

IT Compliance Checklist For Small Businesses

Identify Your Applicable Compliance Requirements

- ☐ Identify sensitive and regulated data your business handles.
- ☐ Determine applicable regulatory, industry, and contractual requirements.
- ☐ Review customer and vendor contracts for compliance obligations.
- ☐ Map requirements to relevant systems, applications, data, and controls.
- ☐ Maintain a centralized register of requirements and responsible controls.
- ☐ Review regulatory and contractual changes regularly.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



Document Your Compliance Policies and Procedures

- ☐ Create written policies for applicable compliance requirements.
- ☐ Define rules for data handling, authentication, remote access, and endpoint security.
- ☐ Assign an owner to maintain and review each policy.
- ☐ Track revisions, approval dates, authors, and sign-offs.
- ☐ Review policies annually and after significant operational changes.
- ☐ Distribute policy updates and record employee acknowledgment.
- ☐ Retain policy versions and approval records centrally.

Enforce Access Control and Identity Management

- ☐ Assign system permissions according to employee roles.
- ☐ Apply least privilege to restrict unnecessary access.
- ☐ Enable MFA for cloud, remote, and sensitive systems.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



- ☐ Use RBAC to standardize permissions by job function.
- ☐ Disable inactive accounts and revoke access after departure.
- ☐ Review user accounts and permissions quarterly.
- ☐ Retain account and permission changes for compliance audits.

Secure Sensitive Data in Transit and at Rest

- ☐ Encrypt sensitive data across servers, databases, cloud platforms, and devices.
- ☐ Protect data in transit with secure encryption protocols.
- ☐ Identify and document where regulated data is stored.
- ☐ Classify data by sensitivity and compliance requirements.
- ☐ Define retention periods for different data types.
- ☐ Securely dispose of data after required retention periods.
- ☐ Record authorized data disposal as compliance evidence.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



Manage Endpoint Security and Patching

- ☐ Maintain a current inventory of hardware and software.
- ☐ Apply security patches to systems, applications, and network devices.
- ☐ Automate patch management where practical.
- ☐ Run regular vulnerability scans for missing patches and weaknesses.
- ☐ Monitor endpoints for suspicious activity and unauthorized software.
- ☐ Replace or isolate unsupported end-of-life systems.
- ☐ Record patches, vulnerabilities, and remediation actions.

Test Backup and Disaster Recovery Readiness

- ☐ Automate backups for critical systems, applications, and data.
- ☐ Follow the 3-2-1 approach for separate backup copies.
- ☐ Protect backups against unauthorized changes and ransomware.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



- ☐ Define RPO and RTO targets for critical systems.
- ☐ Document recovery procedures, responsibilities, and communication steps.
- ☐ Test restorations regularly to verify recovery.
- ☐ Record test results, issues, and corrective actions.

Maintain an Incident Response Plan

- ☐ Define procedures for detecting, containing, investigating, and recovering from incidents.
- ☐ Assign incident response, communication, and escalation roles.
- ☐ Set criteria for escalating serious security events.
- ☐ Document required breach notification procedures.
- ☐ Test the response plan through regular tabletop exercises.
- ☐ Test scenarios such as ransomware, data exposure, and compromised credentials.
- ☐ Update procedures based on gaps identified during exercises.
- ☐ Retain exercise reports and corrective action records.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



Conduct Vendor and Third-Party Risk Assessments

- ☐ Maintain an inventory of vendors with system or data access.
- ☐ Assess vendor security practices before onboarding.
- ☐ Review relevant SOC 2, ISO, or other compliance documentation.
- ☐ Include security and breach reporting requirements in contracts.
- ☐ Categorize vendors by access level and data sensitivity.
- ☐ Reassess high-risk vendors regularly.
- ☐ Retain vendor assessments, contract reviews, and compliance records.

Deliver and Document Employee Compliance Training

- ☐ Provide compliance and security training during onboarding.
- ☐ Repeat training as required by applicable compliance requirements.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



- ☐ Cover phishing, passwords, social engineering, data handling, and incident reporting.
- ☐ Use phishing simulations to test employee awareness.
- ☐ Track participation and training completion.
- ☐ Record completion dates, course details, and assessment results.
- ☐ Follow up on missed training requirements.
- ☐ Retain training records for compliance audits.

Conduct Continuous Auditing and Gap Assessments

- ☐ Conduct internal compliance audits regularly.
- ☐ Review logs, access records, patch histories, and configurations.
- ☐ Compare IT practices with policies and compliance requirements
- ☐ Record gaps, policy exceptions, and failed controls in a central location.
- ☐ Assign an owner and deadline to each issue.
- ☐ Track corrective actions through resolution.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667



- ☐ Retest controls to verify remediation.
- ☐ Retain audit, gap assessment, and remediation records.



www.cloudavize.com



8330 Lyndon B Johnson Fwy, Suite 510
Dallas, TX 75243



(469) 250-1667

