SOX ITGC Checklist for SaaS Companies (2025)

Use this 2025 checklist to evaluate key IT General Controls (ITGCs) for SOX compliance, tailored to SaaS companies. Great for audit prep and internal readiness.

Access Management Controls

[ ] Role-based access (RBAC) is implemented for financial systems
[ ] Access provisioning and deprovisioning are documented and approved
[ ] Periodic access reviews are conducted quarterly
[ ] Multi-Factor Authentication (MFA) is enforced for admin access
[ ] Single Sign-On (SSO) is implemented via a centralized identity provider

Change Management Controls

[ ] All code changes are approved through a formal workflow
[ ] Segregation of duties exists between developers and production deployers
[ ] All system changes are logged and traceable
[ ] Emergency changes are tracked, approved, and reviewed post-deployment

IT Operations Controls

[ ] Regular vulnerability scans are conducted and remediation is tracked
[ ] Logs are monitored with SIEM tools or manual reviews
[ ] Incident response plan is documented and tested regularly
[ ] Vendor risk assessments are performed for third-party financial systems

Backup & Recovery Controls

[ ] Regular data backups are scheduled and verified
[ ] Data is encrypted at rest and in transit
[ ] Disaster Recovery (DR) and Business Continuity (BCP) plans are tested annually
[ ] Backup data is securely stored with access restrictions