
aws
SUMMIT
MUMBAI | MAY 18, 2023

MEG002

Building Centralized Governance on Games Infrastructure

Kriti Gera (She / her)
Security Specialist Solutions Architect
AWS India

Kuldeep Tomar (He / him)
Head of Security
Games24x7

Agenda

How to achieve Business agility with Governance Control

Organizational challenges

Security risks/impact

AWS Control Tower - Governance

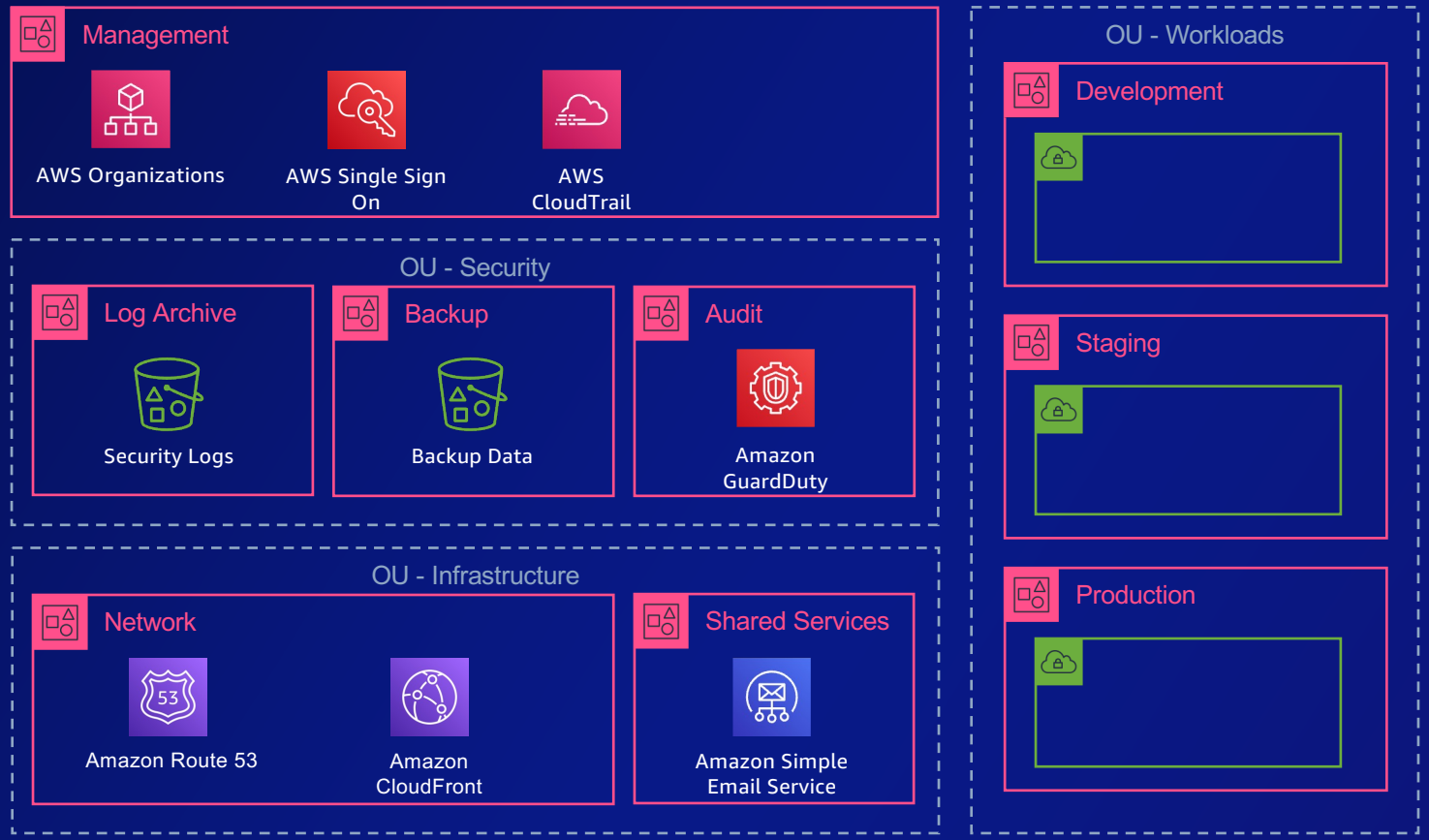
AWS Control Tower- Foundation for Security/Privacy

How everyone starts out (usually)

Single account setup

- Different VPCs for workloads
- IAM control
- Noisy workloads
- Shared account limits

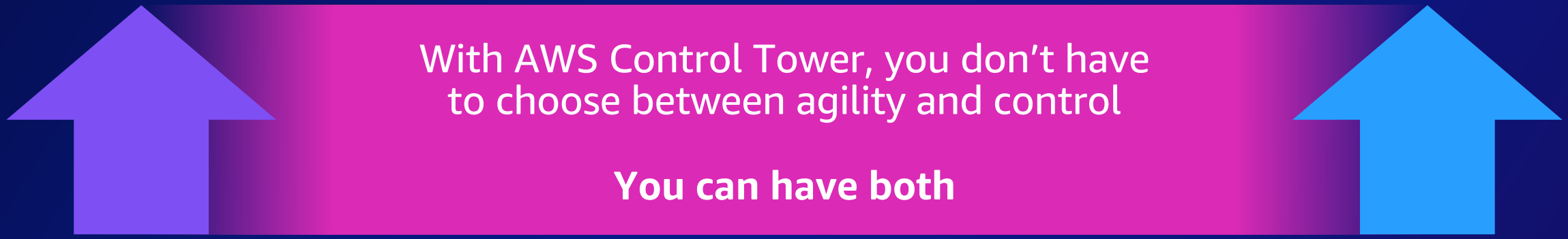
Equivalent scenario in a multi-account setup



Multi-account setup

- Isolate workloads based on
  - Business outcomes
  - Data sensitivity, compliance
- Limit impact of adverse events
- Distinct security controls
- Improved visibility of costs e.g. SaaS

Business agility *and* governance control



Governance

Security

Compliance

Operations

Spend Management

Agility

Self-service access

Experiment fast

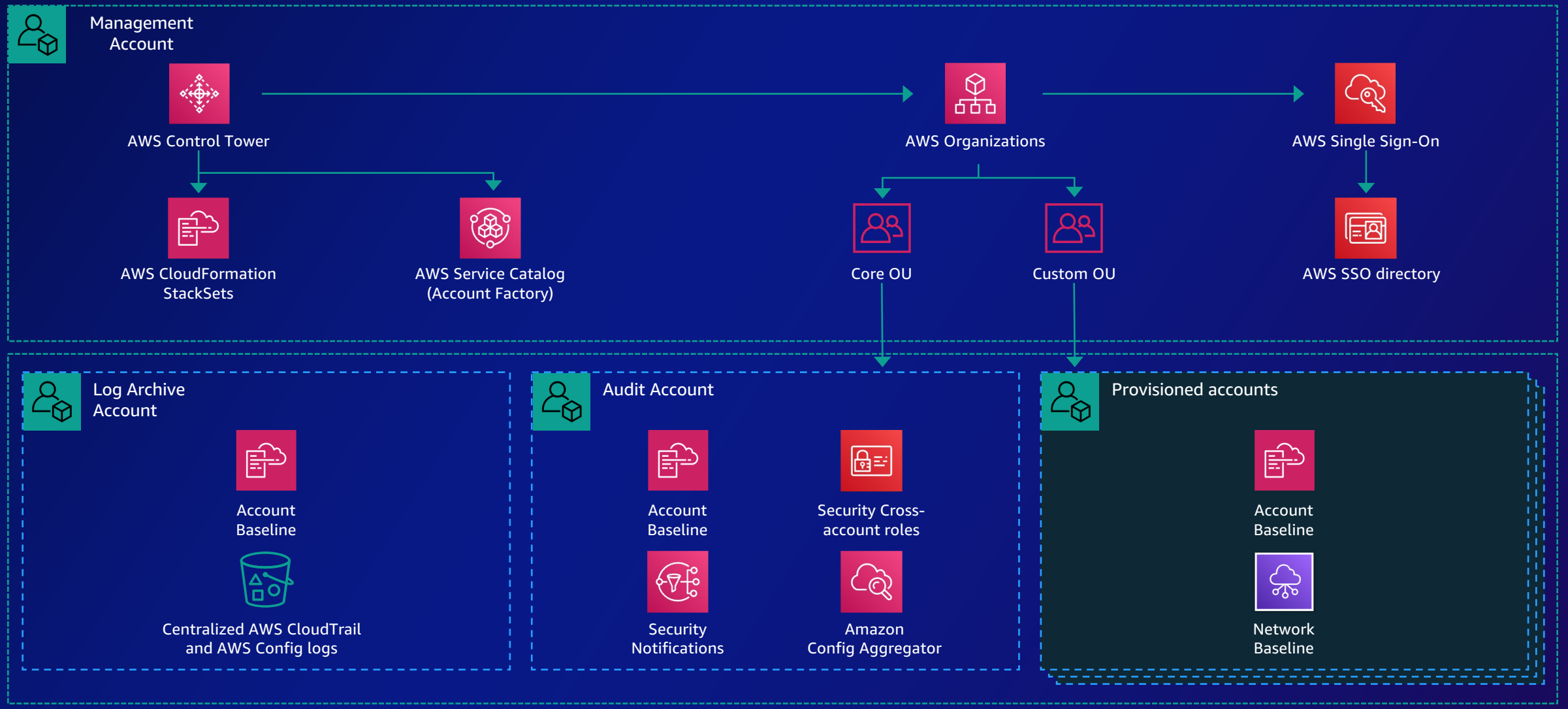
Respond quickly to change

Why use AWS Control Tower?

- Set up a best-practices AWS environment in a few clicks
- Standardize account provisioning
- Centralize policy management
- Enforce governance and compliance proactively
- Enable end user self-service
- Get continuous visibility into your AWS environment
- Gain peace of mind

AWS Control Tower: Easiest way to set up and govern AWS at scale

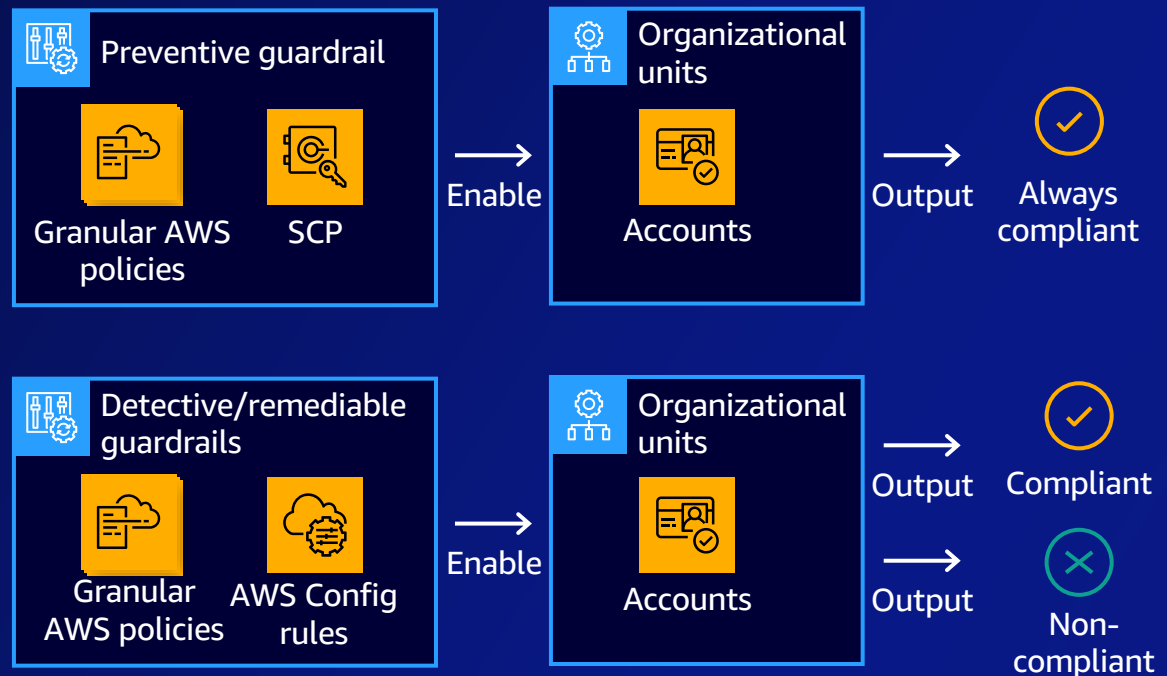
Landing Zone provisioned by AWS Control Tower



Centralize identity and access

- AWS Identity Centre provides default directory for identity
- AWS Identity Centre also enables federated access management across all accounts in your organization
- Preconfigured groups (e.g., AWS Control Tower administrators, auditors, AWS Service Catalog end users)
- Preconfigured permission sets (e.g., admin, read-only, write)

Establish guardrails

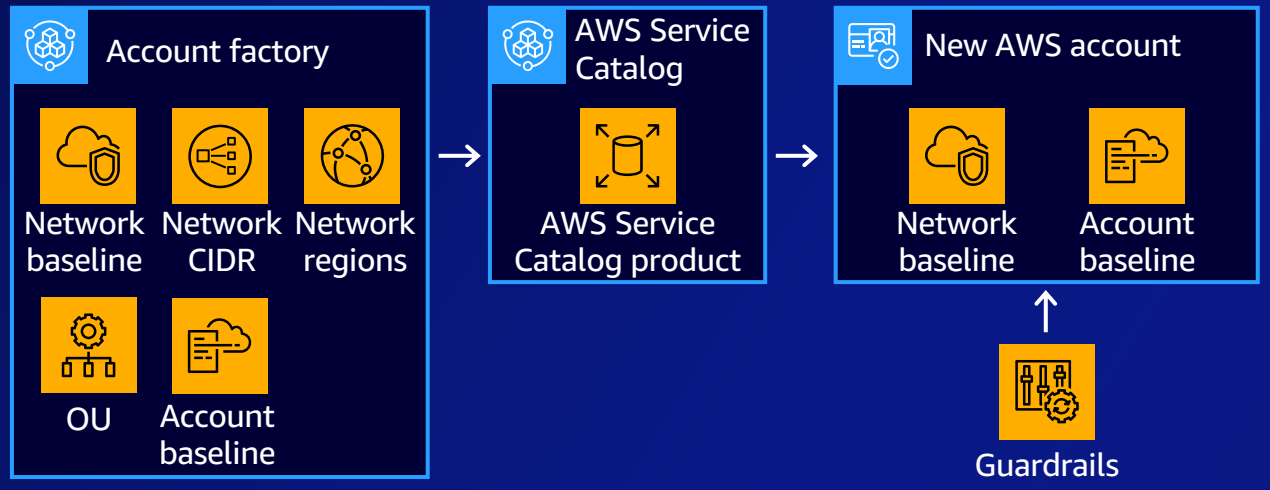


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: detect policy violations and alert in the dashboard; implemented using AWS Config rules
- Mandatory and strongly recommended guardrails for prescriptive guidance
- Easy selection and enablement on organizational units

Guardrail examples

Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with Amazon CloudWatch
Encryption	Ensure encryption of Amazon EBS volumes attached to Amazon EC2 instances
Drift	Disallow changes to AWS Config rules set up by AWS Control Tower

Automate compliant account provisioning



- Built-in account factory provides a template to standardize account provisioning
- Configurable network settings (e.g., subnets, IP addresses)
- Automatic enforcement of account baselines and guardrails
- Published to AWS Service Catalog

Operate with agility + control

Monitor

Monitor resources and workloads

Audit

Audit resource configurations, user access, and policy enforcement

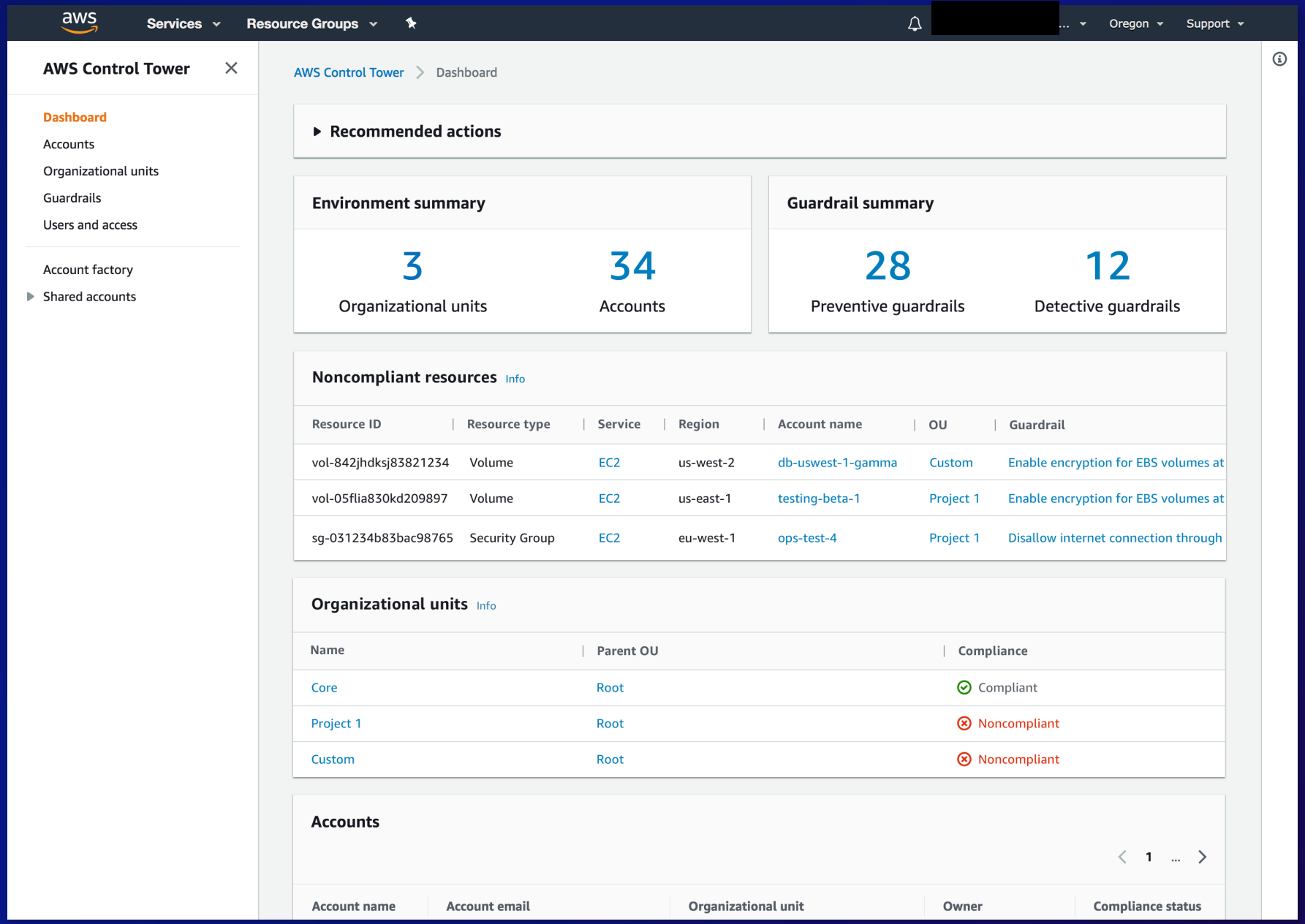
Act

Take operational action on resources

Dashboard

Continuous visibility into your multi-account environment

Dashboard for oversight



How Games24x7 adapted Control Tower to achieve Central Governance

Why?

Games24x7 is India's leading multigame platform, with offerings such as RummyCircle, My11Circle. India's one of the largest fantasy games platform and U Games, a portfolio of casual games.

- Being a pioneer in Real Money Games industry, there is always a mandate to abide by strict regulations. Hence, maintaining highly secure infrastructure becomes a top priority.
- Games24X7 keeps experimenting with new technology to build cutting edge features and new games. In the process of experimentation, multiple linked accounts are created to avoid interruption on the production workloads.
- However, ensuring right security policies on each of these linked account is a challenge. There was a need to ensure high security of infrastructure while the experimentation happens at scale.

Organizational challenges

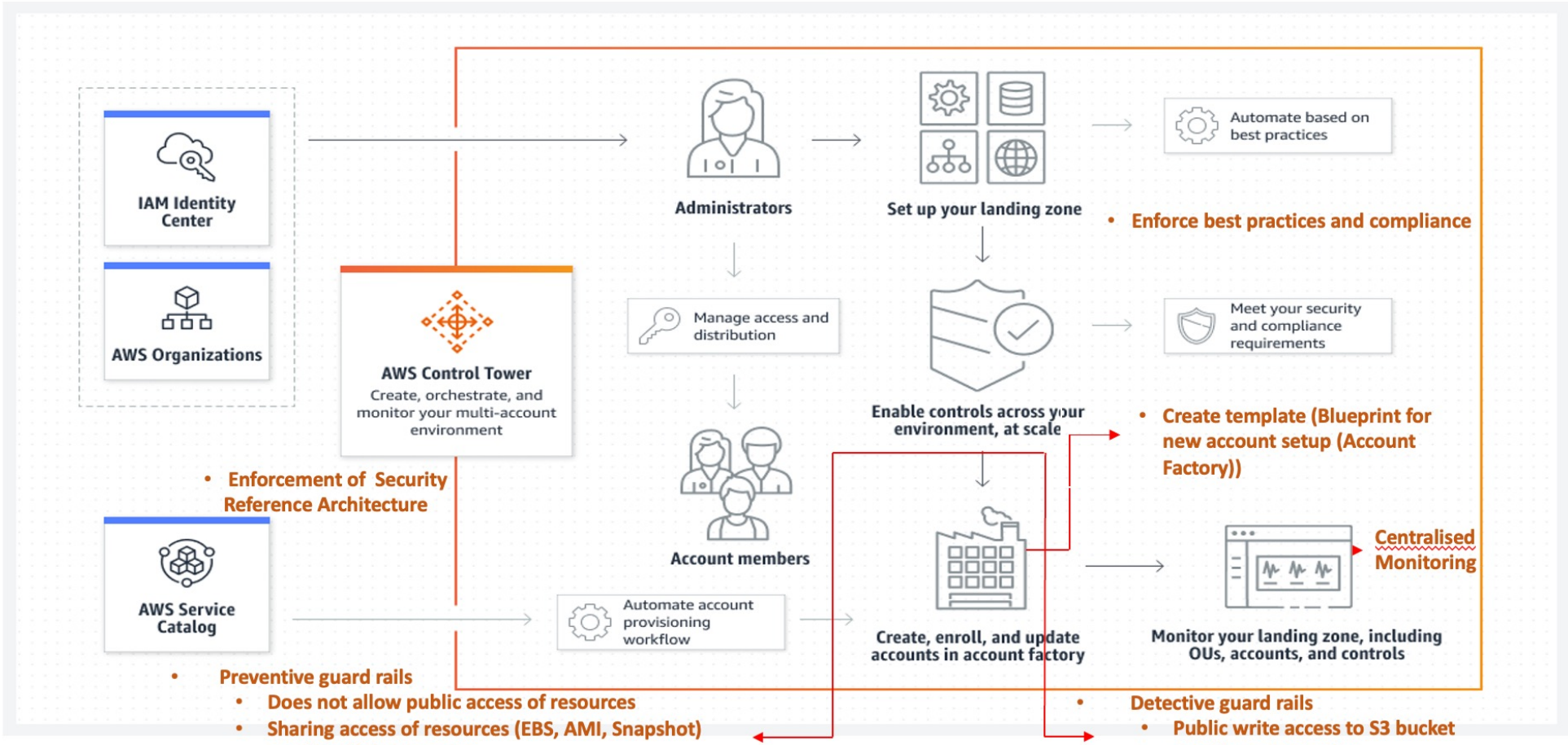
Problem Statement
Multiple accounts for different gaming verticals
Security Reference Architecture was not adopted in cloud adoption. Gaming agility.
Policies setup at account level, absence of centralized guardrails for gaming requirements.
Absence of centralized config rules to identify configuration drift for different gaming accounts

Security risks and impact

Issues	Impact (Attack vectors)
Resources with Public access	Data leakage, Data breach
Public write access to S3 bucket	Unauthorised access, Malware/Ransomware attack
Certificate expiration	Phishing attack, Data breaches
Unused IAM users and access keys exist in the account. No automated/central management and cleanup	Unauthorised access of resources
Sharing of resources with external accounts	Data leakage, Data breach

AWS Control Tower - Governance

[Standardisation and improved compliance through account blueprints, Centralised policy enforcement / account management]



AWS Control Tower – Foundation for Security/Privacy

SSO Implementation - Cleanup of current IAM resources, implementation of AWS Identity Center + KeyCloak as IAM central governance / control / recertification tool
Centralized Security account – AWS Security Services can be accessed by Infosec team only for centralise monitoring and governance
Log archival account – Separate log archival account with no unauthorized access
Security Lake – SIEM tool will be able to consume the logs from central tool for observability
Data Security – Stringent data security control to avoid privacy issues

skillbuilder.aws

Your time is now

Build in-demand cloud skills your way

aws

Thank you!

Please complete the session survey

Kuldeep Tomar
Head of Security
Games24x7

Kriti Gera
Security Specialist Solutions Architect
AWS India