Executive Overview - Automation Architecture

The automation architecture for the Enterprise Motor Insurance Claims Transformation was designed as a structured, layered digital orchestration model aligned with regulated financial services standards.

The objective was not to deploy isolated RPA bots, but to establish a scalable, risk-aware, and governance-embedded operating framework capable of handling high-volume claims while maintaining audit defensibility and regulatory compliance.

The architecture integrates five core layers:

1. **Customer Layer** – Digital claim intake and document submission
2. **Automation Layer** – Workflow orchestration using UiPath Orchestrator and unattended robots
3. **Processing Layer** – OCR ingestion, rule-based eligibility validation, and fraud risk scoring
4. **Core Systems Layer** – Claims, policy, payment, and audit systems integration
5. **Governance Layer** – SLA monitoring, risk dashboards, model oversight, and compliance controls

This layered structure ensures clear separation of responsibilities, controlled system interaction, and proportional risk routing across the claims lifecycle.

A structured fraud scoring model (0–100 scale) drives tiered decision routing, enabling:

- Straight-through processing for low-risk claims
- Claims officer review for medium-risk cases
- Fraud team escalation for high-risk scenarios

Importantly, artificial intelligence components operate in an assistive capacity only. No automated claim rejection is permitted, and all decisions are subject to human oversight and full audit logging.

The architecture embeds proactive SLA governance through real-time intake timestamp tracking, threshold-based alerts, and supervisor escalation triggers, replacing reactive manual monitoring with predictive control mechanisms.

Designed for scalability, the model supports volume surges during catastrophic events through queue prioritisation and unattended bot scaling while maintaining governance safeguards.

Overall, the architecture demonstrates enterprise automation maturity by combining operational efficiency, structured risk management, responsible AI integration, and regulatory defensibility within a cohesive digital framework.