Fraudfinder LTD
71-75 Shelton St
London
WC2H 9JQ
United Kingdom

Email: alexander@fraudfinderai.com

Risk Management Standard 2025

1. Purpose

The purpose of this standard is to ensure that all third-party suppliers, contractors, and service providers engaged by Fraudfinder Ltd are assessed, selected, and monitored to manage information security, privacy, and operational risks in line with ISO/IEC 27001:2022 and applicable legal requirements (including UK GDPR and the Data Protection Act 2018).

---

2. Scope

This standard applies to all third parties that process, store, transmit, or have access to Fraudfinder Ltd's data, systems, or facilities, including but not limited to:

- Cloud service providers
- Data processors and sub-processors
- Software vendors
- Consultants and contractors
- Hosting, infrastructure, and IT support providers

---

3. Principles

Fraudfinder Ltd manages supplier risk according to the following principles:

1. **Risk-based approach:** Suppliers are assessed based on the sensitivity of the information they handle and the criticality of their services.
2. **Due diligence before engagement:** All suppliers undergo a security and privacy review before contracts are signed.
3. **Ongoing monitoring:** Key suppliers are reviewed periodically to ensure ongoing compliance with contractual, security, and data-protection obligations.
4. **Contractual safeguards:** All supplier contracts must include appropriate confidentiality, data-protection, and security clauses.

5. **Right to audit:** Fraudfinder reserves the right to audit suppliers or request evidence of their security controls at any time.

---

4. Responsibilities

- **CEO / ISMS Lead:** Approves supplier onboarding and risk ratings for high-risk vendors.
- **Procurement Owner / Contract Manager:** Ensures due-diligence is completed and contractual obligations are documented.
- **Information Security Officer:** Conducts and documents supplier risk assessments and monitors compliance.
- **All Employees:** Must only engage suppliers approved through this process.

---

5. Supplier Risk Assessment Process

Step	Description	Responsibility
1. Identification	Identify need for supplier engagement and categorise by service type (e.g., IT, data processor, consultant).	Requesting team
2. Initial Risk Rating	Assess data sensitivity and operational criticality (Low / Medium / High).	Information Security Officer
3. Due Diligence	Complete Supplier Security Questionnaire; review certifications (ISO 27001, Cyber Essentials, SOC 2), policies, and past incident history.	Information Security Officer
4. Approval	Approve supplier engagement or implement risk-mitigation actions before contract signing.	CEO / ISMS Lead
5. Contractual Controls	Include appropriate data-protection, confidentiality, and audit clauses.	Legal / Procurement
6. Ongoing Monitoring	Review annually or after major incidents; reassess risk rating and take corrective actions as needed.	Information Security Officer

---

6. Risk Rating Criteria

Risk Level	Description	Example Controls Required
Low	No personal or confidential data processed; minimal operational impact.	Standard NDA.
Medium	Processes limited personal data or supports internal operations.	NDA + DPA + review of security questionnaire.
High	Processes sensitive data, customer data, or critical systems.	Full due diligence, ISO/SOC2 evidence, contractual clauses, annual re-assessment.

---

7. Contractual and Legal Requirements

All supplier agreements must include clauses covering:

- Confidentiality and data-protection obligations
- Compliance with UK GDPR / DPA 2018
- Breach notification within 72 hours
- Right to audit or request security evidence
- Termination rights for material breaches of security or privacy obligations

---

8. Monitoring and Review

- Supplier performance and incidents are logged and reviewed at least annually.
- Suppliers with significant changes in service, ownership, or security posture must be re-evaluated immediately.
- Results are reported as part of the ISMS management review.

---

9. Exceptions

Any exceptions to this standard must be documented, justified, and approved by the CEO or ISMS Lead

before supplier engagement.

---

10. References

- ISO/IEC 27001:2022, Clause 5.19 (Supplier Relationships)
- ISO/IEC 27002:2022, Controls 5.19.1–5.19.3
- UK GDPR & Data Protection Act 2018