Daniel Young Advisory
FRACTIONAL CIO · CYBERSECURITY · AI GOVERNANCE · DUBAI, UAE

daniel@danielpyoung.com
danielpyoung.com
+971 58 563 9178

CASE STUDY · VENDOR GOVERNANCE & THIRD-PARTY RISK

When no one owns the vendor estate - building a vendor governance model that satisfied the regulator, delivered 10% annual savings, and gave the board clear visibility of supplier risk

50%	20+	10%	0
REDUCTION IN ACTIVE VENDOR COUNT	CONTRACTS REVIEWED AND RENEGOTIATED	ANNUAL COST SAVINGS, YEAR-ON-YEAR	AUDIT FINDINGS, THIRD-PARTY MANAGEMENT

THE CHALLENGE

An accumulated vendor estate with no single owner

The firm's vendor relationships had grown organically - each contract signed to solve an immediate need, without a consolidated view of the estate as a whole. The result was overlapping responsibilities between suppliers, SLAs misaligned with operational and regulatory timelines, rising costs without a clear owner, and no structured approach to security obligations across the supply chain.

Under FCA rules, a regulated firm remains fully accountable for the quality and security of any service it outsources. That accountability never transfers; the regulator will come to the firm, not the supplier.

Without a governance model, the firm was carrying risk it could not see, quantify, or report on - a pattern increasingly visible in DFSA- and FSRA-regulated firms as outsourcing grows.

THE RESULT

From 30 vendors to a governed, board-visible model

The firm moved from an unmanaged estate of 30 vendors to a consolidated, board-visible governance model with clear accountability at every level.

The vendor count was reduced by 50% through rationalisation, with savings delivered year-on-year from the first contract cycle - reaching 10% annually against an AED 20M base.

SLAs were standardised against operational and regulatory timelines, and security obligations made consistent across all supplier relationships.

External audits produced no findings related to third-party management throughout. For the first time, the board had a clear, quantified view of supplier dependency and exposure - and documentation to support that position under regulatory scrutiny.

The framework was later extended to govern generative AI suppliers, providing a controlled pathway for adoption rather than blanket restriction.

THE PROGRAMME

Third-party risk is not a compliance exercise - it is a board-owned account of what the firm has agreed to, what it can demonstrate, and what it would do if a critical supplier failed

VENDOR INVENTORY
Built a consolidated register of all active relationships, mapping service dependencies, contract terms, and regulatory classification.

CONTRACT REVIEW
Reviewed all 20+ contracts against operational requirements, regulatory obligations, and security standards to expose gaps and inconsistencies.

RENEGOTIATION
Renegotiated agreements to standardise SLAs and embed security and data-handling obligations across all third-party relationships.

ACCOUNTABILITY & OWNERSHIP
Established clear ownership at contract level - each supplier relationship assigned a named owner with documented scope and escalation path.

BOARD GOVERNANCE
Consolidated third-party risk into a single governance model with regular board reporting - a clear, quantified view of supplier exposure and remediation status.

AI GOVERNANCE INTEGRATION
Extended the framework to cover generative AI suppliers as adoption reached board level - new vendor categories entering a controlled, documented approval process.

Each component fed into a single governance model - reviewed on a fixed cadence, updated as the supplier landscape changed, and structured to produce evidence suitable for regulatory scrutiny.

AI & VENDOR RISK

AI adoption creates a new category of vendor risk. Generative AI tools introduce data-handling obligations, third-party dependencies, and failure modes that standard vendor contracts do not address. Firms without an existing vendor governance framework cannot reliably assess what AI adoption adds to their third-party risk profile. Extending a governance model to cover AI suppliers - with defined authorisation workflows, data classification requirements, and contractual security obligations - is a structured, defensible approach. Building that model from scratch when AI adoption is already in progress is significantly harder.

DIFC & ADGM-REGULATED FIRMS

DFSA- and FSRA-regulated firms in DIFC and ADGM face the same foundational requirement: the regulated firm remains fully accountable for any service it outsources, regardless of what the contract says.

- Map the vendor estate and classify relationships by regulatory obligation and operational risk.
- Standardise SLAs and embed security and data-handling obligations across all third-party contracts.
- Build board-level governance with regular reporting and evidence suitable for regulatory scrutiny.
- Extend coverage to generative AI suppliers before adoption reaches board level.

The approach above was built in an FCA-regulated environment and translates directly to DFSA- and FSRA-regulated firms in DIFC and ADGM.

> *Engagements typically start with a vendor inventory diagnostic: mapping the estate, classifying regulatory exposure, and producing a board-ready view of current gaps and remediation priorities.*