DIGIT ASSURANCE

www.digitassurance.com

Digit Assurance's SOC 2 Checklist

Digit Assurance's SOC 2 Checklist

Control Area	Control Objectives / Criteria	Example Controls	Example Evidence Required	Compliant or non-compliant
Governance, Risk & Compliance				
Information Security Program	Establish, approve, and maintain an information security program that aligns with business objectives.	- Formal ISMS or Security Framework (ISO 27001, NIST, etc.)- Annual program review by management- Designation of security officer or committee	- Information Security Policy- Security Governance Charter- Org chart with roles and responsibilities- Management meeting minutes	☐ **YES** ☐ **NO**
Risk Management	Identify, assess, and treat information security risks	- Risk assessment methodology defined- Periodic risk assessments conducted- Risk register maintained and reviewed	- Risk Assessment Report- Risk Register with mitigation plans- Risk acceptance forms	☐ **YES** ☐ **NO**
Policy Framework	Maintain approved and communicated security policies.	- Policies reviewed annually- Employee acknowledgment of policies	- Policy approval logs- Training or acknowledgement records	☐ **YES** ☐ **NO**
Compliance Monitoring	Comply with legal, regulatory, and contractual requirements	- Compliance calendar maintained- Regular compliance checks	- Compliance reports- Legal/regulatory mapping matrix	☐ **YES** ☐ **NO**

Access Control & Identity Management				
User Provisioning / De-provisioning	Ensure timely granting and removal of access rights.	- HR and IT integration for access lifecycle- Access reviews post-termination	- Access Request Forms- Termination Offboarding Logs- System access review reports	☐ **YES** ☐ **NO**
Role-Based Access Control	Enforce least privilege and segregation of duties.	- Defined roles with privilege mapping- Periodic entitlement review	- Role matrix- Access control policy- Review logs and approvals	☐ **YES** ☐ **NO**
Authentication Controls	Implement strong authentication mechanisms.	- MFA for remote and admin users- Password complexity enforced	- MFA configuration screenshots- AD password policy export	☐ **YES** ☐ **NO**
Access Reviews	Perform periodic user access reviews.	- Quarterly access reviews by system owners	- Review results with sign-off- Corrective action records	☐ **YES** ☐ **NO**
System & Network Security				
Network Segmentation & Perimeter Defense	Protect systems from unauthorized access.	- Firewalls, IDS/IPS in place- Network segmentation for sensitive systems	- Network diagram- Firewall configuration export- IDS/IPS monitoring reports	☐ **YES** ☐ **NO**
Patch & Vulnerability Management	Identify and remediate vulnerabilities.	- Automated patch deployment- Monthly vulnerability scans	- Patch deployment logs- Vulnerability scan reports with remediation status	☐ **YES** ☐ **NO**
Endpoint Security	Protect endpoints from malware and unauthorized software.	- Antivirus centrally managed- Device encryption enforced	- AV compliance report- Encryption enforcement proof	☐ **YES** ☐ **NO**

Secure Configuration Management	Harden system configurations and review periodically.	- Baseline configurations approved- CIS benchmarks applied	- Configuration checklists- Hardening baseline documents	☐ YES ☐ NO
Change Management				
Change Authorization	Ensure all changes are approved before implementation.	- Use of change request tickets- CAB approvals	- Change request forms- CAB meeting notes	☐ YES ☐ NO
Testing & Validation	Verify and test changes before deployment.	- Test environment segregated- Test results reviewed and approved	- Test results and approvals- Deployment sign-off	☐ YES ☐ NO
Emergency Changes	Document and review emergency changes.	- Emergency change policy- post-implementation review	- Emergency change log- Review meeting records	☐ YES ☐ NO
Version Control	Track code and system versions.	- Source control system (Git, SVN) used- Tagging and rollback mechanism	- Version control screenshots- Commit logs	☐ YES ☐ NO
Incident Management				
Incident Response Policy	Define, communicate, and test incident response process.	- IR policy approved and shared- IR team roles defined	- Incident Response Policy document- IR training records	☐ YES ☐ NO
Incident Detection & Logging	Detect and record security incidents.	- SIEM solution or log monitoring- 24×7 alerting	- SIEM alerts and reports- Incident tickets	☐ YES ☐ NO
Response & Escalation	Escalate incidents per predefined severity.	- Escalation matrix defined- Regular IR drills	- Escalation flowchart- Drill test results	☐ YES ☐ NO

Post-Incident Review	Perform root-cause analysis and lessons learned.	- RCA template used- Improvement actions tracked	- Post-incident reports- RCA documentation	☐ YES ☐ NO
Vendor & Third-Party Management				
Vendor Risk Assessment	Evaluate vendors before onboarding.	- Vendor due-diligence checklist- Security questionnaire	- Completed risk assessments- Vendor approval logs	☐ YES ☐ NO
Contractual Controls	Include data protection clauses in contracts.	- Contracts reviewed by legal- SOC 2 or ISO reports obtained	- Signed agreements- Third-party audit reports	☐ YES ☐ NO
Ongoing Monitoring	Periodically review vendor performance and compliance.	- Annual reassessment process- SLA monitoring	- Vendor review meeting minutes- SLA compliance report	☐ YES ☐ NO
Business Continuity & Disaster Recovery				
BCP & DR Policy	Document and maintain continuity plans.	- Approved BCP and DRP- Regular updates	- BCP/DR Policy documents- Review signoffs	☐ YES ☐ NO
DR Testing	Perform regular, tested backups.	- Daily automated backups- Off-site replication	- Backup logs- Restore test results	☐ YES ☐ NO
DR Testing	Conduct annual DR simulation and validate recovery metrics.	- Full or partial DR tests- Lessons learned documented	- DR test reports- Corrective action tracker	☐ YES ☐ NO
System Operations & Monitoring				
Monitoring & Logging	Monitor systems for anomalies and maintain logs.	- Centralized logging- SIEM alerts	- Monitoring dashboard- Log retention policy	☐ YES ☐ NO

Capacity & Performance Management	Ensure systems perform as intended.	- Capacity thresholds defined- Auto-scaling configurations	- Performance reports- Capacity planning documents	☐ **YES** ☐ **NO**
Job Scheduling & Maintenance	Automate and monitor system tasks.	- Scheduled maintenance windows- System maintenance logs	- Maintenance schedule- Task execution logs	☐ **YES** ☐ **NO**
Data Protection & Encryption				
Data Classification	Identify and classify sensitive data.	Data classification matrix- Labelling controls	- Classification policy- Data inventory	☐ **YES** ☐ **NO**
Encryption (At Rest & In Transit)	Ensure encryption for sensitive data.	- TLS 1.2 + for data in transit- AES-256 for data at rest	- Encryption configs- Certificates and key management logs	☐ **YES** ☐ **NO**
Key Management	Secure key generation, storage, rotation, and destruction.	- Key rotation schedule- Access limited to custodians	- KMS policy- Key rotation logs	☐ **YES** ☐ **NO**
Data Disposal	Secure deletion of retired media or data.	- Data sanitization standards applied	- Disposal certificates- Sanitization logs	☐ **YES** ☐ **NO**