Revue-ai
accelerated insights

AI Risk Intelligence Report

Acme Corporation

HIGH

OVERALL RISK CLASSIFICATION

Total Financial Exposure: **GBP 1.3m**

Jurisdiction	UK	**Industry**	Financial Services
Organisation Size	250-1000	**Regulated Sector**	Yes

20 March 2026

CONFIDENTIAL

Executive Risk Summary

Risk Classification

HIGH

Financial Exposure

GBP 1.3m

Regulatory Urgency

The regulatory compliance posture is developing, with several obligations unmet, particularly in AI system inventory and risk classification, exposing the organisation to significant enforcement risk in the UK.

The organisation has a high AI risk exposure, with a score of 38 out of 100. This shows there are major weaknesses in several risk areas. The estimated financial exposure is approximately GBP 1.3m. Most of this risk comes from possible regulatory fines and penalties for not following the UK DSIT AI Framework.

Key findings show that 23% of staff use unapproved AI tools. This widespread shadow AI use caused a serious data breach and led to a regulatory notification (People, Reputational & Ethical Risk score: 25/100). The organisation also lacks AI-specific contract protections with vendors. This gap creates major regulatory risks (Third-Party & Supply Chain AI Risk score: 33/100).

The organisation is still developing its regulatory compliance. Several requirements are unmet, especially around keeping an AI system inventory and classifying risks. The heat map shows three critical risks, five high risks, and eight moderate risks. This highlights the urgent need to fix these issues.

Top priorities are to roll out an AI Acceptable Use Policy within 30 days, with an estimated cost of GBP 5,000 to GBP 10,000. The organisation should also complete a full AI vendor risk assessment in the same period. Improving data loss prevention measures is needed to reduce data exposure risks.

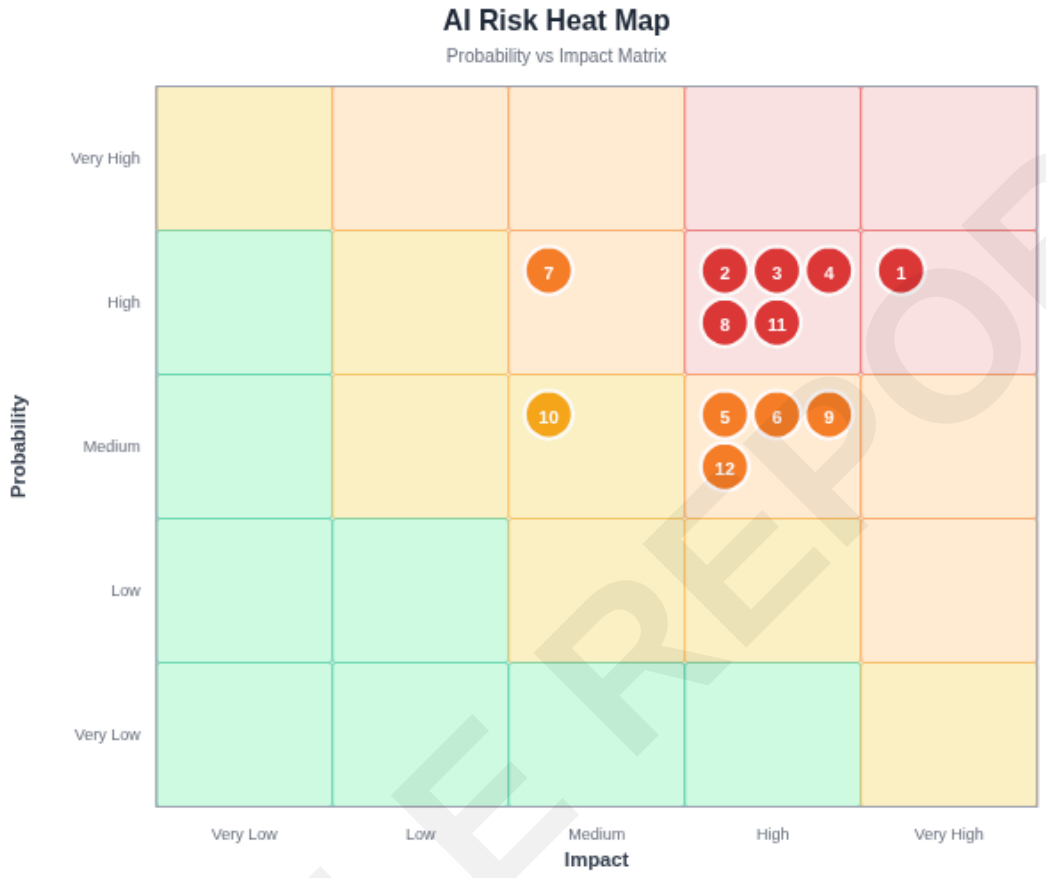
Financial Exposure: GBP 1.3m

Top Critical Risks

- The assessment identified 10 high-priority risks requiring immediate management attention across multiple AI risk domains.
- **Widespread Shadow AI Usage** (Immediate (0–30 days)): Significant exposure due to 23% of staff using unapproved AI tools, leading to critical data breaches and regulatory notifications.
- **Data Exposure via Consumer AI Tools** (Immediate (0–30 days)): Client data has been exposed through consumer AI tools, leading to regulatory notifications and reputational harm.
- **Unassessed Vendor AI Features** (Immediate (0–30 days)): Several vendors have introduced AI features without formal assessment, creating blind spots in risk exposure.

AI Risk Heat Map

Risks plotted by probability of occurrence and potential business impact. Higher scores indicate greater urgency for mitigation.



1. Widespread Shadow AI Usage
2. Data Exposure via Consumer AI Tools

AI Risk Intelligence - Probability x Impact Assessment

Top 10 AI Risks

#1 Widespread Shadow AI Usage

Immediate (0–30 days)

Regulatory

Significant exposure due to 23% of staff using unapproved AI tools, leading to critical data breaches and regulatory notifications.

Exposure: **Probability:** 4/5 **Impact:** 5/5 **Mitigation:** Immediate (0–30 days)

#2 Data Exposure via Consumer AI Tools

Immediate (0–30 days)

Regulatory

Client data has been exposed through consumer AI tools, leading to regulatory notifications and reputational harm.

Exposure: **Probability:** 4/5 **Impact:** 4/5 **Mitigation:** Immediate (0–30 days)

#3 Unassessed Vendor AI Features

Immediate (0–30 days)

Regulatory

Several vendors have introduced AI features without formal assessment, creating blind spots in risk exposure.

Exposure: **Probability:** 4/5 **Impact:** 4/5 **Mitigation:** Immediate (0–30 days)

#4 Absence of AI-Specific Contractual Protections

Immediate (0–30 days)

Regulatory

Most vendors lack AI-specific contractual clauses, exposing the organisation to regulatory and reputational risks.

Exposure: **Probability:** 4/5 **Impact:** 4/5 **Mitigation:** Immediate (0–30 days)

#5 Client Data Exposure via AI Tools

Immediate (0–30 days)

Regulatory

Client data has been exposed through the use of consumer AI tools, leading to regulatory notifications.

Exposure: **Probability:** 4/5 **Impact:** 4/5 **Mitigation:** Immediate (0–30 days)

Financial Exposure Model

TOTAL EXPECTED ANNUAL LOSS

GBP 1.3m

Confidence Assessment: *the organisation faces a large annual AI risk. Expected yearly losses are about GBP 1.3m, with possible peak losses up to GBP 1.3m in the next 12–24 months. The biggest risk comes from regulatory fines and penalties. These are caused by major compliance gaps with the UK DSIT AI Framework and sector regulator guidance, plus a recent severe data breach involving shadow AI. This financial risk shows the organisation needs to invest in fixing these issues soon. The current controls leave the organisation open to enforcement action, reputational damage, and operational problems. These risks could seriously affect both profits and access to the market.*

Exposure by Dimension

DIMENSION	EXPOSURE	CONFIDENCE	NARRATIVE
Regulatory fines and penalties	**GBP 525k**	MODERATE	Confirmed data breach involving client data exposure to ChatGPT, resulting in ICO notification and regulatory scrutiny.. Ad hoc compliance maturity with critical gaps in AI system inventory, model governance, and vendor contract protections.. Sector regulator (FCA) has issued a 'Dear CEO' letter requiring evidence of AI governance, with the organisation not yet fully compliant.
Remediation and compliance costs	**GBP 380k**	HIGH	Board-mandated remediation programme including AI-specific DLP, vendor contract remediation, and AI literacy training.. Estimated compliance cost for EU AI Act and UK regulatory requirements.. Technology and consulting costs for policy development, technical controls, and staff training.
Legal and litigation exposure	**GBP 50k**	MODERATE	Potential claims from clients affected by AI-driven errors or data exposure.. Vendor liability gaps due to absence of AI-specific contractual protections.. Class action or group litigation risk from algorithmic discrimination or data misuse.
Revenue and market impact	**GBP 120k**	MODERATE	Customer attrition following publicised AI incident and regulatory notification.. Potential market access restrictions if non-compliance persists, especially for EU clients.. Reputational damage impacting new business and renewals.

Strategic & Operational AI Risk

47/100 MEDIUM

the organisation faces a high and multi-dimensional AI risk landscape, with material deficiencies in governance, operational resilience, and data protection. The most significant finding is the prevalence of shadow AI, evidenced by widespread unsanctioned use of consumer AI tools with confidential client data, resulting in a recent high-severity data breach and regulatory notification. The absence of effective controls, incomplete AI inventories, and unaddressed third-party AI exposures leave the organisation vulnerable to regulatory action, financial loss, and reputational damage. Immediate Board-level intervention is required to address shadow AI, operational fragility, and vendor risk, as current mitigation efforts are insufficient to meet UK regulatory expectations or the upcoming EU AI Act obligations.

Key Risks

RISK	SEVERITY
No comprehensive AI inventory or risk register exists, and shadow AI is not systematically tracked[^1]	HIGH
Embedded AI features in vendor products are not consistently identified or governed[^2]	HIGH
Concentration risk and cascading failure paths are not documented[^2]	HIGH
No probability estimates or uncertainty ranges are provided for identified risks[^3]	HIGH
No systematic risk scoring or prioritisation methodology is in place[^4]	HIGH

Regulatory & Compliance Risk

34/100 HIGH

the organisation faces a high regulatory compliance risk posture in the UK, with significant deficiencies in AI governance, risk management, and incident response, particularly under the UK DSIT AI Framework and sector-specific FCA/PRA guidance. The most acute exposure arises from incomplete AI system classification, lack of robust vendor oversight, and insufficient technical controls to prevent data breaches, as evidenced by recent incidents involving client data and unapproved AI tool usage. These gaps create a credible risk of regulatory enforcement, reputational harm, and financial penalties, necessitating urgent board-level intervention and a sequenced remediation programme to address critical obligations within the next quarter. The UK remains the jurisdiction of highest enforcement exposure due to direct regulatory oversight and recent supervisory engagement.

Key Risks

RISK	SEVERITY
No evidence of a comprehensive regulatory mapping or systematic cross-jurisdictional conflict analysis[^2][^5]	HIGH
Critical gaps in AI system classification, incident response, and vendor oversight are documented and remain unresolved[^6][^7]	HIGH
Major compliance programmes are in early planning or not yet initiated, with critical deadlines imminent[^4][^6]	HIGH

Regulatory Frameworks

FRAMEWORK	COMPLIANCE	URGENCY
UK AI Regulation (DSIT Pro-Innovation Framework + ICO AI Guidance)	Developing	-