

AWS
re:Invent

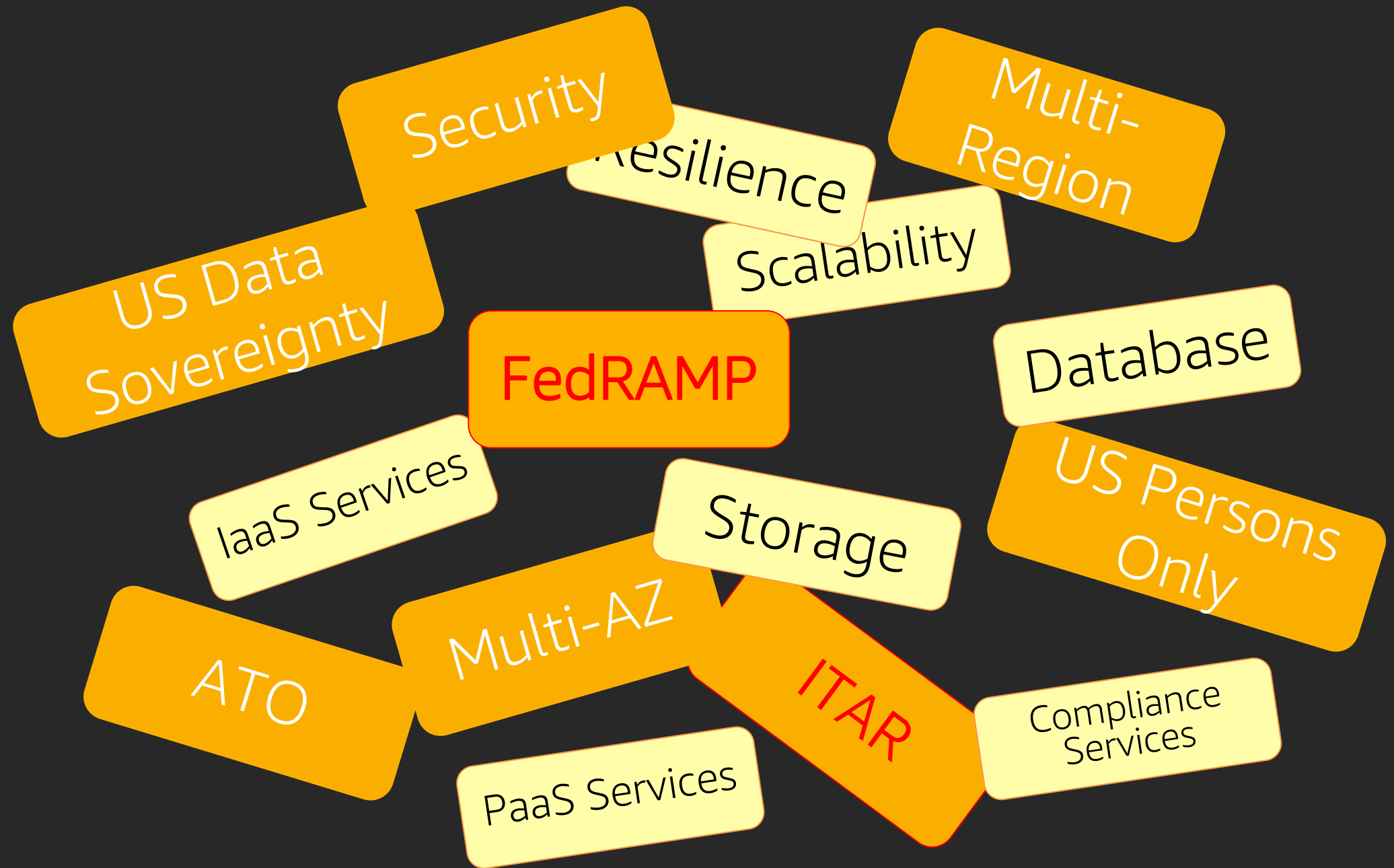
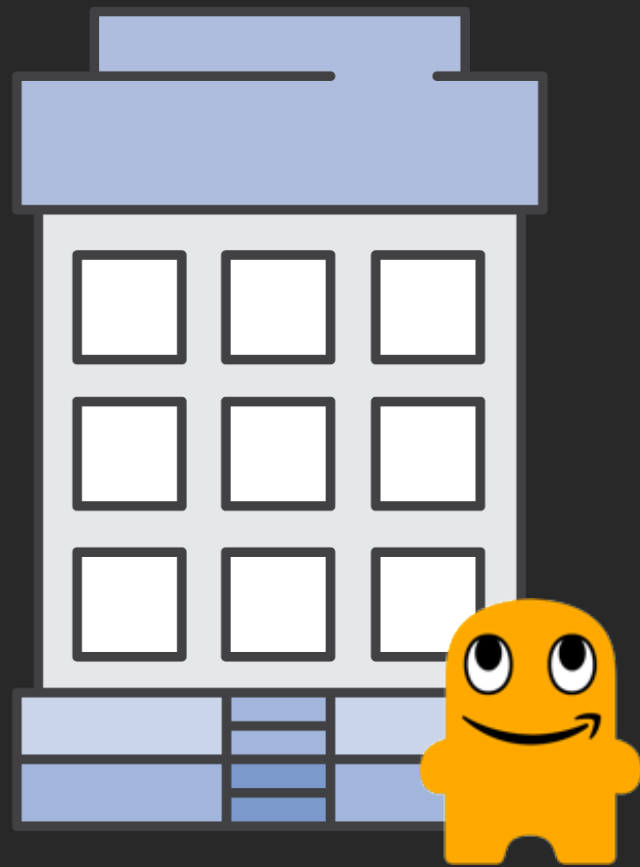
W P S 3 1 6 - R

Getting started in AWS GovCloud (US)

Derek Doerr

Senior Solutions Architect
Worldwide Public Sector
Amazon Web Services

Your requirements . . .



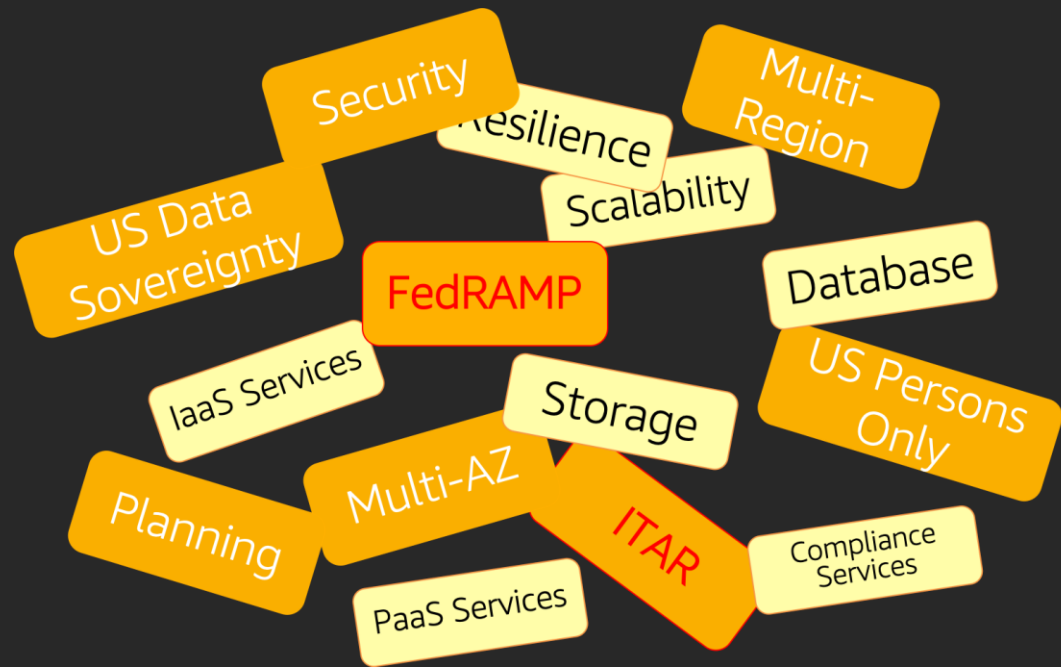
Why do we need FedRAMP?

- Mandatory per OMB for cloud services that hold federal data
- "Do once, use many times" framework
 - Saves government cost—work smarter, not harder
 - Reduces redundant reviews
- Provides tailored set of NIST SP 800-53 security controls
 - Selected to provide protection in cloud environments
 - Subsets defined for FIPS 199 Low, Moderate, and High categorizations
- Established a Joint Authorization Board (JAB)
 - CIOs from DoD, DHS & GSA
 - Establish accreditation standards for 3rd party assessors of cloud solutions

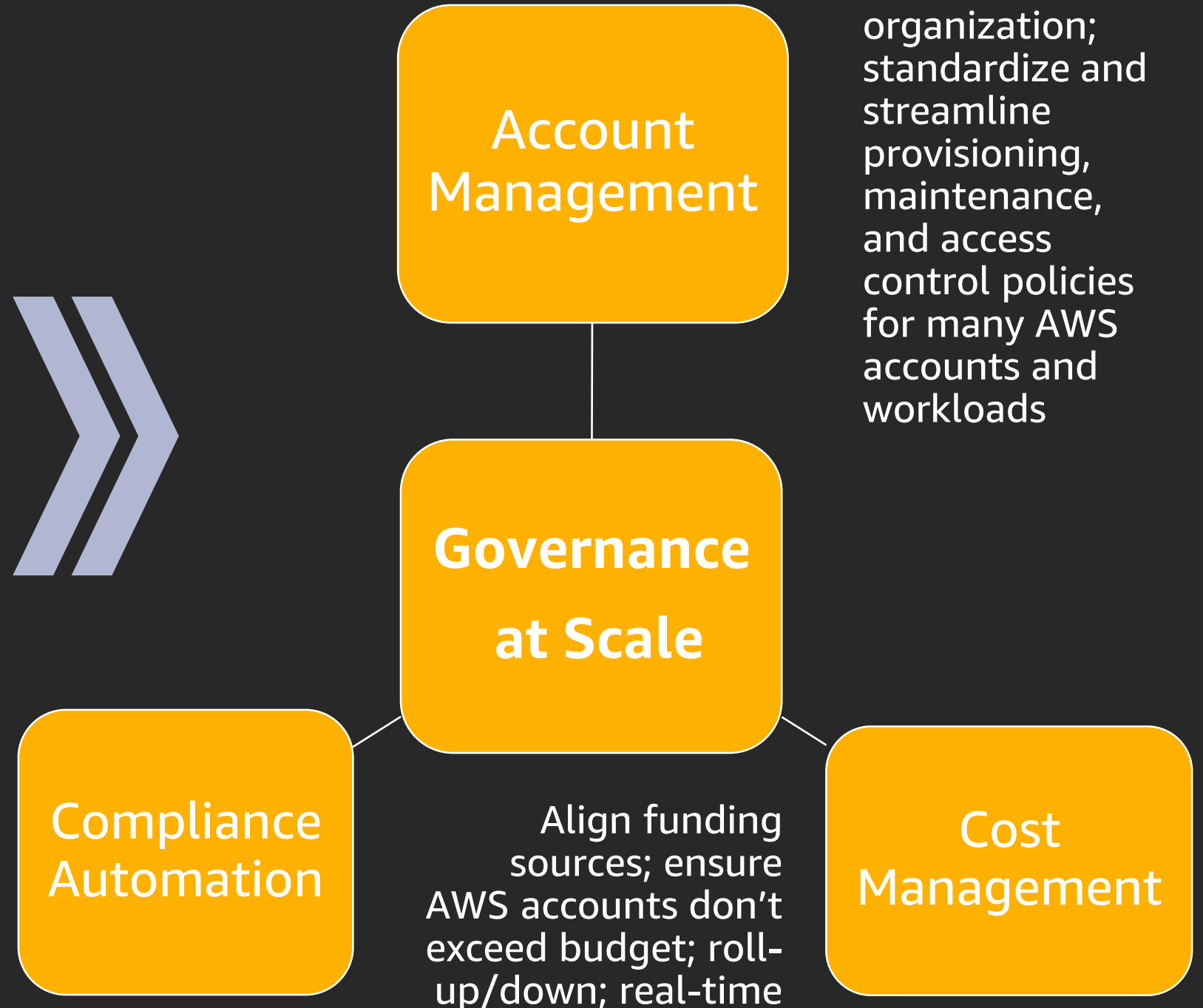
This is how we get assurance about security OF the cloud!

How can public sector and highly regulated customers move their most sensitive workloads to the AWS Cloud?

Governance at Scale framework



Align controls to your security control matrix (SCM); accelerate security authorizations, provide continuous monitoring and configuration management, and enforce security controls



Account Management

Governance at Scale

Compliance Automation

Align funding sources; ensure AWS accounts don't exceed budget; roll-up/down; real-time

Cost Management

Align AWS accounts with the organization; standardize and streamline provisioning, maintenance, and access control policies for many AWS accounts and workloads

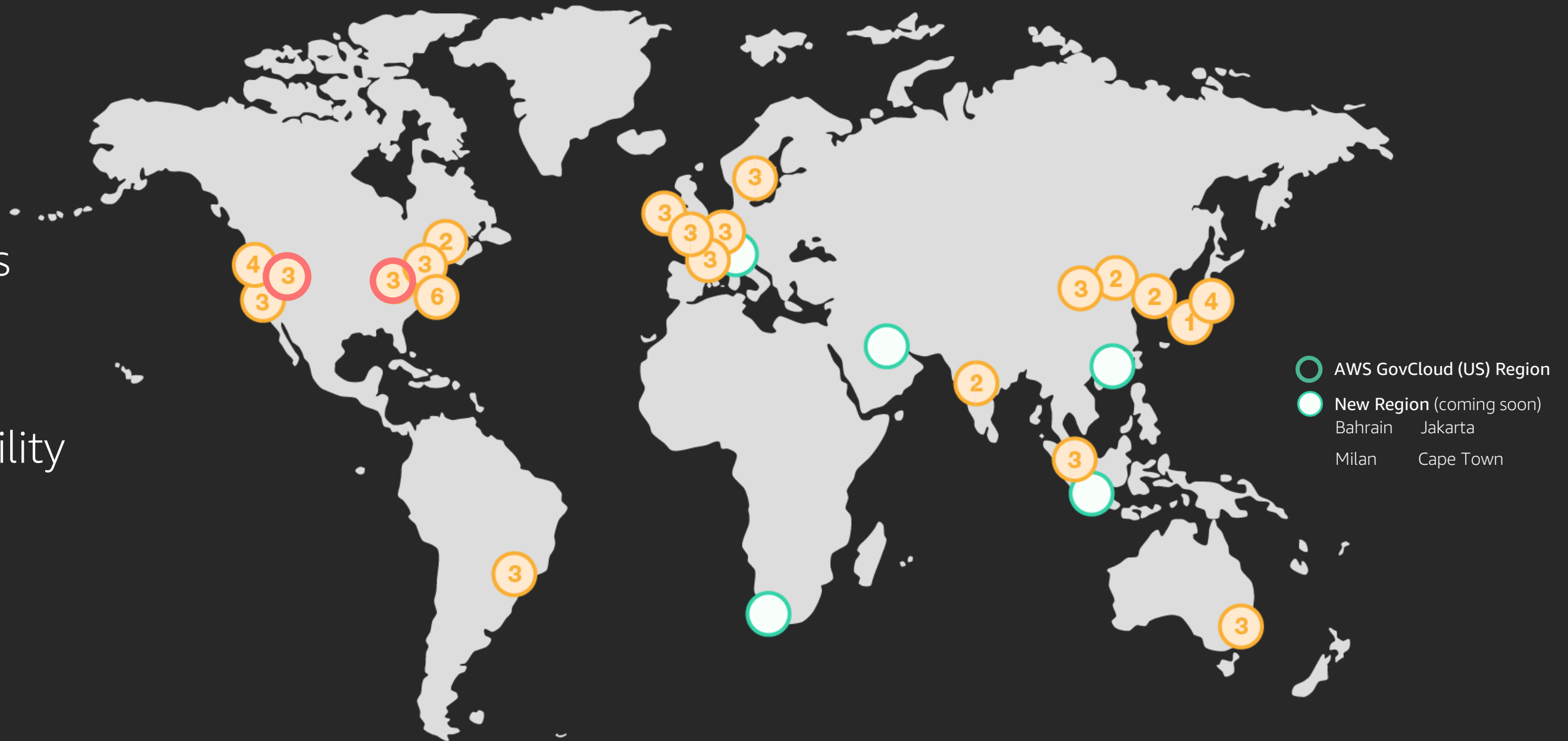
AWS global infrastructure

21

Regions

66

Availability
Zones



AWS GovCloud (US)

Isolated AWS infrastructure and services for customers with strict regulatory and compliance requirements and sensitive data

August 2011

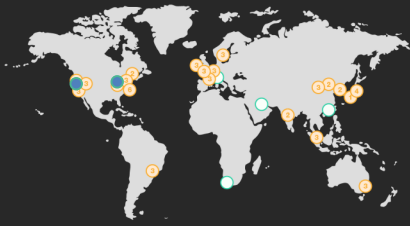
Launch of AWS GovCloud (US-West) Region

November 2018

Launch of AWS GovCloud (US-East) Region

Addresses the most stringent US Government regulations, policies, and security requirements

AWS GovCloud (US) distinguishing features



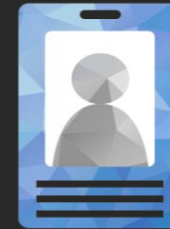
2 AWS GovCloud (US) regions

Bicoastal infrastructure and services for regulated workloads



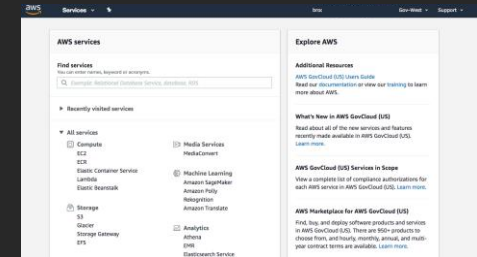
Data, network, and machine isolation

Separate AZs, endpoints



Unique authentication

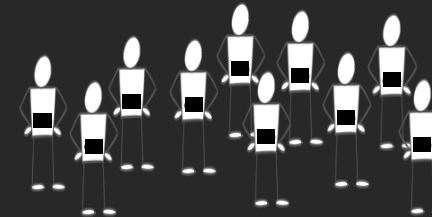
Unique AWS GovCloud (US) credentials



Dedicated AWS GovCloud (US) management console

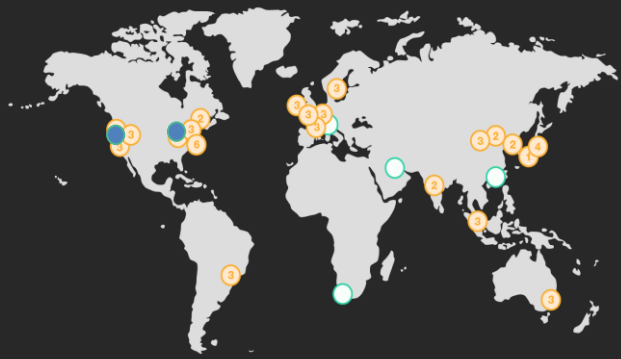


Managed by US citizens on US soil



“Community Cloud” with restricted access

Key takeaways



AWS GovCloud (US)

Is it right for your workload?



NIST

Accelerator

Use as a reference point for your Security Control Matrix



Pathway to ATO



Next Steps

How do I get started with architecting and migrating sensitive and regulated workloads in the cloud?

Understanding the shared responsibility of compliance

Customers

Customer applications & content

Platform, Applications, Identity & Access Management

Operating System, Network, & Firewall Configuration

Client-Side Data
Encryption

Server-Side Data
Encryption

Network Traffic
Protection

Customers choose the configurations for their security **in** the cloud

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global
Infrastructure

Availability Zones

Regions

Edge Locations

AWS is responsible for security **of** the cloud



Security control inheritance delineates responsibility

Customers

Certification, Accreditation and Security Assessment (CA), Awareness & Training (AT), Planning (PL), Personnel Security (PS), Risk Assessment (RA), and System & Services Acquisition (SA)
Access Control (AC), Audit & Accountability (AU), Configuration Management (CM), Maintenance (MA), Contingency Planning (CP), Identity and Authentication (IA), Incident Response (IR), Maintenance (MA), System and Communication Protection (SC), System and Information Integrity (SI)

Shared/hybrid and customer-implemented security controls



AWS Foundation Services

Media Protection (MP) and partial Maintenance (MA)

AWS Global Infrastructure

Physical and Environmental (PE) and partial Contingency Planning (CP)

Full and partially inherited security controls

FedRAMP: Meeting FISMA requirements in the cloud

417

Security controls at high baseline

(NIST 800-53 is foundation)

NIST Special Publication 800-53
Revision 4

**Security and Privacy Controls for
Federal Information Systems
and Organizations**

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

FedRAMP: Meeting FISMA requirements in the cloud



Tools no matter starting point

(Data/server/app migration/cloud native
Quick Starts)



Compliant connectivity

(Amazon VPC/Amazon VPN,
AWS Direct Connect)



Inheritance from AWS

(**44** FedRAMP High Service)

AWS gets customers at least 60% along their compliance journey in terms of security controls

NIST QuickStart accelerator (aka How do you systematically address more of the NIST controls?)

How does AWS make this easier?

The Enterprise Accelerator Compliance Quick Start

<https://aws.amazon.com/quickstart>

Menu **amazon** web services **AWS re:Invent** More English My Account [Sign In to the Console](#)

AWS Quick Starts

Automated, gold-standard deployments in the AWS Cloud

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production or test environment quickly and start using it immediately.

Available Quick Starts:

NEW **BY USE CASE** ALL

ANALYTICS BLOCKCHAIN BUSINESS PRODUCTIVITY COMMUNICATIONS CONTACT CENTER CONTAINERS & MICROSERVICES DATA LAKES
DATABASES DEVOPS HEALTHCARE & LIFE SCIENCES INFRASTRUCTURE IOT MACHINE LEARNING & AI MEDIA SERVICES MIGRATION
NETWORKING & REMOTE ACCESS SAAS **SECURITY & COMPLIANCE** SERVERLESS STORAGE WEBSITES & WEB APPS IBM MICROSOFT SAP

SEE ALSO

- + [AMAZON CONNECT INTEGRATIONS](#)
- [BIOTECH BLUEPRINTS](#)

AWS Enterprise Accelerator Quick Start website

The image displays three panels from the AWS Enterprise Accelerator Quick Start website, all under the heading "SECURITY & COMPLIANCE". Each panel features a "Quick Start" title and a shield icon with a checkmark.

- Panel 1 (Left):** Titled "NIST", it is "Built by AWS" and "Sets up a standardized AWS Cloud environment that helps support NIST FedRAMP TIC Overlay and DoD". The "Time to deploy" is 30 min.
- Panel 2 (Middle):** Titled "NIST high-impact controls", it is "Built by AWS" and "Extends the NIST Quick Start to help support NIST high-impact security controls, featuring Trend Micro Deep Security". The "Time to deploy" is 60 min. The link "Learn more | View guide" is circled in red.
- Panel 3 (Right):** Titled "PCI DSS", it is "Built by AWS" and "Sets up a standardized architecture for Payment Card Industry (PCI) Data Security Standard (DSS)". The "Time to deploy" is 30 min.

AWS Enterprise Accelerator Quick Start website

REFERENCE DEPLOYMENT

Standardized Architecture for NIST High-Impact Controls on AWS

Deploy an AWS Cloud architecture for NIST high-impact security controls, featuring Trend Micro Deep Security

[View deployment guide](#)

[View security controls matrix](#)

This Quick Start extends the [NIST Quick Start](#) to help support:

- NIST SP 800-53 (Rev. 4) high-impact security controls baseline
- CNSS Instruction 1253
- NIST SP 800-171
- FedRAMP and TIC Overlay (pilot)
- DoD Cloud Computing SRG

The Quick Start template automatically configures the AWS resources and deploys a multi-tier, Linux-based web application in a few simple steps, in about an hour. The Quick Start features Deep Security from Trend Micro for host-based protection. The [security controls matrix](#) (Microsoft Excel spreadsheet) shows how the Quick Start components map to security requirements.

This Quick Start is part of a set of AWS compliance offerings, which provide security-focused architecture solutions to help Managed Service Providers (MSPs), cloud provisioning teams, developers, integrators, and information security teams follow strict security, compliance, and risk management controls. For additional Quick Starts in this category, see the [Quick Start catalog](#).

This Quick Start was developed by AWS technical consultants and solutions architects.

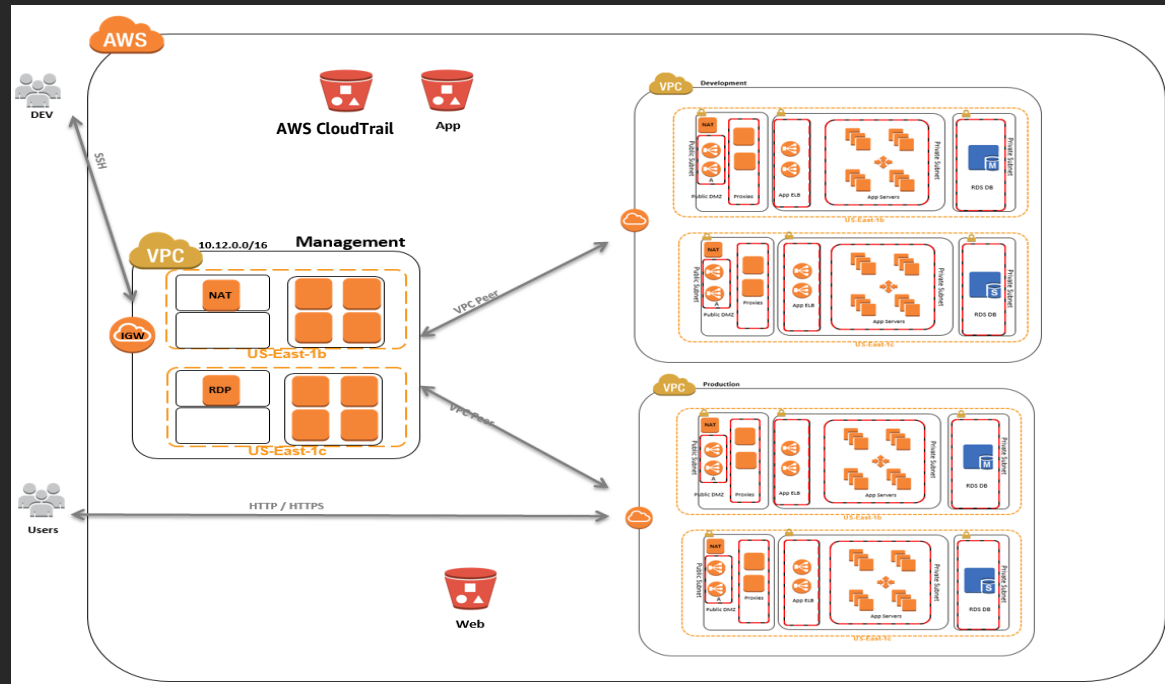


This Quick Start supports the AWS GovCloud (US) Region.



Watch [this webinar](#) to see how the Quick Start works.

What's in the box?



Reference Architecture

AWS Enterprise Accelerator – Compliance

Standardized Architecture for NIST-based Assurance Frameworks in the AWS Cloud

Quick Start Reference Deployment

AWS Professional Services
AWS Quick Start Reference Team

January 2016
(last update: June 2016)

This Quick Start supports the following requirements:

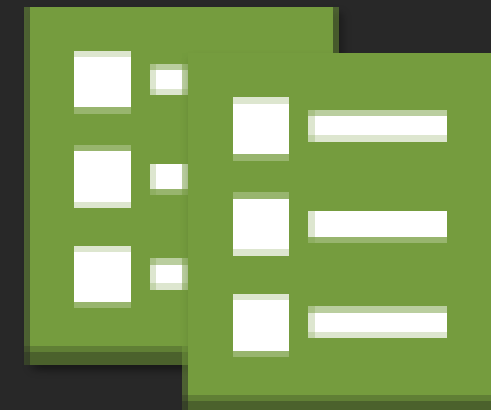
- NIST SP 800-53 and 800-171
- OMB TIC – FedRAMP Overlay (pilot)
- DoD Cloud Computing SRG

This guide is also available in HTML format at <https://docs.aws.amazon.com/quickstart/latest/accelerator-nist/>.

Deployment Guide

NIST SP 800-53 rev4 Controls					CNSS Instruction 1253 Control Selection			FedRAMP Control Selection			DoD Cloud SRG Control Selection				
Family	Control (Major)	Control (Sub-parts)	Title	Description	Control Baselines			Confidentiality	Integrity	Availability	Moderate	High	Minimum	Level 4	Level 5
					Priority	Low	Moderate								
AUDIT AND ACCOUNTABILITY	AU-12	AU-12	AUDIT GENERATION	The information system:	P1	X	X	X	X	X	X	X	X	X	
AUDIT AND ACCOUNTABILITY	AU-12	AU-12a	AUDIT GENERATION	Provides audit record generation capability for the auditable events defined in AU-2 a, a1 [Assignment: organization-defined information system components].				X	X	X	X	X	X	X	
AUDIT AND ACCOUNTABILITY	AU-12	AU-12b	AUDIT GENERATION	Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and				X	X	X	X	X	X	X	

Security Controls Matrix (SCM)



AWS CloudFormation Templates

Demo

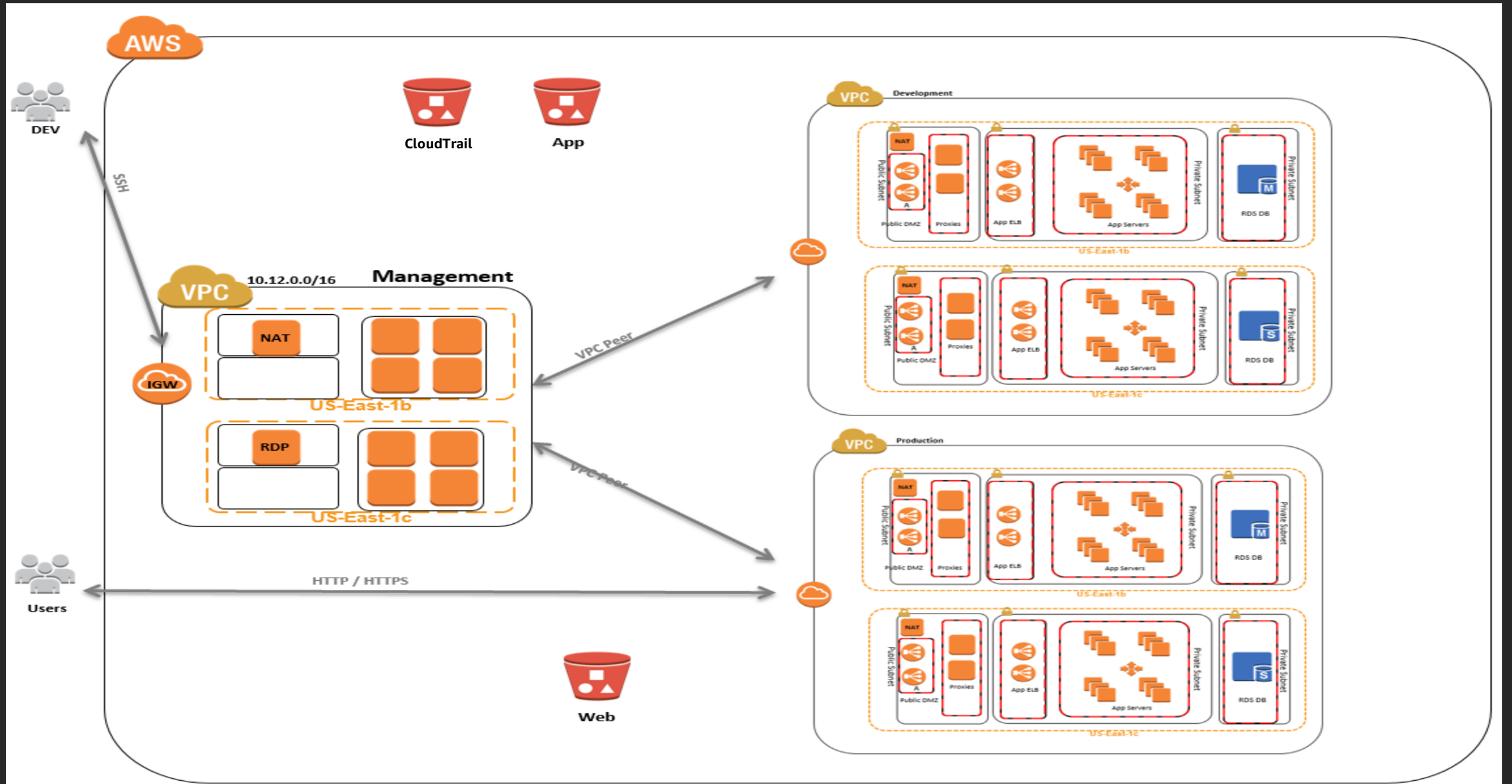
Customizable reference architecture

Example Reference Architecture

- Customizable
- Employs AWS architecture best practices

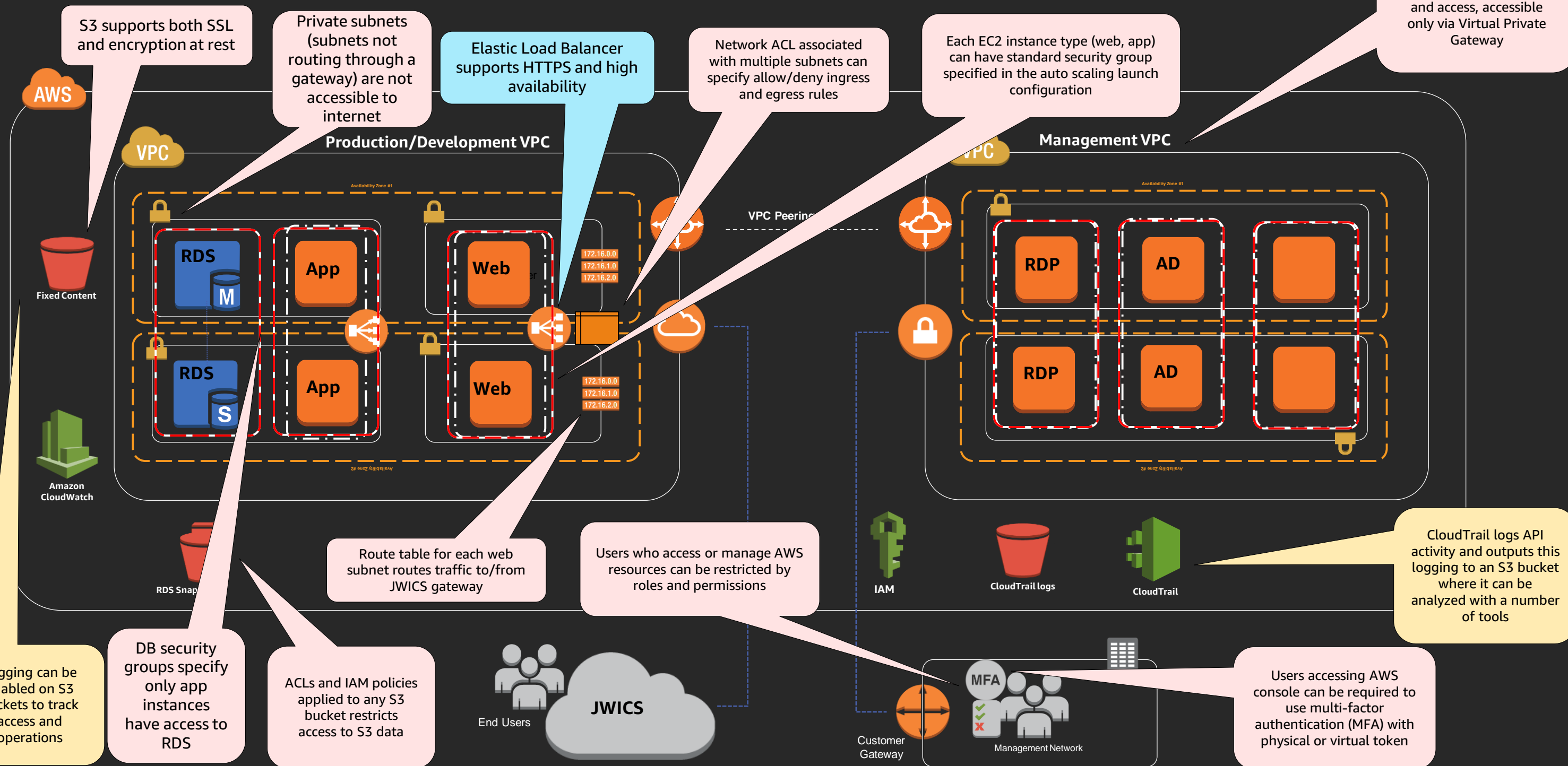
NOTES:

- Circa 2016!
- Missing multi-account, missing AWS Organizations, etc.

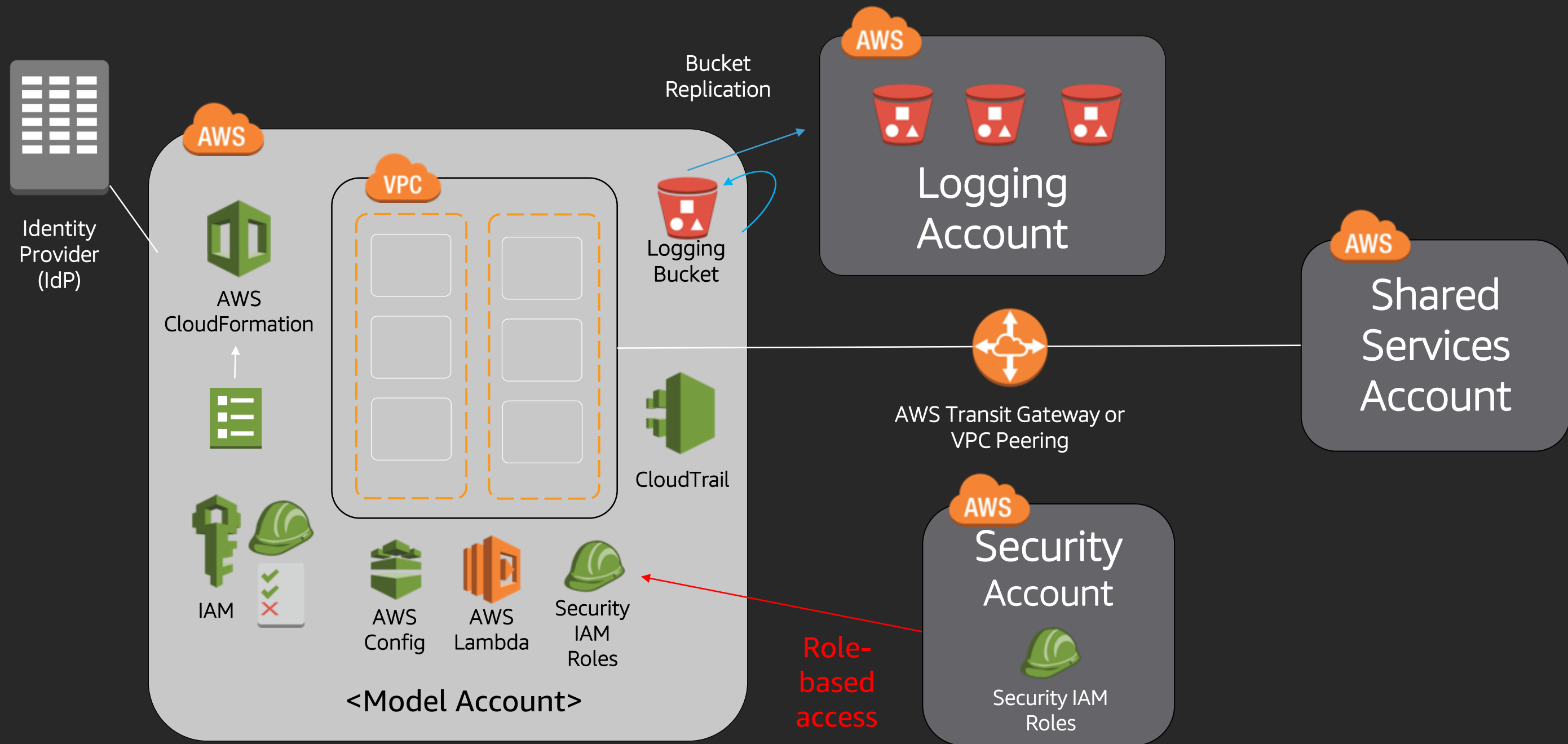


Incorporates security features via AWS best practice

Separate management VPC isolates all management applications and access, accessible only via Virtual Private Gateway



A more generalized reference architecture



What did we just do?

Customers

Certification, Accreditation and Security Assessment (**CA**), Awareness & Training (**AT**), Planning (**PL**), Personnel Security (**PS**), Risk Assessment (**RA**), and System & Services Acquisition (**SA**)
Access Control (**AC**), Audit & Accountability (**AU**), Configuration Management (**CM**), Maintenance (**MA**), Contingency Planning (**CP**), Identity and Authentication (**IA**), Incident Response (**IR**), Maintenance (**MA**), System and Communication Protection (**SC**), System and Information Integrity (**SI**)

Shared/hybrid and customer-implemented security controls



AWS Foundation Services

Media Protection (**MP**) and partial Maintenance (**MA**)

AWS Global Infrastructure

Physical and Environmental (**PE**) and partial Contingency Planning (**CP**)

Full and partially inherited security controls

Environment governance controls versus application controls

Customers

Application-Specific Controls

Certification, Accreditation and Security Assessment (CA), Awareness & Training (AT), Planning (PL), Personnel Security (PS), Risk Assessment (RA), System & Services Acquisition (SA), Access Control (AC), Audit & Accountability (AU), Configuration Management (CM), Maintenance (MA), Contingency Planning (CP), Identity and Authentication (IA), Incident Response (IR), Maintenance (MA), System and Communication Protection (SC), System and Information Integrity (SI)

Shared/hybrid and customer-implemented security controls at the *application* level

Organization-Specific Account/Baseline Controls

Account governance, mapped to *your* SCM; implement through automation

AWS Foundation Services

Media Protection (MP) and partial Maintenance (MA)

Full and partially inherited security controls



AWS Global Infrastructure

Physical and Environmental (PE) and partial Contingency Planning (CP)

Security controls matrix

NIST SP 800-53 rev4 Controls						CNSS Instruction 1253 Control Selection						FedRAMP Control Selection			DoD Cloud SRG Control Selection								
Family	Control (Major)	Control (Sub-parts)	Title	Description	Priority	Control Baselines			Confidentiality			Integrity			Availability			Low	Moderate	High	Minimum	Level 4	Level 5
						Low	Moderate	High	Low	Moderate	High	Low	Moderate	High	Low	Moderate	High						
AUDIT AND ACCOUNTABILITY	AU-12	AU-12	AUDIT GENERATION	The information system:	P1	X	X	X	X	X	X	X	X				X	X	X	X			
AUDIT AND	AU-12	AU-12a	AUDIT	Provides audit record generation capability																			

CloudFormation Template Mapping				
IAM CloudFormation Stack/Template	MANAGEMENT VPC CloudFormation Stack/Template	PRODUCTION VPC CloudFormation Stack/Template	LOGGING CloudFormation Stack/Template	CONFIG-RULES CloudFormation Stack/Template
This stack does not directly implement this control	This stack does not directly implement this control	This stack does not directly implement this control	AWS::S3::Bucket AWS::S3::BucketPolicy AWS::CloudTrail::Trail	This stack does not directly implement this control
AWS::IAM::Group AWS::IAM::InstanceProfile AWS::IAM::ManagedPolicy AWS::IAM::Policy AWS::IAM::Role	This stack does not directly implement this control	This stack does not directly implement this control	AWS::IAM::InstanceProfile AWS::IAM::Role AWS::CloudTrail::Trail AWS::CloudWatch::Alarm AWS::SNS::Topic	This stack does not directly implement this control
This stack does not directly implement this control	This stack does not directly implement this control	This stack does not directly implement this control	AWS::CloudTrail::Trail AWS::S3::Bucket AWS::S3::BucketPolicy	This stack does not directly implement this control
This stack does not directly implement this control	This stack does not directly implement this control	This stack does not directly implement this control	AWS::CloudTrail::Trail AWS::S3::Bucket	This stack does not directly implement this control

Quick Start Architecture Comments for NIST SP 800-53 Controls			
Addressed By This Quick Start	Category: Influence	Category: Responsibility	AWS Quick Start Control Implementation
Yes	Information Systems	Shared	AWS CloudTrail, S3 bucket logging, and RDS Database logging provide the audit record generation capability for the auditable events defined in AU-2a, by logging all security-relevant IAM user and API activities which address AWS infrastructure components (AWS Products and services).
Yes	Information Systems	Shared	While AWS Cloud trail logs all available API events automatically within the AWS infrastructure, AWS Identity and Access Management (IAM) configuration allows privileged users with administrator/audit access to modify Amazon CloudWatch alarms, AWS Config rules, and Amazon S3
Yes	Information Systems	Shared	AWS CloudTrail and S3 bucket logging generate audit records with the content defined in AU-3. Detailed content of CloudTrail logs are documented at http://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-
Yes	Information Systems	Shared	AWS CloudTrail compiles the audit records from all AWS infrastructure components into a system-wide audit trail in an S3 bucket that is time correlated using time stamps as specified in the ISO 8601 standard. IOS 8601 represents local time (with the location unspecified), as UTC, or as

Source:
<https://fwd.aws/bWvRw>

Use the AWS Enterprise Accelerator as a validation tool

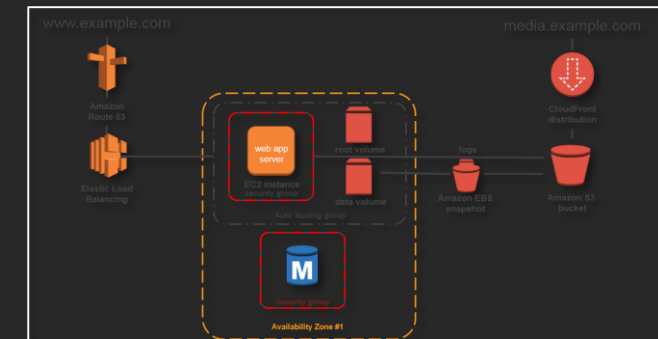
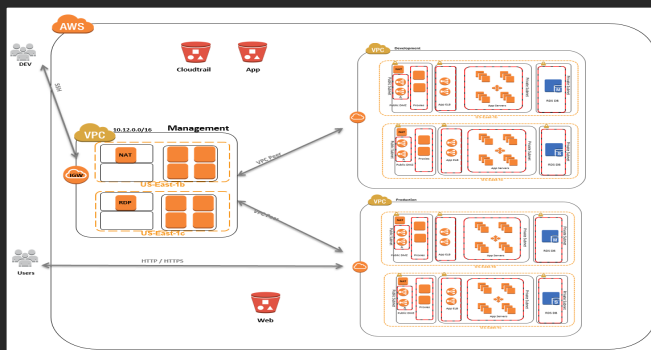
AWS Enterprise Accelerator SCM

Your SCM

CloudFormation Template Mapping				
IAM CloudFormation Stack/Template	MANAGEMENT VPC CloudFormation Stack/Template	PRODUCTION VPC CloudFormation Stack/Template	LOGGING CloudFormation Stack/Template	CONFIG-RULES CloudFormation Stack/Template
This stack does not directly implement this control	This stack does not directly implement this control	This stack does not directly implement this control	AWS::S3::Bucket AWS::S3::BucketPolicy AWS::CloudTrail::Trail	This stack does not directly implement this control
AWS::IAM::Group AWS::IAM::InstanceProfile AWS::IAM::ManagedPolicy AWS::IAM::Policy AWS::IAM::Role	This stack does not directly implement this control	This stack does not directly implement this control	AWS::IAM::InstanceProfile AWS::IAM::Role AWS::CloudWatch::Alarm AWS::SNS::Topic	This stack does not directly implement this control
This stack does not directly implement this control	This stack does not directly implement this control	This stack does not directly implement this control	AWS::CloudTrail::Trail AWS::S3::Bucket AWS::S3::BucketPolicy	This stack does not directly implement this control
This stack does not directly implement this control	This stack does not directly implement this control	This stack does not directly implement this control	AWS::CloudTrail::Trail AWS::S3::Bucket	This stack does not directly implement this control



Control ID	Family	Control Sub-point	Title	Description	Priority	Category	Sub-category	Confidentiality	Integrity	Availability	Additional FedRAMP Defined Assignment / Selection Parameters	Additional FedRAMP Requirements & Evidence	Control Type	Control Status	Control Responsibility	AWS Qualifier Control Implementation Description
16	ACCESS CONTROL	AC-4	INFORMATION FLOW ENFORCEMENT	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on Organization-defined information flow control policies.	P1	X	X	X	X	X	X	X	X	X	Shared	This architecture incorporates route tables that specify which subnets in each VPC are accessible through internet and NAT gateways. AWS Security Groups restrict network ports/network access to EC2/EC3 instances and Elastic Load Balancers. In addition, Amazon S3 buckets that are created are configured with access control policies.
165	ACCESS CONTROL	AC-3(2)	PROTECTION OF CONFIDENTIALITY, INTEGRITY, OR ENCRYPTION	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of sensitive information.	P1	X	X	X	X	X	X	X	X	Shared	TLS is employed for console access, CLI, and API endpoints for AWS service access. Amazon S3 for object access, and AWS Elastic Load Balancing (ELB) endpoints for user web access. S3K is employed for Bucket host access and sessions between the bucket host and internal network nodes, including any EC2-based NAT instances in AWS Regions where Managed NAT Gateways are not yet available. TLS/SSL ports and protocols are enforced by Security Groups.	
164	AUDIT AND ACCOUNTABILITY	AU-2	AUDIT EVENTS	The organization:	P1	X	X	X	X	X	X	X	Shared	See control support details below.		
165	AUDIT AND ACCOUNTABILITY	AU-2a	AUDIT EVENTS	Determines that the information system is capable of auditing the following events: (Assignment: organization-defined audited events)	P1	X	X	X	X	X	X	X	Shared	AWS CloudTrail, S3 bucket logging, Elastic Load Balancing (ELB) logging, and AWS Database logging provide the capability for audit of organizationally defined events by logging of security-relevant user/API activities and S3 data access activities.		
165	AUDIT AND ACCOUNTABILITY	AU-2b	AUDIT EVENTS	Provides a rationale for why the auditable events are deemed to be relevant to support after the fact investigations of security incidents and	P1	X	X	X	X	X	X	X	Shared	AWS CloudTrail, S3 bucket logging, Elastic Load Balancing (ELB) logging, and AWS Database logging provide the capability for audit of organizationally defined events by logging of security-relevant user/API activities, and S3 data access activities.		
165	AUDIT AND ACCOUNTABILITY	AU-2c	AUDIT EVENTS	Determines that the following events are to be audited within the information system: (Assignment: organization-defined audited events) The subset of the auditable events defined in AU-2(a) along with the frequency of (or occasion mapping) auditing for each identified event.	P1	X	X	X	X	X	X	X	Shared	AWS CloudTrail, S3 bucket logging, Elastic Load Balancing (ELB) logging, and AWS Database logging provide the capability for audit of organizationally defined events by logging of security-relevant user/API activities, and S3 data access activities.		
165	AUDIT AND ACCOUNTABILITY	AU-2d	AUDIT EVENTS	Determines that the following events are to be audited within the information system: (Assignment: organization-defined audited events) The subset of the auditable events defined in AU-2(a) along with the frequency of (or occasion mapping) auditing for each identified event.	P1	X	X	X	X	X	X	X	Shared	AWS CloudTrail, S3 bucket logging, Elastic Load Balancing (ELB) logging, and AWS Database logging provide the capability for audit of organizationally defined events by logging of security-relevant user/API activities, and S3 data access activities.		
175	AUDIT AND ACCOUNTABILITY	AU-3	CONTENT OF AUDIT RECORDS	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the actions of the event, and the identity of any individuals or subjects associated with the event.	P1	X	X	X	X	X	X	X	Shared	AWS CloudTrail, S3 bucket logging, and AWS Database logging generate audit records that include the level of detail specified in the control. CloudTrail logs provide information on activities related to the manipulation of the infrastructure, while S3 bucket logs provide data on activities related to the access or manipulation of data stored in S3. Detailed content of audit logs are documented at https://docs.aws.amazon.com/awscloudtrail/awscd-trail-logs/audit-log-events-reference-report-controls.html and detailed S3 bucket log systems are Amazon S3 buckets are established for storage of AWS CloudTrail audit records, S3 bucket logs, Elastic Load Balancing logs, etc, which provide dynamic capacity growth to accommodate organizationally defined storage capacity requirements.		
176	AUDIT AND ACCOUNTABILITY	AU-4	AUDIT STORAGE CAPACITY	The organization allocates audit record storage capacity in accordance with Assignment: organization-defined audit record storage requirements.	P1	X	X	X	X	X	X	X	Shared	AWS CloudTrail, S3 bucket logging, Elastic Load Balancing logs, etc, which provide dynamic capacity growth to accommodate organizationally defined storage capacity requirements.		



Back to the demo

Pathway to ATO

ATO on AWS?



Benefits

Reduce effort to deploy security configurations and collect audit data to meet compliance requirements for solutions on AWS

Build an end-to-end automation capability to streamline regulated workload deployments

Reduce time to build applications in the cloud or to migrate applications into the cloud

Reduce cost to deploy workloads in the cloud

Improve security posture of your cloud estate

Guiding Tenets for ATO on AWS



ATO on AWS

Automation leverages *Infrastructure as Code* concepts

Certification optimizes security processes

Validation enables continual tests and monitoring of security configurations

Empowerment emboldens informed decision-making and drives change

Implement security
and compliant
architectures



Goal

Verifiable compliance control solution for regulated workloads

Outcomes

Accelerated path to production

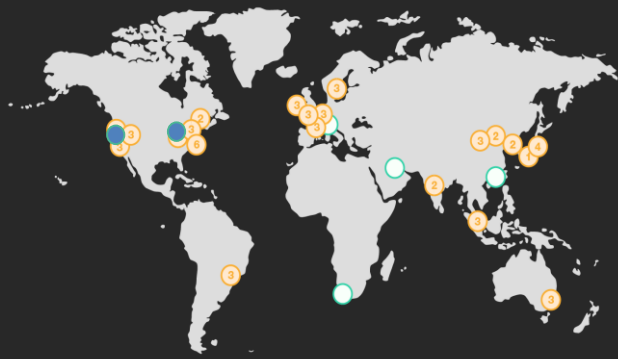
Improved compliance and security posture

Reduction in noncompliant findings and rework

Demonstrable controls to support the assessment process

Summary

Key takeaways



AWS GovCloud (US)

Is it right for your workload?



NIST

Accelerator

Use as a reference point for your security control matrix



Pathway to ATO



Next Steps

What's next?

- Define/create YOUR baseline account automation
 - AWS Landing Zones
 - AWS Control Tower
 - Infrastructure as Code using AWS CloudFormation, Terraform, scripting, etc.
- Find (or create) your security control matrix (SCM)
- Compare to the AWS Enterprise Accelerator SCM
- Address the gaps

AWS GovCloud (US) information

Homepage: <https://aws.amazon.com/govcloud-us>

User Guide: docs.aws.amazon.com/govcloud-us/latest/UserGuide/welcome.html

Services in Scope: <https://aws.amazon.com/compliance/services-in-scope/>

ATO on AWS program information

Partners: <https://aws.amazon.com/partners/ato/partners/>

Customers: <https://aws.amazon.com/partners/ato/>

FAQ: <https://aws.amazon.com/partners/ato/faqs/>

Resources

Related sessions

- WPS318-R – Architecting security and governance across a multi-account strategy
- MGT403-R – How to audit and remediate resource misconfigurations

More resources

- [AWS GovCloud \(US\) - A path to high compliance in the cloud \(GRC344\) – AWS re:Inforce 2019](#)
- [Implementing Governance@Scale – AWS Washington Public Sector Summit 2017](#)

Thank you!

Derek Doerr

awsderek@amazon.com



Please complete the session survey in the mobile app.