

ITAM Integration Health Check

CHECKLIST

Use this checklist to evaluate the strength and reliability of your ITAM integrations.
Select Yes or No for each question and assess your integration risk level.

1. Do HR status changes automatically trigger IT updates (access removal, asset reassignment, license revocation)?

- Yes
- No

2. Can you trace device ownership (person, department, cost center) in one click?

- Yes
- No

3. Are sync failures between systems automatically logged and alerted?

- Yes
- No

4. Do you have a clearly defined single source of truth for asset and ownership data?

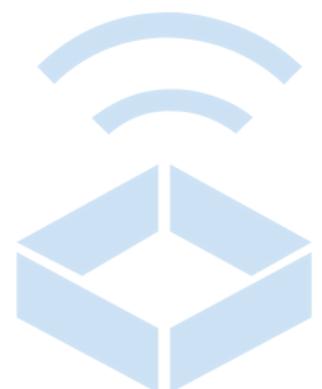
- Yes
- No

5. Can you clearly explain your automation rules and logic to auditors or leadership?

- Yes
- No

6. Are lifecycle events (procurement to disposal) consistently recorded across all connected systems?

- Yes
- No



7. Is identity data standardized across HR, ITAM, and identity providers?

- Yes
- No

8. Are configuration changes automatically reflected in your ITAM records?

- Yes
- No

9. Do offboarding workflows automatically recover or flag unreturned assets?

- Yes
- No

10. Is there documentation governing your integration logic and ownership mappings?

- Yes
- No

Scoring Your Risk Level

8–10 Yes answers → **Low Risk**

Your integrations are structured, governed, and predictable.

4–7 Yes answers → **Moderate Risk**

Some integration gaps may impact reporting accuracy.

0–3 Yes answers → **High Risk**

Significant integration weaknesses may compromise ITAM data integrity and audit readiness.

If your score indicates Moderate or High Risk, review your automation governance, ownership mappings, and system synchronization rules to strengthen reporting confidence.

