ChecklistGuro

ERP Security & Compliance Checklist

Access Control & User Management

Verify user roles, permissions, and authentication protocols for ERP system access.

User Authentication Method

□ Password
□ Multi-Factor Authentication (MFA)
□ Biometrics
□ Single Sign-On (SSO)

Number of Active User Accounts

Enter a number...

Role-Based Access Control (RBAC) Implementation

□ Fully Implemented
□ Partially Implemented
□ Not Implemented

Last User Access Review Date

Enter date...

Privileged Accounts Verified?

□ Yes
□ No
□ Not Applicable

Description of User Access Review Process

Write something...

Data Encryption & Protection

Assess data encryption methods at rest and in transit within the ERP system.

Encryption Method at Rest

□ AES-256
□ Triple DES
□ Other (Specify in Long Text)

Specify Encryption Method (if 'Other' selected)

Write something...

Encryption Method in Transit

□ TLS 1.2 or higher
□ SSL 3.0
□ Other (Specify in Long Text)

Specify Encryption Method (if 'Other' selected)

Write something...

Encryption Key Rotation Frequency (Days)

Enter a number...

Key Management System

□ Integrated into ERP

□ Third-Party KMS

□ Manual

Details regarding access control to Encryption Keys

Write something...

Change Management & Audit Trails

Review change management processes and audit trail configurations for tracking system modifications.

Change Request ID

Write something...

Description of Change

Write something...

Change Request Submission Date

Enter date...

Impacted Modules (Number of)

Enter a number...

Change Type (e.g., Configuration, Code)

□ Configuration

□ Code

□ Data

□ Security

□ Other

Impacted Users/Departments

Planned Implementation Date

Enter date...

Change Approver Signature

Network Security & Firewalls

Evaluate network security measures, including firewalls and intrusion detection systems protecting the ERP environment.

Firewall Rule Count

Enter a number...

Firewall Vendor

□ Cisco
□ Fortinet
□ Palo Alto Networks
□ Check Point
□ Other

Firewall Configuration Documentation Review Notes

Write something...

Number of Network Segments (VLANs)

Enter a number...

Intrusion Detection/Prevention System (IDS/IPS) Status

□ Enabled and Configured
□ Enabled but Not Configured
□ Disabled

Last Firewall Rule Set Review Date

Enter date...

Data Backup & Disaster Recovery

Confirm data backup frequency, storage location, and disaster recovery procedures for ERP data.

Backup Frequency (e.g., Daily, Weekly)

Enter a number...

Backup Location(s) Description

Write something...

Retention Period (in days/months)

Enter a number...

Backup Type (Full, Incremental, Differential)

□ Full

□ Incremental

□ Differential

Last Successful Backup Date

Enter date...

Disaster Recovery Plan Documented?

Write something...

Last Disaster Recovery Drill Date

Enter date...

Recovery Time Objective (RTO) (in hours)

Enter a number...

Regulatory Compliance (e.g., GDPR, SOX)

Assess adherence to relevant industry regulations and compliance standards related to ERP data handling.

Which regulatory frameworks apply?

□ GDPR

□ SOX

□ CCPA

□ HIPAA

□ Other (Specify)

Describe how data subject rights (e.g., right to access, right to erasure) are handled within the ERP system.

Write something...

Number of data processing agreements (DPAs) in place with third-party vendors.

Enter a number...

Last review date of compliance documentation.

Enter date...

Which data residency requirements apply?

☐ EU

☐ US

☐ Canada

☐ Other (Specify)

Summarize how audit trails are used for regulatory compliance reporting.

Write something...

Vulnerability Scanning & Patch Management

Check for regular vulnerability scans and timely application of security patches for ERP software and related infrastructure.

Last Vulnerability Scan Date

Enter date...

Scan Frequency (Days)

Enter a number...

Summary of Last Scan Results

Write something...

Vulnerability Scan Tools Used

□ Nessus

□ Qualys

□ Rapid7 InsightVM

□ Other (Specify)

Last Patch Deployment Date

Enter date...

Patch Management Process Documentation Link

Write something...

Patch Deployment Method

□ Automated

□ Manual

Third-Party Integration Security

Review security protocols and assessments for third-party integrations with the ERP system.

Describe the purpose and criticality of each third-party integration.

Write something...

Integration Authentication Method

- □ API Key
- □ OAuth 2.0
- □ Username/Password
- □ Other

Number of Active Integrations

Enter a number...

Summarize security reviews/assessments performed on each integration (if applicable).

Write something...

Data Encryption in Transit (for each integration)

- □ TLS 1.2 or higher
- □ SSL 3.0
- □ Not Encrypted

Last Integration Security Review Date

Enter date...

Incident Response Plan

Verify the existence and effectiveness of an incident response plan for ERP security breaches.

Incident Definition & Scope

Write something...

Initial Incident Severity Level

- □ Low
- □ Medium
- □ High
- □ Critical

Estimated Impacted Records

Enter a number...

Date of Incident Detection

Enter date...

Time of Incident Detection

Enter time...

Detailed Description of the Incident

Write something...

Potentially Affected Systems

□ Finance

□ Manufacturing

□ Sales

□ Inventory

□ HR

Supporting Documentation (Screenshots, Logs)

Upload File

Security Awareness Training

Confirm ongoing security awareness training for employees accessing the ERP system.

Last Training Completion Date

Enter date...

Topics Covered in Training

- □ Phishing Awareness
- □ Password Security
- □ Data Privacy
- □ Malware Prevention
- □ Social Engineering
- □ Insider Threat

Training Frequency (Months)

Enter a number...

Training Delivery Method

- □ Online Modules
- □ Classroom Training
- □ Webinars

Summary of Recent Security Reminders

Write something...