AI Agent Strategy & Architecture: PRD

In Week 1, your objective is to define the initial PRD for your solution. Before a single node is configured in n8n, you must demonstrate a rigorous understanding of the problem space and the logic required to solve it.

Remember: *An AI PRD is not a static specification; it is a* ***Strategic Alignment Tool*** *designed to synchronize business objectives, user experience, and technical execution.*

WEEK 1: DELIVERABLES

To advance to the development phase, you must submit:

1. **Strategic PRD:** The "Why." Defining business value and ROI.
2. **AI Agent Architecture (PRD):** The "How." Defining the agent's reasoning engine and autonomy.
3. **System Flow Chart:** A visual mapping of data orchestration and decision nodes.
4. **Heuristic Justification:** A defense of why AI (probabilistic logic) is superior to a standard script (deterministic logic) for this use case.

Part 1: Strategic PRD (The Business Layer)

Objective: Define the strategic moat and market necessity. Prove that this initiative justifies the capital and resource allocation.

Component	Strategic Focus	✅ Executive Standard (Example)	❌ Sub-standard Entry
Executive Summary	Success metrics & ROI.	Automate Free-to-Paid conversion pipeline. Target: 95% verification accuracy; reduce TTM (Time-to-Membership) by 80%.	"Building a bot to help with payments." (Lacks KPIs).
Market Opportunity	Scalability & TAM.	Scaling to 1,000+ users increases manual overhead by 40 hrs/week. Automating this captures a 30% operational efficiency gain.	"AI is trending, and we need to stay competitive."
Strategic Alignment	Organizational North Star.	Directly supports the "Seamless Onboarding" initiative by removing manual friction in the payment-to-access loop.	"This is a cool feature for the buildathon."
User Pain Points	JTBD (Jobs to	High churn risk: Participants experience "access anxiety" due to a 12-hour lag between	"The current manual process is a bit slow."

	be Done).	payment and Slack entry.	
Non-Functional Req.	Governance & Trust.	Latency <2s; Hallucination rate <1% via RAG-based grounding; SOC2 compliant data handling.	"The system needs to be fast and safe."

Part 2: AI Agent PRD (The Architectural Layer)

Objective: Define the agent's cognitive boundaries, tool-use capabilities, and degree of autonomy.

1. Persona & Autonomy Framework

- **Role Identity:** Define the agent's specialized domain (e.g., *Cross-Platform Billing Auditor*).
- **Cognitive Tone:** The communication style (e.g., *Analytical, authoritative, yet supportive*).
- **Autonomy Matrix:** * **Human-in-the-Loop (HITL):** Agent performs the heavy lifting (audit/matching); human provides the final authorization for high-stakes actions.
    - **Autonomous Execution:** Agent operates within a predefined "sandbox" for low-risk, high-frequency tasks.

2. Capabilities & Tool-Use (Function Calling)

Detail the "Integrated Stack" the agent will manipulate:

- **Read Access:** Google Sheets (Source of Truth), Gmail API (Transaction Verification).
- **Write Access:** n8n Webhooks (Workflow Triggering), Slack API (User Notifications).
- **Contextual Knowledge:** Vector database or structured RAG containing Buildathon policy documentation.

3. Agentic Workflow (The Core Loop)

Map the **Reasoning Chain (example)**:

1. **Ingestion:** Parse unstructured user intent from Slack DMs.
2. **Triangulation:** Cross-reference User ID in the Registry (Sheets) against Payment Proof (Gmail).
3. **Decision Logic:** If $Matches = True$ → Initiate Migration; If $False$ → Invoke Clarification Protocol.
4. **Exception Handling:** Define fallback states for ambiguous data (e.g., mismatched email aliases).

Part 3: System Visualization & Logic Defense

1. The Architectural Flow Chart

A professional blueprint identifying:

- **Triggers:** The specific event that initiates the agentic loop.
- **Orchestration:** Where n8n manages the flow vs. where the LLM manages the "thought."
- **Guardrails:** Points where the system validates output before proceeding.

2. Logic Defense: Why Generative AI?

Crucial for PMs: Justify the cost and complexity of an LLM.

- **Executive Justification:** "The input is highly non-linear and unstructured (natural language DMs). A deterministic script would fail to map the variety of user intents ('I paid,' 'Where's my link?', 'Substack charged me'). The agent uses **probabilistic reasoning** to synthesize data across disparate platforms (Sheets + Gmail) to resolve identity conflicts that a rigid if/else logic cannot handle."

WEEK 1: Evaluation Scorecard

Submissions are weighted based on:

- **Value Realization (35%):** Quantifiable impact on operational overhead or user retention.
- **Cognitive Depth (30%):** Sophistication of the Core Loop and the robustness of tool integration.
- **System Integrity (20%):** Evidence of hallucination mitigation and data verification protocols.
- **Risk Mitigation (15%):** Clearly defined HITL (Human-in-the-loop) triggers for critical business logic.