IsDB DevOps Governance Proposal

Executive Summary

This proposal introduces an **Enterprise Governance Model for Azure DevOps Release Management** to address critical gaps in the current CI/CD process. Today, the environment is fully Dev-owned, lacking segregation of duties, audit trails, and standardized governance—creating operational risk and compliance challenges.

The proposed solution transitions to a **Governance-as-Code** model, where **Ops owns the delivery mechanism** (pipelines/infrastructure) and **Dev owns the deliverable** (code/logic). This decoupling enforces compliance, protects production environments, and reduces unplanned work without slowing development velocity.

Key elements include:

- **Standardized Golden Templates** for pipelines
- **Mandatory dual-approval** for release branches
- **Immutable artifacts** and controlled production deployments
- **Technical enforcement** via Azure DevOps features (branch policies, code owners, environment gates)

Once the Proposed Process is agreed – We will have a Proof of Concept (PoC) to validate the model over two sprints, measuring KPIs such as change failure rate, deployment lead time, and audit readiness.

Aim is to ensure Ops team creates a Env with governance and standard best practices while SD Team can have a platform from where they can request and get things rolling quickly.

Proposal: RACI Matrix for Azure DevOps

Context

This model is designed considering below:

- **Dev uses Jira**
- **Ops use BMC**
- **Ops owns pipeline governance**
- **Dev owns repository content**
- **Ops controls deployments**
- **Dev and Ops jointly validate releases**

Current Pain Points

TO Team:

- Production releases involve only Dev Team Lead; Ops is excluded — poor practice.
- Limited visibility and control over DevOps; often pulled into firefighting without much context.
- Devs escalate issues (e.g., ODM build failures); Ops takes time to track and troubleshoot due to lack of setup knowledge.

SD Team:

- Skips deployments to lower environments citing high effort and time for re-setup (e.g., Azure Function → Prod SPO integration request by Br. Fadi).
- Dev Team feels pipeline creation takes weeks; deployment approvals take 1–2 days (e.g., Fusion Invest deployment). Hence they avoid involving Ops from beginning

Roles Defined

- **DEV** = SD Team
- **OPS** = TO Team
- **OPS Lead** = Br. Mudassar / Br. Abu Fahad
- **Change Mgr** = Br. Mudassar
- **Security** = Bank Security/Compliance / UAM Team

1. Azure DevOps Project Creation

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Request for new project	R	A	C	C	
Create project	C	R	A	I	I
Set RBAC & permissions	I	R	A	I	C
Enforce branch policies	C	R	A	I	C

Why: Dev should not create or control projects. Governance must be owned by Ops.

2. Repositories (Azure Repos)

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Repo creation request	R	A	C	I	I
Repo creation	I	R	A	I	I
Commit code	R	I	I	I	I
Branch creation	R	C	A (protected Branches) **	I	I
Branch protection rules	C	R	A	I	C
PR review	R	C	A (release PRs)	I	I

Key Enforcement: Dev owns code; Ops owns protected branches (main, prod, release)**.

3. Service Connections (Azure RM, GitHub, Key Vault, etc.)

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Request new connection	R	A	C	I	I
Create service connection	I	R	A	I	C
Approve service connection	I	R	A	I	I
Rotate credentials/secrets	I	R	A	I	C

Reason: Devs must **never** create service connections — compliance risk.

4. Hosted/Private Agents

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Request agent	R	A	C	I	I
Install/Configure agent	I	R	A	C	I
Maintain agent	I	R	A	I	I
Approve network/firewall	I	R	A	C	C

5. Build Pipelines (CI)

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Request CI pipeline	R	A	C	I	I
Create new CI pipeline	I	R	A	I	C
Modify shared templates	I	R	A	I	C
PR validation build rules	C	R	A	I	C
Trigger build	R	I	I	I	I

Rule: Dev writes code; Ops writes pipeline logic.

6. Release Pipelines (CD – Lower Environments)

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Request CD pipeline	R	A	C	I	I
Configure CD to Dev/Test	I	R	A	I	C
Approve QA deployment	R	C	A	I	I
Deploy to QA	I	R	A	I	I
Validate QA smoke tests	R	R	A	I	I

Note: No BMC CR required here, Dev Team to extend the template provided by Ops team.

7. Release Pipelines (CD – Production)

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Raise BMC CR	I	R	A	C	I
Provide functional signoff	R	I	I	I	I
Approve deployment (ADO)	I	R	A	C	I
Deploy to PROD	I	R	A	C	I
Perform smoke test	I	R	A	I	I
Validate functional test	R	C	A	I	I

8. Release Branch Management

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Move Jira ticket → Ready	R	I	I	I	I
Create release branch	I	R	A	I	I
Prepare PR into release	I	R	A	I	I
Review PR	R	C	A	I	I

9. Approvals & CAB – Only for specific ones

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Approve pipeline changes	I	R	A	I	C
Approve production deploy	I	C	A	R	I
CAB for high-risk changes	I	C	C	A	C

10. Incident, Rollback & Support

Task	DEV	OPS	OPS Lead	Change Mgr	Security
Detect issue	R	R	A	I	I
Trigger rollback	I	R	A	I	I

| Validate rollback | R | C | A | I | I |
| Post-incident RC analysis | R | R | A | C | C |