



ERP Role-Based Access Control (RBAC) Audit Checklist 2026

Governance and Policy Review

Review of existing RBAC policies, documentation, and alignment with corporate security standards and regulatory requirements for 2026.

Last Policy Review Date

RBAC Policy Status

- ☐ Active & Up-to-date
- ☐ Under Revision
- ☐ Expired/Outdated
- ☐ Missing/Not Documented

Regulatory Frameworks Covered

- ☐ GDPR
- ☐ SOX
- ☐ HIPAA
- ☐ ISO 27001
- ☐ Other

Policy Gap Analysis Summary

Write something...

Upload Current RBAC Policy Document

 Upload File

Compliance Officer Approval

User Identity & Authentication Audit

Verification of user identity provisioning processes, Multi-Factor Authentication (MFA) enforcement, and Single Sign-On (SSO) integration integrity.

Audit Execution Date

Enter date...

MFA Status for Administrative Accounts

- ☐ Fully Enforced
- ☐ Partially Enforced
- ☐ Not Enforced

Verified Authentication Methods

- ☐ Biometrics
- ☐ Hardware Tokens
- ☐ SMS/OTP
- ☐ Authenticator App
- ☐ Certificate-based

Number of Unauthenticated Login Attempts Detected

Enter a number...

Description of Authentication Discrepancies Found

Write something...

SSO Configuration Export/Log Report

 Upload File

Auditor Verification Signature

Role Definition & Hierarchy Validation

Evaluation of defined user roles, job functions, and the structural hierarchy to ensure roles are granular and prevent permission creep.

Role Name/ID

Write something...

Role Criticality Level

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

Associated Business Modules

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

Role Description & Functional Purpose

Write something...

Last Hierarchy Review Date

Enter date...

Role Documentation/Matrix

 Upload File

Privileged Access Management (PAM) Inspection

Audit of administrative, super-user, and system-level accounts to ensure high-level permissions are restricted and monitored.

Admin Account Audit Status

- ☐ Compliant
- ☐ Non-Compliant
- ☐ In Progress

Monitored Privileged Activities

- ☐ Password Changes
- ☐ Permission Escalations
- ☐ System Configuration Changes
- ☐ Data Exports

Unidentified Admin Account Found

Write something...

Last Privilege Audit Date

Enter date...

Privileged Access Log Export

 Upload File

Remediation Plan for Unauthorized Access

Write something...

Segregation of Duties (SoD) Analysis

Identification and mitigation of conflicting permissions that could allow a single user to execute fraudulent or unauthorized end-to-end processes.

Identified Conflicting Permission Pairs

- ☐ Procurement vs. Payment Authorization
- ☐ Vendor Creation vs. Invoice Approval
- ☐ Inventory Receiving vs. Inventory Adjustment
- ☐ Order Entry vs. Credit Limit Override
- ☐ Master Data Maintenance vs. Transaction Execution

Description of Identified Risk

Write something...

Risk Severity Level

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

Mitigating Controls Implemented

Write something...

Date of Conflict Resolution

Enter date...

Internal Auditor Approval

Permission & Entitlement Verification

Deep-dive review of specific module-level permissions, read/write/delete capabilities, and object-level security settings within the ERP.

Module Under Review

- ☐ Finance/Accounting
- ☐
- ☐ Supply Chain Management (SCM)
- ☐ Sales & CRM
- ☐ Manufacturing/Production

Permission Levels Verified

- ☐ Read-Only Access
- ☐ Create/Insert Access
- ☐ Update/Edit Access
- ☐ Delete/Remove Access
- ☐ Execute/Run Access

Identified Permission Discrepancies

Write something...

Last Verification Date

Enter date...

Evidence of Permission Export/Screenshot

 Upload File

Auditor Approval

User Access Review & Deprovisioning

Assessment of the periodic access re-certification process and the timeliness of account revocation for terminated or transferred employees.

Review Completion Date

Departments Audited

- ☐ Finance
- ☐ Human Resources
- ☐ Supply Chain
- ☐ Sales & Marketing
- ☐ IT & Operations

Number of Terminated Users Verified

Deprovisioning Delay Status

- ☐ Within SLA
- ☐ Outside SLA - Immediate Action Required
- ☐ Not Applicable

Discrepancies Found & Remediation Steps

Write something...

Auditor Authorization Signature

Audit Logging & Monitoring Oversight

Verification that all role-based permission changes and unauthorized access attempts are captured in immutable logs and integrated with SIEM tools.

Log Integrity Status

- ☐ Immutable/Tamper-proof
- ☐ Vulnerable to modification
- ☐ Not implemented

Monitored Event Types

- ☐ Failed Login Attempts
- ☐ Privilege Escalation
- ☐ Data Export/Extraction
- ☐ Configuration Changes
- ☐ User Deletion/Creation

Last Log Audit Completion Date

Enter date...

Identified Logging Discrepancies

Write something...

Audit Log Sample/Evidence

 Upload File

Auditor Verification Signature

Compliance & Incident Remediation

Review of the workflow for addressing discovered access discrepancies and documenting corrective actions for audit traceability.

Date of Compliance Review Completion

Enter date...

Identified Compliance Gaps

- ☐ Unauthorized Privilege Escalation
- ☐ Segregation of Duties (SoD) Conflict
- ☐ Stale/Inactive Account Found
- ☐ Incomplete Audit Logging
- ☐ Missing Documentation

Remediation Action Plan Description

Write something...

Number of High-Risk Issues Resolved

Enter a number...

Evidence of Remediation (Screenshots/Logs)

 Upload File

Compliance Officer Sign-off

< Previous

> Next

✔ Finish

🔧 Generate Sample Report