SUMMIT BRIDGE

AI Governance Starter Pack

A 36-point readiness assessment across 7 governance domains, aligned to ISO/IEC 42001, the EU AI Act and UK regulator expectations.

How to use this checklist

Work through each section with your risk, compliance and AI leadership team. Mark each item Yes, Partial, or No. A pattern of Partial or No answers in any section signals where governance investment is needed before scaling AI. Aligns to ISO/IEC 42001, EU AI Act, NIST AI RMF and UK regulator guidance (ICO, FCA, MHRA, Ofcom).

Scoring guide: 30+ Yes = certification-ready - 20-29 Yes = foundations in place - Under 20 Yes = material exposure.

1. Principles & Policy

- [ ] We have a documented AI policy approved at executive or board level.
- [ ] The policy covers fairness, transparency, human oversight, accountability and safety.
- [ ] An acceptable-use policy exists for generative AI tools (ChatGPT, Copilot, Claude, Gemini).
- [ ] Disclosure rules for AI-generated content are defined.
- [ ] The policy is reviewed at least annually and version-controlled.

2. Risk Assessment

- [ ] Every AI use case is classified using a risk-tiering model.
- [ ] Tiering aligns to EU AI Act categories (prohibited, high, limited, minimal).
- [ ] AI impact assessments are completed before deployment.
- [ ] DPIAs are completed where personal data is processed.
- [ ] An AI bill of materials (models, data, prompts, consumers) is maintained.

3. Standards & Controls

- [ ] Pre-deployment evaluation against representative datasets is required for high-risk systems.
- [ ] Red-teaming covers prompt injection, jailbreaks, and data exfiltration.
- [ ] Human-in-the-loop review is defined for high-impact decisions.
- [ ] Inputs, outputs and decisions are logged with appropriate retention.
- [ ] A documented rollback plan exists for production AI systems.
- [ ] Controls are mapped to ISO/IEC 42001 and NIST AI RMF function libraries.

4. Roles & Accountability

- [ ] Each AI system has a named accountable business owner.
- [ ] An executive sponsor is identified (COO, CDO, CTO, or equivalent).
- [ ] A named AI lead owns the governance framework.
- [ ] A cross-functional AI steering or ethics group meets regularly.
- [ ] Escalation routes into existing risk and audit committees are documented.

5. Monitoring & Incident Response

- [ ] Performance monitoring covers accuracy, latency and hallucination rates.
- [ ] Behavioural monitoring covers bias, toxicity and prompt-injection attempts.
- [ ] Business-outcome monitoring tracks the KPI the AI was deployed to move.
- [ ] AI-specific triggers exist in the IT/security incident playbook.
- [ ] Severity thresholds and notification obligations (UK GDPR, EU AI Act) are defined.
- [ ] Post-incident reviews feed back into controls and policy.

6. Assurance & Review

- [ ] Model cards or system cards exist for production AI systems.
- [ ] A live register of AI systems in use is maintained.
- [ ] A supplier assurance pack is used for third-party AI tools.
- [ ] Internal audit has visibility of AI governance evidence.
- [ ] Annual external or independent review is scheduled.

- [ ] Evidence is mapped to ISO/IEC 42001 clauses ready for certification if needed.

7. People & Culture

- [ ] Role-specific AI training is delivered to staff using AI in their work.
- [ ] Leaders receive briefings on AI risk and regulation at least annually.
- [ ] A confidential channel exists for staff to raise AI concerns.
- [ ] Whistleblowing policy explicitly covers AI-related harms.

Your score: ____ / 36 Yes **Date assessed: _____**

What next?

If your score reveals gaps in policy, risk tiering, controls or assurance, Summit Bridge can help you turn this checklist into a board-ready governance programme.

Policy & principles gap
Stand up a board-approved AI policy, acceptable-use rules and disclosure standards.
See: AI Governance Framework - summit-bridge.co.uk/ai-governance-framework

Risk & controls gap
Implement risk-tiering, impact assessments, red-teaming and human-oversight controls.
See: AI Governance Framework - summit-bridge.co.uk/ai-governance-framework

Assurance & monitoring gap
Establish AI register, model cards, monitoring and incident response aligned to ISO/IEC 42001.
See: Book a scoping call - info@summit-bridge.co.uk

Book a complimentary 30-minute governance health check

No obligation. No sales pitch. Just honest, informed guidance on closing your highest-impact governance gaps in the next 90 days.

info@summit-bridge.co.uk - 07802 707 423
summit-bridge.co.uk - linkedin.com/company/summit-bridge-ai

Typical engagement range: GBP 15,000 - GBP 85,000 depending on scope, duration and number of business units involved.