



ERP Cybersecurity Incident Response Checklist 2026

Pre-Incident Preparation & Readiness

Steps to ensure the ERP environment, security tools, and response teams are prepared before an incident occurs.

Last Security Audit Date

Incident Response Team Lead

- ☐ IT Manager
- ☐ CISO
- ☐ Security Analyst
- ☐ DevOps Engineer

Verified Backup Locations

- ☐ On-Premise Server
- ☐ Cloud Storage (AWS/Azure/GCP)
- ☐ Off-site Immutable Backup
- ☐ Disaster Recovery Site

ERP Criticality Assessment Summary

Write something...

Incident Response Plan (PDF)

 Upload File

Compliance Officer Approval

Detection & Identification

Procedures for identifying potential security breaches, unauthorized access, or anomalous ERP system behavior.

Incident Detection Timestamp

Enter date...

Alert Source/Monitoring Tool

Write something...

Incident Severity Level

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

Affected ERP Modules

- ☐ Finance
- ☐ Human Resources
- ☐ Supply Chain
- ☐ Manufacturing
- ☐ Sales & CRM

Description of Detected Anomaly

Write something...

Initial Log Snippets or Screenshots

 Upload File

Containment Strategies

Immediate actions required to isolate affected ERP modules, databases, or user accounts to prevent lateral movement.

Primary Containment Action Taken

- ☐ Isolate Affected Server/Instance
- ☐ Disable Compromised User Accounts
- ☐ Disconnect Network Segment
- ☐ Revoke API Access Keys
- ☐ Shutdown ERP Application Services

Affected ERP Modules

- ☐ Finance/Accounting
- ☐ Human Capital Management (HCM)
- ☐ Supply Chain Management (SCM)
- ☐ Customer Relationship Management (CRM)
- ☐ Inventory/Warehouse Management

Containment Timestamp

Write something...

Detailed Containment Summary

Write something...

Containment Evidence Logs

 Upload File

Incident Response Lead Approval

Investigation & Forensic Analysis

Deep-dive procedures for analyzing ERP logs, audit trails, and database activity to determine the scope of the breach.

Incident Detection Timestamp

Affected ERP Module/Component

Identified Attack Vectors

- ☐ SQL Injection
- ☐ Unauthorized Privilege Escalation
- ☐ Compromised User Credentials
- ☐ API Vulnerability Exploitation
- ☐ Malware/Ransomware
- ☐ Insider Threat

Detailed Description of Anomalous Activity

Write something...

System Log Extracts & Audit Trail Evidence

 Upload File

Severity Level

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

Lead Forensic Investigator Signature

Eradication & Remediation

Steps to remove the root cause of the threat, such as patching vulnerabilities, removing malware, or revoking compromised credentials.

Remediation Actions Completed

- ☐ Malware/Virus Removal
- ☐ Compromised Account Deactivation
- ☐ Security Patch Deployment
- ☐ Vulnerability Closure
- ☐ Configuration Reset
- ☐ Unauthorized API Key Revocation

Root Cause Identified

Write something...

Detailed Remediation Summary

Write something...

Remediation Completion Date

Enter date...

Evidence of Patching/Remediation

 Upload File

Security Officer Approval

Recovery & System Restoration

Protocols for safely restoring ERP services, validating data integrity, and bringing business processes back online.

System Restoration Completion Date

Enter date...

Recovery Priority Level

- ☐ Critical (Immediate)
- ☐ High (Urgent)
- ☐ Medium (Standard)
- ☐ Low (Non-Essential)

Restored ERP Modules

- ☐ Finance & Accounting
- ☐ Human Resources (HCM)
- ☐ Supply Chain Management (SCM)
- ☐ Sales & CRM
- ☐ Manufacturing/Production
- ☐ Inventory & Warehouse

Data Integrity Verification Summary

Write something...

Post-Restoration Validation Report

 Upload File

IT Security Manager Approval

Communication & Stakeholder Management

Guidelines for notifying internal executives, legal teams, regulatory bodies, and external customers regarding the incident.

Incident Notification Date

Enter date...

Incident Severity Level

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

Internal Stakeholders Notified

- ☐ IT Security Team
- ☐ Legal/Compliance Department
- ☐ C-Suite Executives
- ☐ ERP Module Owners
- ☐ Public Relations/Communications

Primary Incident Commander

Write something...

Summary of Communication Sent to External Partners

Write something...

Copy of Official Incident Press Release/Statement

 Upload File

Incident Response Manager Approval

Post-Incident Review & Hardening

Activities focused on analyzing lessons learned and updating the ERP security posture to prevent recurrence.

Incident Review Completion Date

Enter date...

Root Cause Analysis Summary

Write something...

Identified Vulnerabilities

- ☐ Unauthorized Access
- ☐ Malware/Ransomware
- ☐ Misconfigured Permissions
- ☐ Unpatched Software
- ☐ Phishing/Credential Theft
- ☐ Data Leakage

Corrective Action Plan & Hardening Steps

Write something...

Final Incident Report Document

 Upload File

Security Officer Approval

< Previous

> Next

✔ Finish

🔧 Generate Sample Report