ISO 37001 for Mid-Market Companies:

What Leadership Needs to Know

A practical reference for finance and compliance leaders managing anti-bribery risk

fortifai

What ISO 37001 Is and Why It Matters

ISO 37001 is the international standard for Anti-Bribery Management Systems — ABMS. Published in 2016, it provides the governance framework for implementing, maintaining, and improving controls designed to prevent, detect, and respond to bribery across your organisation and its third-party relationships.

Certification is voluntary. The anti-bribery laws ISO 37001 helps you comply with are not.

The legal landscape mid-market companies need to understand: The UK Bribery Act, the US Foreign Corrupt Practices Act, Norwegian anti-corruption law under Straffeloven, and the OECD Anti-Bribery Convention all create legal exposure for companies — regardless of size. The UK Bribery Act is particularly significant: it applies to any company carrying on business in the UK, creates a strict liability corporate offence of failing to prevent bribery, and the only complete defence is demonstrating that adequate procedures were in place. **ISO 37001 is explicitly recognised as evidence of adequate procedures.**

For mid-market companies with government contracts, international operations, or significant third-party relationships, the question is not whether bribery risk exists — it is whether it is documented, managed, and auditable.

Why ISO 37001 is increasingly a commercial requirement

- Public sector procurement teams are embedding it in tender qualification criteria
- Large enterprise customers are pushing anti-corruption due diligence down their supply chains
- Banks and investors are asking about governance frameworks during due diligence
- International partners and joint ventures require documented anti-bribery controls as a condition of doing business

fortifai

What ISO 37001 Covers

The standard addresses three distinct bribery risk vectors:

Risk Type	What It Means	Where It Lives in Your Organisation
Bribery by the organisation	Employees, agents, or contractors paying bribes to obtain business or advantage	Sales team, agents, intermediaries, procurement decisions involving public officials
Bribery of the organisation	Third parties attempting to bribe your employees	Procurement, contract awards, regulatory approvals
Third-party facilitation	Agents or partners using your company as a vehicle for corrupt payments	Agent commissions, consultant fees, joint venture distributions

For most mid-market companies, the **third-party facilitation risk** is the most significant and the least well-controlled. Agent commissions that are disproportionate to the services provided, consultant fees paid around contract award timing, and joint venture distributions in higher-risk jurisdictions are all classic bribery vectors — and all run through finance.

Why This Is Primarily a CFO Problem

Of all the governance standards covered in this series, ISO 37001 has the strongest CFO ownership profile. The highest-risk controls sit in the finance function:

Financial Approval Controls

Unusual payments, payments to third parties in higher-risk jurisdictions, commission payments, and facilitation payments all require documented approval processes with appropriate thresholds and escalation procedures.

Gifts and Hospitality Register

A documented policy with monetary thresholds and a register of gifts given and received. Finance owns the register and the approval process. The register must be current and retrievable — not a spreadsheet nobody updates.

Third-Party Due Diligence

Agents, intermediaries, and consultants who represent your company in commercial or public sector engagements require documented due diligence before engagement. Finance typically owns or co-owns these relationships through contract approval and payment processes.

Political Contributions and Charitable Donations

Both are high-risk bribery vectors requiring documented approval at an appropriate level and periodic review. Finance approves the payments and maintains the records.

Whistleblower Channel

ISO 37001 requires a confidential reporting mechanism for bribery concerns. Finance and compliance typically manage the process and the investigation response.

What ISO 37001 Requires From You as Leadership

ISO 37001 requires top management to demonstrate active leadership of the anti-bribery function — not just policy approval but visible commitment, resource allocation, and accountability for outcomes. The standard includes a specific requirement for governing body oversight that makes board-level involvement explicit.

These are the key approvals and actions ISO 37001 requires from executive leadership:

What You're Signing or Owning	When	What the Auditor Checks
Anti-Bribery Policy	Before certification, reviewed annually	Signed version, approval date, version history, top management sign-off
ABMS Scope Document	Start of implementation	Which entities, activities, and geographies are included
Bribery Risk Assessment	Before controls implemented, reviewed annually	Documented methodology, risk scoring, named owners, signed off
Third-Party Due Diligence Decisions	Before engaging higher-risk third parties	Due diligence completed, risk level assessed, approval documented
Gifts and Hospitality Register	Maintained continuously	Current, complete, approvals documented above threshold
Financial Control Framework	Before certification	Approval thresholds, segregation of duties, unusual payment controls
Whistleblower Reports and Investigation Outcomes	Following any report	Documented investigation, outcome, corrective action, sign-off
Management Review	Annually minimum	Minutes, decisions, action items, governing body sign-off
Annual Compliance Report to Board	Annually	Board evidence of anti-bribery oversight — not just awareness

The governing body oversight requirement is the most important distinction from other standards. ISO 37001 is one of the few management system standards that explicitly requires the board — not just management — to exercise oversight. The board must approve the anti-bribery policy, receive regular compliance reports, and demonstrate that it exercises genuine oversight rather than rubber-stamping management decisions. This requires documented board minutes that show substantive engagement with anti-bribery risk and performance.

The third-party due diligence sign-off is the highest-risk CFO decision in the system. When your company engages an agent in a higher-risk market, the ISO 37001 requirement is that the decision to engage — and the due diligence conducted — is documented with a named approver. If that agent subsequently facilitates a bribe, the documented due diligence decision is what determines whether your company has a defensible position under the UK Bribery Act or equivalent legislation.

High-Level Implementation Plan

Phase 1 — Foundations and Risk Assessment

- Define ABMS scope — which entities, geographies, and business activities are included
- Appoint anti-bribery compliance function — with named board-level sponsor
- Complete bribery risk assessment — identify all activities and relationships with bribery exposure
- Map third-party relationships — agents, intermediaries, consultants, joint venture partners, by risk level
- Map high-risk geographies — use recognised indices (Transparency International CPI) to identify elevated risk markets
- Select certification body and confirm audit dates
- Set up document management system with version control

Phase 2 — Policy and Procedure Documentation

- Draft and approve Anti-Bribery Policy — board sign-off required
- Draft Gifts and Hospitality Policy — monetary thresholds, approval process, register requirement
- Draft Third-Party Due Diligence Procedure — risk-tiered approach, required documentation by risk level
- Draft Financial Controls Procedure — payment approval thresholds, unusual payment escalation, segregation of duties
- Draft Political Contributions and Charitable Donations Policy — approval process, register
- Draft Whistleblower and Investigation Procedure — confidential reporting, investigation process, outcome documentation
- Obtain formal sign-off from named approver and board for each documen

Phase 3 — Financial Controls Implementation

- **Payment Approval Thresholds**

  Review and update payment approval thresholds — ensure appropriate segregation of duties

- **Gifts and Hospitality Register**

  Implement gifts and hospitality register — build and activate

- **Agent and Consultant Commissions**

  Review agent and consultant commission structures — document rationale for all current arrangements

- **Unusual Payment Escalation**

  Implement unusual payment escalation procedure — define what triggers escalation and to whom

- **Political and Charitable Donations**

  Review political and charitable donation records — confirm all meet policy requirements

- **Contract Templates**

  Update contract templates — include anti-bribery representations and warranties for all third-party agreements

Implementation Phases 4–8

Phase 4 — Third-Party Due Diligence

- Conduct due diligence on all existing higher-risk third parties — agents, intermediaries, consultants
- Document due diligence findings and approval decisions with named owner
- Send anti-bribery questionnaires to higher-risk suppliers and partners
- Build third-party onboarding procedure — due diligence required before any new higher-risk third party is engaged
- Build periodic review schedule — higher-risk third parties reviewed annually

Phase 5 — Training and Awareness

- Deliver anti-bribery training to all staff — record completions
- Deliver enhanced training to higher-risk roles — sales, procurement, finance, agents
- Board and senior management anti-bribery training — completion records
- Activate whistleblower channel — confirm confidentiality and accessibility
- Test whistleblower channel — simulated report, documented response

Phase 6 — Internal Audit and Management Review

- Complete internal audit — auditor independent of anti-bribery function
- Produce internal audit report with findings rated by severity
- Assign corrective actions with owners and due dates
- Conduct management review — board-level — covering: risk assessment status, compliance report, incident summary, third-party due diligence outcomes, resource requirements
- Document management review outputs with board sign-off

Phase 7 — Certification Audit

- Stage 1 audit — document review by certification body
- Remediate any Stage 1 findings
- Stage 2 audit — controls testing, staff interviews, financial controls review, evidence testing
- Certificate issued — surveillance audits follow annually

Phase 8 — Ongoing Compliance

- Annual bribery risk assessment update
- Annual policy reviews with board approval
- Annual anti-bribery training for all staff — completion records
- Annual third-party due diligence reviews for higher-risk relationships
- Annual compliance report to board
- Gifts and hospitality register maintained continuously
- Monitor Transparency International CPI and higher-risk market developments

The Five Controls That Matter Most to Auditors and Regulators

1

Documented Bribery Risk Assessment with Executive Sign-Off

The risk assessment is the foundation. Auditors check that it is current, covers all relevant business activities and geographies, uses a recognised methodology, and has been approved at an appropriate level. **A risk assessment created at implementation and never updated is an immediate finding.**

2

Third-Party Due Diligence with Documented Decisions

For every agent, intermediary, and consultant in a higher-risk context — evidence that due diligence was conducted before engagement, a risk level was assigned, and an appropriately senior person approved the engagement. **The absence of this trail for even one significant third party is a material finding.**

3

Gifts and Hospitality Register with Complete Entries

The register must be current and complete. Auditors cross-check the register against finance records for hospitality expenditure. Missing entries are findings. Entries without documented approval above threshold are findings.

4

Financial Controls with Evidence of Operation

Approval thresholds and segregation of duties are policy — auditors test whether they operate. They will sample payment records and check that the approval process was followed. **Payments that bypassed the threshold without documented escalation are findings.**

5

Board Compliance Report with Evidence of Substantive Engagement

The board minutes must show substantive engagement with anti-bribery risk and performance — not just that the compliance report was presented. Boards that receive the report without discussion, challenge, or documented decision-making are failing the governing body oversight requirement.

Manual vs. Automated: What Good Looks Like

ISO 37001 Requires	Manual Reality	With Governance Automation
Current bribery risk register with sign-offs	Spreadsheet last updated at implementation	Live register with review dates, owner tracking, and annual refresh trigger
Third-party due diligence with approval trail	Email chain, inconsistent documentation, gaps for smaller agents	Structured workflow with risk tiering, completion tracking, and signed-off decision record
Gifts and hospitality register	Spreadsheet, incomplete entries, no approval tracking	Structured register with threshold alerts and automatic approval routing
Annual compliance report to board	Drafted under time pressure, inconsistent content	Structured report generated from live compliance data with board sign-off trail
Training completion records	Spreadsheet, gaps for newer staff, hard to produce under audit	Automated tracking with completion records retrievable immediately
Audit evidence on request	Week-long scramble across finance, legal, and compliance	Complete, current, retrievable in minutes

fortifai

The Connection to Åpenhetsloven, ISO 27001, and GDPR

ISO 37001 does not exist in isolation. For mid-market companies managing multiple compliance obligations the overlaps are significant:

ISO 37001 and Åpenhetsloven

Both require supply chain due diligence. The third-party risk assessment under ISO 37001 and the supplier due diligence under Åpenhetsloven address overlapping questions about the integrity and conduct of your business relationships. A unified due diligence workflow handles both and the evidence base is shared.

ISO 37001 and ISO 27001

Both require documented risk assessments, management reviews, internal audits, and corrective action processes. The governance infrastructure is largely shared — sign-off workflows, document management, and audit evidence structures are identical in form even where the content differs.

ISO 37001 and GDPR

Whistleblower reports and investigation records involve personal data and require GDPR-compliant handling. The intersection of anti-bribery investigation procedures and data protection obligations requires careful governance — particularly around data subject rights during investigations.

For mid-market companies managing multiple frameworks, **Fortifai handles all of them from a single governance infrastructure** — which means each additional framework after the first costs a fraction of the original.

fortifai

How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing and mid-market companies. The platform automates the three workflows ISO 37001 requires:

Sign-Off Routing and Tracking

Anti-bribery policy approvals, risk assessment sign-offs, third-party due diligence decisions, and board compliance report approvals — all routed and tracked automatically.

Disclosure Document Management

Gifts and hospitality register, compliance reports, and investigation outcomes — managed in a single structured system.

Information Request Handling

Third-party due diligence questionnaires, audit evidence requests, and regulatory information requests — pre-configured for ISO 37001 with templates ready on day one.

The same platform supports **Åpenhetsloven, ISO 27001, NIS2, GDPR, EU AI Act, ISO 45001, and VSME** simultaneously. For mid-market companies managing multiple compliance obligations, the governance workflows overlap significantly and the evidence base is shared.

> Used by compliance teams at **Cognite, Aker BioMarine, and Telenor.**

Book a 30-minute walkthrough at fortifai.co

fortifai