



ERP SOC2 & Internal Control Compliance Checklist 2026

Security & Access Management Controls

Verification of logical access controls, multi-factor authentication (MFA) enforcement, and periodic user entitlement reviews to prevent unauthorized ERP entry.

MFA Status for Administrative Accounts

- ☐ Fully Enabled
- ☐ Partially Enabled
- ☐ Not Enabled

Last User Access Review Date

Verified Access Control Mechanisms

- ☐ Role-Based Access Control (RBAC)
- ☐ Multi-Factor Authentication (MFA)
- ☐ IP Whitelisting
- ☐ Single Sign-On (SSO) Integration

Description of Identified Access Discrepancies

Write something...

User Access Audit Logs Evidence

 Upload File

Compliance Officer Validation

Data Encryption & Protection Protocols

Assessment of encryption standards for data at rest and data in transit within the ERP environment, ensuring compliance with SOC2 privacy requirements.

Encryption Standard for Data at Rest

- ☐ AES-256
- ☐ AES-128
- ☐ RSA (Higher bit rate)
- ☐ Other/Legacy

Encryption Protocols in Use for Data in Transit

- ☐ TLS 1.2
- ☐ TLS 1.3
- ☐ HTTPS/SSL
- ☐ IPsec VPN

Last Encryption Key Rotation Date

Enter date...

Encryption Key Management Procedure Summary

Write something...

Encryption Policy Document

 Upload File

Compliance Officer Verification

Change Management & Software Integrity

Audit of the lifecycle of system changes, including development, testing, and deployment protocols to ensure no unauthorized code enters production.

Change Request Date

Enter date...

Change Request ID

Write something...

Description of Proposed Change

Write something...

Change Impact Level

- ☐ Low
- ☐ Medium
- ☐ High
- ☐ Critical

Testing Performed

- ☐ Unit Testing
- ☐ Regression Testing
- ☐ User Acceptance Testing (UAT)
- ☐ Security/Vulnerability Scan

Upload Testing Evidence/Logs

 Upload File

Change Approval Signature

System Monitoring & Audit Logging

Validation of continuous monitoring capabilities, log retention policies, and the detection of suspicious activities or unauthorized administrative actions.

Monitored Log Categories

- ☐ User Authentication Logs
- ☐ System Configuration Changes
- ☐ Database Access Logs
- ☐ API Transaction Logs
- ☐ Privileged Account Activity
- ☐ Data Export/Extraction Logs

Last Log Review Date

Log Retention Period Compliance

- ☐ Compliant (Meets Policy)
- ☐ Non-Compliant (Gap Identified)
- ☐ Not Applicable

Identified Anomalies or Log Discrepancies

Write something...

Evidence of Log Review (Audit Trail Sample)

 Upload File

Compliance Officer Verification

Availability & Incident Response Readiness

Review of system uptime monitoring, redundancy configurations, and the effectiveness of incident notification procedures during a security event.

System Redundancy Status

- ☐ Fully Redundant (High Availability)
- ☐ Partial Redundancy (Warm Standby)
- ☐ No Redundancy (Single Point of Failure)

Last Disaster Recovery Drill Date

Enter date...

Incident Response Plan Summary

Write something...

Monitored Critical Services

- ☐ Database Availability
- ☐ API Connectivity
- ☐ User Authentication Services
- ☐ Data Backup Completion

Latest Backup Verification Report

 Upload File

Compliance Officer Approval

Physical & Environmental Security

Evaluation of the security of the physical data centers (or cloud provider's compliance) and environmental controls protecting the underlying ERP infrastructure.

Data Center Hosting Model

- ☐ On-Premise
- ☐ Cloud (SaaS/PaaS/IaaS)
- ☐ Hybrid

Physical Access Controls Verified

- ☐ Biometric Scanners
- ☐ CCTV Surveillance
- ☐ Security Guard Patrols
- ☐ Badge/Keycard Access
- ☐ Visitor Logs

Last Physical Security Audit Date

Enter date...

Data Center SOC2/ISO Certificate

 Upload File

Environmental Control Observations

Write something...

Compliance Officer Verification

Third-Party & Vendor Risk Management

Assessment of SOC2 reports from ERP hosting providers and management of third-party integrations that touch sensitive financial or personal data.

Critical Third-Party Service Providers

- ☐ Cloud Hosting Provider (IaaS/PaaS)
- ☐ ERP Managed Service Provider (MSP)
- ☐ External API/Integration Partners
- ☐ Payment Gateway Processors
- ☐ Data Backup & Recovery Services

Last SOC2 Report Review Date

Vendor Security Risk Rating

- ☐ Low Risk
- ☐ Medium Risk
- ☐ High Risk
- ☐ Critical Risk

Vendor SOC2 Type II Certificate

 Upload File

Identified Vendor Vulnerabilities & Mitigation Plan

Write something...

Compliance Officer Approval

Data Processing Integrity & Accuracy

Verification of automated controls that ensure transactions are processed completely, accurately, and in a timely manner without unauthorized alteration.

Data Validation Rule Verification Status

- ☐ Passed
- ☐ Failed
- ☐ In Progress
- ☐ Not Applicable

Description of Automated Reconciliation Controls

Write something...

Validated Data Fields

- ☐ Financial Transaction Totals
- ☐ Inventory Quantities
- ☐ Customer Master Data
- ☐ Vendor Payment Information
- ☐ Tax Calculation Logic

Last Reconciliation Audit Date

Enter date...

Evidence of Data Integrity Testing (e.g., Log/Report)

 Upload File

Number of Discrepancies Identified

Enter a number...

Compliance Officer Approval

Compliance Documentation & Audit Trail Maintenance

Ensuring all configuration changes, user access requests, and security incident logs are documented and retrievable for external auditors.

Last Audit Completion Date

Enter date...

Compliance Status

☐ Compliant

☐ Non-Compliant

☐ In Progress

☐ Not Applicable

Discrepancy Notes & Remediation Plan

Write something...

Evidence Upload (Audit Logs/Certificates)

 Upload File

Compliance Officer Sign-off

Documented Controls Verified

- ☐ Access Logs
- ☐ Change Request Records
- ☐ Incident Reports
- ☐ Training Records

Employee Awareness & Security Training

Validation of periodic security awareness training for ERP administrators and end-users regarding SOC2-related compliance responsibilities.

Date of Last Security Training Session

Training Completion Status

- ☐ Completed
- ☐ In Progress
- ☐ Not Started

Topics Covered in Current Training

- ☐ Phishing & Social Engineering
- ☐ Password Management & MFA
- ☐ Handling Sensitive ERP Data
- ☐ Incident Reporting Procedures

Training Attendance Log/Certificate

 Upload File

Compliance Officer Attestation

< Previous

> Next

✔ Finish

🔧 Generate Sample Report