

AGS

AUTOMATED GOVERNANCE SYSTEMS

Enterprise-Wide AI & Automation Governance

A practical framework for keeping AI initiatives technically sound, ethically responsible and aligned with business objectives across three tiers: Corporate, PMO and Operational.

Presented by Andy Wake · Automated Governance Systems Ltd (AGS)

Version 2.0 · Updated October 2026 (supersedes v1.0)

Three-tier governance structure

Governance scales across strategic, programmatic and operational levels. Each tier has distinct responsibilities, but all three share one risk appetite, one evidence trail and one accountable owner per AI system.

1. CORPORATE

Strategy

- Policy and direction
- Risk appetite
- Ethical standards
- AI system inventory and board reporting

2. PMO

Change

- Portfolio management
- Project oversight
- Change assurance
- Impact assessments before approval

3. OPERATIONAL

Delivery

- Implementation
- Monitoring and incident handling
- Human oversight in daily use
- Continuous improvement

New in v2.0: AI inventory, impact assessment and human-oversight duties now sit explicitly at each tier, reflecting ISO/IEC 42001 and the EU AI Act deployer obligations.

Corporate governance: strategic alignment

Corporate governance sets the tone from the top, aligning AI use with strategy and establishing clear accountability.

AI management system

ISO/IEC 42001:2023 AI management system · ISO/IEC 38507:2022 governance implications of AI for boards

Risk management

ISO 31000:2018 enterprise risk · ISO/IEC 23894:2023 AI risk guidance · NIST AI RMF 1.0 and Generative AI Profile (NIST AI 600-1)

Information management

ISO/IEC 38500 governance of IT · ISO/IEC 24143 information governance

Quality, security & privacy

ISO 9001 quality (revision in progress) · ISO/IEC 27001:2022 security · ISO/IEC 27701:2025 privacy, now a standalone management system

Board actions: approve an AI policy and risk appetite, appoint an accountable executive, and require a live register of every AI system in use.

PMO governance: portfolio control

PMOs evaluate AI initiatives against the enterprise risk appetite, and ensure privacy, security and impact are assessed before anything goes live.

Risk management	ISO 31000, PRINCE2 risk theme, ISO/IEC 23894 for AI-specific risks
Portfolio & information	ISO/IEC 38500, ISO 21504 portfolio management
Quality	ISO 10006 quality in projects
Security	ISO/IEC 27005:2022 information security risk management
Privacy & safeguarding	ISO/IEC 29134 DPIA guidelines; UK GDPR DPIAs where processing is high risk
AI impact (new)	ISO/IEC 42005:2025 AI system impact assessment; EU AI Act risk classification at gate 0

Gate rule: no AI project passes approval without a named owner, a risk classification, an impact assessment and a defined route for human review and override.

Operational governance: execution & monitoring

Operational governance embeds good practice in daily work, so AI systems stay secure, compliant and valuable after go-live.

Risk management

ISO/IEC 27005 and NIST AI RMF (Govern, Map, Measure, Manage) for day-to-day risk mitigation.

Information & quality

ISO/IEC 20000-1 service management and ISO 9004 for sustained success; model and data drift checks.

Security & privacy

ISO/IEC 27002:2022 controls and ISO/IEC 29100 privacy framework; NCSC guidance and the UK AI Cyber Security Code of Practice.

Human oversight & incidents

Named reviewers who can pause, correct or override; logging, incident reporting and post-incident learning.

Measure what matters: accuracy, timeliness, fairness across groups, complaints, overrides and unintended effects, reviewed on a fixed cycle.

Cross-cutting principles

AI governance is not just compliance; it is how organisations keep public and customer trust. These themes apply at every tier.

Transparency & explainability

People can understand how AI-supported decisions were reached, and are told when they are dealing with AI.

Accountability & auditability

Every AI system has a clear owner and an audit trail of decisions, evidence and changes.

Human-centred, ethical design

People first: fairness, accessibility (WCAG 2.2) and meaningful human review.

Lifecycle management

Plan, Build, Run, Monitor, Retire, with governance checkpoints at each stage.

Data quality & provenance

Data is lawful, representative, current and traceable to its source.

Proportionality

Controls match the level of risk; never automate just because it is possible.

Ethical AI & regulatory landscape (as at October 2026)

Regulators and standards bodies have moved quickly since v1.0. Organisations need frameworks that adapt as rules change.

Standards

ISO/IEC 42001:2023 AI management system
ISO/IEC 23894:2023 AI risk
ISO/IEC 42005:2025 impact assessment
ISO/IEC 42006:2025 certification bodies
BS 8611:2023 ethical design of robots
NIST AI RMF and NIST AI 600-1

UK law & guidance

UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, which changes the automated decision-making rules
ICO guidance on AI and data protection
UK AI Security Institute; AI Cyber Security Code of Practice

EU & international

EU AI Act in force since August 2024: prohibitions apply from February 2025; general-purpose AI duties from August 2025; most high-risk duties phased from August 2026, with EU proposals to delay some dates
OECD AI Principles (updated 2024); UNESCO Recommendation; Council of Europe AI Convention

Check before relying: EU AI Act dates for high-risk systems are subject to proposed changes, and UK reforms are being commenced in stages. Confirm current status with official sources or legal advisers.

What has changed since v1.0

The key developments that should shape your governance programme now.

Certifiable AI governance

ISO/IEC 42001 certification is now available from accredited bodies, supported by ISO/IEC 42006.

Impact assessment standard

ISO/IEC 42005 gives a consistent method for assessing effects on people and society.

EU AI Act obligations live

Banned practices, AI literacy duties and general-purpose AI rules already apply.

UK data reform

The Data (Use and Access) Act 2025 relaxes some automated decision limits but keeps safeguards: information, human review and challenge.

Generative and agentic AI

AI agents that take actions need tighter limits: step caps, spending caps, approval before external actions.

Privacy standard refreshed

ISO/IEC 27701:2025 can now be certified on its own, without ISO/IEC 27001.

Implementation roadmap

0-30 days

Set up a cross-functional AI governance board with a clear mandate. Build the AI system inventory and classify each system by risk.

30-90 days

Gap analysis against ISO/IEC 42001 and the EU AI Act; agree AI policy, risk appetite and AI literacy training.

90-180 days

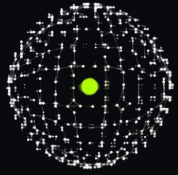
Add governance checkpoints at key lifecycle decisions: impact assessments, DPIAs, risk registers, human-oversight design.

Ongoing

Monitoring, quality audits, incident reviews and management review; prepare for certification where it adds value.

Success factors

Executive sponsorship · Clear roles and responsibilities · Regular monitoring and review · Continuous improvement mindset



AGS

AUTOMATED GOVERNANCE SYSTEMS

Start with one accountable step.

AGS helps organisations build an AI inventory, assess risk and impact, and keep an audit trail with human review built in.

contact@automatedgovernancesystems.com

automatedgovernancesystems.com

This document is general guidance, not legal, regulatory or certification advice. References reflect AGS's understanding as at October 2026; verify current requirements with official sources and qualified advisers before relying on them.