

DOUG Training Day - 2025

Multi-Cloud Governance

ACHIEVING CONTROL WITHOUT LOSING
AGILITY

Presented By:

Arun Yadav

Oracle ACE
Associate

**DALLAS
ORACLE
USERS
GROUP**



Arun Yadav



Oracle ACE
Associate

accenture

- Oracle ACE Associate
- Working with Accenture since 2011
- Vice-President Dallas Oracle Users Group
- Over 20 years of experience in infrastructure, cloud operations, and enterprise architecture.
- Based out of Dallas since 2017
- Visit my blog: <https://itnoesis.com>



Let's connect on LinkedIn: [arun-yadavit](#)



Why Multicloud Governance Matters?

- Many enterprises are now moving towards using two or more clouds providers
- Drivers:
 - Cost optimization
 - Avoiding vendor lock-in
 - Regulatory compliance
 - Service specialization etc.
- Multicloud \neq chaos — but without governance, it can be !





The Multicloud Landscape – How Gaps Arise?

SHARED RESPONSIBILITY
MODEL, UNIQUE
GOVERNANCE
MECHANISMS

FRAGMENTED IDENTITY
AND MANAGEMENT

INCONSISTENT TAGGING &
COST TRACKING

VARIED SECURITY BASELINES
& SHADOW IT

How do we solve it?

- **CSCC**
 - **C**onsistency in **S**ecurity, **C**ompliance, and **C**ost Management across different cloud platforms by implementing a single set of policies, procedures, and controls. Aka Multicloud governance



Multicloud Operating Models

- **Distributed model**
 - Business units operate independently
 - Fast but inconsistent, risks sprawl
- **Centralized model**
 - One platform team controls all clouds
 - Strong governance, but can bottleneck
- **Federated model (target)**
 - Centrally defined guardrails
 - Decentralized execution & innovation

Governance Architecture Overview

- **THREE-LAYER ARCHITECTURE:**
- **ENTERPRISE LAYER:**
 - POLICIES, STANDARDS, REGULATORY REQUIREMENTS
- **SHARED SERVICES LAYER:**
 - IDENTITY FEDERATION
 - LOGGING & MONITORING
 - FINOPS DASHBOARDS
 - AUTOMATION & IAC
- **CLOUD EXECUTION LAYER:**
 - NATIVE GUARDRAILS (CLOUD GUARD, CONFIG, AZURE POLICY)
 - LANDING ZONES, COMPARTMENTS, ACCOUNTS, SUBSCRIPTIONS
- THIS CREATES CONSISTENT CONTROL ACROSS ALL CLOUDS.



Pillars of Cloud Governance

Main Framework:

Identity & Access Governance

- Use centralized IdP (Azure AD, Okta, Oracle IDCS, Google IdP).
- Enforce least privilege via federation across clouds.

Cost & Financial Governance

- Establish tagging and chargeback standards.
- Use FinOps principles — budgets, alerts, right-sizing.

Security & Compliance Governance

- CIS benchmarks, NIST, ISO27001.
- Automate compliance checks (Oracle Cloud Guard, AWS Config, Azure Policy).

Resource & Policy Governance

- Define naming conventions and lifecycle management.
- Use IaC (Terraform) with policy-as-code enforcement (OPA, Sentinel).

Data Governance

- Data classification, residency, encryption, and sovereignty controls.
- Data catalogs and lineage across platforms.

Operational Governance

- Centralized monitoring (OCI Observability, Azure Monitor, CloudWatch, Stackdriver).
- SRE model for unified incident management.



Designing a Multicloud Governance Model

DEFINE ENTERPRISE
GOVERNANCE
OBJECTIVES

CREATE A CLOUD COE


ADOPT A POLICY AS
CODE APPROACH

IMPLEMENT AUTOMATION
GUARDRAILS

INTEGRATE
GOVERNANCE INTO
CI/CD PIPELINES

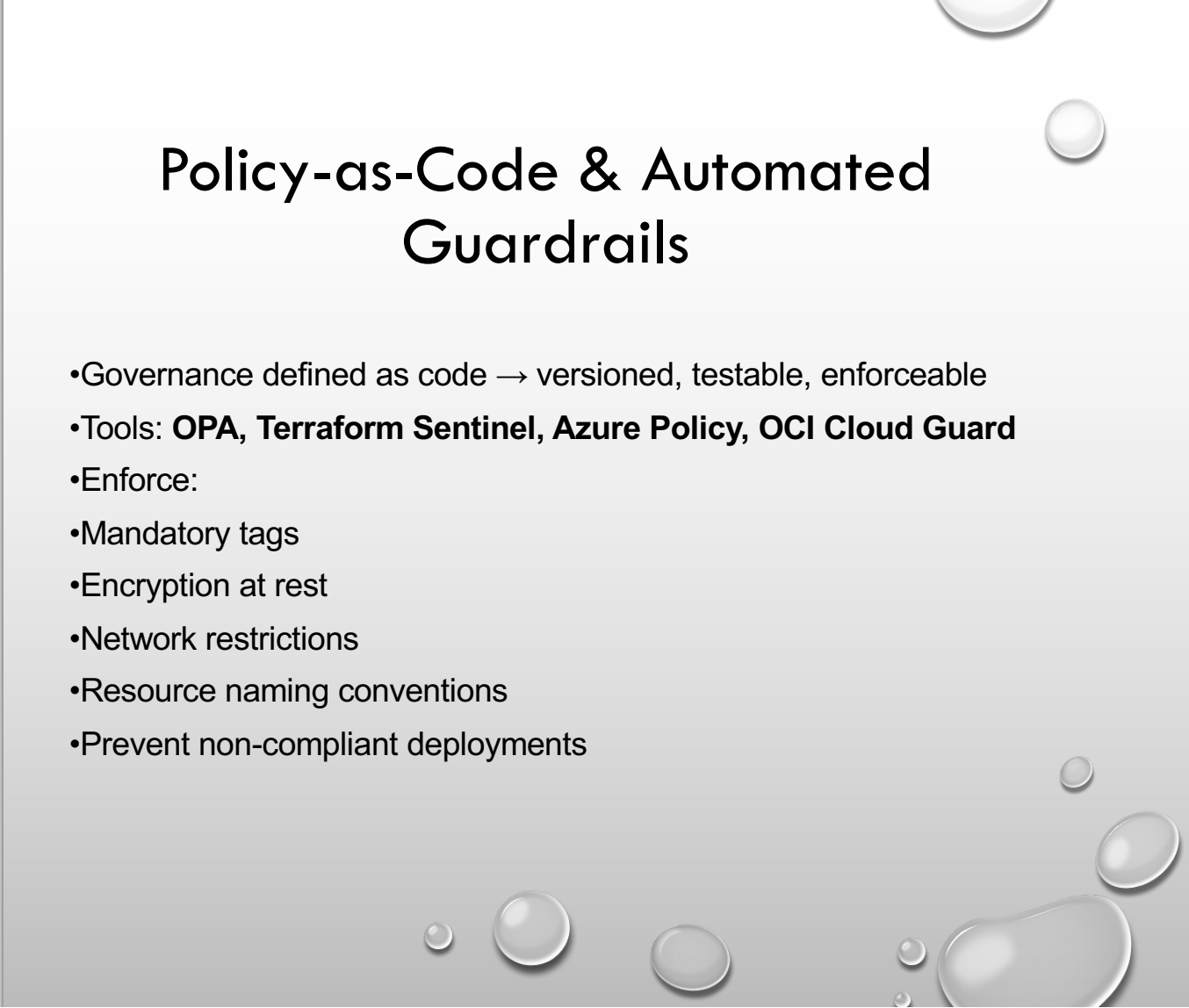


Organizational Alignment & CCoE

- **Cloud Center of Excellence (CCoE) responsibilities**
 - Define governance frameworks & standards
 - Provide reusable templates, iac modules & patterns
 - Approve cloud landing zones
 - Drive alignment between security, finops & devops
 - Manage training & cloud competency development
- 



Policy-as-Code & Automated Guardrails

- Governance defined as code → versioned, testable, enforceable
 - Tools: **OPA**, **Terraform Sentinel**, **Azure Policy**, **OCI Cloud Guard**
 - Enforce:
 - Mandatory tags
 - Encryption at rest
 - Network restrictions
 - Resource naming conventions
 - Prevent non-compliant deployments
- 

Governance Maturity Model

Level	Name	Characteristics	Typical State	Key Focus to Advance
1. Ad Hoc	Cloud Chaos	No central policy; each team deploys freely; minimal visibility or cost tracking.	Individual business units using multiple clouds independently.	Establish visibility — implement centralized inventory and tagging.
2. Reactive	Isolated Controls	Some policies exist but are inconsistent across providers; compliance is manual.	Security or cost overruns trigger audits or reviews.	Standardize identity and cost tagging; document baseline governance framework.
3. Defined	Structured Governance	Centralized CCoE defines policies; IAM federation and cost policies established; governance manual exists.	Enterprise has repeatable patterns and partial automation.	Automate enforcement using policy-as-code and CI/CD integration.
4. Automated	Integrated Guardrails	Automated guardrails and continuous compliance across clouds; unified identity, FinOps, and SecOps integration.	Governance as code in production; dashboards for compliance posture.	Expand to predictive governance using AI/ML-based insights.
5. Optimized	Self-Governing Cloud Ecosystem	Continuous feedback loops, AI-driven compliance, cross-cloud orchestration, and automated remediation.	Governance is proactive and self-tuning.	Continuous improvement and benchmarking against industry standards (CIS, NIST).

OCI Cloudguard in Multicloud Governance



Cloud Guard provides continuous **Security Posture Management (CSPM)** for OCI workloads



Integrates detection + remediation with automated guardrails



Works alongside AWS Config, Azure Policy, and GCP Organization Policies



Central role in a multicloud governance architecture:



Detect misconfigurations



Respond with automated actions

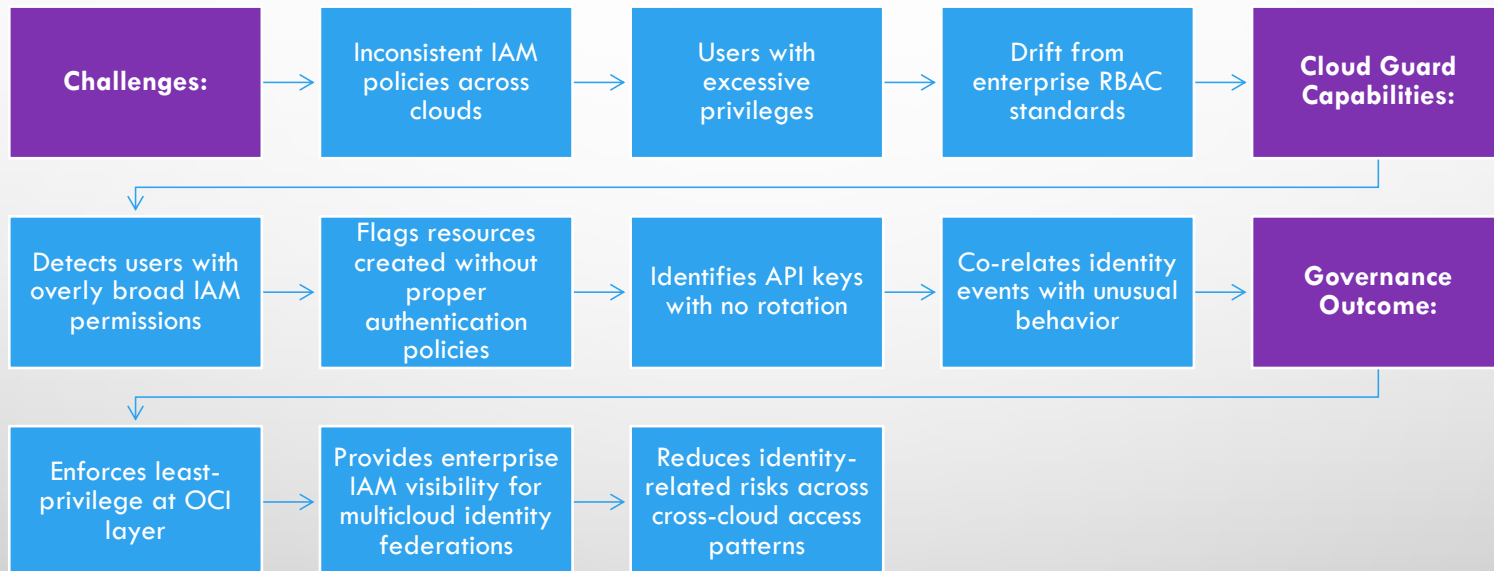


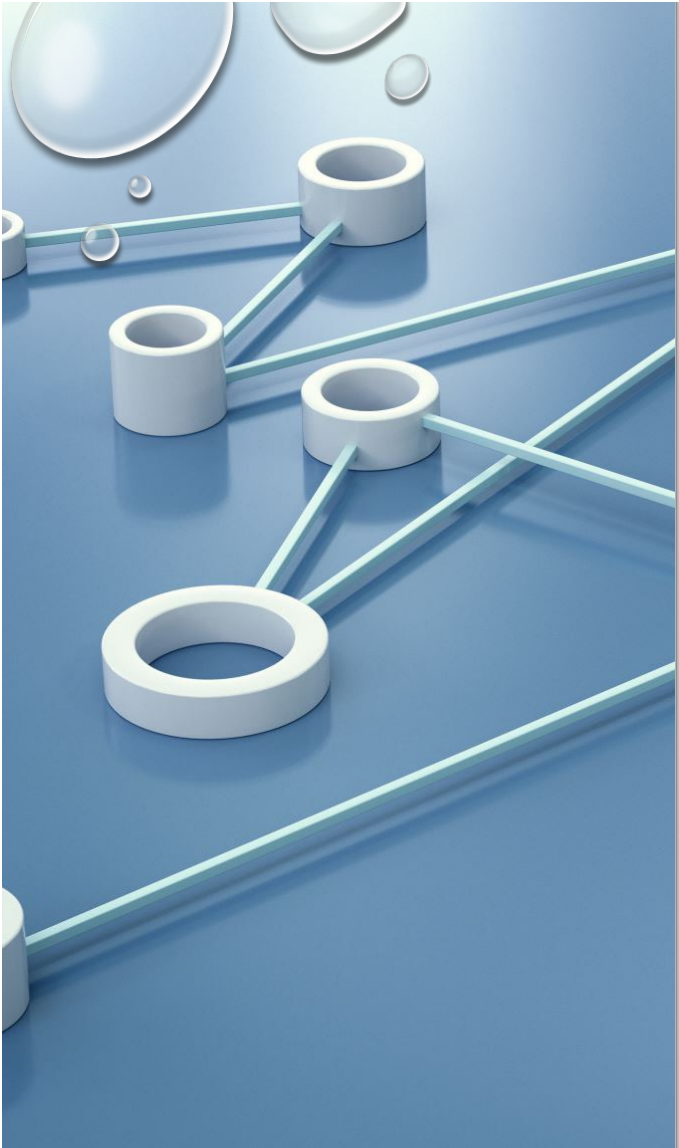
Provide unified reporting for cross-cloud risk posture



Supports governance across **shared services, networking, identity, storage, and database layers**

OCI Cloudguard Sample Use Case





BEST PRACTICES & KEY TAKEAWAYS

- Governance must be built in, not bolted on.
- Use policy-as-code and automation to scale control.
- Standardize identity and tagging across all clouds.
- FinOps and SecOps must collaborate.
- Establish a Cloud Center of Excellence (CCoE) to own governance.

Multicloud Governance Checklist (Template)

Governance Domain	Key Activity	Status
Identity & Access	<input type="checkbox"/> Centralized IdP across clouds (IDCS, Azure AD, Okta)	
	<input type="checkbox"/> Role-based access model (least privilege enforced)	
	<input type="checkbox"/> MFA and conditional access policies	
Financial (FinOps)	<input type="checkbox"/> Standardized tagging schema across all clouds	
	<input type="checkbox"/> Budget thresholds and alerts configured	
	<input type="checkbox"/> Chargeback/showback model implemented	
Security & Compliance	<input type="checkbox"/> CIS/NIST baseline mapped to each provider	
	<input type="checkbox"/> Continuous compliance scanning enabled (Cloud Guard / AWS Config / Azure Policy)	
	<input type="checkbox"/> Automated remediation for policy violations	
Resource & Policy Governance	<input type="checkbox"/> Terraform or IaC templates standardized	
	<input type="checkbox"/> Policy-as-code implemented (Sentinel / OPA)	
	<input type="checkbox"/> Naming convention and lifecycle rules enforced	
Data Governance	<input type="checkbox"/> Data classification and residency mapping complete	
	<input type="checkbox"/> Encryption policies enforced via centralized KMS	
Operations & Monitoring	<input type="checkbox"/> Centralized observability (logs, metrics, alerts)	
	<input type="checkbox"/> Unified incident response process across clouds	
Organizational	<input type="checkbox"/> Cloud Center of Excellence (CCoE) established	
	<input type="checkbox"/> Governance KPIs and reporting cadence defined	



Thank You !!

Presented By:

Arun Yadav



**DALLAS
ORACLE
USERS
GROUP**

