



# DOS Cloud Strategy & AppDev

## Today & Beyond

**Brian Merrick** | Acting DCIO, IRM/OPS

June 17, 2021



# A Narrative for Change

Focus on 3 key impact areas to increase responsiveness, agility, and customer-centricity within DOS



## Customer Engagement

- Help bureaus understand IRM solutions, tools, and recommendations to meet mission needs
- Identify duplicative requests and streamline development across DOS
- Provide cross-bureau portfolio prioritization
- Coordinate Go to the Gemba



## Cloud Strategy

- Define and build a platform for Agile development
- Infrastructure As Code and easy-to-stand up instances that can be used across DOS
- Implement DevSecOps to reduce ATO time



## Modern Application Development Practices

- Define outcomes & goals
- Help bureau leadership and development teams with Agile adoption & understanding
- Coordinate Agile across DOS
- Support FAM/FAH updates
- Initial application MVPs deployed within 90 days
- Build and run applications with a human-centered design & UX/UI focus
- Build in compliance with 508, security, privacy, etc. to speed delivery of working software to production



# Gathering Customer Requirements



Build configurable apps on enterprise cloud platforms tailorable for local business needs



Provide consistent security controls enabling internal and external users

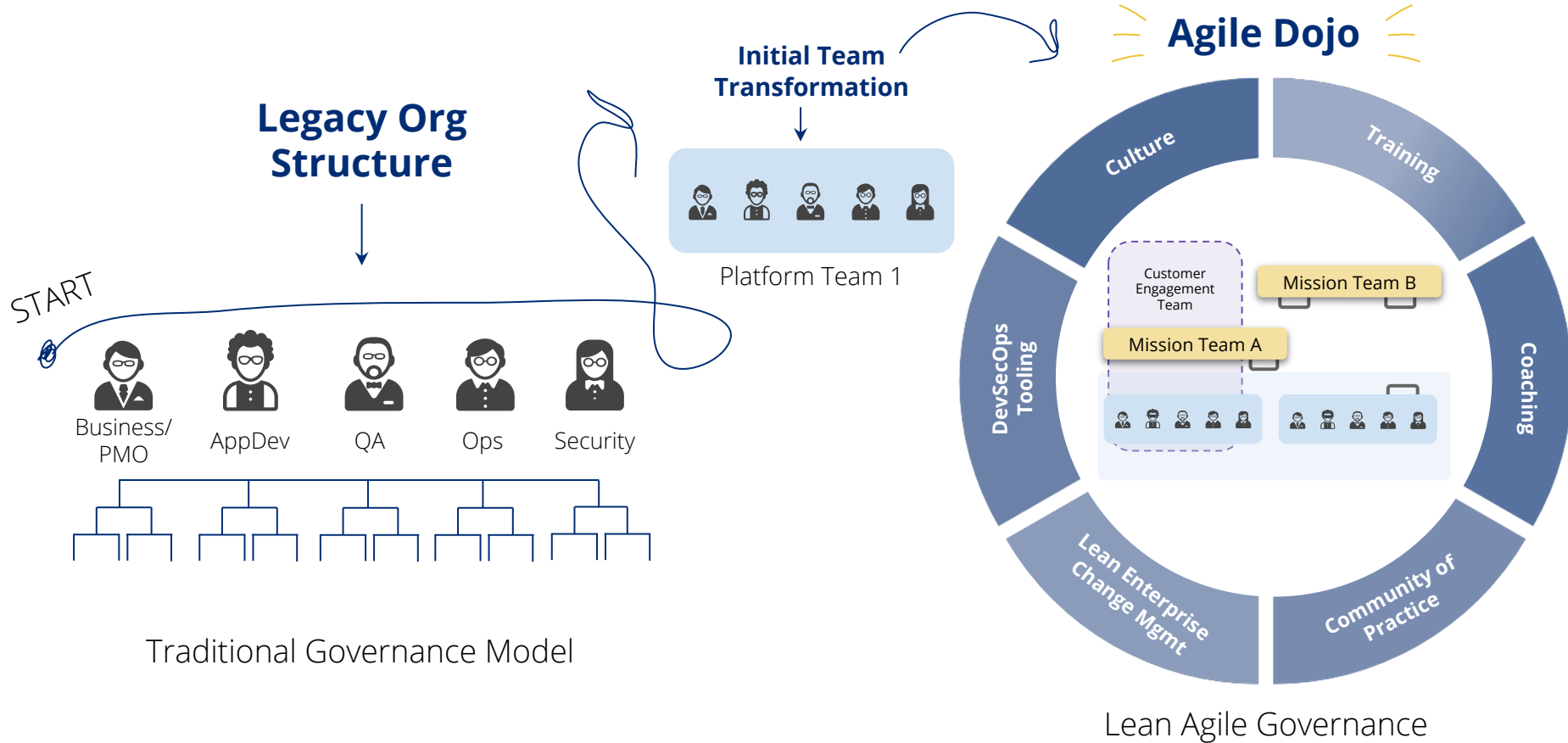


Reduce hardware footprint and management costs at post



Partner with Regional development groups to support custom development and change management

# Agile Dojo - Incubator for Agile Transformation





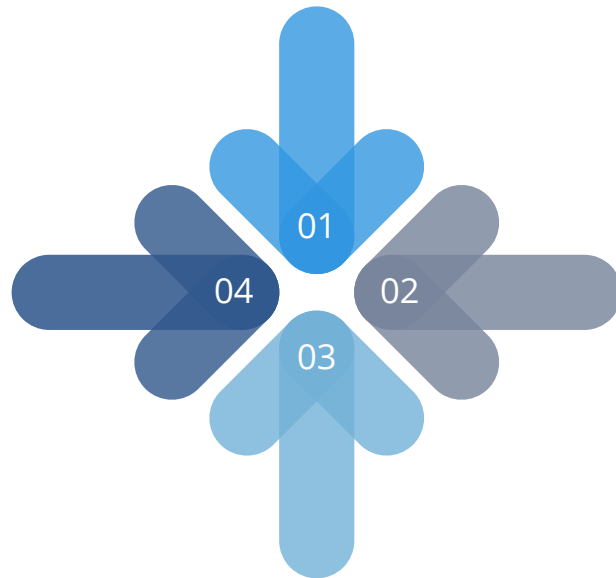


# Cloud as a Service Strategy



Centralized cloud services  
procurement vehicle, with  
Client-managed pay-as-you-go  
Task Orders

Shared  
Responsibility  
Model for  
accelerated ATO



Centralized  
security policy  
management

Infrastructure as Code and  
CI/CD-enabled customer  
cloud account provisioning

# DOS Multi-Cloud Service Portfolio



Google Cloud Platform



Currently Available

**FISMA Moderate ATO;**  
**FISMA High Expected Fall '21**

**servicenow**

Currently Available

**FISMA Moderate ATO**  
**FISMA High In-Progress**



Currently Available

**FISMA High ATO**

Google Workspace



Currently Available

**FISMA Moderate ATO**

**SE-Tools (Jira, GitLab,  
Security Tools, etc.)**

Coming Soon; FISMA Moderate  
ATO Expected Late '21/Early '22



Currently Available

**FISMA Moderate ATO**

**box**

Coming Soon; ATO in Progress

**FISMA Moderate ATO**  
**Expected Fall 2021**

**okta**

Currently Available

**FISMA Moderate ATO**

**Azure  
COMMERCIAL**

Coming Soon; ATO in Progress

**FISMA Moderate ATO**  
**Expected Summer '21**

Coming Soon; ATO in Progress

**FISMA Moderate ATO**

**Expected Winter '21**



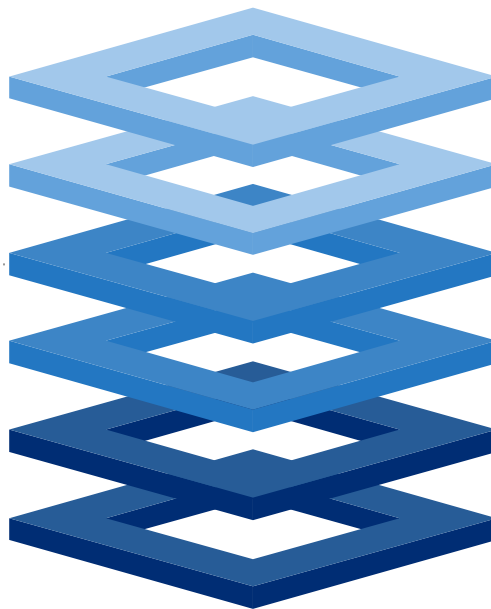
Who is responsible for what?

# Shared Responsibility Model

Security and compliance responsibilities are shared between **CSP**, **IRM**, and **Customers**.

## IRM Service Provider

- Perimeter security (virtual networks; ports/protocols, security groups)
- Threat detection & security monitoring of platform
- Identity and access (console & API)
- Configuration, auditing, & administration of cloud services
- Account administration, organization policy, billing, contract



## IRM CUSTOMERS

- Customer data
- Platform, applications, identity & access (at platform/system/application level)
- Operating System, COTS software
- Client-side & server-side data encryption, key management, authentication
- Threat detection, auditing, monitoring of subscription



## Cloud Service Provider (CSP)

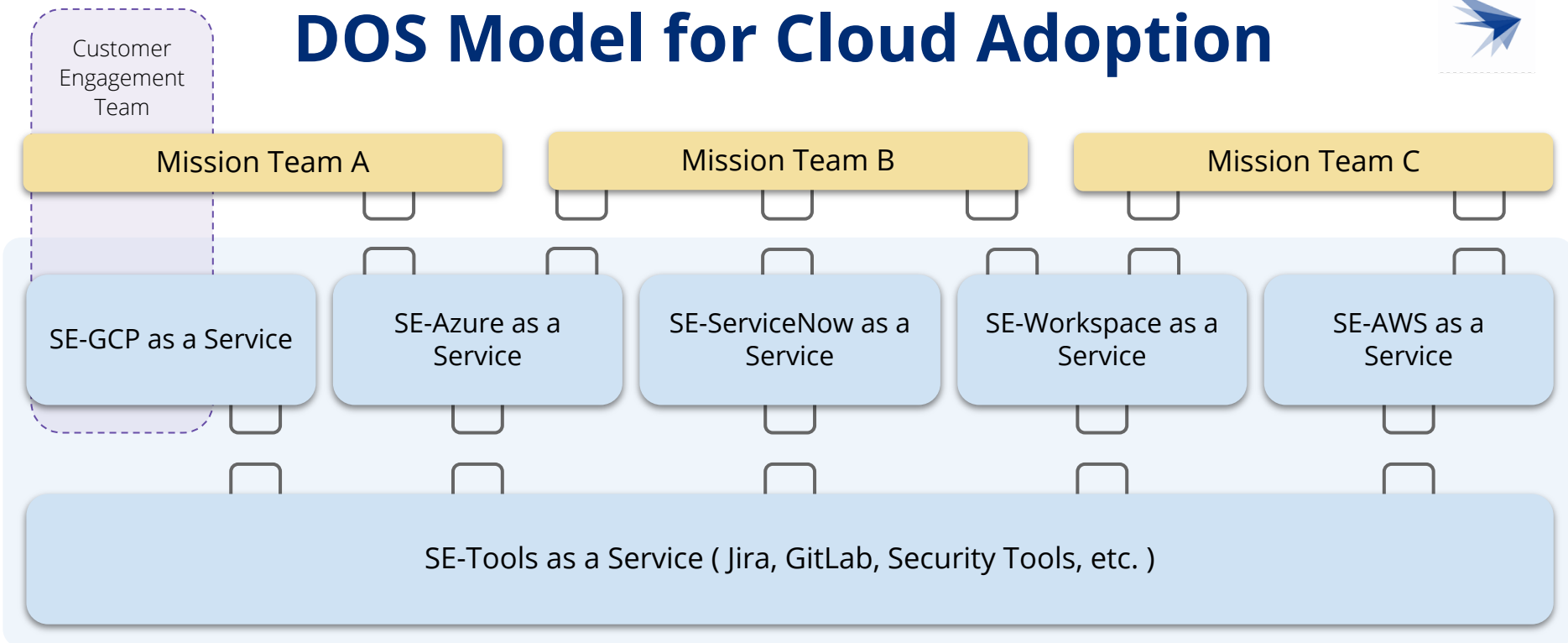
- Compute, storage, database, networking (IaaS & PaaS services)
- Regions, availability zones, edge locations







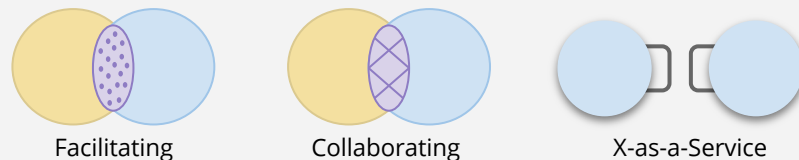
# DOS Model for Cloud Adoption



## Key: Team Types



## Key: Three Interaction Models





# Thank you for attending!