

Lifecycle phase

Governance controls

Owner

Design

Scope definition, risk classification, use-case approval

Product owner

Development

Policy-as-code implementation, guardrail coding, security testing

DevSecOps

Testing

Boundary validation, adversarial testing, edge-case scenarios

QA + Security

Deployment

Permission provisioning, guardrail activation, monitoring setup

Platform engineering

Runtime

Real-time monitoring, escalation handling, guardrail enforcement

Operations

Monitoring

Log analysis, KPI tracking, drift detection, compliance reporting

Governance office

Decommission

Access revocation, audit archive, lessons-learned documentation

Security + Compliance