AY SaaS Consulting

SAMPLE REPORT · FICTIONAL COMPANY AND DATA

A.Y.M SENTINEL – SECURITY AUDIT FOR WORKDAY

Workday Security Audit Report

Northwind Global (fictional)

Package	Standard Audit with module review, regulatory alignment and AI agent security review
Tenant	Production
Data as of	September 15, 2026
Prepared by	AY SaaS Consulting

> **About this sample.** This is an excerpt of a full A.Y.M Sentinel report. Northwind Global, its people, vendors and agents are invented; the findings were produced by running our audit on a fictional tenant built to show common Workday security problems. A full report also includes every finding by area, the module and regulatory breakdowns, a findings workbook with a detail tab for each check, and a readout deck.

In this excerpt

1. Executive summary and security posture scorecard
2. Results by module and questionnaire check
3. Example findings: business process approvals, sensitive data, AI agents
4. The findings workbook and what you receive
5. Scope and limits

© 2026 AY SaaS Consulting · aysaasconsulting.com

audit@aysaasconsulting.com · 682-233-2833

1 Executive summary

This audit reviewed how Northwind Global's Workday tenant controls who can see and change worker data, who can start and approve business processes, and how implementer, integration, service center and AI agent accounts are governed.

1.6 / 5	36	55	23
Overall posture (Weak)	High risk	Medium risk	Low risk

Highest-priority findings

- **Critical business processes complete without approval (B-01).** Hire, Assign Roles and three other critical processes have no approval step.
- **Approvals skip themselves when the initiator is an approver (B-02).** Edit Government IDs, Pay Cycle Event and Withholding Elections.
- **Government IDs / SSN visible beyond the roles that need it (D-01).** Six groups, including an AI agent group, can reach SSNs.
- **Service center representatives combine security and HR/payroll administration (B-05).** One person can grant access and use it.

Security posture scorecard

AUDIT AREA	SCORE	RATING	HIGH	MED	LOW
Business process approvals & SoD	1	★☆☆☆☆ Critical	12	7	0
Privileged & implementation access	1	★☆☆☆☆ Critical	5	4	0
Non-worker & service center accounts	2	★★☆☆☆ Weak	2	4	0
Sensitive worker data	1	★☆☆☆☆ Critical	3	1	0
Integration security	2	★★☆☆☆ Weak	1	3	0
Security groups & custom domains	2	★★☆☆☆ Weak	1	2	3
Organization role assignments	3	★★★☆☆ Fair	0	2	0
Reports & scheduled processes	2	★★☆☆☆ Weak	1	4	2
AI agent security	1	★☆☆☆☆ Critical	4	5	2
Security governance & processes	1	★☆☆☆☆ Critical	7	23	16

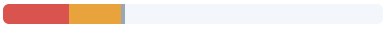
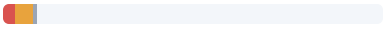
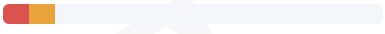
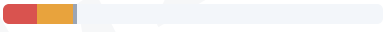
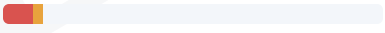
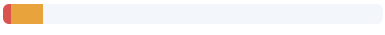
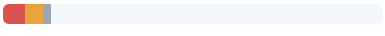
Scale: 5 = Strong (meets Workday best practice), 4 = Good, 3 = Fair, 2 = Weak, 1 = Critical. Each area is scored from its findings.

SAMPLE

© 2026 AY SaaS Consulting · aysaasconsulting.com

2 Results by module and questionnaire check

Every finding is tagged to the Workday modules it affects, so each module owner sees their own list. Cross-module findings are security foundations (accounts, authentication, segregation of duties, governance) that apply everywhere.

MODULE	RATING	HIGH	MED	LOW	FINDINGS
Core HCM	★☆☆☆☆	15	12	1	
Compensation	★☆☆☆☆	3	4	1	
Benefits	★☆☆☆☆	6	6	0	
Onboarding	★★☆☆☆	1	0	0	
Absence	★★★★★	0	0	0	
Time Tracking	★★★★★	0	0	0	
Payroll (Core)	★☆☆☆☆	8	8	1	
Recruiting	★☆☆☆☆	7	2	0	
Talent and Performance	★★★★★	0	0	0	
Integrations	★★☆☆☆	2	7	0	
Workday AI and Agents	★☆☆☆☆	5	4	2	
Cross-module (security foundation)	★☆☆☆☆	22	43	22	

High Medium Low

What the team said vs. what Workday shows

Before the audit, the client's team answers a short security questionnaire. Each answer is checked against the Workday data, so gaps between policy and practice surface before the readout.

8
Contradicted
Answered "Yes", but the data shows the exception

44
Consistent
Answer matches the data

16
Not confirmed
"Don't know" or no answer – confirmed at the readout

41
Readout follow-ups
Items to agree with owners and dates

SAMPLE

© 2026 AY SaaS Consulting · aysaasconsulting.com

3 Example findings

Every finding follows the same format: what was found, why it matters, what to change, and the exact Workday tasks to make and verify the fix. Three of Northwind's 114 findings are shown here.

B-01 HIGH Critical business processes complete without approval

Area Business process approvals & SoD **Modules** Core HCM, Payroll (Core), Recruiting **Laws & frameworks** SOC 2, SOX

Finding
5 critical business processes have no approval step: Assign Roles, Hire, Job Requisition, Payment Election Enrollment Event and User-Based Security Group Event.

Impact
Changes to people, pay or access take effect with no second review. A single user can create and complete a sensitive transaction.

Recommendation
Add an approval step that excludes the initiator (for example HR Partner, Compensation Partner, or a payroll or security approver) and review which groups can initiate each process.

How to fix in Workday
Workday tasks: Edit Definition; Edit Business Process Security Policy; Activate Pending Security Policy Changes.

Add an Approval step to each listed process, routed to a role other than the initiator. Add the approving group to the business process security policy and activate it before selecting it in the step.

Check: Run a test transaction in a sandbox and confirm the process history shows the approval.

Questionnaire check
Contradicted The client answered "Yes" to the approvals question, but the Workday data shows this exception. Listed for confirmation at the readout.

BUSINESS PROCESS	GROUPS THAT CAN START IT
Assign Roles	HR Administrator; HR Partner; Security Administrator
Hire	HR Administrator; HR Partner; Implementers; +2 more
Job Requisition	Manager; Recruiter; Recruiting Administrator
Payment Election Enrollment Event	HR Administrator; Payroll Administrator
User-Based Security Group Event	Implementers; Security Administrator

From the BP Approvals tab of the findings workbook.

© 2026 AY SaaS Consulting · aysaasconsulting.com

D-01 HIGH Government IDs / SSN visible beyond the roles that need it

Area Sensitive worker data **Modules** Core HCM, Benefits, Payroll (Core), Workday AI and Agents

Laws & frameworks GDPR, UK GDPR, CCPA, HIPAA, PIPEDA, LGPD and 13 more in scope

Finding 6 security groups outside the approved list can access Government IDs / SSN.

Impact Sensitive personal data is exposed to roles without a job need, creating privacy and compliance risk.

Recommendation Remove Government ID / SSN domains from groups without a documented need. Limit access to HR Administrator and Security Administrator.

How to fix in Workday *Workday tasks: View Security for Securable Item; Edit Domain Security Policy; Activate Pending Security Policy Changes.*

For each domain listed, confirm the exposure with View Security for Securable Item, remove the groups that do not need it, and activate. Where only some segments are needed, use a segment-based group instead of the base domain.

Check: Repeat View Security for Securable Item as a member of a removed group; the field is no longer visible.

Questionnaire check Consistent Matches the questionnaire answer “Partially”.

SECURITY GROUP	ACCESS	DOMAINS
Benefits Administrator	Modify	Person Data: Government IDs
Global Mobility Partner	View	Person Data: Government IDs
HR Auditor	View	Person Data: Government IDs; View: National IDs
Implementers	Modify	Person Data: Government IDs; View: National IDs
Payroll Insights Agent – Ambient Agent Security Group	Get	Person Data: Government IDs
Personal Information – View Only	View	Person Data: Government IDs; View: National IDs

From the Sensitive Access tab of the findings workbook.

© 2026 AY SaaS Consulting · aysaasconsulting.com

AG-02 HIGH Agent security groups can read or change security configuration

Area AI agent security **Modules** Workday AI and Agents, Recruiting **Laws & frameworks** SOC 2 (access control)

Finding	The ambient agent security group for “Pilot Recruiting Bot” holds Put access on the Security Configuration domain.
Impact	An agent that can change security or agent configuration can widen its own access or another agent’s, without a person approving the change.
Recommendation	Remove these grants. No agent skill should administer security, tenant setup or agents.
How to fix in Workday	*Workday tasks: View Security for Agent Skill; Edit Domain Security Policy Permissions; Activate Pending Security Policy Changes.* For each agent, run View Security for Agent Skill and note the recommended security policies for its enabled tools. Remove the ambient agent security group from every other domain and business process policy, then activate with the change ticket in the comment. **Check:** View Security for Agent Skill shows Full Match for each tool, and the agent group appears only on its recommended policies.
Questionnaire check	Not confirmed The AI agent questions were not answered. Listed for confirmation at the readout.

Why AI agents are in scope. Workday agents act through their own security groups and accounts. Ambient agents run on a schedule with no user involved, so an over-permissioned agent group is reachable around the clock. The optional AI agent review checks agent accounts, agent security groups, skill security and the agent audit trail.

SAMPLE

© 2026 AY SaaS Consulting · aysaasconsulting.com

4 The findings workbook

Alongside the report, your team receives an Excel workbook: a findings register to track remediation, a scorecard, and a detail tab for every check listing the exact people, groups, processes and accounts behind each finding.

NorthwindGlobal_AYM_Sentinel_Findings.xlsx — Findings | Scorecard | By Module | BP Approvals | Sensitive Access | AI Agents | +27

ID	FINDING	RISK	QUESTIONNAIRE	OWNER	TARGET DATE	STATUS
B-01	Critical business processes complete without approval	HIGH	Contradicted	HRIS Director	2026-11-14	In progress
B-02	Approvals skip themselves when the initiator is an approver	HIGH	Consistent	Payroll Manager	2026-11-14	Not started
P-02	Enabled implementer accounts not used recently	HIGH	Consistent	Security Lead	2026-10-31	Done
A-01	Integration system users can sign in to the Workday UI	HIGH	Consistent	Integrations Lead	2026-10-31	In progress
D-01	Government IDs / SSN visible beyond the roles that need it	HIGH	Consistent			
AG-02	Agent security groups can read or change security configuration	HIGH	Not confirmed			
P-08	Security policy changes activated without a comment	MEDIUM	Contradicted			
R-01	Scheduled processes are owned by implementer accounts	HIGH	Consistent			

Excerpt of the Findings tab (8 of 114 rows). Yellow columns are for your team to fill in during remediation.

What you receive

Written report
Executive summary, scorecard and every finding with Workday fix steps.

Findings workbook
Register for tracking, plus a detail tab for each check listing every affected item.

Readout deck
Slides for a 60–90 minute session with HRIS, security and data owners.

Readout meeting
Findings agreed, owners and dates set, so remediation starts that day.

SAMPLE

© 2026 AY SaaS Consulting · aysaasconsulting.com

5 Scope and limits

The audit is read-only. Your team runs a set of Workday reports and sends the exports; we never sign in to your tenant or change anything.

What this review does not cover

- Activity in the tenant: who actually viewed, changed or exported data (activity logs are not analysed, except the AI agent audit trail when that review is included).
- Identity provider settings: SSO and MFA configuration outside Workday (questionnaire answers are reported as provided).
- Systems that receive Workday data: integration endpoints, vendors and file destinations.
- Field-level data quality and the accuracy of the data itself.
- Tenants other than the one the reports were run in, and changes made after the data-as-of date.

Regulatory mapping shows which laws and frameworks a finding may affect. It is not legal advice; confirm obligations with your counsel.

See the full sample on a scoping call

In 30 minutes we walk through the complete sample report and workbook, confirm your modules and tenant size, and you receive a fixed quote within two business days.

audit@aysaasconsulting.com | 682-233-2833 | aysaasconsulting.com

SAMPLE

© 2026 AY SaaS Consulting · aysaasconsulting.com