Workday configuration scan

Tenant: Acme Corp (Workday Demo)

Health score: 50/100

Completed: 09/05/2026, 01:37:44

Executive summary

EXECUTIVE VERDICT

Acme Corp's Workday tenant scores 50/100 (Needs Attention), indicating significant control gaps that require immediate executive attention. The primary risk profile is access governance and financial controls, with unconstrained security groups creating direct fraud exposure and compensation processes lacking mandatory approval workflows that could enable undetected payroll manipulation.

PRIORITY RISK ANALYSIS

The most critical exposure stems from the "Payroll Super Users" security group operating without constraints while holding Banking and Settlement write access across the entire organisation. Any member of this security group can modify sensitive payroll, banking, or security data for every worker in the organisation without restriction — a direct financial fraud and data manipulation risk. This violates SOX §404 ITGC requirements and creates immediate compliance exposure under PCI-DSS Req. 7 and ISO 27001 A.9.1.2.

Compounding this risk, two compensation change processes ("Compensation Change" and "Merit Salary Adjustment") operate without approval steps, allowing any user with compensation initiation access to unilaterally change employee pay without review. This creates direct payroll fraud risk and payroll tax compliance exposure under SOX §404 ITGC Change Management Controls and DOL Wage and Hour Regulations. Together, these findings represent a complete breakdown of segregation of duties in the compensation lifecycle, where users can both initiate and approve their own financial changes without oversight.

REMEDIATION ROADMAP

The remediation effort spans 277–559 hours across 13 findings, with 3 High severity and 10 Medium severity issues requiring attention. IT Security and Workday Security Administrator teams must address the unconstrained security group immediately (75–105 hours), followed by Compensation Manager and HR Systems Administrator teams implementing approval workflows for compensation processes (90–130 hours combined). Integration teams face 66–142 hours of work to resolve personal account dependencies and recurring failures across three critical integrations. The highest-priority findings (Priority Weight 9–10) demand immediate executive sponsorship and should be addressed within the next 30 days to restore basic financial controls and prevent potential fraud exposure.

DISCLAIMERS

1. This report reflects tenant configuration as of 2026-05-08. Configuration may have changed subsequently.
2. This audit accessed only system configuration objects. No individual employee records, compensation data, or personal information was accessed or processed.
3. Findings represent automated configuration analysis against industry-practice benchmarks. They are not legal opinions, regulatory compliance certifications, or guarantees of security.
4. Findings should be reviewed by qualified HR platform professionals before remediation. Some configurations may be intentional based on business requirements not visible through configuration analysis alone.
5. Risk thresholds used in this report are industry practitioner conventions. Where no official vendor threshold exists, this report discloses this. Workday does not publish mandatory numeric thresholds for these metrics.

1. [HIGH] Unconstrained group with Banking and Settlement write access

Security group "Payroll Super Users" is unconstrained and has Modify access to "Banking and Settlement". Any member can access and modify this data for ALL workers organisation-wide. Impact: Members of "Payroll Super Users" can modify Banking and Settlement data for every worker in the tenant without restriction.

2. [HIGH] Compensation change process "Compensation Change" has no approval step

The business process "Compensation Change" allows compensation changes to complete without any approval. Any user with initiation access can change compensation without review. Impact: Direct payroll fraud risk — pay changes can be made without oversight.

3. [HIGH] Compensation change process "Merit Salary Adjustment" has no approval step

The business process "Merit Salary Adjustment" allows compensation changes to complete without any approval. Any user with initiation access can change compensation without review. Impact: Direct payroll fraud risk — pay changes can be made without oversight.

4. [MEDIUM] Integration "Workato Benefits Sync" runs under a personal user account

The ISU for integration "Workato Benefits Sync" is linked to a personal worker account. When this worker is terminated, their account deactivation will immediately break this integration. Impact: Integration will break without warning when the linked worker leaves the organisation.

5. [MEDIUM] Integration "SAP Concur Expense Feed" runs under a personal user account

The ISU for integration "SAP Concur Expense Feed" is linked to a personal worker account. When this worker is terminated, their account deactivation will immediately break this integration. Impact: Integration will break without warning when the linked worker leaves the organisation.

6. [MEDIUM] Integration "ADP Payroll Export" failed 8 times in the last 30 days

Integration "ADP Payroll Export" (type: Core Connector) has failed 8 times in the past 30 days. The downstream system is not receiving reliable data from Workday. Impact: Data synchronisation between Workday and the target system is unreliable — downstream records may be stale or incorrect.

7. [MEDIUM] Integration "Workato Benefits Sync" failed 5 times in the last 30 days

Integration "Workato Benefits Sync" (type: EIB) has failed 5 times in the past 30 days. The downstream system is not receiving reliable data from Workday. Impact: Data synchronisation between Workday and the target system is unreliable — downstream records may be stale or incorrect.

8. [MEDIUM] Integration "SAP Concur Expense Feed" failed 4 times in the last 30 days

Integration "SAP Concur Expense Feed" (type: Studio) has failed 4 times in the past 30 days. The downstream system is not receiving reliable data from Workday. Impact: Data synchronisation between Workday and the target system is unreliable — downstream records may be stale or incorrect.

9. [MEDIUM] Calculated field "Bonus Target Amount" has a critical error

Calculated field "Bonus Target Amount" (business object: Compensation) has a critical error status. Any report or process depending on this field is producing incorrect data. Impact: Incorrect data output from a broken calculated field may affect payroll calculations, reports, or business process routing.

10. [MEDIUM] Calculated field "Time to Fill (Days)" has a critical error

Calculated field "Time to Fill (Days)" (business object: Recruiting) has a critical error status. Any report or process depending on this field is producing incorrect data. Impact: Incorrect data output from a broken calculated field may affect payroll calculations, reports, or business process routing.

11. [MEDIUM] 14 open transactions in "Compensation Change" — oldest 31 days

Business process "Compensation Change" has 14 incomplete transaction(s). The oldest has been open for 31 days. Impact: Compensation change neither implemented nor cancelled — employee pay is in an uncertain state.

12. [MEDIUM] 187 open transactions in "Performance Review" — oldest 45 days

Business process "Performance Review" has 187 incomplete transaction(s). The oldest has been open for 45 days. Impact: Business process has been pending for 45 days — investigate for approver availability and escalate as needed.

13. [MEDIUM] 50% of job profiles missing job family

5 job profiles have no job family assigned. Job family is required for Illuminate Workforce Planning AI. Impact: Workforce planning and succession planning AI features will produce inaccurate results.

Remediation plan

P1 — Unconstrained group with Banking and Settlement write access

- In Workday, search 'Edit Security Group' and open the group named in this finding.
- Locate the 'Intersection Type' or constraint field and change it from Unconstrained to a Constrained scope mapped to specific Supervisory Organisations.
- Navigate to 'Maintain Domain Permissions for Security Group' and confirm no excessive Modify/Put permissions remain for sensitive domains.
- Search 'Activate Pending Security Policy Changes' and confirm to apply the constraint.
- Validate the change in a non-production environment before activating in production.
- Document the change with business justification and run the Workday Security Audit worklet to confirm resolution.

P1 — Compensation change process "Compensation Change" has no approval step

- Search 'Manage Business Processes' in Workday and open the Compensation Change process definition.
- Click Edit on the process.
- After the data entry step, click '+' to insert a new step and select 'Approval Step'.
- Configure the approver routing: typically the employee's manager or Compensation Partner, routed by Supervisory Organisation.
- Optionally add a condition rule: require approval only for changes above a defined threshold (e.g., more than 10% or more than a set amount).
- Save and Activate the updated process definition.
- Test in a sandbox tenant with a sample compensation change before activating in production.

P1 — Compensation change process "Merit Salary Adjustment" has no approval step

- Search 'Manage Business Processes' in Workday and open the Compensation Change process definition.
- Click Edit on the process.
- After the data entry step, click '+' to insert a new step and select 'Approval Step'.
- Configure the approver routing: typically the employee's manager or Compensation Partner, routed by Supervisory Organisation.
- Optionally add a condition rule: require approval only for changes above a defined threshold (e.g., more than 10% or more than a set amount).
- Save and Activate the updated process definition.
- Test in a sandbox tenant with a sample compensation change before activating in production.

P2 — Integration "Workato Benefits Sync" runs under a personal user account

- Search 'Create Integration System User' in Workday.
- Create a new ISU: set the user type to 'Integration System' — do NOT link it to any worker or employee record.
- Set session timeout to 0 minutes to prevent timeout during long-running integration jobs.
- Create or reuse an Integration System Security Group (ISSG) and assign only the domain permissions the integration actually requires.
- Assign the new ISU to the ISSG.
- Update the integration configuration to use the new ISU credentials (OAuth client ID/secret or username/password depending on integration type).
- Test the integration end-to-end in a non-production environment before switching production.
- Search 'Activate Pending Security Policy Changes' to confirm, then decommission the old personal user account from the integration.

P2 — Integration "SAP Concur Expense Feed" runs under a personal user account

- Search 'Create Integration System User' in Workday.
- Create a new ISU: set the user type to 'Integration System' — do NOT link it to any worker or employee record.
- Set session timeout to 0 minutes to prevent timeout during long-running integration jobs.
- Create or reuse an Integration System Security Group (ISSG) and assign only the domain permissions the integration actually requires.
- Assign the new ISU to the ISSG.
- Update the integration configuration to use the new ISU credentials (OAuth client ID/secret or username/password depending on integration type).
- Test the integration end-to-end in a non-production environment before switching production.
- Search 'Activate Pending Security Policy Changes' to confirm, then decommission the old personal user account from the integration.

P2 — Integration "ADP Payroll Export" failed 8 times in the last 30 days

- Navigate to Workday !' Reports !' Integration Run History.
- Filter to the integration named in this finding and open the most recent failed run.
- Review the error message to determine whether the failure is authentication, network, or data-related.
- If authentication: rotate ISU credentials and update the integration configuration.
- If data: review the failed records and correct the source data before re-running.
- If network: coordinate with IT to verify firewall and endpoint reachability.
- Monitor for 7 consecutive successful runs before closing the finding.

P2 — Integration "Workato Benefits Sync" failed 5 times in the last 30 days

- Navigate to Workday !' Reports !' Integration Run History.
- Filter to the integration named in this finding and open the most recent failed run.
- Review the error message to determine whether the failure is authentication, network, or data-related.
- If authentication: rotate ISU credentials and update the integration configuration.
- If data: review the failed records and correct the source data before re-running.
- If network: coordinate with IT to verify firewall and endpoint reachability.
- Monitor for 7 consecutive successful runs before closing the finding.

P2 — Integration "SAP Concur Expense Feed" failed 4 times in the last 30 days

- Navigate to Workday !' Reports !' Integration Run History.
- Filter to the integration named in this finding and open the most recent failed run.
- Review the error message to determine whether the failure is authentication, network, or data-related.
- If authentication: rotate ISU credentials and update the integration configuration.
- If data: review the failed records and correct the source data before re-running.
- If network: coordinate with IT to verify firewall and endpoint reachability.
- Monitor for 7 consecutive successful runs before closing the finding.