



## Automation Readiness Checklist

Use this checklist to evaluate your organisation's readiness for secure, sustainable, and operationally responsible workflow automation.

Check each item currently in place.

### Automation and Productivity Readiness Assessment

- 1. We use approved automation tools across the organisation.
- 2. Employees understand what workflows may be automated safely.
- 3. We maintain visibility into active automation systems and integrations.
- 4. Employees receive guidance regarding shadow automation risks.
- 5. Automation workflows are documented appropriately.
- 6. Sensitive workflows require human review and approval.
- 7. AI-assisted communication is reviewed before external distribution.
- 8. Access permissions follow least-privilege principles.
- 9. Multi-factor authentication protects connected workflow systems.
- 10. Employees understand the risks of excessive automation dependency.
- 11. Automation platforms are reviewed for cybersecurity and privacy exposure.
- 12. Workflow failures can be identified and escalated quickly.
- 13. Employees understand approved AI-assisted productivity practices.
- 14. Remote employees receive automation governance guidance.
- 15. Automation improves workflow clarity rather than increasing confusion.
- 16. Sensitive customer and financial data is protected appropriately within automated systems.
- 17. Managers reinforce responsible automation practices consistently.

- 18. Employees understand verification expectations for automated outputs.
  - 19. Connected integrations are reviewed periodically for security risks.
  - 20. Automation systems support operational consistency across teams.
  - 21. Employee workload reduction is considered alongside productivity goals.
  - 22. Governance procedures exist for approving new automation workflows.
  - 23. Employees know how to report suspicious workflow behaviour or automation issues.
  - 24. Operational accountability remains clearly defined despite automation usage.
  - 25. Leadership views automation as part of long-term operational resilience strategy.
- 

## Scoring Guide

### Strong Maturity

#### 20–25 checked items

Your organisation demonstrates strong operational readiness for responsible automation and AI-assisted productivity.

You likely maintain:

- effective governance,
- workflow visibility,
- employee awareness,
- and operational accountability.

Continue refining:

- automation oversight,
- employee training,
- cybersecurity monitoring,
- and workflow optimization.

### Moderate Exposure

#### 12–19 checked items

Your organisation has implemented some productivity and automation safeguards, but important governance gaps remain.

You may benefit from stronger:

- workflow visibility,
- employee guidance,
- automation documentation,
- and cybersecurity oversight.

Operational consistency and governance improvement should become near-term priorities.

## High Vulnerability

### 0–11 checked items

Your organisation may face significant operational and cybersecurity exposure from poorly governed automation.

Employees may currently use:

- unauthorised tools,
- unmanaged workflows,
- or risky integrations

without sufficient oversight.

Immediate improvement is recommended involving:

- governance,
- visibility,
- employee awareness,
- workflow review,

and operational accountability.