

SOX compliance checklist

What needs to be set up

- ☐ A system is in place that tracks all user logins and access attempts across computers, databases, and storage.
- ☐ All incoming data is automatically timestamped, stored offsite, and protected with encrypted checksums.
- ☐ Data access is fully logged, including who accessed it, when, and by what method.
- ☐ Automated workflows are set up to generate and send daily reports showing that internal controls are running.
- ☐ Scheduled reports are configured to summarize all critical system messages, alerts, and incidents.
- ☐ Real-time alerting is configured to analyze system messages, filter noise, and escalate verified security breaches.
- ☐ Role-based access is set up to give SOX auditors view-only permissions to reports and system logs.
- ☐ All security breaches are automatically logged, notifications are sent, and incident resolutions are documented in a central system.
- ☐ Automated integrity checks are scheduled to validate system performance and identify failures in logging or monitoring.

Outcome if implemented

- Data tampering is prevented
- Timelines are securely recorded
- Data access is traceable
- System status is verified daily
- Safeguard activity is documented
- Breaches are detected immediately
- Auditor access is enabled
- Breach logs are audit-ready
- Failures are detected and logged