

The Governance Landscape

Frameworks create expectations. Practical oversight turns them into accountable action.

AI governance is shaped by standards, risk models, security guidance and regulation — not one rulebook. For UK businesses, the question is where written requirements end and daily oversight begins.

01 GLOBAL STANDARD ISO/IEC 42001

A management-system structure for AI. Translate its requirements into named responsibilities, documented decisions and review cycles.

02 RISK LANGUAGE NIST AI Risk Management Framework

A common language to identify and discuss AI risk. Connect those principles to decisions, owners and measurable oversight.

03 AUTONOMOUS AGENTS Singapore's agentic AI guidance

Emerging guidance on autonomy. Set authority boundaries, intervention routes and evidence requirements for agent workflows.

04 REGULATORY FOUNDATION EU AI Act

Risk-based obligations for systems in scope, including some UK uses. Map applicable systems and organise governance evidence accordingly.

05 SECURITY & ENGINEERING OWASP Top 10 for LLM Applications

Prompt injection, sensitive-data disclosure and unsafe agent behaviour belong in governance reviews alongside technical safeguards.

06 LEADERSHIP & EXECUTION AI governance handbooks

Leadership guidance sets direction; operational governance clarifies who owns each system, what gets reviewed and when to intervene.

WHERE TRESTANO FITS

Trestano focuses on the operational layer: ownership, oversight, evidence and authority boundaries for AI systems, including autonomous agents. Governance should be something your team can act on, not just a framework on a shelf.