnerabilities in third-party components.	Monitor for vulnerabilities in third-party libraries (SCA).	1. Verify use of SCA tools (e.g., Snyk). 2. Review vulnerability alerts.	SCA Tool reports.	CSA CCM TVM-04
Zero-Day Response Plan	Inability to react quickly to new threats.	Develop a plan for responding to zero-day vulnerabilities.	1. Review the zero-day response procedure. 2. Check for recent incident examples.	Zero-Day Response Procedure.	NIST SP 800-53 SI-5
Vulnerability Remediation Timelines	Critical vulnerabilities remaining unpatched.	Enforce strict timelines for remediating vulnerabilities based on severity.	1. Review remediation logs. 2. Compare with policy timelines.	Remediation Tracking Log.	CSA CCM TVM-05
Configuration Drift Monitoring	Security posture degradation over time.	Monitor and alert on unauthorized configuration changes.	1. Verify AWS Config / Azure Policy rules. 2. Review drift alerts.	Configuration Drift Reports.	CSA CCM TVM-06

6. Logging and Monitoring

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Centralized Logging	Fragmented logs hindering incident investigation.	Aggregate logs from all cloud services into a	1. Verify log aggregation config. 2. Check log integrity	SIEM/Log Management config.	CSA CCM LOG-01

		central repository.	controls.		
Audit Log Enablement	Lack of visibility into administrative actions.	Enable audit logging for all cloud management activities.	1. Verify CloudTrail/Activity Logs are enabled. 2. Check for global coverage.	CloudTrail Config screenshot.	NIST SP 800-53 AU-2
Log Retention Policy	Loss of historical data for forensic analysis.	Retain logs for a period compliant with regulations.	1. Review log retention settings. 2. Verify compliance with policy.	Retention Policy settings.	ISO 27001 A.12.4.2
Real-Time Alerting	Delayed response to security incidents.	Configure alerts for critical security events.	1. Review alert rules. 2. Verify alerts are sent to the SOC.	Alert Configuration list.	CSA CCM LOG-02
Log Access Control	Tampering with audit logs by attackers.	Restrict access to logs to authorized personnel only.	1. Review IAM policies for log buckets. 2. Check for MFA on log access.	Log Bucket Policy.	CSA CCM LOG-03
Monitoring of Privileged Actions	Unnoticed abuse of admin rights.	Specifically monitor and alert on privileged account activity.	1. Review alerts for admin logins. 2. Check for unusual admin API calls.	Privileged Activity Alerts.	CSA CCM LOG-04
Network Traffic Monitoring	Undetected data exfiltration or C2 traffic.	Monitor network flow logs for anomalous patterns.	1. Review flow log analysis reports. 2. Verify automated threat detection.	Flow Log Analysis logs.	CSA CCM LOG-05
Application Logging	Inability to debug or investigate app-level attacks.	Ensure applications log security-relevant events.	1. Review application log samples. 2. Verify logging of failed logins.	Application Log samples.	OWASP Logging Guide
Log Integrity Protection	Attackers deleting logs to hide their tracks.	Use write-once-read-many (WORM) storage for logs.	1. Verify S3 Object Lock or similar config. 2. Check for log file validation.	Log Integrity Config.	NIST SP 800-53 AU-9
NTP Synchronization	Inaccurate timestamps complicating log correlation.	Synchronize clocks across all cloud resources.	1. Check NTP settings on instances. 2. Verify log timestamp consistency.	NTP Config screenshot.	ISO 27001 A.12.4.4

7. Incident Response and Business Continuity

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Incident Response Plan (IRP)	Chaotic response to security breaches.	Develop and maintain a cloud-specific incident response plan.	1. Review the IRP document. 2. Verify it includes cloud-specific scenarios.	Approved Incident Response Plan.	CSA CCM IRM-01
Incident Response Team	Lack of clear ownership during an incident.	Define roles and responsibilities for the IR team.	1. Review the IR team roster. 2. Verify contact	IR Team Roster.	NIST SP 800-61

			information is up to date.		
Tabletop Exercises	Ineffective response due to lack of practice.	Conduct regular tabletop exercises for cloud incidents.	1. Review the latest exercise report. 2. Verify lessons learned are documented.	Tabletop Exercise Report.	CSA CCM IRM-02
Automated Incident Response	Slow manual response to common threats.	Implement automated response playbooks for known threats.	1. Review Lambda/Logic App response scripts. 2. Verify trigger conditions.	Automation Script code.	CSA CCM IRM-03
Forensic Readiness	Inability to collect evidence in a volatile cloud.	Ensure capability to perform cloud forensics (e.g., disk snapshots).	1. Review forensic procedures. 2. Verify access to forensic tools.	Forensic Procedure document.	CSA CCM IRM-04
Business Continuity Plan (BCP)	Prolonged downtime during a disaster.	Develop a BCP that accounts for cloud service outages.	1. Review the BCP. 2. Verify it covers multi-region failover.	Business Continuity Plan.	CSA CCM BCR-01
Disaster Recovery (DR) Testing	Failure of DR mechanisms when needed.	Perform annual DR tests for critical cloud workloads.	1. Review the latest DR test results. 2. Verify RTO/RPO targets were met.	DR Test Report.	ISO 27001 A.17.1.3
Backup Integrity Checks	Backups being unusable during recovery.	Regularly test the restorability of cloud backups.	1. Review backup restore logs. 2. Perform a sample restore test.	Restore Test Log.	CSA CCM BCR-03
Communication Plan	Misinformation during a crisis.	Establish a plan for communicating with stakeholders during an incident.	1. Review the communication plan. 2. Verify contact lists for regulators.	Communication Plan document.	NIST SP 800-53 CP-2
Post-Incident Review	Repeating the same mistakes in future incidents.	Conduct a 'Lessons Learned' session after every major incident.	1. Review recent post-incident reports. 2. Verify remediation of root causes.	Post-Incident Report.	CSA CCM IRM-05

8. Application and DevSecOps Security

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Secure SDLC Policy	Security being an afterthought in development.	Integrate security into every phase of the software development lifecycle.	1. Review the SDLC policy. 2. Verify security gates in the pipeline.	Secure SDLC Policy.	CSA CCM AIS-01
Static Analysis (SAST)	Vulnerabilities in source code.	Perform automated SAST on all code commits.	1. Verify SAST tool integration in CI/CD. 2. Review scan findings.	SAST Tool reports.	CSA CCM AIS-02

Dynamic Analysis (DAST)	Runtime vulnerabilities in web applications.	Perform DAST on applications in staging/production.	1. Verify DAST tool configuration. 2. Review latest scan results.	DAST Scan Reports.	OWASP ASVS
Software Composition Analysis (SCA)	Vulnerable open-source libraries.	Scan for vulnerabilities in third-party dependencies.	1. Verify SCA tool usage. 2. Check for outdated libraries.	SCA Inventory report.	CSA CCM AIS-03
Infrastructure as Code (IaC) Scanning	Misconfigured infrastructure deployed via code.	Scan IaC templates (Terraform, CloudFormation) for security issues.	1. Verify IaC scanning in the pipeline. 2. Review policy violations.	IaC Scan logs.	CSA CCM AIS-04
Secrets in Code Prevention	Credentials leaked in git repositories.	Use pre-commit hooks to prevent secrets from being pushed to code.	1. Verify use of tools like 'git-secrets'. 2. Check repository for leaked keys.	Repository scan results.	NIST SP 800-53 SA-11
Container Security	Compromised container runtimes.	Implement runtime security for containers (e.g., Falco).	1. Review container security config. 2. Check for unauthorized container activity.	Container Security logs.	CSA CCM AIS-05
API Security	Insecure APIs exposing sensitive data.	Implement authentication, authorization, and rate limiting for APIs.	1. Review API Gateway config. 2. Verify use of OAuth/JWT.	API Gateway settings.	OWASP API Security Top 10
Environment Isolation	Development errors affecting production data.	Strictly isolate Dev, Staging, and Production environments.	1. Review network and IAM isolation. 2. Verify no production data in Dev.	Environment Architecture diagram.	ISO 27001 A.12.1.4
Deployment Authorization	Unauthorized changes to production.	Require multi-party approval for production deployments.	1. Review CI/CD approval workflows. 2. Verify audit trail for deployments.	Deployment Approval logs.	CSA CCM AIS-06

9. Third-Party and Supply Chain Risk

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Vendor Risk Assessment	Security weaknesses in third-party services.	Assess the security posture of all cloud vendors before onboarding.	1. Review vendor assessment questionnaires. 2. Verify risk scoring.	Vendor Assessment Reports.	CSA CCM STA-01
Contractual Security Requirements	Lack of legal recourse for security failures.	Include security and privacy clauses in vendor contracts.	1. Review sample vendor contracts. 2. Verify 'Right to Audit' clauses.	Vendor Contracts (Security Annex).	ISO 27001 A.15.1.2
Third-Party Access Control	Vendors having excessive access to cloud data.	Limit and monitor vendor access to the	1. Review vendor IAM roles. 2. Verify use of	Vendor Access logs.	CSA CCM STA-02

		cloud environment.	temporary access.		
Supply Chain Security	Compromised software updates or components.	Verify the integrity of third-party software and updates.	1. Review software procurement process. 2. Check for code signing.	Procurement Policy.	NIST SP 800-161
Vendor Compliance Monitoring	Vendor security posture declining over time.	Regularly review vendor SOC 2 reports and certifications.	1. Review the schedule for vendor report reviews. 2. Inspect latest review notes.	Vendor Review Log.	CSA CCM STA-03
Data Portability & Exit Strategy	Vendor lock-in or data loss during offboarding.	Develop an exit strategy for critical cloud vendors.	1. Review the exit plan. 2. Verify data export capabilities.	Exit Strategy document.	CSA CCM STA-04
Fourth-Party Risk Management	Risks from your vendor's vendors.	Understand and assess the risks of sub-processors.	1. Review vendor's sub-processor list. 2. Verify vendor's oversight of sub-processors.	Sub-processor list.	GDPR Article 28
Vendor Incident Notification	Unaware of breaches at the vendor level.	Ensure vendors are contractually obligated to report breaches promptly.	1. Review incident notification clauses. 2. Check for recent vendor notifications.	Contractual Notification clauses.	CSA CCM STA-05
SaaS Application Security	Insecure configurations in SaaS apps (e.g., M365, Salesforce).	Audit the security settings of critical SaaS applications.	1. Review SaaS security baselines. 2. Verify MFA and data sharing settings.	SaaS Security Config report.	CSA CCM STA-06
Managed Service Provider (MSP) Oversight	MSPs making unauthorized changes.	Monitor and audit the actions of MSPs with admin access.	1. Review MSP activity logs. 2. Verify adherence to change management.	MSP Activity Reports.	CSA CCM STA-07

10. Compliance and Legal

Control Area	Risk	Control Objective	Test Steps	Evidence Required	Framework
Data Sovereignty & Residency	Data stored in unauthorized jurisdictions.	Ensure data is stored in locations compliant with laws.	1. Review cloud region settings. 2. Verify data residency requirements.	Region Config screenshot.	GDPR / CSA CCM UEM-01
Privacy Impact Assessment (PIA)	Privacy risks to personal data.	Conduct PIAs for cloud projects involving personal data.	1. Review the latest PIA report. 2. Verify privacy controls.	PIA Report.	ISO 29134
Regulatory Mapping	Missing specific regulatory	Map cloud controls to	1. Review the control mapping matrix.	Regulatory Mapping Matrix.	CSA CCM GRC-07

	controls.	specific regulatory requirements (PCI, HIPAA).	2. Verify coverage of all requirements.		
E-Discovery Readiness	Inability to produce data for legal requests.	Ensure the ability to search and export cloud data for legal purposes.	1. Review e-discovery procedures. 2. Verify tool capabilities.	E-Discovery Procedure.	CSA CCM UEM-02
Service Level Agreement (SLA) Monitoring	CSP failing to meet availability commitments.	Monitor CSP performance against agreed SLAs.	1. Review monthly uptime reports. 2. Verify service credit claims.	SLA Monitoring Reports.	CSA CCM UEM-03
Records Retention Policy	Illegal deletion or excessive storage of records.	Enforce records retention in accordance with legal requirements.	1. Review the records retention schedule. 2. Verify automated deletion.	Retention Schedule.	NIST SP 800-53 MP-6
Data Privacy Officer (DPO) Oversight	Lack of independent privacy oversight.	Involve the DPO in cloud security and privacy decisions.	1. Review DPO sign-off on cloud projects. 2. Interview the DPO.	DPO Approval records.	GDPR Article 37
Legal Review of Cloud Contracts	Unfavorable legal terms in cloud agreements.	Ensure legal counsel reviews all cloud service agreements.	1. Review legal sign-off for cloud contracts. 2. Check for liability limits.	Legal Review notes.	CSA CCM UEM-04
Cross-Border Data Transfer	Illegal transfer of data across borders.	Implement legal mechanisms for cross-border data transfers (e.g., SCCs).	1. Review data transfer agreements. 2. Verify use of Standard Contractual Clauses.	Data Transfer Agreements.	GDPR Article 46
Audit Log Admissibility	Logs being inadmissible in court.	Ensure audit logs are collected and stored in a legally defensible manner.	1. Review log chain-of-custody procedures. 2. Verify log integrity.	Chain-of-Custody document.	ISO 27037

Follow me on:

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

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

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