

14-Point JML Blind Spot Checklist

For mid-market and enterprise IT & security leaders. Score yourself in about 10 minutes. Each **No** is a gap that commonly becomes a breach, an audit finding, or reclaimable SaaS waste.

How to use: Mark Yes / Partial / No for each item. Count your Nos. 3+ Nos = elevated lifecycle risk. 6+ Nos = board-level conversation territory.

Joiner - Day-one access

#	Check	Y	P	N
1	New hires get core systems on day one without a spreadsheet chase <i>Okta / Entra / Google, email, Slack/Teams, badge</i>	[]	[]	[]
2	Role templates exist for at least your top 5 job families <i>Engineering, Sales, Finance, Support, Contractor</i>	[]	[]	[]
3	Contractors and vendors follow a separate, shorter-lived joiner path <i>Not the same as FTEs</i>	[]	[]	[]

Mover - Role and org changes

#	Check	Y	P	N
4	When someone changes role, old entitlements are removed - not only added <i>Privilege accumulates silently</i>	[]	[]	[]
5	Department moves trigger an access review within 7 days <i>HRIS change to ticket or automation</i>	[]	[]	[]
6	Managers can see what their team currently has access to <i>Without opening a ticket to IT</i>	[]	[]	[]

Leaver - Offboarding

#	Check	Y	P	N
7	Terminated employees lose all access within 24 hours <i>IdP, SaaS, cloud, VPN, badge</i>	[]	[]	[]
8	You can list every account disabled for leavers in the last 90 days <i>Evidence for auditors</i>	[]	[]	[]
9	Personal / forwarding rules and shared mailboxes are reviewed on exit <i>Classic blind spot</i>	[]	[]	[]
10	GitHub / cloud PATs and API keys are revoked on exit - not only the IdP login <i>Orphaned machine access</i>	[]	[]	[]

Non-human and AI identities

#	Check	Y	P	N
11	Service accounts and API keys have named human owners <i>No "shared" or "nobody"</i>	☐	☐	☐
12	You know how many AI agents / bots have production credentials <i>Even a rough count counts</i>	☐	☐	☐
13	AI / automation tokens are scoped least-privilege - not admin by default <i>Jira, Salesforce, Slack bots</i>	☐	☐	☐
14	You have a quarterly review of non-human identities <i>Same cadence as privileged humans</i>	☐	☐	☐

Your score

Total **No** answers: _____ Total **Partial**: _____ Overall risk (circle): Low / Medium / High

What this checklist reveals: Joiner-Mover-Leaver failures hide in the gaps between HR, IT, and security. A free self-score finds the pattern. Closing it across every human, machine, and AI-agent identity is the next problem.