Vendor Risk Assessment for AI Analytics

Scenario Overview

A logistic startup just signed a contract with a third-party AI analytics vendor. This vendor helps optimize delivery routes by processing your GPS, driver, and delivery data. Before granting this vendor full access to our internal data systems, we must conduct a formal risk assessment to ensure the security and privacy of the company's data.

Identified Data

The first step in creating a risk assessment for AI analytics vendor integration is to identify what specific data the vendor will have access to. In this case, the vendor will access the following data:

- GPS Data: Real-time location tracking from vehicles.
- Driver Schedules: Information regarding driver names and shifts.
- Delivery Details: Delivery timestamps and location-based customer data.

While this data may not be considered personally identifiable information (PII) in the traditional sense, it can still be used to identify individuals when combined.

Risk Categories

In order to conduct a comprehensive risk assessment, it is important to break down the risk areas into specific categories. These categories include:

Data Access

- Who at the vendor can access the data?
- How the data protected from unauthorized access?
- What measures are in place to prevent data breaches?

Storage Practices

- Are the data stored securely?
- Is the data only processed temporarily or is it stored long-term?
- What encryption methods are used to protect the data at rest and in transit?

Contractual Protections

- Does the vendor have a Data Processing Agreement (DPA) or Service Level Agreement (SLA) in place?
- Are there provisions in the agreement for data breaches, data retention, and data deletion?
- What are the consequences for non-compliance with the agreement?

- Is there a Data Processing Agreement (DPA) or Service Level Agreement (SLA) in place to cover breaches, retention, and deletion?

AI Risk

- Is the vendor using the data to train any AI models?
- What ethical and security implications are associated with the AI models being developed?
- How is the data being used to ensure fairness, accountability, and transparency in the AI models?

Risk Assessment Methodology

Before conducting a risk assessment, it is important to establish a risk assessment methodology. This defines the risk criteria, score each risk area, and monitor results over time.

Risk Criteria Definition

- Likelihood: How likely is unauthorized data access or misuse?
- Impact: The potential damage or data exposure, if a breach occurs.

Risk Scoring Model

Each risk's overall score is simply:

Risk Score = Likelihood × Impact

We rate each risk by combining the probability of it occurring: for example, vendor history, and system exposure) with its potential impact (e.g., data breach severity, operational downtime).

We then map that number into three practical categories:

Low (1–6): Acceptable with standard controls.

Medium (7–15): Requires specific mitigations and regular check-in.

High (16–25): Demands immediate, robust countermeasures.

Based on these factors, each risk area is assigned a level: Low, Medium, or High.

Industry Frameworks Alignment

To ensure this risk assessment is both thorough and in line with industry best practices, we aligned our evaluation with recognized cybersecurity and data privacy frameworks. This alignment not only supports consistency and clarity in how we identify and score risks, but also helps demonstrate compliance readiness.

NIST Cybersecurity Framework (CSF):

Each risk area such as data access, storage practices, and AI usage has been mapped to relevant functions within the NIST CSF: Identify, Protect, Detect, Respond, and Recover. This helps ensure a well-rounded assessment that considers both technical and governance aspects of vendor engagement.

ISO/IEC 27001:2022:

Risk areas were aligned with relevant ISO 27001 control domains:

A.5 (Organizational Controls): Covers third-party and contractual protections.

5.19 – Information security in supplier relationships.

5.20 – Addressing information security within supplier agreements.

5.24 – Information security incident management planning and preparation.

A.8 (Technological Controls): Supports technical measures like access controls and data storage.

8.1- Access control.

8.10 - Information deletion.

8.11 - Data masking.

8.12- Data leakage prevention.

GDPR Principles:
For any processing of personal or indirectly identifiable data (e.g., driver location and schedules), we ensured the following principles were considered:

Data Minimization – Only necessary data should be shared.

Storage Limitation – Data should not be retained longer than necessary.

Purpose Limitation – Data must only be used for the agreed-upon service (route optimization).

Breach Notification – Contractual obligations should follow GDPR-aligned response timelines and responsibilities.

Data Sources

To build a well-rounded view of the vendor's security posture, we draw on multiple sources:

- Vendor Self-Assessment Questionnaire covering their security posture, their policies, controls, and certifications.
- Documentation Review: Data Processing Agreement (DPA), Service Level Agreement (SLA), encryption standards and retention policies.
- Interviews with the vendor's IT security lead and our internal stakeholders and summaries of recent penetration tests (if available) for additional assurance.

Risk Areas and Assessment

The table below breaks down our main risk areas by the key questions each addresses, likelihood and impact scores, the risk levels, and the recommended mitigation actions:

Risk Area	Key Question	Likelihood (1–5)	Impact (1–5)	Score	Risk Level	Recommended Mitigation	Framework Controls
Data Access	Who at the vendor has access to GPS, schedule, and delivery data?	4	5	20	High	Require Role-Based Access Control (RBAC), audit logs, and enforce MFA on vendor systems.	NIST: Protect PR.AC-1, PR.AC -4. ISO 27001: A.8.1, A.5.15. GDPR: Data Minimization (Article 5.1c).
Storage Practices	Is data stored temporarily or long term? Where and how is it stored? Is encryption used?	3	4	12	Medium	Request documentation of storage architecture, retention, encryption and deletion policies from vendor.	NIST: Protect PR.DS-1, PR.DS -2. ISO 27001: A.8.10, A.8.25. GDPR: Storage Limitation (Article 5.1e).
Contractual Protections	Do we have a signed DPA or SLA that defines rights, responsibilities, and breach notification timelines?	2	3	6	Low	Ensure a DPA is signed and SLA includes breach reporting timelines, retention clauses, and right to audit.	NIST: Recover (RC.IM) ID.GV-3, RS.CO-3. ISO 27001: A.5.19 & A.5.20. GDPR: Accountability & Data Processing Agreements (Article 28).
AI Risk	Is vendor using our data to train models? Are there safeguards?	4	5	20	High	Prohibit model training without prior approval and conduct periodic reviews of model usage and ethics policy.	NIST: Identify& Protect (PR.IP-3, PR.DS-6. ISO 27001: A.5.23, A.5.10. GDPR: Purpose Limitation (Article 5.1b).
Incident Response	How will the vendor handle	3	5	15	Medium	Request incident response policy,	NIST: Respond RS.RP-1, DE.DP-1.

Risk Area	Key Question	Likelihood (1–5)	Impact (1–5)	Score	Risk Level	Recommended Mitigation	Framework Controls
	data breaches or access violations?					breach notification process, and history of past breaches (if any). Vendor must notify us within 72 hours of a data breach.	ISO 27001: A.5.25, A.8.16. GDPR: Breach Notification (Article 33–34).
Compliance & Legal	Is the vendor compliant with local privacy laws and industry regulations?	2	4	8	**Medium**	Verify vendor's compliance posture with regional privacy regulations.	NIST: Identify ID.GV-2, PR.IP-1. ISO 27001: A.5.31, A.6.32. GDPR: Article 5,28&33

Continuous Assessment & Versioning

The risk assessment will be updated regularly as our relationship with the vendor evolves and as new security threats or compliance requirements emerge. Then stay ahead of change by scheduling check-ins every quarter, to validate that the vendor's controls remain robust and to quickly address any new risks or shifts in their security environment. Each update will be versioned and documented, providing a clear history of revisions and the rationale behind any changes. Over time, this transparent record not only demonstrates our diligence but also helps us refine our risk management practices as new lessons and requirements emerge.

Summary and Recommendations

Overall, this vendor presents medium to high risks in key areas without stronger controls, particularly related to access controls and the potential use of data for AI model training.
Before proceeding:

- Enforce strong access controls (Role Based Access Control (RBAC) and Multi-Factor Authentication (MFA).
- Finalize legal agreements (DPA/SLA) with clear breach response, retention, and deletion, and add explicit contractual restrictions regarding the use of data for AI training.
- Restrict AI training on our data without a second risk review.
- Validate resilience through agreed incident-response timelines, disaster-recovery metrics, and regular drills.
- Ensure compliance with local privacy laws and secure any required data-transfer approvals.