

One-page overview

v1.0 · 2 October 2026 · aibcf.org

Govern

- GV . 1 The organization's position on AI, including the goals, opportunities and limits for its use, is documented.
- GV . 2 Roles and responsibilities concerning AI are assigned and documented.
- GV . 3 Personnel that uses AI is trained on its responsible, safe and effective use. Training content and attendance is recorded.
- GV . 4 AI risks are registered and reviewed at least annually as part of the organization's risk management process.

Comply

- CM . 1 Relevant laws and regulatory requirements are known, documented and managed.
- CM . 2 AI-generated content and AI interactions are marked as AI when published or used externally.
- CM . 3 High-risk uses of AI are logged, human oversight is conducted, and affected subjects are informed.
- CM . 4 A Fundamental Rights Impact Assessment is performed before high-risk use of AI.

Register

- RG . 1 Deployed AI systems and providers are registered and classified.
- RG . 2 For each AI use, its purpose is registered. Where AI acts autonomously (agents, scripts or automations), what it does is described.
- RG . 3 For each AI use, proportionality of the AI system to the task is weighed against documented alternatives.
- RG . 4 At decommissioning, AI systems follow the organization's regular offboarding process. Access and accounts are removed, and the AI register is updated.
- RG . 5 AI risks and data exposure to training are considered in privacy assessments of new and existing suppliers.

Access

- AC . 1 An access review is conducted before an AI system inherits users' access rights.
- AC . 2 AI systems with separate access rights are given a named identity, and these rights are limited to a documented scope.
- AC . 3 Each autonomous AI system is assigned a named owner who is accountable for its actions.
- AC . 4 Access rights for AI systems are granted according to the organization's access control model.

Track

- TR . 1 Key performance indicators for deployed AI systems are established to measure their effectiveness.
- TR . 2 Internal feedback regarding deployed AI usage is collected and reviewed.
- TR . 3 Errors in AI output are logged and communicated to strengthen awareness of AI risk.