An Introduction to Continuous Governance at NAB

Deploy your most important workloads into cloud with confidence

Yuri Belenky
Head of Application and Cloud Platforms
National Australia Bank

Brandon Grenier
Senior Cloud Architect
Amazon Web Services
Talk Agenda

• What is Continuous Governance?
• Why would you adopt Continuous Governance?
• How Continuous Governance works at NAB
• Demo
• Architecture - Key Insights & Tips
• Q&A
What is Continuous Governance?

• In regulated environments (banking), governance is **non-negotiable** and **non-trivial**. Complicated + Manual = Slow

• Uplift: codification and automated enforcement of organizational and industry best practices to continuously quantify and manage risk.

• Continuous Governance allows NAB to deploy their most important workloads into cloud at pace, at scale with greater confidence.

• Nascent technology; a preview of...DevGovOps?
What is Continuous Governance?

• A governance framework that defines what good looks like (CAST)
• A technology platform that assesses and enforces compliance (Deputy)
• Continuous Governance mechanism, initiated by Continuous Integration pipelines – compliance assessments for *every* build
Drivers for adoption – business challenges

- Start of the cloud journey
  - Enthusiast & innovation teams – enterprise governance is not streamlined
- Migrating material workloads is a lengthy process which requires a high level of controls, including regulatory engagement - can be time consuming. Hundreds of material workloads would take **years** to assess.
- Engineers had access to production environment, hard to enforce compliance & consistency.
- No visibility into teams production deployment activities.
Gen3 AWS @NAB

**Non-prod AWS Account**
- Tooling VPC
- Pipeline
- Asset VPC

**Prod AWS Account**
- Tooling VPC
- Pipeline
- Asset VPC

GitHub Enterprise
Artifactory

**Helpful Hint:**
- Use a consistent naming convention for easy identification.
- Ensure secure connections and access controls.
- Automate deployment processes for efficiency.

**Challenges:**
- Resource allocation and management can be complex.
- Monitoring and maintenance require ongoing attention.

**Tips:**
- Utilize monitoring tools to track performance.
- Regularly update infrastructure to stay current with security patches.
- Implement robust access controls for data integrity.
Drivers for adoption – business outcomes

- Ability to perform rapid material workload migrations at scale
- Stronger organizational security posture
- More consistent and repeatable production deployments
- Advanced telemetry around organizational behavior and performance
NAB Continuous Governance Pillars

CAST
NAB’s cloud governance framework

Deputy
Governance enforcement point, and makes governance frameworks programmable.
Deputy evolution – step 1

Non-prod Account
- Tooling VPC
  - Pipeline
- Asset VPC

Deputy Account
- Build Telemetry
- Compliance Engine
- Deploy
- Fan-out SNS

Prod Account
- Tooling VPC
  - Pipeline
- Asset VPC

Promoter/Deployer

GitHub Enterprise
Artifactory
Deputy evolution - step 1

- Make sure you deploy what you built
  - BuildId

- Code quality tools – attestors
  - SonarQube
  - Checkmarx
  - Container scanning
  - Software composition analysis tools
Deputy evolution – Step 2

- Service management
  - Change record validation
  - Auto-approve change (still in plans)
  - Change moratorium
Deputy evolution – step 2

Non-prod Account
- Tooling VPC
- Pipeline
- Asset VPC

Deputy Account
- Build Telemetry
- Compliance Engine
- Deploy
- Fan-out SNS
- AWS API Gateways
- Amazon SNS
- DynamoDB

Prod Account
- Tooling VPC
- Pipeline
- Promoter/Deployer
- Asset VPC

GitHub Enterprise
Artifactory

nab Service Management
Deputy evolution – step 3

• CAST – Cloud Adoption Standards and Techniques

About CAST

NAB has designed the CAST Framework for safe and scalable migration of material workloads to Public Cloud. The framework defines minimum standards, techniques and controls to ensure risks associated with hosting material workloads in Public Cloud are assessed, documented and managed.
Deputy evolution – CAST attestation
Deputy evolution – manual attestation
Deputy evolution – CAST

Non-prod Account

- Tooling VPC
  - Pipeline
- Asset VPC

Deputy Account

- Build Telemetry
- Compliance Engine
- Deploy

Prod Account

- Tooling VPC
- Pipeline
- Promoter/Deployer
- Asset VPC

GitHub Enterprise
Artifactory
Interesting challenges

• How to get all the Deputy components into the asset accounts
• How to promote AMIs
• How to promote a production pipeline
Demo

Video
Architecture - Key Insights & Tips

• Kong API Gateway, Lambda, DynamoDB, RDS, SNS, SQS
• API-driven microservices architecture
• Event driven architecture & well-defined service boundaries
DEVOPS TALKS CONFERENCE 2019

Architecture - Key Insights & Tips

Attestation Partner 1 - AWS Account
- SQS Queue
- Event Handler
- Compliance Check
- Findings

Asset Team - AWS Account
- CI Pipeline
- Pipeline Events

Deputy - AWS Account
- API Gateway

Attestation Partner 2 - AWS Account
- SQS Queue
- Event Handler
- Compliance Check
- Findings

Attestation Partner 3 - AWS Account
- SQS Queue
- Event Handler
- Compliance Check
- Findings
The end!

Questions?
Appendix
Gen3 AWS @NAB with Deputy

Non-prod Account
- Tooling VPC
  - Pipeline
- Asset VPC

Deputy Account
- Kong
- Deploy (AWS Lambda)
- Fan-out (AWS SNS)

Prod Account
- Tooling VPC
  - Pipeline
- Promoter/Deployer
- Asset VPC

GitHub Enterprise
Artifactory
Deputy evolution – 3rd party

Non-prod RG

Pipeline

Application assets

Kong

Build Telemetry

Compliance Engine

Deploy

Fan-out SNS

3rd party companion

Cloud Func

Prod RG

Pipeline

Application Assets

GitHub Enterprise

Artifactory