Enterprise Actions Reference

This document describes the risk-tiered action catalog and constraint policies enforced by ATB's OPA policy engine.

Risk Tier Overview

Tier	Count	Approval Required	Examples
High	60+	Dual control (2 distinct approvers)	SAP payments, bulk PII export, IAM escalation, OT safety overrides
Medium	40+	Single approver	CRM updates, order management, inventory adjustments
Low (allowlisted)	45+	None (valid PoA sufficient)	Read-only queries, status checks, catalog browsing

---

High-Risk Actions

Actions in this tier require **dual control**: two distinct approvers in `leg.dual_control.approvers`, neither of whom may be the PoA subject.

SAP ERP

Action	Description	Constraint Rules
`sap.vendor.create`	Create new vendor master	Dual control
`sap.vendor.change`	Modify vendor master	Amount ≤ 5000 or dual + liability_cap ≥ amount
`sap.vendor.bank_change`	Change vendor bank details	Second-channel verification, reason ≥ 10 chars
`sap.payment.execute`	Execute single payment	Amount ≤ payment_limit (default 100k)
`sap.payment.batch_release`	Release payment batch	Batch count ≤ max_batch_count, total ≤ max_batch_amount
`sap.goods_receipt.post`	Post goods receipt	Dual control
`sap.invoice.post`	Post vendor invoice	Dual control
`sap.journal_entry.post`	Post journal entry	GL account + cost center required, amount ≠ 0
`sap.cost_center.create`	Create cost center	Dual control
`sap.gl_account.create`	Create GL account	Dual control

Financial Transactions

Action	Description
`erp.payment.process`	Process ERP payment
`erp.payment.batch`	Batch payment processing
`erp.refund.process`	Process refund

Action	Description
`erp.credit_note.issue`	Issue credit note
`finance.wire_transfer.execute`	Execute wire transfer
`finance.ach.batch_submit`	Submit ACH batch
`finance.fx.trade_execute`	Execute FX trade

Salesforce

Action	Description	Constraint Rules
`salesforce.bulk.export`	Bulk data export	Dataset in allowlist, rows ≤ max_rows (10k default)
`salesforce.bulk.delete`	Bulk record deletion	Object in deletable list, count ≤ max_delete_count (1k default)
`salesforce.bulk.update`	Bulk record update	Dual control
`salesforce.apex.execute`	Execute Apex script	Script in approved_apex_scripts list
`salesforce.permission_set.assign`	Assign permission set	Dual control
`salesforce.profile.modify`	Modify user profile	Dual control
`salesforce.report.export_all`	Export all report data	Report in exportable_reports list

CRM Bulk Operations

Action	Description
`crm.contacts.bulk_delete`	Bulk delete contacts
`crm.contacts.bulk_export`	Bulk export contacts
`crm.accounts.bulk_merge`	Merge multiple accounts
`crm.data.mass_update`	Mass data update

HR/PII Sensitive

Action	Description	Constraint Rules
`hr.employee.export_pii`	Export employee PII	Purpose in [audit, legal_hold, regulatory_compliance, internal_investigation], count ≤ max_pii_export (500 default)
`hr.employee.terminate`	Terminate employee	Offboarding checklist complete, reason ≥ 10 chars
`hr.payroll.run`	Run payroll	Period specified, employee count ≤ max_payroll_employees
`hr.payroll.adjust`	Adjust payroll	Dual control
`hr.compensation.change`	Change compensation	Percentage ≤ max_compensation_pct_change (25% default), ≥ -50%, justification ≥ 20 chars
`hr.ssn.view`	View SSN	Dual control
`hr.bank_details.update`	Update bank details	Dual control

Customer Data

Action	Description	Constraint Rules
`customer.data.export`	Export customer data	Dual control
`customer.data.bulk_delete`	Bulk delete customer data	Dual control
`customer.pii.access`	Access customer PII	Purpose in [support_case, billing_inquiry, identity_verification, fraud_investigation], reference_id required
`customer.gdpr.erasure`	GDPR erasure request	Request ID required, days_since_request ≤ 30
`customer.ccpa.export`	CCPA data export	Request ID required, format in [json, csv, pdf]

IAM/Identity

Action	Description	Constraint Rules
`iam.role.assign`	Assign role to user	Role + target_user required, no self-assign, role in assignable_roles (if constrained)
`iam.role.create`	Create new role	Dual control
`iam.permission.grant`	Grant permission	Dual control
`iam.user.create_admin`	Create admin user	Dual control
`iam.mfa.disable`	Disable user MFA	Incident reference required, target_user required, identity verified
`iam.api_key.create`	Create API key	Dual control
`iam.service_account.create`	Create service account	Dual control
`azure.ad.group_add`	Add to Azure AD group	Dual control
`azure.ad.role_assign`	Assign Azure AD role	Dual control
`okta.user.unlock`	Unlock Okta user	Dual control
`okta.factor.reset`	Reset Okta MFA factor	Dual control

Cloud Infrastructure

Action	Description	Constraint Rules
`aws.iam.policy_attach`	Attach IAM policy	Admin policies blocked unless allow_admin_policy=true
`aws.s3.bucket_policy`	Set S3 bucket policy	Dual control
`aws.ec2.security_group_modify`	Modify security group	Dual control
`azure.rbac.assign`	Assign Azure RBAC role	Subscription-level Owner blocked unless allow_subscription_owner=true
`azure.keyvault.secret_set`	Set Key Vault secret	Protected vaults blocked unless allow_protected_vault_write=true
`gcp.iam.binding_add`	Add GCP IAM binding	Dual control
`k8s.rbac.clusterrole_bind`	Bind K8s ClusterRole	Dual control
`k8s.secret.create`	Create K8s secret	Dual control

OT/Safety Critical

Action	Description	Constraint Rules
`ot.system.manual_override`	Manual system override	HIL approval required, window ≤ 900s (15 min)
`ot.safety.interlock_bypass`	Bypass safety interlock	Justification ≥ 20 chars, duration ≤ max_bypass_duration (3600s default), safety_officer_approved

Action	Description	Constraint Rules
`scada.setpoint.change`	Change SCADA setpoint	Value within [setpoint_min, setpoint_max], safety_review_acknowledged
`scada.alarm.acknowledge_critical`	Acknowledge critical alarm	Dual control
`plc.program.upload`	Upload PLC program	Dual control
`hmi.mode.change_to_manual`	Switch HMI to manual	Dual control

ServiceNow

Action	Description	Constraint Rules
`servicenow.change.emergency_approve`	Emergency change approval	Change number required, CAB approved OR emergency with justification ≥ 20 chars
`servicenow.incident.priority1_create`	Create P1 incident	Business impact ≥ 10 chars, affected_users > 0
`servicenow.cmdb.bulk_update`	Bulk CMDB update	Dual control

Workday

Action	Description	Constraint Rules
`workday.worker.terminate`	Terminate worker	Dual control
`workday.compensation.change`	Change compensation	Percentage ≤ max_compensation_pct_change, effective_date required
`workday.org.restructure`	Org restructure	Dual control

Dynamics 365

Action	Description	Constraint Rules
`dynamics.entity.bulk_delete`	Bulk entity deletion	Entity in deletable_entities (if constrained), count ≤ max_delete_count
`dynamics.workflow.deactivate`	Deactivate workflow	Dual control
`dynamics.security_role.assign`	Assign security role	Dual control

Medium-Risk Actions

Actions in this tier require **single approver**: `leg.approval.approver_id` must be present and different from PoA subject.

CRM Operations

Action	Description
`crm.contact.update`	Update contact record
`crm.contact.delete`	Delete contact
`crm.lead.create`	Create lead

Action	Description
`crm.lead.convert`	Convert lead to opportunity
`crm.opportunity.update`	Update opportunity
`crm.account.update`	Update account

ERP/Order Management

Action	Description
`erp.order.create`	Create order
`erp.order.update`	Update order
`erp.order.cancel`	Cancel order
`erp.invoice.create`	Create invoice
`erp.invoice.void`	Void invoice
`erp.purchase_order.create`	Create purchase order
`erp.purchase_order.approve`	Approve purchase order

HR (Limited PII Access)

Action	Description
`hr.employee.view_limited`	View limited employee info
`hr.employee.update_contact`	Update employee contact info
`hr.timesheet.approve`	Approve timesheet
`hr.leave.approve`	Approve leave request
`hr.org_chart.update`	Update org chart

Support/Ticketing

Action	Description
`support.ticket.create`	Create support ticket
`support.ticket.update`	Update ticket
`support.ticket.escalate`	Escalate ticket
`support.ticket.reassign`	Reassign ticket
`support.case.merge`	Merge cases

Inventory/Warehouse

Action	Description
`inventory.stock.adjust`	Adjust stock levels
`inventory.transfer.create`	Create inventory transfer
`inventory.count.submit`	Submit inventory count
`warehouse.location.update`	Update warehouse location

Product/Catalog

Action	Description
`catalog.product.update`	Update product
`catalog.product.publish`	Publish product
`catalog.price.update`	Update pricing
`catalog.category.update`	Update category

Marketing

Action	Description
`marketing.campaign.launch`	Launch marketing campaign
`marketing.email.send_batch`	Send batch email
`marketing.segment.update`	Update marketing segment

Collaboration

Action	Description
`sharepoint.document.share_external`	Share document externally
`teams.channel.create`	Create Teams channel
`confluence.space.permission_update`	Update Confluence permissions

Low-Risk Allowlist

Actions in this tier are **allowed without special approval** when a valid PoA is present. They can also bypass PoA entirely if `ALLOW_UNMANDATED_LOW_RISK=true`.

System/Infrastructure

- `system.health.check`
- `system.status.get`
- `system.version.get`
- `system.config.read`

Knowledge Base/Documentation

- `kb.faq.query`
- `kb.docs.search`
- `kb.article.read`

Reporting (Non-PII)

- `reporting.dashboard.view`
- `reporting.metrics.get`
- `report.sales.summary`
- `report.inventory.status`
- `report.support.metrics`
- `analytics.dashboard.view`

Agent Introspection

- `agent.self.capabilities`
- `agent.self.identity`

CRM Read Operations

- `crm.contact.read`, `crm.contact.list`
- `crm.lead.read`, `crm.lead.list`
- `crm.opportunity.read`, `crm.opportunity.list`
- `crm.account.read`, `crm.account.list`

ERP Read Operations

- `erp.order.read`, `erp.order.list`
- `erp.invoice.read`
- `erp.purchase_order.read`
- `erp.product.read`
- `erp.vendor.read`
- `erp.customer.read`

HR Read Operations (Non-PII)

- `hr.org_chart.read`
- `hr.department.list`
- `hr.job_posting.read`
- `hr.holiday.list`

Support/Ticketing Read Operations

- `support.ticket.read`, `support.ticket.list`
- `support.kb.search`, `support.kb.read`

Inventory Read Operations

- `inventory.stock.read`
- `inventory.location.list`
- `warehouse.status.read`

Catalog Read Operations

- `catalog.product.read`, `catalog.product.list`
- `catalog.category.list`
- `catalog.price.read`

Collaboration Read Operations

- `sharepoint.document.read`, `sharepoint.list.read`
- `teams.channel.list`, `teams.message.read`

Constraint Schema Reference

Common Constraint Fields

Field	Type	Description
`dual_control`	boolean	Require dual control for the action
`liability_cap`	number	Maximum liability amount covered
`max_rows`	number	Maximum rows for bulk operations
`max_delete_count`	number	Maximum records for deletion
`dataset_allowlist`	string[]	Allowed datasets for export
`approved_apex_scripts`	string[]	Allowed Apex scripts
`exportable_reports`	string[]	Allowed report IDs for export
`deletable_objects`	string[]	Objects allowed for deletion
`deletable_entities`	string[]	Entities allowed for deletion
`assignable_roles`	string[]	Roles allowed for assignment
`protected_vaults`	string[]	Key Vault names that are protected

OT/Safety Constraints

Field	Type	Description
`override_window_seconds`	number	Max duration for manual override (≤ 900)
`max_bypass_duration`	number	Max interlock bypass duration (default 3600)
`setpoint_min`	number	Minimum safe setpoint value
`setpoint_max`	number	Maximum safe setpoint value

HR/Compensation Constraints

Field	Type	Description
`max_compensation_pct_change`	number	Max percentage change (default 25%)
`max_pii_export`	number	Max PII records to export (default 500)
`max_payroll_employees`	number	Max employees in payroll run

Cloud Constraints

Field	Type	Description
`allow_admin_policy`	boolean	Allow Administrator policy attachment
`allow_subscription_owner`	boolean	Allow subscription-level Owner
`allow_protected_vault_write`	boolean	Allow writes to protected vaults

Extending the Action Catalog

To add new actions:

1. **Identify risk tier** based on:
   - Financial impact
   - PII/sensitive data access

    - Privilege escalation potential
    - Safety implications
    - Reversibility

2. **Add to appropriate list** in `opa/policy/poa.rego`:

    - `low_risk_allowlist` (objects with action/methods)
    - `medium_risk_actions` (strings)
    - `high_risk_actions` (strings)

3. **Add constraint rules** (optional) for high-risk actions:

    ```
    action_allowed {
        act == "your.new.action"
        your_new_action_allowed
    }

    your_new_action_allowed {
        # Constraint validation logic
    }
    ```

4. **Add to explicit_high_risk_rule** if action has constraint rules

5. **Add tests** in `opa/policy/` to validate enforcement

6. **Update documentation** in this file