Marketplace Optimisation Agents

# Abstract

BlueMart's online marketplace ingests millions of seller-supplied SKUs every month. Images are often low-resolution, copy is incomplete or non-compliant, and search-critical keywords are missing. Manual QA cannot keep pace, resulting in long approval queues, lower search ranking, and lost GMV. Content-Perfect proposes a Google Cloud-native, LangGraph-orchestrated agent suite that enriches content, enforces policy compliance, and exposes a high-quality catalogue through an agent-to-agent (A2A) Google API—reducing time-to-publish from 24 h to < 5 min and lifting SKU conversion by ≥ 10 %.

# Background

* **Company**: BlueMart – retail giant with chains in 30+ cities plus an e‑commerce platform.
* **Scale**: Thousands of third‑party sellers, millions of SKUs, high daily churn.
* **Pain Points**:  
  • Manual listing review delays go‑live.  
  • Vendors complain that “the algorithm hides my product.”  
  • Brand‑consistency & legal exposure from unvetted copy.

# Objective & Success Metrics

Design and implement an automated pipeline that:

1. Crafts SEO-optimized titles, rich descriptions, and hero images.
2. Scores each submission against a policy knowledge graph and offers fix tips.
3. Publishes or rejects listings in < 5 min with minimal human touch.
4. Serves a curated catalogue to shoppers and external agents.

**Target KPIs**

* *Time‑to‑publish*: 24 h → **< 5 min**
* *SKU conversion*: **+10 %** uplift
* *Vendor rejection rate*: 18 % → **< 3 %**
* *AnswerBot top‑3 accuracy*: **≥ 95 %**

# Data Assets

|  |  |  |
| --- | --- | --- |
| Asset | File | Purpose |
| Compliance Rules | compliance\_rules.txt | Knowledge base for Inspector Agent. |
| Seller Submission Samples | seller\_submission\_samples.csv | Ten draft listings used by Phase 1 for ingestion tests. |
| Content Crafter Samples | content\_crafter\_samples.csv | Ten partially filled listings the Crafter Agent enriches. |
| Product Catalogue | catalog\_answer\_dataset.sqlite (table **catalog**) | Master dataset storing **both sample SKUs and all subsequent vendor uploads** after compliance validation. |
| Category Taxonomy | Google Retail Taxonomy (taxonomy.en‑US.txt) <https://www.google.com/basepages/producttype/taxonomy.en-US.txt> | Reference list for category & attribute validation. |
| Sample Images | Any image files | Used to test vision quality checks; linked URLs in datasets are dummy placeholders. |

# Solution Design & Detailed Phases

**Phase 1 – Seller Submission Intake & Pre‑Processing**

**1. API Ingestion:**

* Vendors submit SKUs through /v1/sku/submit REST endpoint.
* Data is accepted in JSON or CSV format.

**2. Staging & Storage:**

* Submissions stored in Cloud Storage.
* Records inserted into SQLite (catalog table, status = “draft”).

**3. Pre-Processing:**

* Language detection to route to correct prompts.
* Metadata extraction (brand, category, seller info).
* HTML sanitization to prevent unsafe tags.

**4. Optional Archiving:**

* Raw payloads stored in Firestore for backup & auditing.
* Value: Ensures a clean, structured entry point, reducing garbage-in, garbage-out issues.

**Phase 2 – Content Crafter Agent**

**1.Data Input:**

* Draft data (title, attributes, partial descriptions).

**2. Content Enrichment:**

* Vertex AI Gemini LLM generates:
* SEO titles with keywords.
* Rich descriptions highlighting features/benefits.
* Structured attributes (color, size, material, etc.).
* Imagen model creates hero images from vendor input.

**3. Persistence:**

* Outputs saved to Cloud Storage.
* Updates applied to same SQLite row.

**4. Audit Logging:**

* Prompt chain stored for future review & RLHF tuning.
* Value: Converts sparse, low-quality input into high-conversion listings.

**Phase 3 – Compliance Inspector Agent**

**1.Rule Validation:**

* Applies rules from compliance\_rules.txt (e.g., restricted keywords, legal disclaimers).

**2. Category Alignment:**

* Checks against Google Retail Taxonomy using Vertex AI Vector Search.

**3. Scoring & Verdict:**

* Each listing gets a 0–100 score.
* Fix tips generated inline (e.g., “Replace term X with approved variant”).
* Status updated to approved / needs\_fix / rejected in SQLite.

**4. Routing:**

* Failed listings pushed to vendor self-service UI for correction.
* Value: Guarantees trust, compliance, and brand consistency at scale.

**Phase 4 – Orchestrator Workflow**

**1.LangGraph Workflow:**

* Flow = Crafter → Inspector → Decision.

**2. State Management:**

* Tracks progress, ensures idempotent updates to SQLite.

**3. Error Handling:**

* Edge cases routed to Pub/Sub → human review.

**4. Security:**

* API keys & secrets stored in Secret Manager.
* Value: Central nervous system of the pipeline, ensuring smooth automation.

**Phase 5 – Catalog Answer Agent & A2A Google API**

**1.API Exposure:**

* Provides Google API Discovery Service–compliant endpoint.
* Serves only listings where status = approved.

**2. Agent-to-Agent Queries:**

* Supports queries like:
  + “Recommend similar products.”
  + “Is product X in stock?”
  + “What’s the latest price?”

**3. Performance:**

* Popular queries cached in Memorystore (Redis) for <100 ms response.  
  Value: Acts as a real-time product concierge, improving discoverability & conversion.

**Phase 6 – Observability & Guardrails**

1. **Metrics Collection:**

* **Cloud Logging** → token usage, latency, agent outputs.
* **Cloud Monitoring** → CPU, memory, error rates.

2. **Dashboards & Alerts:**

* Visual dashboards for ops teams.
* Alerts triggered on anomalies (e.g., error > 5%).

3. **Safety Filters:**

* Vertex AI Safety APIs block harmful or non-compliant outputs.  
  Value: Ensures reliability, transparency, and safe AI adoption.

**Phase 7 – Containerisation & Deployment**

**1.Containerisation:**

* Each agent + orchestrator packaged into Docker images.
* Stored in Artifact Registry.

**2. Deployment:**

* Run on Cloud Run with auto-scaling.

**3. CI/CD:**

* Managed via Cloud Build with triggers on Git merges.  
  Value: Enables scalable, repeatable deployments.

**Phase 8 – Pilot Rollout & Continuous Improvement *(Optional)***

***1.*Pilot Launch:**

* Activate on 5% of daily submissions.
* Compare KPIs vs. control group.

**2. Analytics-Driven Tuning:**

* Adjust LLM prompts, compliance thresholds, image quality.

**3. Scale-Up:**

* Gradually increase to 100% traffic once KPIs are met.  
  Value: Reduces rollout risk and ensures measurable improvements.

# Architecture

The processing pipeline is orchestrated by **LangGraph**, managing the flow through distinct phases:

* **Content Crafter Agent** enriches the incoming data using Vertex AI Gemini model, creating SEO-optimized product titles, detailed descriptions, and extracting relevant product attributes. Additionally, the Crafter generates hero images using Vertex AI Imagen. Enriched content and metadata log via Cloud Logging for observability and persist back into Cloud Storage, updating the relevant SQLite entry.
* **Compliance Inspector Agent** evaluates enriched content using predefined compliance rules (compliance\_rules.txt) and category alignment checks with the Google Retail Taxonomy indexed in Vertex AI Vector Search. The agent assigns each listing a score, offers inline fix tips for minor issues, and updates listing statuses in SQLite ("approved," "needs\_fix," or "rejected"). Significant compliance issues trigger automatic routing to vendor self-service UIs for corrections.
* **LangGraph Orchestrator** manages the overall workflow, sequencing the agents, handling edge-case escalations via Pub/Sub (for human intervention), and securely managing system secrets through Secret Manager.
* **Catalog Answer Agent** serves as the final interaction point, exposing approved product listings through a read-only Google API 3.1 compliant API. It efficiently handles agent-to-agent (A2A) queries, caching frequent requests using Memorystore for Redis to maintain sub-100 ms response times.

# Expected Deliverables

1. **Source Code**
   * LangGraph workflow definitions and node handlers.
   * Prompt templates and image‑generation scripts.
2. **Google Cloud Configuration**
   * Cloud Deployment Manager templates for all GCP resources.
   * Container image URIs in Artifact Registry.
   * Cloud Run service configurations.
   * Secret Manager and IAM policy configurations**.**
3. **Google API Specifications**
   * Seller Submission API
   * A2A Catalog Answer API.
4. **Observability Artifacts**
   * Cloud Monitoring dashboard configurations.
   * Cloud Logging query templates and alert policies.
5. **Operational Runbook**
   * Deployment guide, scaling procedures, rollback steps, incident playbook.
6. **Security & Compliance Docs**
   * Threat model, data‑flow diagrams, PII handling statement.