OPERATIONAL AI GOVERNANCE: TURNING VENDOR OVERSIGHT INTO STRATEGIC ADVANTAGE

By Theodora Monye

Part of the Complete AI Governance Toolkit

Version 1.0 | March 2026

THE BIG IDEA

AI adoption is accelerating across regulated industries, but the real bottleneck is not technology, it is governance. Vendor oversight, often treated as a compliance obligation, is in fact the operational backbone of responsible AI adoption.

Drawing on lessons from life sciences, this article introduces a structured governance framework that transforms fragmented vendor data into actionable intelligence. By aligning qualification standards and risk assessment with ICH E6(R3), FDA draft guidance (2025), EMA reflection paper (2024), the EU AI Act (2024), and ISO/IEC 42001/23894, organisations can move beyond compliance to achieve faster decisions, reduced risk, and stronger strategic partnerships.

WHY VENDOR GOVERNANCE MATTERS

A global pharmaceutical organisation faced a familiar challenge: vendor information scattered across silos, spreadsheets, and systems. With more than 2,000 vendor–solution relationships, study teams struggled to identify qualified partners quickly.

This problem is not unique to life sciences. Financial services, healthcare providers, energy companies, and public sector organisations all face similar issues: fragmented oversight, inconsistent qualification, and rising regulatory scrutiny of AI systems.

THE FRAMEWORK

The organisation developed an Operational AI Governance Framework with three pillars:

1. Structured Data Model

A consolidated Global Vendor and Solution Index capturing identity, taxonomy, study context, qualification status, and provenance.

2. Qualification Standards

- Tiered approach: vendor-level, solution-level, and study-level qualification.
- Aligned with GCP/GMP expectations and ISO/IEC 42001 principles of accountability and lifecycle risk management.

3. Risk Assessment Integration

- Risk scoring methodology covering compliance history, data security, validation status, performance, and strategic importance.
- Explicitly aligned with ISO/IEC 23894 for AI risk management.

RESULTS

The framework delivered measurable impact:

- **Visibility:** A centralised repository replaced fragmented spreadsheets, providing real-time oversight of 2,000+ vendor–solution relationships.
- **Decision Quality:** Standardised qualification criteria enabled consistent, risk-based vendor selection aligned with ICH E6(R3) and EU AI Act requirements.
- **Efficiency:** Duplicate assessments were eliminated, accelerating study start-up timelines.
- **Strategic Outcomes:** Auditable documentation satisfied FDA and EMA expectations, while performance insights supported vendor consolidation and strategic partnerships.

LESSONS FOR LEADERS

Four success factors stand out:

1. **Executive Sponsorship:** Cross-functional leadership alignment was essential.
2. **Iterative Approach:** Starting with Excel enabled rapid adoption before scaling to database integration.
3. **Standardisation Before Automation:** Definitions and taxonomy were established before building technical infrastructure.
4. **Change Management:** Stakeholder engagement ensured adoption and ongoing data quality.

Cross-Industry Implications

This framework is broadly applicable:

- **CROs:** Demonstrating qualification rigour to sponsors and regulators.
- **Medical Device Firms:** Oversight of AI vendors in product development and post-market surveillance.
- **Healthcare Providers:** Risk management for AI diagnostic tools under HIPAA and the EU AI Act.
- **Financial Services:** Vendor oversight for AI-driven risk models and compliance systems.

REGULATORY EVOLUTION

The landscape is shifting rapidly, requiring operational readiness:

- **FDA Draft Guidance (2025):** Adaptive AI algorithms require monitoring and change control.
- **EU AI Act (2024):** High-risk AI systems demand conformity assessment and documentation.
- **EMA Reflection Paper (2024):** Lifecycle risk management for AI in clinical research.
- **ICH E6(R3):** Enhanced vendor oversight and risk-based monitoring expectations.
- **ISO/IEC 42001 & 23894:** Global standards for AI management and risk governance.

CONCLUSION

Effective AI governance requires operational rigour, not just regulatory compliance. By transforming fragmented vendor data into structured intelligence, organisations can:

- Make faster, better decisions.
- Reduce risk through consistent qualification and oversight.
- Strengthen compliance with auditable documentation aligned to global standards.

As AI becomes embedded across industries, vendor governance becomes AI governance. The path from compliance burden to strategic advantage starts with making governance operational, not aspirational.