COO Multi-Agent Workbench

Inception & Architecture Document (Frozen v1.0)

---

1. Introduction

The COO organisation operates at the intersection of **front office enablement, risk & control assurance, regulatory obligations, client servicing, and strategic execution**. Over time, this has resulted in multiple tools, manual processes, spreadsheets, emails, and siloed workflows across different COO functions.

This document captures the **inception, vision, and finalised architecture** of the **COO Multi-Agent Workbench** — a unified, future-ready platform designed to support COO teams using **task-aware Agentic AI**, while remaining **governance-safe, auditable, and human-centric**.

This is a **vision-level and architecture-level document**, intended to be the single reference point for the project's foundation.

---

2. Vision

To create one unified COO Workbench that: - Brings together all COO functions under a single operational backbone - Mirrors how COO teams actually work (tasks, reviews, controls, evidence) - Uses Agentic AI as a **co-pilot**, not a decision maker - Improves efficiency, transparency, and early risk visibility - Is scalable across regions, desks, and future COO mandates

Key principle:

> Agents assist, humans decide, and everything is auditable.

---

3. Current COO Setup (As-Is)

3.1 Organisational Reality

The COO ecosystem today consists of **multiple independent systems and manual processes**, including (illustrative): - NPA House - ROBO / desk support trackers - RICO / risk tooling - DEGA for DCE client servicing - BCP trackers - Spreadsheets, email chains, shared drives

3.2 Key Challenges

- Fragmented view of work and ownership
- Heavy manual coordination between functions

- Repeated data gathering and copy-paste activities
- Limited proactive risk signalling
- High dependency on individual experience
- Audit and evidence scattered across systems

---

4. COO Functions in Scope (Vision Level)

The Workbench is designed to support **all COO functions**, including:

1. Desk Support
2. NPA (New Product Approval)
3. Strategic Programme Management
4. Business Lead & Analysis
5. Operational Risk Management (ORM)
6. DCE Client Services
7. Business Analysis & Planning

While implementation may be phased, the **architecture is intentionally designed to support all functions** without re-work.

---

5. How COO Work Really Happens (Key Insight)

Across all COO functions, work ultimately consists of: - Clearly defined **responsibilities** (pillars) - Concrete **tasks** performed repeatedly - Reviews, approvals, and checks (maker–checker) - Documents, data, and evidence - Regulatory and audit obligations

This insight directly shapes the architecture.

---

6. Core Architectural Concept — The Work Item

6.1 What is a Work Item?

A **Work Item** is the universal operational unit in the COO Workbench.

Anything that the COO team must: - Track - Own - Review - Approve - Evidence - Audit

...is modelled as a **Work Item**.

6.2 Examples

- An NPA submission
- A desk control breach
- A regulatory report

- A monthly KRI review
- A DCE client issue

---

7. Work Item Modes (Critical Design Element)

To avoid forcing all work into an "NPA-like" flow, each Work Item declares a **Mode**:

- **Approval** – structured reviews and sign-offs (e.g. NPA)
- **Monitoring** – continuous or signal-based oversight
- **Recurring** – periodic obligations (monthly / annual)
- **Reporting** – data aggregation and governance packs
- **Exception** – urgent escalations and breaches

Same backbone, different behaviour.

---

8. Lifecycle: Macro vs Micro

- **Macro lifecycle**: Linear, stage-based (e.g. NPA 6 stages)
- **Micro iteration**: Loop-backs, rework, clarifications *within* a stage

This accurately reflects real COO operations without introducing chaos.

---

9. Task-Aware Agentic Design (Core Differentiator)

9.1 Why Task-Aware Agents?

Each COO function is explicitly broken down into: - **Pillars** (stable responsibility areas) - **Tasks** (concrete operational actions)

Agents must therefore be **task-aware**, not generic.

---

10. Agent Architecture (Final)

10.1 Agent Layers

1. **Agent Orchestrator (Platform-wide)**

2. Routes work based on Function, Pillar, Task, and Work Item Mode

3. **Function (Domain) Agents**

4. Desk Support Agent

5. NPA Agent
6. ORM Agent
7. DCE Agent

8. etc.

9. **Task-Level Agents (Function-specific)**

10. Mapped 1:1 to real COO tasks

11. Example:

   - Desk → Controls → Transaction Anomaly Agent
   - NPA → Review → Completeness Check Agent

12. **Utility Agents (Shared)**

13. Document / Data Extraction
14. Policy & SOP RAG
15. Validation & Rules
16. Explainability & Citations
17. Proactive Risk & Delay Alerts
18. Notification & Reminder

---

11. Agents' Role & Boundaries

Agents **can**: - Read and analyse data - Pre-populate templates - Validate completeness - Highlight risks and delays - Draft summaries and recommendations - Explain "why" with evidence

Agents **cannot**: - Approve - Override policy - Change official state without human/system action

This ensures trust, governance, and auditability.

---

12. Core Building Blocks (Frozen)

The platform is built around five non-negotiable objects:

1. **Work Item** – the operational backbone
2. **Workflow / Stage** – lifecycle control
3. **Task** – actionable unit of work
4. **Artifact** – documents, data, evidence (versioned)
5. **Audit Event** – immutable history (human + agent)

These are fixed to ensure UI scalability and consistency.

---

13. Cross-Function Collaboration

Work Items can: - Depend on other Work Items - Link across functions (e.g. NPA ↔ Desk Support ↔ ORM) - Block progression until dependencies are resolved

This reflects real COO inter-dependencies.

---

14. Dual Decisioning Model

For key decisions, the Workbench supports:

- **Rule-based view** – policies, limits, regulatory rules
- **Practice-based view** – historical patterns and precedents

Both are shown transparently; humans decide.

---

15. Why This Architecture Works

- Mirrors real COO work
- Avoids siloed tools
- Scales across functions and regions
- Enables phased rollout
- Keeps humans in control
- Makes agents visible and explainable
- Reduces manual glue work

---

16. Conclusion

The COO Multi-Agent Workbench architecture is now **frozen at v1.0**.

It provides a robust, future-ready foundation that: - Supports all COO functions - Embeds task-aware Agentic AI - Preserves governance and audit integrity - Enables modern, scalable UI design

This document represents the **official inception and architectural baseline** for the project.

Status: Architecture v1.0 — Locked