AI GOVERNANCE
SELF-ASSESSMENT CHECKLIST

Complete this checklist before booking your discovery call with Axionly.

Organisation:

_____

Date:

_____

Completed by:

_____

HOW TO USE THIS CHECKLIST

Work through each section with your IT, legal, and compliance teams. **Tick items you have in place.** Leave items blank if they are missing or unclear — these become the focus of your Axionly assessment. *There are no wrong answers: the purpose is to surface gaps, not to pass a test.*

📋 SECTION 1 — AI SYSTEM INVENTORY

✓	ITEM	NOTES / OBSERVATIONS
☐	We have a complete, up-to-date register of all AI tools used across our organisation.	*Notes / observations*
☐	Our register includes AI tools adopted by individual teams or departments without central IT approval (shadow AI).	*Notes / observations*
☐	We know which AI tools are connected to or process personal data of employees or customers.	*Notes / observations*
☐	We have identified which AI tools are provided by third-party vendors versus built or fine-tuned in-house.	*Notes / observations*
☐	Each AI tool in our inventory has a named owner responsible for its use and compliance.	*Notes / observations*
☐	We review and update our AI tool inventory at least once per quarter.	*Notes / observations*

⚖️ SECTION 2 — EU AI ACT COMPLIANCE

✓	ITEM	NOTES / OBSERVATIONS
☐	We have assessed whether any of our AI systems fall into the 'high-risk' category under Annex III of the EU AI Act.	*Notes / observations*
☐	We understand which of our AI systems, if any, would be prohibited under Article 5 of the Act.	*Notes / observations*
☐	We have identified which AI use cases involve HR decisions, credit, healthcare, education, or law enforcement.	*Notes / observations*
☐	We have a designated person responsible for AI regulatory compliance.	*Notes / observations*
☐	We have reviewed the EU AI Act's transparency obligations for any customer-facing AI systems (e.g. chatbots).	*Notes / observations*
☐	We are aware of the distinction between our role as a provider, deployer, or importer under the Act.	*Notes / observations*
☐	We are tracking the EU AI Act enforcement timeline and upcoming compliance deadlines.	*Notes / observations*

🔒 SECTION 3 — DATA GOVERNANCE & GDPR

✓	ITEM	NOTES / OBSERVATIONS

☐	We have reviewed our AI vendors' data processing agreements (DPAs) and privacy policies.	*Notes / observations*
☐	We know whether personal data submitted to AI tools is retained or used for model training by the vendor.	*Notes / observations*
☐	We have a documented lawful basis under GDPR for processing personal data through each AI system.	*Notes / observations*
☐	We have conducted or updated our Records of Processing Activities (RoPA) to include AI-driven processing.	*Notes / observations*
☐	Employees and customers are informed when AI systems are used to make or influence decisions about them.	*Notes / observations*
☐	We have assessed the data residency and cross-border transfer implications of our AI vendors.	*Notes / observations*

🛡 SECTION 4 — AI SECURITY

✓	ITEM	NOTES / OBSERVATIONS
☐	We have assessed whether our customer-facing or internal AI systems are vulnerable to prompt injection attacks.	*Notes / observations*
☐	API keys and credentials for AI services are properly managed, scoped, and rotated on a regular schedule.	*Notes / observations*
☐	We have controls or policies preventing employees from submitting confidential or client data to public AI tools.	*Notes / observations*
☐	We have reviewed access controls for who can interact with AI systems and at what permission level.	*Notes / observations*
☐	We have assessed the risk of sensitive data leakage through AI tool integrations or third-party APIs.	*Notes / observations*
☐	We have a documented process for detecting, escalating, and responding to AI-related security incidents.	*Notes / observations*

📄 SECTION 5 — INTERNAL POLICY & GOVERNANCE

✓	ITEM	NOTES / OBSERVATIONS
☐	We have a written AI use policy that covers acceptable uses, prohibited uses, and consequences for misuse.	*Notes / observations*
☐	Our AI use policy has been formally communicated to all employees and is easily accessible.	*Notes / observations*
☐	We have a defined process for evaluating and approving new AI tools before teams adopt them.	*Notes / observations*
☐	Leadership has discussed and formally acknowledged AI-related risks at board or senior management level.	*Notes / observations*
☐	We have an appointed or designated person for AI governance decisions and escalations.	*Notes / observations*
☐	We conduct staff training on responsible and compliant AI use at least annually.	*Notes / observations*
☐	We have a mechanism for employees to raise concerns or questions about AI use within the organisation.	*Notes / observations*

0 – 10 ticked	**11 – 22 ticked**	**23 – 32 ticked**
High exposure. An assessment is strongly recommended before any further AI adoption.	Moderate exposure. Gaps likely in compliance or security. An assessment will identify priorities.	Strong foundation. An assessment confirms your posture and surfaces any remaining blind spots.

SUMMARY TALLY

SECTION	SCORE	PRIORITY GAPS & ACTIONS IDENTIFIED
1 — AI System Inventory	/ 6	
2 — EU AI Act Compliance	/ 7	
3 — Data Governance & GDPR	/ 6	
4 — AI Security	/ 6	
5 — Internal Policy & Governance	/ 7	
TOTAL	**/ 32**	**Overall assessment:**

REFLECTION QUESTIONS

Use these questions to prompt a short internal conversation before your discovery call. *Write your answers directly in the space provided.*

Which AI tools in your organisation concern you most from a compliance or security perspective?

Has your legal or compliance team been involved in reviewing your AI tool usage? If not, why not?

Are there AI tools being used by teams that IT and leadership are not aware of?

Has any customer or regulator asked you about your AI practices in the past 12 months?

What would happen to your operations if a key AI vendor changed their data policy tomorrow?

What is the single most urgent AI governance action your organisation should take in the next 30 days?

WHAT HAPPENS NEXT?

Share this completed checklist with Axionly before your discovery call. It helps us tailor the conversation to what matters most for your organisation.
No items need to be ticked. Blank items simply become the starting point.

Book your free
discovery call
axionly.io
No commitment. No jargon. Just clarity.