Architecture Summary – Multi-Domain Goal-Oriented Multi-Agent Systems

1. Executive Overview

This project implements structured, goal-oriented multi-agent workflows across five enterprise domains (Banking, E-Commerce, HR Operations, SaaS Support, and Supply Chain). Each system is built using CrewAI and follows a consistent architectural pattern emphasizing controlled decision-making, structured handoffs, and risk-aware escalation logic.

2. Agent Roles and Responsibilities

- Classification Agent – Identifies user intent or incident category.
- Policy / Knowledge Agent – Applies static rules, SLA logic, or domain policies (non-RAG).
- Response / Action Agent – Drafts structured customer response or operational action plan.
- Escalation Agent – Determines whether human intervention is required based on risk and safeguards.

3. Task Flow and Handoff Design

User Query → Classification → Policy Reasoning → Response Generation → Escalation Decision → Final Structured Handoff

Each agent communicates strictly via structured JSON outputs to ensure deterministic processing and reduce ambiguity. Handoffs include fields such as intent, confidence, allowed actions, draft response, risk score, and escalation status.

4. Escalation Logic and Risk Control

The system applies a hybrid escalation model combining LLM reasoning with deterministic safeguards. Escalation triggers include high-risk keywords (e.g., fraud, outage, harassment), low classification confidence, SLA breach risk, parsing failures, and domain-specific hard thresholds. If risk score exceeds predefined limits, escalation is enforced regardless of LLM judgment.

5. Sample Structured Output

```
{ "intent": "transaction_issue", "confidence": 0.95, "allowed_actions": ["check_statement",
"raise_dispute"], "draft_response": "...", "escalate": false, "risk_score": 45 }
```

6. Design Rationale

This architecture prioritizes safety, modularity, and reusability. By separating classification, reasoning, response, and escalation, the system prevents over-centralized logic and enables domain adaptation. Deterministic overrides ensure critical scenarios are never under-escalated. The design is extensible to healthcare, insurance, compliance, and enterprise IT automation domains.