SOX

SOX Compliance Checklist

*This checklist is provided for informational purposes only and does not constitute legal advice or a comprehensive SOX compliance solution.

gart.

🌐 gartsolutions.com

✉ info@gartsolutions.com

1. Financial Data Integrity

□ Data Validation: Implement systems to verify the accuracy of all financial data being reported.

□ Audit Trails: Ensure all transactions and financial activities are logged and traceable to provide an audit trail.

□ Access Control: Limit access to financial data to authorized personnel only. Implement Role-Based Access Control (RBAC) and multi-factor authentication (MFA) for critical systems.

2. Internal Control Over Financial Reporting (ICFR)

□ Section 302 Compliance: Ensure the CEO and CFO sign off on the accuracy and completeness of all financial reports.

□ Internal Control Evaluation: Regularly assess the effectiveness of internal controls and document any deficiencies.

□ Testing Controls: Implement an annual testing procedure to evaluate the effectiveness of internal controls over financial reporting.

□ Section 404 Compliance: Include a management report on the effectiveness of internal controls in annual reports.

□ Disclosure of Deficiencies: Disclose any significant deficiencies or fraud impacting financial reports in a timely manner.

SOX

3. Independent Audits

□ External Auditor Selection: Ensure that an independent external auditor is chosen to evaluate internal controls and financial disclosures.

□ Audit Planning: Establish an audit schedule to perform regular audits throughout the year.

□ Conflict of Interest: Confirm the independence of the external auditor to avoid conflicts of interest with other company audits.

□ Audit Reports: Ensure auditors provide a detailed report on the adequacy of internal controls over financial reporting.

4. IT Controls and Security

- □ IT General Controls (ITGC): Establish IT controls for access management, system changes, and data security, ensuring compliance with Section 404.
- □ Cybersecurity: Implement cybersecurity measures, including firewalls, encryption, and intrusion detection systems, to protect sensitive financial data.
- □ Real-Time Monitoring: Utilize real-time monitoring systems to detect unusual activities, data breaches, or unauthorized access to financial systems.
- □ Disaster Recovery: Develop a robust disaster recovery plan for financial data and systems. Regularly test backup and recovery procedures.
- □ Access Management: Implement role-based access controls to ensure that only authorized users can modify financial data.

5. Reporting and Documentation

- □ Document Internal Controls: Maintain detailed documentation of all internal controls related to financial reporting, including policies, procedures, and control matrices.
- □ Material Disclosures: Ensure timely and transparent disclosure of material changes in financial condition or operational status (Section 409).
- □ Management Attestations: Require management to certify that financial disclosures are accurate and internal controls are functioning correctly (Sections 302 and 906).
- □ SOX Audit Documentation: Maintain records of all financial transactions, control assessments, and audit results for auditors and regulators.

6. Risk Management

- □ Risk Assessments: Conduct periodic risk assessments to identify new or evolving risks that may impact financial reporting or internal controls.
- □ Fraud Detection and Prevention: Implement systems for detecting and addressing fraud attempts. Ensure employees have a clear understanding of how to report suspicious activities.
- □ Automated Controls: Where possible, automate control procedures (e.g., approval workflows, access controls) to reduce human error.

SOX

7. IT Change Management

- □ Change Approval Processes: Document all system changes related to financial data and controls, ensuring that no unauthorized changes occur.
- □ System Configuration Management: Use configuration management tools to maintain a consistent environment and track all changes to IT systems.
- □ Version Control: Ensure that all updates or patches to financial systems follow a clear version control process, with logs maintained for audit purposes.

8. Continuous Monitoring and Testing

□ Automated Monitoring Tools: Implement automated tools to continuously monitor internal controls, including network security, data integrity, and financial reporting systems.

□ Regular Control Reviews: Regularly review control effectiveness through internal audits, spot checks, and assessments of key financial processes.

□ Incident Response Plan: Develop an incident response plan for financial systems to quickly address security breaches, unauthorized access, or control failures.

9. Audit Readiness

□ Audit Trail Maintenance: Maintain a complete audit trail for all financial transactions and system changes, ensuring auditors have clear visibility into financial controls.

□ Pre-Audit Preparation: Regularly prepare for audits by reviewing internal controls, documenting processes, and testing system readiness for compliance.

□ Compliance Reporting: Automate the generation of compliance reports (e.g., access logs, system changes) to simplify audit reporting.

□ SOX Training: Provide regular SOX compliance training to all relevant employees, especially those handling financial data or IT systems related to financial reporting.

SOX

10. Cybersecurity Controls

□ Data Encryption: Ensure that all sensitive financial data is encrypted both in transit and at rest.

□ Incident Reporting: Implement a protocol for reporting security breaches or vulnerabilities that impact financial systems.

□ Vulnerability Assessments: Conduct regular vulnerability scans and penetration testing to identify and mitigate potential security risks.

□ IT Asset Management: Keep an up-to-date inventory of all IT assets, including hardware, software, and databases, used for financial reporting.

11. Fraud Prevention and Detection

□ Whistleblower Protections: Establish mechanisms for employees to report fraud or unethical practices without fear of retaliation (Section 806).

□ Segregation of Duties: Ensure that duties related to financial reporting are properly segregated to minimize fraud risk.

□ Fraud Detection Systems: Implement automated systems for detecting anomalies in financial transactions or unusual patterns that may indicate fraud.

SOX

12. Transparency and Accountability

□ Real-Time Reporting: Implement systems that support real-time reporting of material events affecting the company’s financial health, in compliance with Section 409.

□ Executive Accountability: Ensure senior executives (CEO, CFO) are aware of and adhere to their responsibilities under SOX. They must be able to certify the accuracy of financial reports.

□ SOX Certification: Ensure executive officers sign off on SOX certifications after reviewing the accuracy and completeness of financial reports.

SOX

13. Compliance Automation

□ Automation of Reporting: Automate the process of generating reports on access control, system changes, and data integrity for financial audits.

□ Audit Preparation Tools: Use audit tools to collect and analyze data from financial systems to streamline audit processes.

□ Compliance-as-Code: Use Infrastructure-as-Code (IaC) tools to enforce compliance policies in cloud environments, making it easier to maintain a compliant infrastructure.

14. Legal Compliance and Penalties

- □ PCAOB Audits: Prepare for Public Company Accounting Oversight Board (PCAOB) inspections, which ensure auditors follow strict guidelines.
- □ Criminal Penalties: Be aware of the legal ramifications of SOX non-compliance, including personal liability for executives and criminal penalties (Section 802).
- □ Fines and Reputational Damage: Implement preventive measures to avoid fines, penalties, and damage to the company's reputation due to SOX violations.

SOX

Simplify SOX Compliance with Gart Solutions

Meeting SOX compliance requirements can be streamlined with the right partner. At Gart Solutions, we focus on DevOps and cloud services to help your business maintain accurate financial reporting and secure internal controls.

Here's how we can assist you:

- Comprehensive Risk Assessment: We evaluate your IT systems and processes to ensure compliance with SOX's internal control requirements.
- Internal Control Implementation: Our team implements effective controls to safeguard financial data and ensure accurate reporting.
- Automated Compliance Monitoring: We deploy tools to continuously monitor and report on your compliance status, reducing the burden of manual oversight.
- Ongoing Training & Support: We provide continuous education and resources to keep your team up to date on SOX compliance requirements.

Secure your financial data with Gart Solutions. Contact us today!

gart.

gartsolutions.com

✉ info@gartsolutions.com