CurrentWare

AI TOOLKIT

AI Governance Readiness Checklist

Measure how ready your organization is to see, control, and measure AI use, so you can move from making assumptions to evidence-backed decisions.

Step 1
Review Your AI Preparedness

Step 2
Book A Time With Our Team

Step 3
Discuss How to Improve

From The AI Blind Spot webinar

currentware.com

INTRODUCTION

How to use this checklist

Score your environment across six areas of AI governance, find the gaps that carry the most risk, and decide what to tackle first. Repeat annually, or as needed.

For enterprise clients, we recommend completing this checklist with your IT, security, legal/compliance teams, and that you provide answers based on what is already in place.

Score each statement

0	**No**	Not in place, or no evidence to confirm that controls exist.
1	**Partly**	In place for some teams, tools, or devices.
2	**Yes**	In place across the organization, with strong evidence.

The Six Domains Required For Strong AI Governance

01	**Ownership and Accountability**	Someone owns AI decisions, and each team knows their role within the decision infrastructure.
02	**Policy**	Employees clearly know which AI tools they can use, and for what purpose they are allowed to use them.
03	**Visibility**	You can see which AI tools are in use, who is using them, and how often they are using them.
04	**Data Protection**	Sensitive information stays out of tools you have not approved, and is appropriately restricted in approved tools.
05	**Control and Enforcement**	Your AI policy lives outside of the document it was printed on, and is enforced in practice.
06	**Measurement and Adoption**	You can benchmark the workflows that show what AI is doing for the business, and costs associated with this investment.

WHERE CURRENTWARE HELPS

Statements marked CurrentWare name the BrowseReporter, BrowseControl, or AccessPatrol feature that provides the evidence or control for the specific section.

DOMAIN 01

Ownership and Accountability

Someone owns AI decisions, and each team knows their role within the decision infrastructure.

		NO	PART	YES
1.1	A named executive or team owns AI governance decisions.	0	1	2
1.2	IT, security/compliance, and human resources each have a defined role.	0	1	2
1.3	A documented process exists for requesting and approving new AI tools.	0	1	2
1.4	AI risks are reviewed with leadership teams on a regularly set schedule.	0	1	2
1.5	Regulations that apply to your AI use (such as GDPR, the EU AI Act, HIPAA, or PIPEDA) are identified and reviewed.	0	1	2
1.6	Budget and ownership of AI licenses is assigned to a specific person.	0	1	2

DOMAIN SCORE _____ / 12

DOMAIN 02

Policy

Employees clearly know which AI tools they can use, and for what purpose they are allowed to use them.

		NO	PART	YES
2.1	A written AI Acceptable Use Policy is published and accessible to the entire team. CurrentWare · AI Acceptable Use Policy Template	0	1	2
2.2	The AI AUP lists approved, restricted, and prohibited AI tools.	0	1	2
2.3	The policy defines which data must never be entered into public AI tools.	0	1	2
2.4	The policy covers personal accounts on approved AI tools.	0	1	2
2.5	Employees have acknowledged the policy in writing.	0	1	2
2.6	Employees are informed how AI use is monitored and restricted.	0	1	2

DOMAIN SCORE _____ / 12

DOMAIN 03

Visibility

You can see which AI tools are in use, who is using them, and how often they are using them.

		NO	PART	YES
3.1	You have a complete inventory of AI tools used across the organization. CurrentWare · BrowseReporter	0	1	2
3.2	AI usage can be broken down by user, department, and device. CurrentWare · BrowseReporter	0	1	2
3.3	Visibility covers remote and hybrid employees, on and off the main network. CurrentWare · CurrentWare Suite	0	1	2
3.4	Desktop AI applications are tracked, as well as browser-based tools. CurrentWare · BrowseReporter	0	1	2
3.5	You are alerted when someone accesses a new AI tool for the first time. CurrentWare · BrowseReporter	0	1	2
3.6	A two to four week baseline of normal AI activity has been collected. CurrentWare · BrowseReporter	0	1	2

DOMAIN SCORE _____ / 12

DOMAIN 04

Data Protection

Sensitive information stays out of tools you have not approved, and is appropriately restricted in approved tools.

		NO	PART	YES
4.1	Sensitive data types (customer, financial, health, source code, IP) are classified. CurrentWare · AccessPatrol	0	1	2
4.2	You know which teams handle sensitive data and the AI tools they use. CurrentWare · BrowseReporter	0	1	2
4.3	Risky file uploads to unapproved AI tools can be blocked instantly. CurrentWare · AccessPatrol	0	1	2
4.4	USB and removable media use is controlled and appropriately restricted. CurrentWare · AccessPatrol	0	1	2
4.5	Behaviour-triggered screenshots capture evidence when risky activity occurs. CurrentWare · BrowseReporter	0	1	2
4.6	An incident response process covers AI-related data exposure.	0	1	2

DOMAIN SCORE _____ / 12

DOMAIN 05

Control and Enforcement

Your AI policy lives outside of the document it was printed on, and is enforced in practice.

		NO	PART	YES
5.1	Approved AI tools are monitored and unapproved tools are restricted. CurrentWare · BrowseControl	0	1	2
5.2	Access policies can differ by group, or schedule. CurrentWare · BrowseControl	0	1	2
5.3	Controls stay in effect when devices leave the corporate network. CurrentWare · BrowseControl	0	1	2
5.4	Each restricted tool has an approved alternative, so work does not move to personal devices.	0	1	2
5.5	Alerts flag policy violations and unusual activity. CurrentWare · BrowseReporter	0	1	2
5.6	Exceptions are documented with an owner and an end date.	0	1	2

DOMAIN SCORE _____ / 12

DOMAIN 06

Measurement and Adoption

You can benchmark the workflows that show what AI is doing for the business, and costs associated with this investment.

		NO	PART	YES
6.1	Adoption of approved AI tools is tracked for each team. CurrentWare · BrowseReporter	0	1	2
6.2	Paid AI licenses are compared with actual usage. CurrentWare · BrowseReporter	0	1	2
6.3	Regularly scheduled AI usage reports are sent to leadership. CurrentWare · BrowseReporter	0	1	2
6.4	Governance KPIs are defined, such as volume of Shadow AI tools found, number of policy violations, and overall adoption rate.	0	1	2
6.5	Audit-ready evidence of policy enforcement can be produced on request. CurrentWare · BrowseReporter	0	1	2
6.6	Training on approved AI use is delivered and tracked.	0	1	2

DOMAIN SCORE _____ / 12

RESULTS

Your Readiness Scorecard

01	Ownership and Accountability	_____ / 12
02	Policy	_____ / 12
03	Visibility	_____ / 12
04	Data Protection	_____ / 12
05	Control and Enforcement	_____ / 12
06	Measurement and Adoption	_____ / 12

TOTAL SCORE

_____

out of 72

Date completed:

_____

0 – 30

Exposed

AI use is largely invisible. We recommend you begin with an AI tool inventory and policy writing.

31 – 54

Developing

Good foundations exist, but gaps in visibility or enforcement leave policies largely untested.

55 – 72

Governed

AI use is visible, controlled, and measured. Regular reviews are recommended to stay current.

Your top three priorities

Start with your lowest-scoring domain. Any "No" in Data protection should be treated as urgent.

01	Owner / due
02	Owner / due
03	Owner / due

Ready to close the remaining gaps?

CurrentWare

Use the Shadow AI Investigation Playbook and AI Acceptable Use Policy Template in this toolkit, or start a free trial and book a demo at currentware.com.

NEW CLIENTS
sales@currentware.com

EXISTING CLIENTS
success@currentware.com

PHONE
1-888-912-9619