FREE TOOLKIT

The AI Governance Toolkit

Use generative AI without losing control of your data or your decisions. A GenAI risk register, an AI use policy template and ten governance controls mapped to ISO/IEC 42001, with notes for Ghanaian regulators.

Free, and no email required. Last reviewed 17 November 2026.

WHAT'S INSIDE

Three tools to govern AI from day one.

Most organisations are already using AI, often without knowing where. Start by finding it, deciding the rules and managing the risks that matter.

1

GenAI risk register

18 risks, from confidential data in public chatbots to deepfake payment fraud, each with example controls and an owner.

2

AI use policy template

Eleven sections you can adapt and adopt, written in plain language for every employee.

3

Governance controls

Ten controls that cover ISO/IEC 42001's clauses and Annex A topics, ready to grow into certification.

GENAI RISK REGISTER

18 risks to assess first.

Score each one for likelihood and impact in the CSV version, choose a treatment and record its status.

ID	Risk	What can go wrong	Example controls	ISO 42001 area
AI-R01	Confidential data entered into public AI tools	Staff paste customer records, contracts or source code into a public chatbot, and the provider stores or trains on it.	Approved tools list; enterprise plans with no training on your data; data loss prevention rules; training	A.2 Policies, A.7 Data, A.9 Use
AI-R02	Personal data processed without a lawful basis	AI use involves personal data outside the purposes people were told about.	Record AI uses in the ROPA; privacy review before launch; update privacy notices	A.5 Impact assessment, A.7 Data
AI-R03	Solely automated decisions about people	Credit, hiring or fraud decisions are made by a model with no human review and no explanation.	Human review for significant decisions; explanation process; reconsideration route (Act 843 s.41)	A.5 Impact assessment, A.9 Use
AI-R04	Wrong or invented answers	A model gives confident but false information to staff or customers.	Human review of outputs before use; limits on customer-facing use; accuracy testing	A.6 Life cycle, A.9 Use
AI-R05	Prompt injection	Hidden instructions in a document, email or web page make an AI assistant leak data or take unwanted actions.	Treat retrieved content as untrusted; limit tool permissions; filter inputs and outputs; red-team tests	A.6 Life cycle
AI-R06	Agents with too much power	An AI agent can send payments, emails or change records without approval.	Least-privilege tool access; human approval for irreversible actions; full logging	A.6 Life cycle, A.9 Use
AI-R07	Shadow AI	Teams adopt AI tools nobody approved or knows about.	AI inventory; procurement gate; network and expense monitoring; amnesty and register drive	A.3 Internal organisation, A.4 Resources
AI-R08	Bias and unfair outcomes	A model treats groups of customers or applicants unfairly.	Fairness testing before release and in production; diverse test data; impact assessment	A.5 Impact assessment, A.7 Data
AI-R09	Model drift	Accuracy degrades as real-world data changes.	Performance monitoring with thresholds; scheduled revalidation	A.6 Life cycle
AI-R10	Poisoned or poor-quality training data	Training data is manipulated, unrepresentative or unlicensed.	Data provenance records; quality checks; access control on training data	A.7 Data
AI-R11	AI supplier failure or lock-in	A provider changes terms, raises prices, has an outage or is breached.	Supplier due diligence; contract terms on data use, location and exit; fallback plan	A.10 Third parties
AI-R12	Data leaving the country	AI services process data in jurisdictions you haven't assessed.	Confirm processing locations; check transfer rules and regulator	A.7 Data, A.10 Third

			approvals	parties
AI-R13	Intellectual property problems	Outputs reproduce copyrighted material, or inputs disclose your trade secrets.	Usage rules on IP; review of published outputs; supplier IP terms	A.2 Policies, A.9 Use
AI-R14	Insecure AI-generated code	Code from AI assistants introduces vulnerabilities.	Code review and security testing for all code, whatever its source	A.6 Life cycle
AI-R15	Deepfake fraud and social engineering	Attackers clone a leader's voice or video to authorise payments.	Call-back verification for payments and changes; staff awareness	A.9 Use
AI-R16	No transparency to customers	Customers don't know they are dealing with AI, or how it affects them.	Disclosure when AI is used; plain-language explanations	A.8 Information for interested parties
AI-R17	AI incidents not reported	Model failures or AI-related breaches aren't recognised as incidents.	Add AI incident types to the incident process; regulator reporting triggers (for example BoG CISD para 115)	A.6 Life cycle, A.8 Information
AI-R18	Over-reliance and skills loss	Staff stop checking outputs or lose the skills to do so.	Training on limits of AI; spot checks; keep accountability with people	A.4 Resources, A.9 Use

AI USE POLICY TEMPLATE

A policy your staff will actually read.

Adapt each section to your organisation, then have it approved by management and acknowledged by staff.

1. **Purpose and scope.** Why the policy exists and who it covers: staff, contractors and anyone using AI on the organisation's behalf.
2. **Approved tools.** Only tools on the approved list may be used for work. Anyone can request a new tool through the approval process.
3. **What you must never enter.** Customer personal data, special personal data, passwords and keys, unreleased financial information or confidential contracts, unless the tool is approved for that data.
4. **Check before you use.** You are responsible for anything AI helps you produce. Check facts, figures, code and citations before relying on or sharing them.
5. **Decisions about people.** AI may support but not solely make significant decisions about customers, applicants or staff without approved human review.
6. **Be transparent.** Tell customers when they are interacting with AI. Label AI-generated content where it could mislead.
7. **Security.** Sign in with company accounts only. Don't connect AI tools to company systems, email or files without approval.
8. **Report problems.** Report suspected data leaks, harmful outputs or misuse through the normal incident process straight away.
9. **Training.** Complete AI awareness training before using approved tools, and refresh it every year.
10. **Breaches and exceptions.** Breaking this policy may lead to disciplinary action. Exceptions need written approval from the CISO.
11. **Review.** The policy owner reviews this policy at least once a year and after significant changes in AI use or regulation.

GOVERNANCE CONTROLS

Ten controls, mapped to ISO/IEC 42001.

ISO/IEC 42001:2023 is the certifiable standard for AI management systems. These references are to its clauses and Annex A topic areas; buy the standard for the full requirements.

Control	What to do	ISO/IEC 42001
Know where AI is used	Keep an AI inventory: every AI system you build, buy or embed, its owner, purpose, data and risk level.	Clause 4, A.4
Set the rules	Adopt an AI policy and an acceptable use policy for generative AI.	Clause 5.2, A.2
Name who is accountable	Assign roles for AI risk, approval and oversight, up to the Board.	Clause 5.3, A.3
Assess the impact	Run an AI impact and risk assessment before launch and after material change.	Clauses 6.1, 8.2 to 8.4, A.5

Control the life cycle	Define requirements, testing, validation, release approval and monitoring for each system.	Clause 8.1, A.6
Govern the data	Record data provenance, quality, labelling and permitted use.	A.7
Tell people	Explain to users and affected people when and how AI is used.	A.8
Use AI responsibly	Define intended use, human oversight and limits for each system.	A.9
Manage suppliers	Check AI providers and set contract terms on data, security and exit.	A.10
Check and improve	Monitor performance, audit the AI management system and fix what you find.	Clauses 9 and 10

GHANA NOTES

Where Ghanaian rules already touch AI.

1

Data Protection Act (Act 843)

People can require that significant decisions about them are not based solely on automated processing, and can ask for reconsideration within 21 days (s.41). AI that processes personal data must meet all the Act's principles.

2

Bank of Ghana CISD 2026

Regulated financial institutions need an AI/ML governance and control framework (para 114 and Annexure E), must report their AI inventory and model incidents quarterly, and must notify serious AI incidents immediately (para 115).

3

Board approval

Under the CISD, adopting digital innovations, including AI, goes to the Board before implementation (para 98).

This toolkit is general guidance, not legal advice. ISO/IEC 42001 references are to clause and Annex A topic areas only; no standard text is reproduced. Check the current law and regulator guidance for your situation. Last reviewed 17 November 2026.

Need help putting this into practice? Assurelo runs gap assessments, readiness programmes and internal audits. Email hello@assurelo.com or visit assurelo.com to book a free 30-minute call.