**Business Requirements Document (BRD)**  
**Agent Management Platform (AMP)**

**1. Executive Summary & Project Vision**

**Project Goal:**  
To empower organizations to effectively leverage AI for productivity gains, workflow automation, and knowledge worker assistance Agent Management Platfo….

**Core Objectives:**

* **Automate Workflows:** End-to-end orchestration of business processes via AI-driven tasks, with error handling, retries, and conditional logic Agent Management Platfo….
* **Enhance Productivity:** Library of pre-designed workflow templates, generic prompts, and AI assistants to streamline repetitive work Agent Management Platfo….
* **Assist Knowledge Workers:** Semantic, role-based knowledge base for rapid Q&A, document summarization, and contextual insights using Retrieval-Augmented Generation (RAG) Agent Management Platfo….
* **Empower Agent Creation:** Definition, building, and deployment of AI agents grounded in internal policies, procedures, and integrations Agent Management Platfo….

**Overall Approach:**  
Hybrid UI combining conversational chat, visual workflow builders, and embedded browser agents; dual audiences of non-technical business users and technical developers Agent Management Platfo….

**2. Target Audience & User Personas**

**2.1 Non-Technical Users (Business Users)**

* **Goal:** Automate simple tasks and access information without coding.
* **Needs:** Guided tutorials, tooltips, role-based workflow templates, contextual help Agent Management Platfo….
* **UI Features:**
  + Guided workflow execution interface
  + Role-based pre-built workflows
  + Interactive tutorials, tooltips, contextual help
  + Dashboards focused on performance and results
  + *Inspirations:* Gumloop’s guided tutorials; Botpress’s bot-creation wizard Agent Management Platfo….

**2.2 Technical Users (Developers, IT Professionals)**

* **Goal:** Build complex, custom workflows and integrate with external systems.
* **Needs:** Robust interface, APIs/SDKs (e.g., LangChain), advanced configuration Agent Management Platfo….
* **UI Features:**
  + Drag-and-drop workflow canvas
  + JSON/YAML editor for advanced customization
  + Custom tool/prompt creation
  + Live debugging, logs, version control
  + *Inspirations:* n8n’s node-based editor; Flowise’s visual LangChain builder Agent Management Platfo….

**2.3 Organizational Users**

* **Enterprise:** AI at scale with advanced compliance, security.
* **SMBs:** Balance of functionality, usability, affordability AI-Integrated Automatio….
* **AI-First Teams:** Prioritize AI-driven workflows and modern UX AI-Integrated Automatio….

**3. Functional Requirements**

**3.1 AI Applications & Core Functionality**

* **Workflow Automation:** Modular task orchestration; error handling, retries, conditional logic Agent Management Platfo….
* **Productivity Tools:** Workflow template library, prompt catalog, AI-powered helpers for common tasks (e.g., content generation, data analysis, email marketing) Agent Management Platfo….
* **Knowledge Worker Assistance:**
  + Search, summarize, interact with internal documents via RAG Agent Management Platfo….
  + Role-based knowledge base with data residency/retention policies Agent Management Platfo….
  + AI-powered search and data insights Agent Management Platfo….

**3.2 User Experience Layers**

* **Hybrid UI Approach:** Conversational chat + visual workflow builder + embedded browser agents Agent Management Platfo….
* **Dual-Audience Focus:** No-code/low-code for business users; SDKs (LangChain) for developers Agent Management Platfo….

**3.3 Workflow Builder**

* **Inspiration:** Make.com, n8n, Gumloop, Stack AI Agent Management Platfo….
* **Drag-and-Drop Interface:** Visual canvas for workflow creation Agent Management Platfo….
* **Pre-built Component Library:**
  + Data Processing (DBs, APIs, file storage)
  + AI Model Integration (Azure OpenAI, Vertex AI)
  + Logic & Control Flow (conditions, loops)
  + Output Generation (reports, notifications)
  + System/API Integration Agent Management Platfo….
* **Canvas Elements:** Connectors for AI services, ingestion/transformation, control structures, SDK for custom components Agent Management Platfo….
* **Versioning & Collaboration:** Workflow version control, rollback, team collaboration features Agent Management Platfo….
* **AI-Assisted Creation:** Natural-language to workflow description; AI suggestions initial research.
* **Collaboration Tools:** Commenting, annotation, approval workflows initial research.

**3.4 Knowledge Base**

* **Role-based Data Residency:** Configurable expiry Agent Management Platfo….
* **Document Ingestion:** Multimodal (text, files, images) Agent Management Platfo….
* **Vector Embeddings & RAG:** Indexed for retrieval Agent Management Platfo….
* **Search Interface:** Internal Q&A and semantic search Agent Management Platfo….

**3.5 AI Agent Studio / Creation & Management**

* **Agent Templates:** e.g., IT helpdesk, HR assistant, compliance monitor Agent Management Platfo….
* **Prompt Library & Task Chaining** Agent Management Platfo….
* **Natural Language → Agent Creation** Agent Management Platfo….
* **Integration:** Connect to internal systems/APIs Agent Management Platfo….
* **Knowledge Grounding:** Link agents to KB sections for context Agent Management Platfo….
* **Tool Usage:** Agents invoke internal/external tools & APIs Agent Management Platfo….
* **Governance & Oversight:** Analytics and dashboards for agent performance/compliance Agent Management Platfo….

**3.6 Integration Capabilities**

* **API Gateway:** Secure gateway with rate limiting & validation initial research.
* **Webhook System:** Real-time event notifications; user-configurable UI initial research.

**3.7 User Interface (General Features)**

* Responsive desktop & mobile design initial research.
* Consistent branding, dark mode, accessibility (screen reader, keyboard nav) initial research.

**4. Non-Functional Requirements**

**4.1 Security & Compliance**

* **GCP Private Tenant:** Data residency, security, compliance initial research.
* **RBAC:** Role-based access control Agent Management Platfo….
* **Encryption:** At rest and in transit Agent Management Platfo….
* **Audit Logs:** Comprehensive user/system activity logs Agent Management Platfo….
* **Org Policy Service:** Enforce policies (allowed regions, machine types) Agent Management Platfo….
* **Compliance Monitoring & Dashboards** initial research.
* **Automated Secrets Management:** Service credential rotation, no credentials in code Agent Management Platfo….

**4.2 Scalability & Performance**

* **Microservices Architecture:** Independent services for scalability Agent Management Platfo….
* **Load Balancing & Auto-scaling:** Cloud Run/GKE with HPA Agent Management Platfo….
* **Storage:** Multi-regional Cloud Storage with lifecycle rules Agent Management Platfo….
* **Database:** Cloud SQL (read replicas), Bigtable for throughput Agent Management Platfo….
* **Networking:** Auto-scaled load balancers, global backends Agent Management Platfo….
* **Caching:** Intelligent caching with invalidation strategies initial research.

**4.3 Monitoring & Analytics**

* **Performance Monitoring:** Real-time tracking, optimization tools Agent Management Platfo….
* **Metrics & Dashboards:** Latency, success rates, agent usage, model performance, SLO/SLI dashboards Agent Management Platfo….
* **Alerting:** Failures, anomalies, SLA breaches Agent Management Platfo….
* **Usage Analytics:** Workflow usage reports, customizable analytics initial research.

**4.4 Maintainability & Continuous Improvement**

* **Minimal Deployments:** Module grouping to reduce cycles initial research.
* **Layer Reusability:** Shared networking, IAM, storage modules initial research.
* **Documentation as Code:** Markdown docs alongside code initial research.
* **Versioning & Changelog:** Release tags, auto-published changelogs via CI/CD initial research.
* **Feedback Mechanism & A/B Testing** initial research.

**4.5 Cost & Budget Management**

* **Budgets & Alerts:** Billing Budget API alerts Agent Management Platfo….
* **Cost Ceilings:** Environment-specific cost caps, automated notifications initial research.
* **Quota Management:** API usage caps via Quota Management initial research.
* **Regular Review:** Automated budget reports; idle resource optimization initial research.

**5. Technical Architecture (GCP Private Tenant)**

**5.1 Cloud Foundation**

* **Private GCP Tenant:** Ensures data residency, security, compliance Agent Management Platfo….
* **Core GCP Services:** Cloud Run, Cloud Functions, Cloud Storage, Cloud Build, Secret Manager, Dataflow, Pub/Sub, Vertex AI Matching Engine Agent Management Platfo….
* **Networking:** VPC/subnets, private Google access, firewall rules, Cloud NAT Agent Management Platfo….

**5.2 Five-Layer Architecture**

**5.2.1 Pipeline Layer**

* **Data/Knowledge Base Pipeline:** Pub/Sub → Dataflow → Cloud Storage for ingestion/transformation Agent Management Platfo….
* **Code/Deployment Pipeline:** Git-triggered IaC (Terraform) in Cloud Build; Artifact Registry for modules; GitOps branching (feature/dev/main) Agent Management Platfo….
* **Cloud Operations Pipeline:** Cloud Monitoring, Cloud Logging, Cloud Functions for automated rollbacks Agent Management Platfo….

**5.2.2 Tools Layer**

* **Internal Tools:** Hosted on Cloud Run/Functions within tenant Agent Management Platfo….
* **External Connectors:** Azure OpenAI, Vertex AI, generic REST APIs Agent Management Platfo….
* **Secret Management:** Secret Manager with auto-rotation and replication Agent Management Platfo….

**5.2.3 Models Layer**

* **Model Registry:** Artifact Registry & Container Registry Agent Management Platfo….
* **Versioning & Packaging:** Cloud Build + QA gates (tflint, Conftest) Agent Management Platfo….
* **Vector Database:** Vertex AI Matching Engine or managed vector store for RAG Agent Management Platfo….

**5.2.4 Agents Layer**

* **Agent Runtimes:** Microservices on Cloud Run & Functions Agent Management Platfo….
* **IAM Service Accounts:** Least-privilege roles per agent Agent Management Platfo….
* **Deployment Strategies:** Canary, blue-green, horizontal autoscaling Agent Management Platfo….

**5.2.5 Workflows Layer**

* **Orchestration:** Google Workflows, Cloud Composer, Cloud Tasks Agent Management Platfo….
* **Definitions & Logic:** YAML-driven definitions; error handling, retries, conditional branches Agent Management Platfo….

**5.3 CI/CD Principles**

* **Declarative IaC:** Terraform (preferred) or Deployment Manager Agent Management Platfo….
* **Pipeline Automation:** cloudbuild.yaml steps: terraform init → plan → policy checks → manual approval → apply Agent Management Platfo….
* **Immutable Infrastructure & Rollbacks:** Resource replacement, canary deployments, Terraform state versioning, Cloud Build rollback on failed smoke tests Agent Management Platfo….
* **Automated Testing:** Unit tests for Terraform modules; integration via Test Kitchen/Molecule; simulation-based agent tests Agent Management Platfo….
* **Sandbox Environment:** Isolated sandbox for safe workflow/agent testing Agent Management Platfo….

**5.4 Environment Management**

* **Parameterized Configuration:** tfvars per environment (dev/test/preprod), substitution maps in Cloud Build Agent Management Platfo….
* **Service Accounts:** Dedicated account per environment initial research.

**6. Training, Documentation & Support**

* **User Guides:** Comprehensive guides for non-technical and technical users Agent Management Platfo….
* **Video Tutorials & Walkthroughs** Agent Management Platfo….
* **Contextual Tooltips & In-App Help** Agent Management Platfo….
* **Support Ticketing & Community Forum** Agent Management Platfo….
* **Developer API Docs & Extension Guides** initial research.

**7. Unique Selling Propositions (USPs)**

* **Customizable AI Solutions** Agent Management Platfo….
* **Seamless Integration** with existing systems initial research.
* **Continuous Learning & Improvement** of AI agents via feedback loops Agent Management Platfo….
* **Robust Data Security** measures—SOC2, GDPR-grade initial research.
* **AI-Native Design** (Gumloop-inspired) Agent Management Platfo….
* **Enterprise-Grade Capabilities** (Stack AI-inspired) AI-Integrated Automatio….
* **Open-Source Flexibility** (n8n-inspired) Agent Management Platfo….
* **Extensive Integrations & User-Friendliness** (Make-inspired) AI-Integrated Automatio….
* **Browser-Integrated Productivity** (Max AI-inspired) AI-Integrated Automatio….

**8. Competitive Landscape & Inspiration**

* **Conversational AI:** ChatGPT, Gemini, Claude, Mistral, Grok Agent Management Platfo….
* **AI Search Engines:** Perplexity, Deepseek, Phind, You.com Agent Management Platfo….
* **No-Code/Low-Code Automation:** Make.com, n8n, Zapier, Flowise, LangFlow initial research.
* **Specialized Agent Platforms:** Cognition AI, MultiOn, Adept AI initial research.
* **Browser Extensions:** MaxAI.me, Monica initial research.
* **Model Hubs & Dev Platforms:** Hugging Face, Replicate, LangChain, LlamaIndex Agent Management Platfo….