AI IN FINANCE | AI GOVERNANCE · INTERNAL CONTROLS · DATA PRIVACY

AI governance for CFOs: a one-page policy for the finance function

Published 9 October 2026 · The Finance Intellect · Source-based summary

Every finance team using AI needs simple rules: which tools are allowed, what data can go in, who reviews the output and what is logged. This one-page policy draws on NIST, ISO/IEC 42001 and the financial regulators' guidance.

Global reference

- Scope: Finance functions in any sector
- Frameworks: NIST AI Risk Management Framework; ISO/IEC 42001 (AI management systems)
- Regulatory guidance: MAS Guidelines on AI Risk Management (2026); CBUAE AI guidance note (2026)

The one-page policy

- Purpose: AI is used to improve speed and quality; people remain accountable for results.
- Approved tools: only tools on the approved list, reviewed by IT security and legal.
- Data: no confidential, personal or price-sensitive data in public AI tools; enterprise tools only, with no training on our data.
- Inventory: every AI use case is recorded with an owner, purpose, data used and risk rating.
- Risk rating: high where output affects financial statements, tax filings, payments or customers.
- Human review: high-risk output is reviewed and signed off before use.
- Evidence: prompts, outputs and approvals for high-risk uses are kept for audit.
- Vendors: AI suppliers give audit rights, data location and an exit plan.
- Training: staff complete AI training before using approved tools.
- Incidents: errors or data leaks are reported within 24 hours.
- Review: the policy and inventory are reviewed every year.

Why these elements

- Regulators such as MAS and the CBUAE start with board accountability and an inventory.
- NIST's framework is built on four functions: govern, map, measure and manage.
- ISO/IEC 42001 lets a company certify its AI management system.
- External auditors increasingly ask how AI-produced numbers are controlled.

Links to existing controls

- Treat AI tools like spreadsheets that matter: version control, review and access limits.
- Fold AI risks into the risk register, not a separate silo.

- Apply the same segregation of duties to AI agents as to staff.

What to do now

- Adopt the policy, even in draft, this quarter.
- Build the inventory: most teams find more AI use than expected.
- Brief the audit committee once a year.

Our take

Governance should make safe AI use easy, not block it. One page that people follow beats a long policy nobody reads.

Sources

- NIST: AI Risk Management Framework
- ISO: ISO/IEC 42001 Artificial intelligence management system
- MAS: Guidelines on Artificial Intelligence Risk Management for Financial Institutions
- CBUAE: Guidance note on responsible use of AI in the financial sector

Important. This summary is for general information and is not legal, regulatory or financial advice. It is based on public NIST, ISO, Monetary Authority of Singapore and Central Bank of the UAE publications, together with adviser commentary, and may be incomplete or out of date. The official publications prevail; check the official source before acting.

ABOUT THE FINANCE INTELLECT

A Finance Knowledge & Resource Platform by Neocor Consultancy. Weekly tax and finance insights, Excel templates, calculators and a learning hub for finance leaders and professionals.

Platform: thefinanceintellect.com | **Owner:** neocorconsultancy.com