CONFIDENTIAL — ANONYMISED SAMPLE

AXIONLY · AI Governance & Security Consulting

AI READINESS ASSESSMENT REPORT

with Security Deep-Dive

Client

[Organisation Name Redacted]

Sector

Financial Services / Fintech

Report date

[Date Redacted]

Prepared by

Axionly — a division of Axiontic

OVERALL READINESS RATING

2.1 / 5

MODERATE RISK

Significant gaps identified across compliance and security domains. Action required before Aug 2026.

1. EXECUTIVE SUMMARY

This report presents the findings of an AI Readiness Assessment with Security Deep-Dive conducted by Axionly. The assessment was commissioned by the client organisation to understand their current AI governance posture, identify legal obligations under the EU AI Act, and surface security risks associated with their AI tool ecosystem.

The assessment was conducted over five business days following a structured scoping call. It included a review of AI tools in use, vendor contracts and data processing agreements, internal governance policies, and technical security configurations.

1.1 Domain Ratings Overview

ASSESSMENT DOMAIN	RATING	SUMMARY FINDING
AI System Inventory	**1.5 / 5**	No formal inventory exists. 14 AI tools identified during scoping, 6 unknown to IT.
EU AI Act Compliance	**2.0 / 5**	Two use cases likely trigger high-risk classification under Annex III. No gap analysis performed.
Data Governance & GDPR	**2.5 / 5**	DPAs exist for primary vendors but are absent for 4 of 14 tools. RoPA not updated.
Internal Policy & Governance	**1.5 / 5**	No AI use policy in place. No designated AI owner. Leadership awareness is low.
Security — Prompt Injection	**2.0 / 5**	Customer-facing chatbot vulnerable to indirect prompt injection. No input validation.
Security — API & Access Control	**3.0 / 5**	API keys rotated annually. Overly permissive scopes on 3 of 7 integrations.
Security — Data Leakage	**2.5 / 5**	Evidence of confidential client data submitted to public AI tools by two business units.
Security — Incident Response	**1.5 / 5**	No AI-specific incident response plan. General IR plan does not address AI scenarios.
OVERALL READINESS	**2.1 / 5**	Moderate risk. Immediate action required on inventory, compliance classification, and security findings prior to Aug 2026 enforcement.

1.2 Key Observations

- The organisation operates 14 AI tools across five business units. Of these, six were not visible to the IT department prior to this assessment — a significant shadow AI exposure.
- Two AI use cases (automated credit decision support and employee performance flagging) are likely to fall within the high-risk category under Annex III of the EU AI Act, triggering conformity assessment obligations ahead of the August 2026 deadline.
- The customer-facing AI chatbot exhibits a vulnerability to indirect prompt injection that could be exploited to manipulate its outputs or extract information from connected systems.
- Confidential client data — including names, account identifiers, and transaction summaries — was identified as having been submitted to public generative AI tools by staff in two business units, in the absence of any governing policy.
- No internal AI use policy exists. No individual has been formally designated as responsible for AI governance. This creates legal and operational exposure that must be addressed regardless of technical remediation.

2. AI SYSTEM INVENTORY

The following AI system inventory was compiled through a combination of the scoping questionnaire, IT asset review, stakeholder interviews, and network traffic analysis. Tools are classified against the EU AI Act risk framework.

14 AI systems were identified in total. 6 were not previously registered in IT asset management systems.

#	AI SYSTEM	FUNCTION / USE CASE	BUSINESS UNIT	EU AI ACT RISK	IT KNOWN?
01	[Vendor A] — Chatbot	Customer-facing support & query resolution	Customer Services	Limited Risk	Yes
02	[Vendor B] — Credit Scoring	Automated credit decision support	Risk & Lending	**HIGH RISK ⚑**	Yes
03	[Vendor C] — HR Analytics	Employee performance flagging & attrition prediction	Human Resources	**HIGH RISK ⚑**	Yes
04	[Vendor D] — Document AI	Contract analysis and clause extraction	Legal	Minimal Risk	Yes
05	[Vendor E] — Fraud Detection	Real-time transaction anomaly detection	Risk & Lending	Minimal Risk	Yes
06	[Vendor F] — Copilot	Internal productivity assistant (Microsoft 365)	All departments	Minimal Risk	Yes
07	[Vendor G] — GenAI Tool	Ad-hoc text generation and summarisation	Marketing	Minimal Risk	**No ⚑**
08	[Vendor H] — Data Enrichment	Customer data enrichment via third-party AI API	Sales	Limited Risk	**No ⚑**
09	[Vendor I] — Meeting AI	Meeting transcription and action item extraction	All departments	Minimal Risk	**No ⚑**
10	[Vendor J] — Sentiment AI	Customer feedback sentiment classification	Customer Services	Minimal Risk	Yes
11	[Vendor K] — GenAI (Public)	Public LLM used ad-hoc by staff (ChatGPT)	Multiple — uncontrolled	Minimal Risk	**No ⚑**
12	[Vendor L] — GenAI (Public)	Public LLM used ad-hoc by staff (Gemini)	Multiple — uncontrolled	Minimal Risk	**No ⚑**
13	[Vendor M] — Resume Screener	CV screening and candidate ranking	Human Resources	**HIGH RISK ⚑**	**No ⚑**
14	[Vendor N] — Pricing AI	Dynamic pricing recommendations	Product	Minimal Risk	Yes

⚑ Systems 02, 03, and 13 require priority attention due to their likely classification as high-risk under Annex III.

⚑ Systems 07, 08, 09, 11, 12, and 13 were not registered in IT asset management. All carry data governance implications requiring immediate review.

3. REGULATORY GAP ANALYSIS

This section maps the organisation's obligations under the EU AI Act (Regulation 2024/1689) and GDPR against current practice. The analysis focuses on the three high-risk use cases identified in the inventory and the organisation's general obligations as a deployer of AI systems.

REQUIREMENT	LEGAL BASIS	CURRENT STATUS	GAP / FINDING
Conformity assessment (high-risk systems)	*EU AI Act Art. 43*	**NOT COMPLETED**	No conformity assessment has been initiated for Systems 02, 03, or 13. Required before Aug 2026.
Technical documentation	*EU AI Act Art. 11 & Annex IV*	**NOT IN PLACE**	No technical documentation exists for any high-risk system. Vendor documentation not obtained.
Registration in EU AI database	*EU AI Act Art. 71*	**NOT COMPLETED**	None of the three high-risk systems have been registered or assessed for registration requirement.
Human oversight mechanism	*EU AI Act Art. 14*	**PARTIAL**	Credit scoring outputs reviewed by analysts, but no formal oversight protocol. HR and CV tools have no human review step.
Fundamental rights impact assessment	*EU AI Act Art. 27*	**NOT COMPLETED**	No FRIA has been conducted. Required given HR and lending use cases involving protected characteristics.
Transparency to affected individuals	*EU AI Act Art. 50 / GDPR Art. 13–14*	**NOT IN PLACE**	Individuals subject to AI-assisted credit and HR decisions are not informed. GDPR transparency breach identified.
Data processing agreements (AI vendors)	*GDPR Art. 28*	**PARTIAL**	DPAs absent for 4 vendors (Systems 07, 09, 11, 12). Existing DPAs for high-risk vendors do not address AI-specific processing.
Records of Processing Activities (RoPA)	*GDPR Art. 30*	**INCOMPLETE**	RoPA has not been updated to reflect AI-driven processing activities. Last updated 18 months ago.
AI use policy — internal governance	*EU AI Act Art. 26 (deployer obligations)*	**NOT IN PLACE**	No internal AI use policy exists. Deployer obligations require documented oversight and usage controls.
Incident reporting for high-risk AI	*EU AI Act Art. 73*	**NOT IN PLACE**	No process for reporting serious incidents involving high-risk AI systems to national supervisory authority.

4. RISK ASSESSMENT BY DOMAIN

This section provides a domain-by-domain risk assessment based on the findings above. Each domain is rated on a 1–5 scale, where 1 represents critical unmanaged risk and 5 represents full compliance and control.

AI SYSTEM INVENTORY & VISIBILITY	1.5 / 5 — Critical

Six of fourteen AI systems in use were not known to the IT department. The organisation cannot assess, control, or report on systems it does not know exist. Shadow AI adoption is concentrated in Sales, Marketing, and HR — in each case adopted at team level with no procurement review, security assessment, or data protection consideration.

The two public generative AI tools (Systems 11 and 12) are in active use across multiple departments with no controls on the type of data submitted.

EU AI ACT COMPLIANCE	2.0 / 5 — High Risk

Three systems trigger high-risk obligations under Annex III: the credit scoring tool (System 02) under point 5(b), and the HR analytics and CV screening tools (Systems 03, 13) under point 4. None has undergone a conformity assessment, and none has been registered with the relevant supervisory authority.

The August 2026 enforcement deadline is approximately 14 months away at the time of this report. Given the lead time required for conformity assessments and technical documentation, immediate action is required.

DATA GOVERNANCE & GDPR	2.5 / 5 — Elevated Risk

Data processing agreements are absent for four vendors — a direct breach of Article 28 GDPR. The organisation's Records of Processing Activities have not been updated to reflect AI-driven processing, representing a material compliance gap given the sensitivity of data processed by Systems 02, 03, and 08.

The most significant GDPR finding is transparency: individuals subject to AI-assisted credit and employment decisions have not been informed, in breach of Articles 13 and 14.

INTERNAL POLICY & GOVERNANCE	1.5 / 5 — Critical

The organisation has no documented AI use policy and no designated AI governance owner. There is no approval process for new AI tools and no prohibition on sharing confidential data with public AI tools. During interviews, responsibility for AI governance was cited by multiple functions simultaneously — indicating an absence of clear ownership.

Senior leadership was unaware of the high-risk classification of three existing systems and had not been briefed on the August 2026 compliance deadline.

5. SECURITY FINDINGS — DEEP-DIVE TIER

This section presents the technical security findings from the Deep-Dive tier assessment. Findings are rated by severity: Critical, High, Medium, and Low.

A total of 7 security findings were identified across four domains. Two findings are rated High. One finding in the prompt injection domain warrants immediate remediation.

F-01

Indirect Prompt Injection — Customer Chatbot (System 01)

Severity: HIGH

The customer-facing chatbot (System 01) is vulnerable to indirect prompt injection via malicious content in user-uploaded documents. An attacker can embed instructions in a document to override the chatbot's system prompt, causing it to disclose information from connected systems or produce unintended outputs.

Recommendation: Implement input sanitisation on all document ingestion pipelines. Apply strict system prompt constraints. Review and limit the chatbot's connected tool access scope with the vendor.

Business implication: *Exploitation could result in disclosure of other customers' data, reputational damage, and GDPR Article 33 breach notification obligations.*

F-02

Overly Permissive API Scopes — Three AI Integrations

Severity: HIGH

Three AI API integrations (Systems 02, 05, and 08) are configured with full read/write API key permissions. The principle of least privilege has not been applied. A compromised key grants an attacker unrestricted access to the connected data sources.

Recommendation: Audit all AI API key configurations. Reduce scopes to minimum necessary. Rotate keys at 90-day intervals (currently annual). Store keys in a secrets manager rather than configuration files.

Business implication: *A compromised key could expose customer financial data, triggering GDPR breach notifications and potential NIS2 obligations.*

F-03

Confidential Data Submitted to Public AI Tools

Severity: HIGH

Evidence confirms that staff in Sales and HR have submitted confidential client data and internal HR records to public generative AI tools (Systems 11 and 12), including client names, account identifiers, compensation data, and performance review content.

Recommendation: Issue an immediate policy communication prohibiting submission of personal or confidential data to public AI tools. Implement technical DLP controls to detect and block sensitive data exfiltration to unapproved AI endpoints.

Business implication: *This may constitute a GDPR personal data breach. A Data Protection Impact Assessment should be conducted without delay.*

F-04

No AI-Specific Incident Response Procedures

Severity: MEDIUM

The existing incident response plan does not address AI-specific scenarios — including prompt injection, model poisoning, unexpected outputs, or EU AI Act Article 73 regulatory notification obligations for high-risk system incidents.

Recommendation: Extend the IR plan to include AI-specific scenarios, escalation paths, and a designated AI incident owner. Define criteria for regulatory notification.

Business implication: *Without defined procedures, response time to AI incidents will be delayed, increasing both business impact and regulatory exposure.*

F-05

No Output Logging on High-Risk AI Systems

Severity: MEDIUM

Systems 02, 03, and 13 have no output logging or monitoring. Anomalous or discriminatory outputs cannot be detected, investigated, or reported. EU AI Act Article 12 requires high-risk systems to retain logs enabling post-market monitoring.

Recommendation: Implement logging of all inputs and outputs for the three high-risk systems. Define anomaly thresholds, assign a review owner, and establish a log retention period.

Business implication: *Absence of logs makes it impossible to demonstrate EU AI Act compliance, respond to individual complaints, or detect systematic bias in AI-assisted decisions.*

6. PRIORITISED ACTION PLAN

The following action plan presents all findings as discrete, assignable actions, ranked by risk severity and grouped into three implementation horizons: Immediate (within 2 weeks), 30 days, and 90 days.

Each action references the relevant finding or gap from earlier sections. Ownership should be confirmed in the executive briefing call and recorded in your governance register.

REF	ACTION REQUIRED	OWNER	DEADLINE	HORIZON
A-01	Issue immediate internal communication prohibiting submission of personal or confidential data to public AI tools (Systems 11, 12) pending formal policy.	Legal / CISO	2 weeks	**Immediate**
A-02	Conduct security remediation on chatbot prompt injection vulnerability (F-01). Engage vendor for patching timeline.	IT / Vendor	2 weeks	**Immediate**
A-03	Audit and remediate all AI API key permissions. Reduce scopes to least privilege. Rotate compromised or overly-broad keys (F-02).	IT / DevOps	2 weeks	**Immediate**
A-04	Designate a named AI Governance Owner with board-level accountability. Define scope and escalation path.	CEO / Board	30 days	**30 days**
A-05	Obtain or execute DPAs for the four vendors currently lacking agreements (Systems 07, 09, 11, 12). Do not use these systems for personal data until complete.	Legal / DPO	30 days	**30 days**
A-06	Update Records of Processing Activities to include all 14 AI systems. Flag high-risk systems for priority review.	DPO / Legal	30 days	**30 days**
A-07	Implement output logging for Systems 02, 03, and 13. Define anomaly thresholds and review cadence (F-05).	IT / Risk	30 days	**30 days**
A-08	Draft and publish internal AI Use Policy covering acceptable use, data submission rules, approval process, and consequences.	Legal / HR / IT	90 days	**90 days**
A-09	Initiate conformity assessment process for Systems 02, 03, and 13. Engage external legal counsel with EU AI Act specialism.	Legal / Risk	90 days	**90 days**
A-10	Prepare transparency notices for individuals subject to AI-assisted credit and HR decisions. Update privacy notices accordingly.	Legal / DPO	90 days	**90 days**
A-11	Conduct Fundamental Rights Impact Assessment for Systems 02, 03, and 13 in conjunction with conformity assessment process.	Legal / DPO	90 days	**90 days**
A-12	Extend incident response plan to cover AI-specific scenarios, notification obligations, and designated AI incident owner (F-04).	CISO / Legal	90 days	**90 days**
A-13	Implement technical controls (DLP rules) to detect and block submission of sensitive data to unapproved AI endpoints.	IT / CISO	90 days	**90 days**
A-14	Establish quarterly AI governance review cadence: inventory refresh, policy compliance check, regulatory update briefing.	AI Gov. Owner	90 days	**90 days**

7. METHODOLOGY & SCOPE

This assessment was conducted using Axionly's structured five-day methodology. The scope was defined and agreed during the scoping call and has not been modified. All work was conducted remotely.

PHASE	ACTIVITIES	OUTPUTS
Scoping (Day 0)	60-minute structured scoping call. Definition of in-scope departments, systems, and stakeholders. Document collection request sent.	Agreed scope document, stakeholder list, document request log.
Discovery (Day 1)	Review of submitted documents: vendor contracts, DPAs, existing policies, IT asset register, privacy notices.	Document review log, initial gap observations.
Stakeholder Interviews (Days 1–3)	30-minute structured interviews with IT lead, DPO, Head of HR, Head of Risk, and two department managers. Remote via video call.	Interview notes, shadow AI identification, qualitative risk data.
Technical Review (Days 2–4)	API configuration review, key scope audit, chatbot security testing (prompt injection), network traffic review (with consent), log analysis.	Technical findings log, vulnerability evidence, F-01 to F-05.
Analysis & Reporting (Days 4–5)	Regulatory mapping against EU AI Act and GDPR. Risk rating. Action plan compilation. Report drafting and review.	This report. Executive summary slide deck.
Briefing Call (Day 5)	30-minute executive walkthrough of findings with key stakeholders. Q&A. Action ownership confirmation.	Confirmed action register. Recording available on request.

8. LIMITATIONS & CONFIDENTIALITY

This assessment does not constitute legal advice. The findings and recommendations reflect the information available at the time of the assessment. Legal obligations should be confirmed with qualified legal counsel.

Axionly does not share client information with third parties. All documents, interview notes, and system access provided during the assessment are treated as strictly confidential and are not retained beyond the engagement unless explicitly agreed.

This report is an anonymised sample. All client-identifying information — including organisation name, sector, system names, vendor names, and personnel — has been replaced with generic placeholders. The findings and structure are representative of a real assessment.

NEXT STEPS

The findings in this report should be reviewed by your legal, IT, and senior leadership teams. We recommend scheduling the executive briefing call as soon as possible to confirm action ownership and begin remediation.

Axionly is available to support implementation through policy drafting, vendor due diligence, quarterly governance reviews, and EU AI Act technical documentation. Please contact us at the address below to discuss.

Axionly

a division of Axiontic

axionly.io

Book a free discovery call