ATB Operating Model

This document defines the operational governance for the Agent Trust Broker (ATB) platform.

---

1. RACI Matrix

Activity	Broker-Team	AgentAuth-Team	Security	Legal	Platform-Ops
Define low-risk allowlist (`low_risk_allowlist`)	C	R	A	I	I
Approve high-risk agent actions (dual control)	I	R	A	C	I
Issue PoA mandates	I	R	C	A	I
Update OPA policy (`poa.rego`)	R	C	A	I	I
Maintain connector registry	R	I	C	I	C
Define legal basis templates (`leg` schema)	I	C	C	R	I
Review audit logs for compliance	I	I	R	C	I
Incident response (security events)	C	C	R	I	A
Platform upgrades / deployments	C	C	I	I	R

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

2. Approval Flows

2.1 PoA Issuance – Standard Flow

```
Agent → POST /issue → AgentAuth
                      ├─ Validate SPIFFE identity (mTLS)
                      ├─ Validate request schema
                      └─ Issue EdDSA-signed PoA (5 min TTL)
```

- **Pre-requisite:** Agent must present valid SPIFFE SVID.
- **Audit:** Every issuance is logged with `event_type: poa_issued`.

2.2 PoA Issuance – Dual Control (High-Risk)

```
Agent → POST /issue { requires_dual_control: true, approvers: [...] }
                      ├─ Validate ≥2 distinct approvers
                      ├─ Validate approver SVID subjects differ from requester
                      └─ Issue EdDSA-signed PoA (short TTL)
```

- **Trigger:** Action flagged as high-risk by policy (e.g., bulk delete, PII export).
- **Approvers:** Must be distinct principals; self-approval is blocked.
- **Audit:** `event_type: poa_issued_dual_control`, includes approver IDs.

2.3 Policy Change Flow

```
Developer → PR to opa/policy/poa.rego
```

```
                    ├─ CI: opa test (unit + integration)
                    ├─ Security review (required CODEOWNER)
                    └─ Merge → GitOps deploy to OPA sidecar
```

- **Gate:** All policy changes require Security team approval.
- **Rollback:** Revert commit triggers automatic rollback via ArgoCD / Flux.

2.4 Connector Onboarding Flow

```
Requestor → Open issue: "Add connector: <system>"
                    ├─ Security review egress allowlist
                    ├─ Legal review data classification
                    ├─ Broker-Team implements config
                    └─ Merge → Helm upgrade → Connector active
```

---

3. Risk Thresholds

Risk Level	Definition	Control	OPA Enforcement
Low	Read-only, non-PII, internal data	PoA required (or allowlist)	`low_risk_allowlist` if AL-LOW_UNMANDATED_LOW_RISK=
Medium	Write operations, limited PII	PoA + single approver	`leg.approval.approver_id` required, must differ from requester
High	Bulk operations, PII export, financial transactions	PoA + dual control (2 approvers)	`leg.dual_control.approve` with ≥2 distinct principals
Critical	Cross-tenant, privileged access, deletion	Dual control + manual approval	Same as High, plus external ticket reference

Risk-Tiered Actions (in OPA policy)

> **Full catalog:** See `docs/enterprise-actions.md` for complete action reference with constraint rules.

Medium-Risk Actions (`medium_risk_actions`) — 40+ actions including: - **CRM:** `crm.contact.update`, `crm.lead.create`, `crm.opportunity.update` - **ERP:** `erp.order.create`, `erp.order.cancel`, `erp.invoice.create` - **HR:** `hr.employee.view_limited`, `hr.timesheet.approve`, `hr.leave.approve` - **Support:** `support.ticket.create`, `support.ticket.escalate` - **Inventory:** `inventory.stock.adjust`, `inventory.transfer.create` - **Marketing:** `marketing.campaign.launch`, `marketing.email.send_batch`

High-Risk Actions (`high_risk_actions`) — 60+ actions including: - **SAP:** `sap.vendor.change`, `sap.payment.execute`, `sap.journal_entry.post` - **Salesforce:** `salesforce.bulk.export`, `salesforce.apex.execute` - **HR/PII:** `hr.employee.export_pii`, `hr.payroll.run`, `hr.compensation.change` - **Customer:** `customer.gdpr.erasure`, `customer.ccpa.export`, `customer.pii.access` - **IAM:** `iam.role.assign`, `iam.mfa.disable`, `azure.ad.role_assign` - **Cloud:** `aws.iam.policy_attach`,

azure.rbac.assign, azure.keyvault.secret_set - **OT/SCADA:** ot.system.manual_override, scada.setpoint.change, ot.safety.interlock_bypass - **ServiceNow:** servicenow.change.emergency_approv servicenow.incident.priority1_create

Low-Risk Allowlist (low_risk_allowlist) — 45+ read-only actions: - **CRM reads:** crm.contact.read, crm.lead.list, crm.opportunity.read - **ERP reads:** erp.order.read, erp.invoice.read, erp.vendor.read - **Catalog:** catalog.product.read, catalog.category.list - **Support:** support.ticket.read, support.kb.search - **Reporting:** reporting.dashboard.view, analytics.dashboard.view

Example leg Claims by Tier

Medium-risk (single approver):

```
{
  "leg": {
    "jurisdiction": "US",
    "accountable_party": {"type": "employee", "id": "emp-100"},
    "approval": {
      "approver_id": "manager-001",
      "approved_at": "2024-01-15T10:00:00Z"
    }
  }
}
```

High-risk (dual control):

```
{
  "leg": {
    "jurisdiction": "EU",
    "accountable_party": {"type": "employee", "id": "emp-200"},
    "dual_control": {
      "required": true,
      "approvers": [
        {"id": "approver-a", "type": "manager"},
        {"id": "approver-b", "type": "compliance"}
      ]
    }
  }
}
```

---

4. Mandate Templates

Templates for common leg (legal basis) claims:

4.1 Legitimate Interest

```
{
  "leg": {
    "basis": "LI",
    "ref": "LI-2024-001",
    "description": "Routine system maintenance"
  }
}
```

4.2 Contractual Necessity

```
{
  "leg": {
    "basis": "CONTRACT",
    "ref": "MSA-12345",
    "description": "Fulfill customer order #789"
  }
}
```

4.3 Consent

```
{
  "leg": {
    "basis": "CONSENT",
    "ref": "CONSENT-TOKEN-abc123",
    "data_subject": "user@example.com",
    "purpose": "Marketing email"
  }
}
```

4.4 Legal Obligation

```
{
  "leg": {
    "basis": "LEGAL",
    "ref": "GDPR-Art17",
    "description": "Right to erasure request"
  }
}
```

---

5. Escalation Paths

Severity	Response Time	Escalation
P1	15 min	On-call → Security Lead → CISO
P2	1 hour	On-call → Team Lead
P3	4 hours	Ticket queue
P4	Next sprint	Backlog

Security Event Triggers (P1)

- `ATBSecurityPolicyDenialSpike` alert fires
- Audit log shows repeated `poa_single_use_replay_blocked`
- Guardrails blocks confirmed prompt injection attempt

---

6. Audit Retention

Log Type	Retention	Storage
Access logs	90 days	Splunk / Elastic
Audit events	7 years	Immutable blob (compliance)
Prometheus metrics	30 days	Thanos / Cortex

---

7. Change Management

All production changes follow the standard CAB process:

1. **RFC Submission:** Describe change, risk, rollback plan.
2. **CAB Review:** Weekly meeting; emergency changes via on-call.
3. **Approval:** Requires Security + Platform-Ops sign-off.
4. **Execution:** GitOps deployment with canary rollout.
5. **Validation:** Smoke tests + SLO dashboards.

---

8. Contact Points

Role	Team / Alias
Broker-Team	`#atb-broker` / broker@corp.com
AgentAuth-Team	`#atb-agentauth` / agentauth@…
Security	`#security-oncall` / security@…
Legal / Compliance	`#legal-privacy` / legal@…
Platform-Ops	`#platform-ops` / ops@…

Last updated: 2026