Autonomous Business Intelligence Agent

Product Requirements Document

### 1) Hypothesis & Strategic Fit

**Problem:**  
Decision-makers face information overload while missing critical insights, spending more time searching through data than acting on it. Traditional analytics require constant human interpretation and often miss emerging patterns.

**Why now:**  
The volume and velocity of enterprise data continue to increase, and executives risk losing competitive advantage without predictive and autonomous intelligence.

**Strategic fit:**  
This agentic autonomy aligns with goals of faster, proactive decision-making and efficiency. It directly advances objectives tied to agility and risk management, unlocking value by autonomously surfacing insights and acting on them.

### 2) Users, JTBD & Success Outcomes

**Primary Persona:**

**Ragini - Customer Management Head at a Global Oil Company**

* **Role:** Senior executive overseeing customer escalations and managing customer operations across the company’s global locations.
* **Needs**: Acknowledge customer concerns, ensure timely responses, and track high-risk oil shipments.
* Goals: Identify patterns and anomalies to guide decisions on vendors, transport modes, and delivery performance.
* **Challenges**: Overloaded with meetings and reviews; lacks time for manual analysis and needs intelligent tools for real-time insights.

**Jobs-To-Be-Done**

* When I need to monitor operational trends, I want to receive a weekly report of insights generated from the Master Data system across transport creation and shipment processes, so that I can make informed decisions and spot emerging patterns.
* When I receive critical customer queries via email, I want to be able to send an initial response quickly, so that customers feel acknowledged and supported without delay.
* When a customer email requests specific data, I want the system to autonomously cross-reference and reply, so that routine queries are resolved efficiently without manual intervention.
* When I want to find a particular insight or data from the database, I want to ask a conversational AI that can help me get the information in minutes.

**Top outcomes (v1):**

* Time to First Insight ≤ 30 seconds after dataset upload.
* Reply Rate on critical emails.
* Percentage of mails responded autonomously.
* No of insights generated.

**Contra-indicators:**

* **Sensitive or Regulated Contexts:** Not suitable for highly regulated compliance environments requiring zero autonomy, or domains where false positives could lead to severe financial or legal consequences.
* **Complex or Ambiguous Queries**: Avoid automation for emails that require nuanced judgment, empathy, or involve confidential or unstructured content.
* **Security and Experience Risks**: Automation may compromise data security if improperly credentialed, and overuse can result in impersonal customer interactions.

### 3) Scope (In), Non-Goals (Out), and Trade-offs

**In-scope v1:**

* Simulating Database and email Data
* Autonomous action of initial response to customer mails.
* Autonomously answering customer queries whose response can be cross referenced from Database.
* Generating insights and historical patterns and showing these insights on a customer website.
* Chat agent that can fetch data/insights requested by the user.

**Non-goals / phase II+:**

* Real-time streaming ingestion.
* Human-in-loop feature for critical decisions.
* Feedback to agent to improve confidence scores.
* Complex predictive ML models.
* Multi-tenant enterprise security.
* Integration with SAP/Salesforce/ServiceNow/Slack/Teams.

**Assumptions:**

* Users will start with small batch datasets.
* Users are only communicating through email.
* Users are only focusing on transport related issues.
* User feedback is not passed through mail.

**Trade-offs:**

* Functioning MVP over authorisation and compliance checks
* Batch simplicity prioritized over streaming latency.
* Autonomy over control
* Efficiency over personalization

### 4) Data & Grounding

**Sources:**

* Database Source provided in .xlsx
* Email data provided as a google spreadsheet

**Access & sensitivity:**  
Local ingestion only; no external PII or sensitive customer data used in PoC.

**Grounding method:**  
Gemini API and n8n’s simple memory used for grounding to provided data.

**Freshness:**  
Database provided on weekly bases and email in-flow continuous once inbox of user is configured.

**Citations:**  
Insights contain relevant data points.

### 5) Sample Prompts

**Representation Prompts:**

**Prompt #1** – **Expected Use Case**

"*Can you send me the latest shipment status for Shipment #4589 and confirm if it’s still marked as high risk?"*

Purpose: Tests the agent’s ability to handle routine data requests by cross-referencing shipment records and replying with structured information.

**Prompt #2 – Edge Case**

*"We’ve received multiple complaints from our Singapore clients about delayed deliveries. Can you investigate and share any patterns or anomalies?"*

Purpose: Evaluates the agent’s ability to synthesize insights from multiple data sources, detect anomalies, and respond with contextual analysis.

**Prompt #3 (stretch) - Stretch/Creative Scenario**

*"If we were to switch to rail transport for our South American routes, what risks or benefits could we expect based on past customer feedback?"*

Purpose: Challenges the agent to combine historical data, customer sentiment, and operational insights to support strategic decision-making.

**Output format:**  
UI to display insights in human language from a structured JSON output.

**Style & tone:**  
Professional, clear, concise, urgency indicated in critical alerts.

### 6) Quality, Safety & Policy Guardrails

**Quality risks:**  
Hallucinations or misclassification of anomalies.

**Safety & privacy:**  
Sandbox email prevents real exposure of sensitive data.

**Security:**  
Local storage; no external database dependency.

**Bias & fairness:**

Introduce bias audits and human-in-the-loop checkpoints to ensure equitable agentic decisions, especially in sensitive or regulated contexts.

**Telemetry:**  
Automatic responses, insights generated, alerts raised, and continuous improvement.

### 7) Evaluation Plan

**Offline eval set:**  
Database provided with anomalies. Mails provided with urgent information or high criticality requests.

**Metrics & thresholds:**

* Valid Insight Generation ≥ 90% accuracy in test cases.
* Rate of automated responses
* Insight generation rate

**Acceptance criteria:**  
End-to-End working scenario with email generation.

Agent based insights generated and displayed on UI.

Real-time queries answered by agent using Doc grounding through RAG.

### 8) Risks & Trade-offs (Top 3)

**Risk #1: Misaligned Autonomous Decisions**

**Description: Autonomous agents may take actions that diverge from user intent or business goals, especially in multi-agent systems with broad action spaces.**

**Mitigation: Implement human-in-the-loop oversight for high-stakes decisions, define clear boundaries for agent autonomy, and use intent verification mechanisms.**

**Risk #2: Regulatory and Compliance Violations**

**Description: Agents operating in regulated domains (e.g., finance, healthcare) may inadvertently trigger compliance breaches through automated decision-making.**

**Mitigation: Restrict agent autonomy in sensitive workflows, enforce manual review for high-risk actions, and align with Responsible AI standards and privacy assessments.**

**Risk #3: Lack of Transparency and Accountability**

**Description: Users and downstream systems may not realize they are interacting with autonomous agents, reducing trust and traceability.**

**Mitigation: Ensure clear disclosure of agentic behaviour, maintain audit trails for all agent actions, and adopt governance frameworks that attribute responsibility.**