
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PEX104

Accelerate global compliance for your SaaS solution

Tim Sandage

Senior Manager, Security Partners –
Global Security and Compliance Acceleration
AWS

Bill Tarr

Senior Partner Solutions Architect –
SaaS Factory Program
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

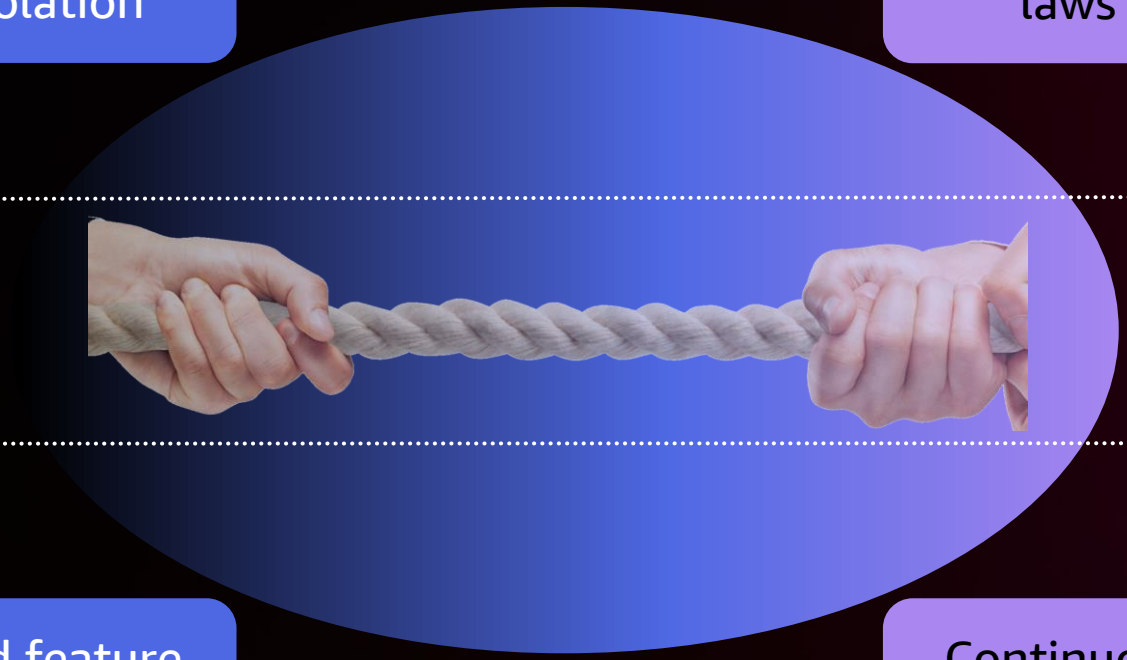
Software as a service (SaaS) is a business and software delivery model that enables organizations to offer their solution in a low-friction, service-centric approach

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance and SaaS challenges

SaaS design decisions

- Tenant isolation
- Multi-Region
- Data partitioning
- Rapid feature release

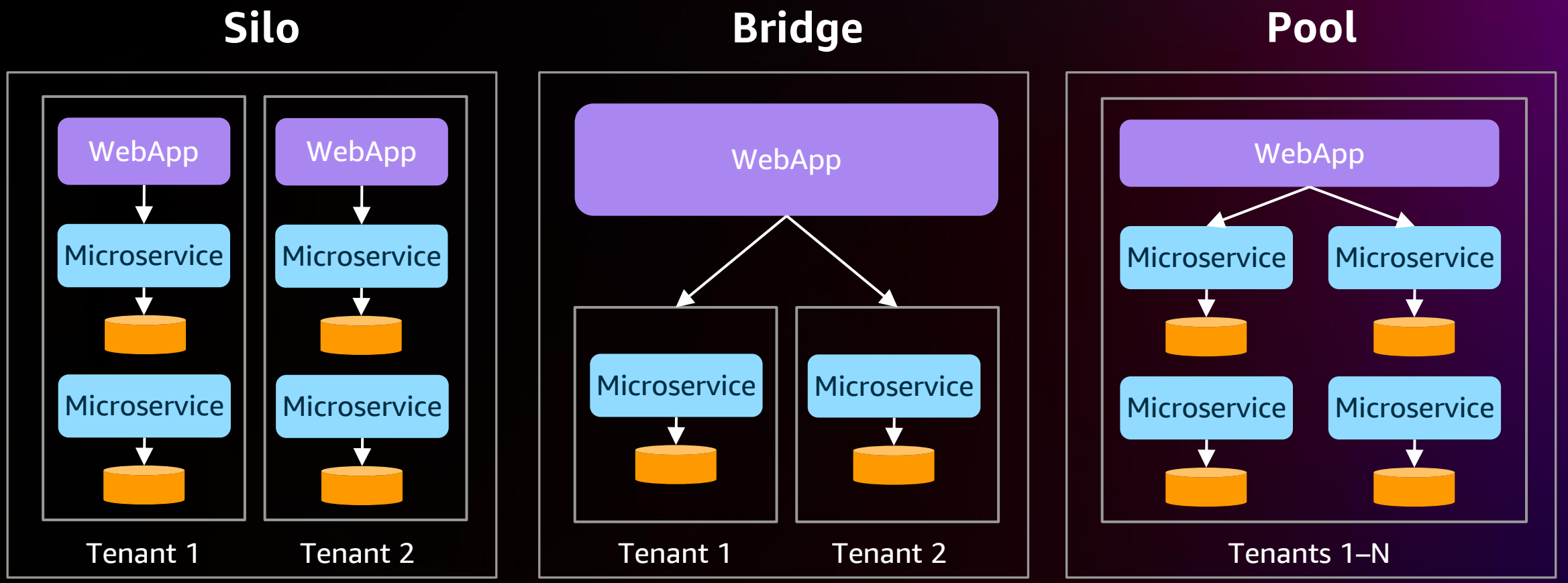


Compliance challenges

- Data privacy laws
- Data sovereignty
- Encryption of data at rest
- Continuous compliance

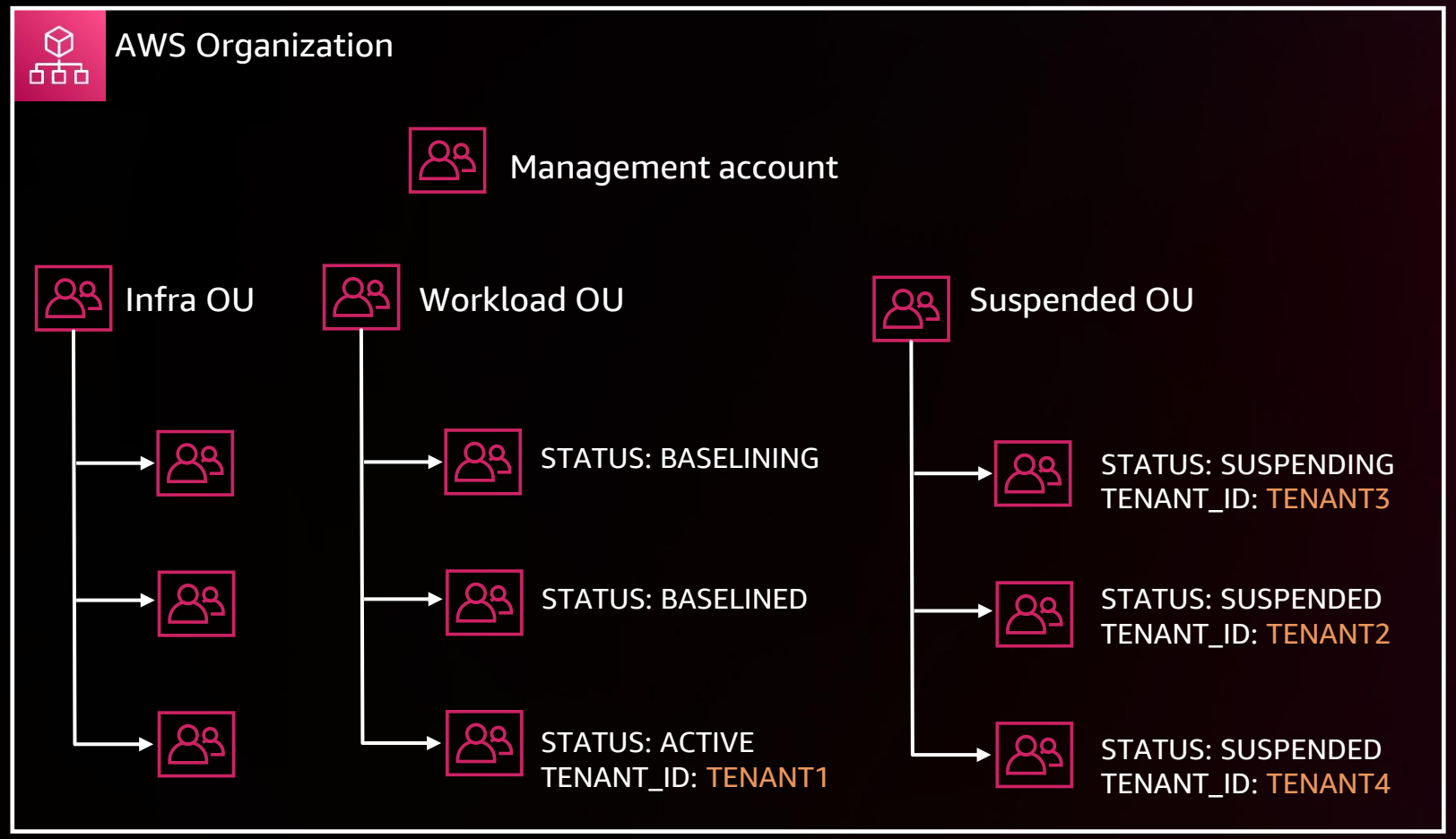
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SaaS tenant isolation models



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

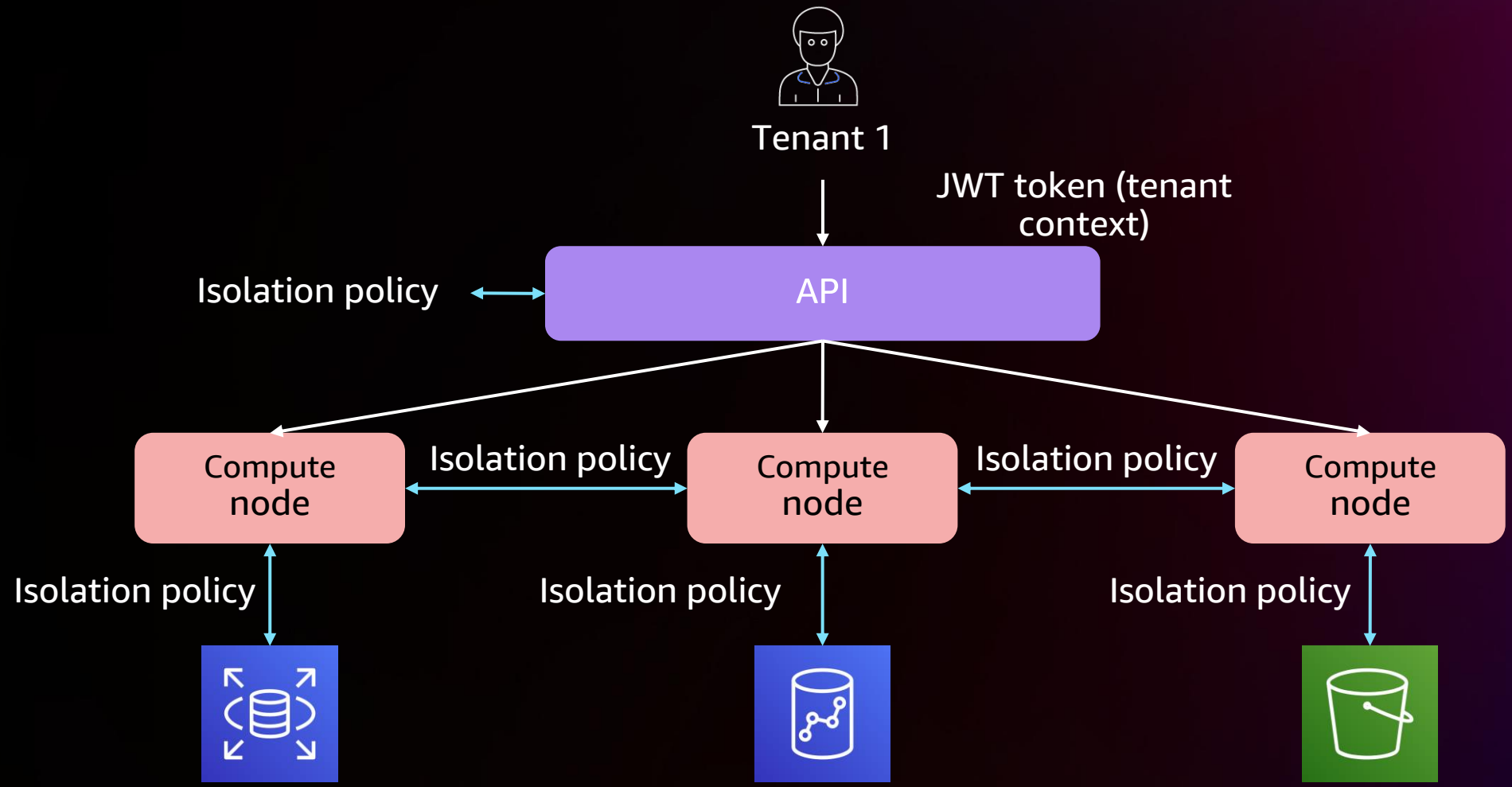
AWS Organizations and AWS Control Tower to the rescue



- **Centrally provision** tenant accounts
- Secure and **audit** your environment for **compliance**
- **Share resources and control access** to accounts, AWS Regions, and services
- **Optimize costs** and identify cost-saving measures

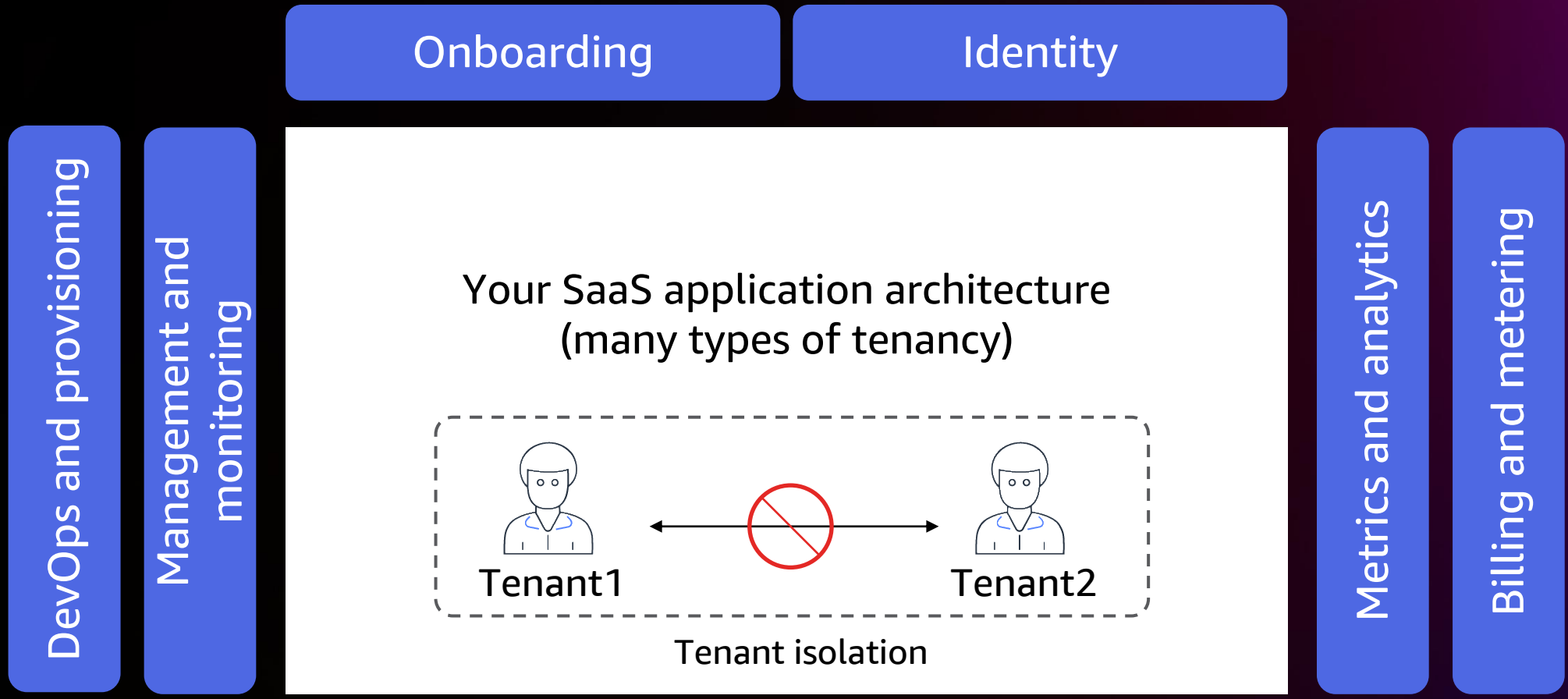
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Leverage runtime policies to control access



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Control plane and compliance concerns



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

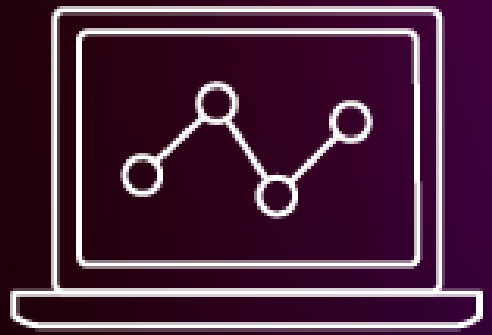
Multi-Region roadmap for compliance



Data tokenization



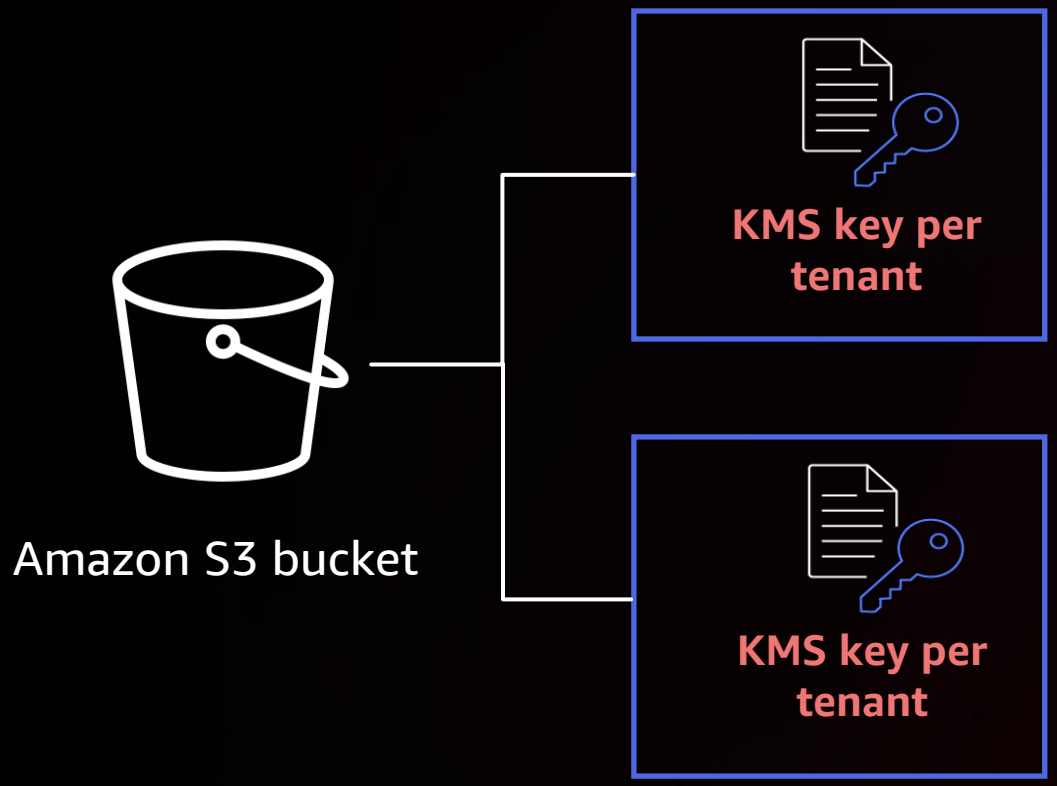
Onboarding concerns



Single pane of glass

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Apply tenant-level encryption using keys at the storage layer

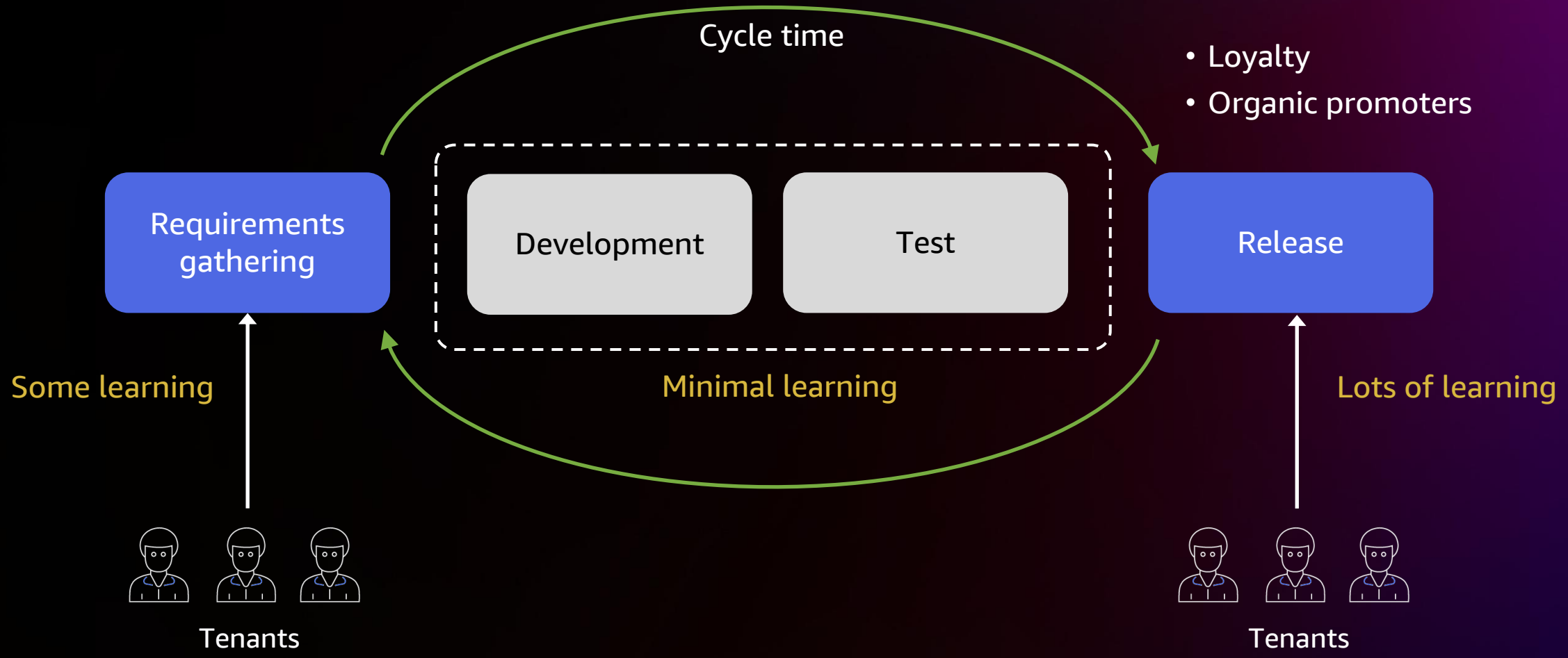



```
put-object
  --bucket <value>
  --key <value>
  [--sse-customer-key <value>]
```

Create an AWS KMS key per tenant during onboarding and pass the key as a parameter when saving objects in the tenant-specific prefix or folder

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

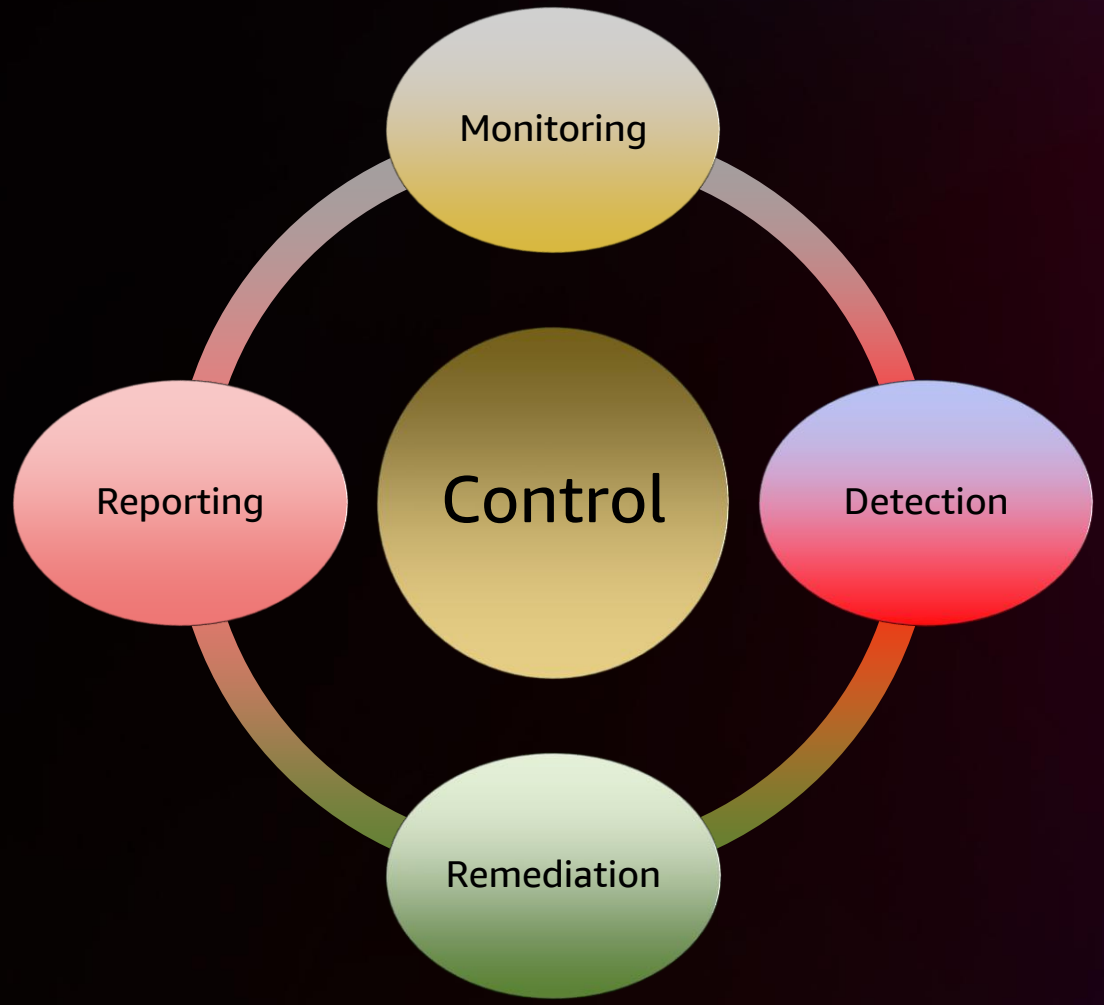
SaaS demands tighter cycle times



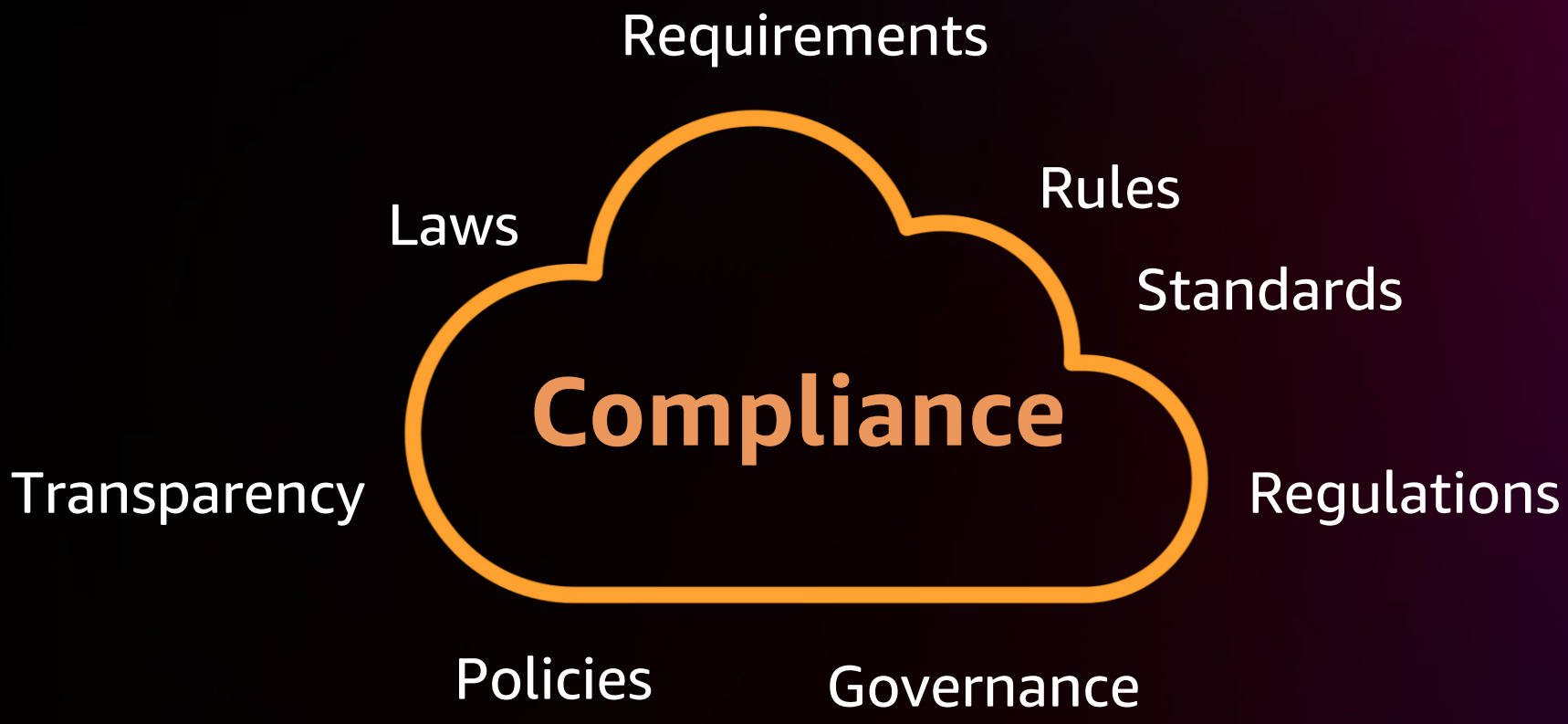
- Loyalty
- Organic promoters

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Continuous compliance monitoring fits



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility – The line varies . . .



Amazon EC2



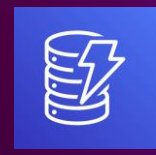
Amazon RDS



Amazon S3



AWS KMS



DynamoDB

More customizable
+
More customer responsibility

Infrastructure Services		Container Services		Abstracted Services	
Customer data	Customer IAM	Customer data	Customer IAM	Customer data	Customer IAM
Platform & application management		Network traffic protection		Client-side data encryption	
OS, network, firewall configuration		Client-side data encryption		Server-side encryption	AWS IAM
Network traffic protection		Firewall configuration		Network traffic protection	
Server-side encryption		Platform & application management	AWS IAM	Platform & application management	
Client-side data encryption/integrity		OS, network, firewall Configuration		OS, network, firewall Configuration	
Compute/storage/ database/network	AWS IAM	Compute/storage/ database/network		Compute/storage/ database/network	
Hardware/AWS Global Infrastructure		Hardware/AWS Global Infrastructure		Hardware/AWS Global Infrastructure	

Less customizable
+
Less customer responsibility
+
More best practices built in

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance influence on AWS services choices

AWS Services in Scope page

See which services have been assessed and approved by independent auditors and regulators for different compliance frameworks and regulations – https://aws.amazon.com/compliance/services-in-scope/

AWS Artifact

On demand access to AWS's security and compliance reports and select online agreements – https://aws.amazon.com/artifact/

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance – Key factors for consideration

- Improve overall security posture
- Regulatory environment – HIPAA, GDPR, FedRAMP
- What is your customer base requesting – SOC 2, ISO 27001, HITRUST
- Earn customer trust
- Faster sales cycles
- Accelerate growth in new verticals and geographies

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

First steps – AWS best practices

AWS Startup Security Baseline – A set of controls that create a minimum foundation for businesses to build securely on AWS; the controls in this guide are designed with early startups in mind, mitigating the most common security risks without requiring significant effort

- https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-startup-security-baseline/welcome.html

AWS Well-Architected Tool and SaaS Lens – AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. The AWS WA Tool is designed to help you review the state of your applications and workloads, and it provides a central place for architectural best practices and guidance.

- https://aws.amazon.com/well-architected-tool/
- https://docs.aws.amazon.com/wellarchitected/latest/saas-lens/saas-lens.html

AWS Foundational Technical Review (FTR) – Helps identify AWS Well-Architected best practices specific to your software or solution

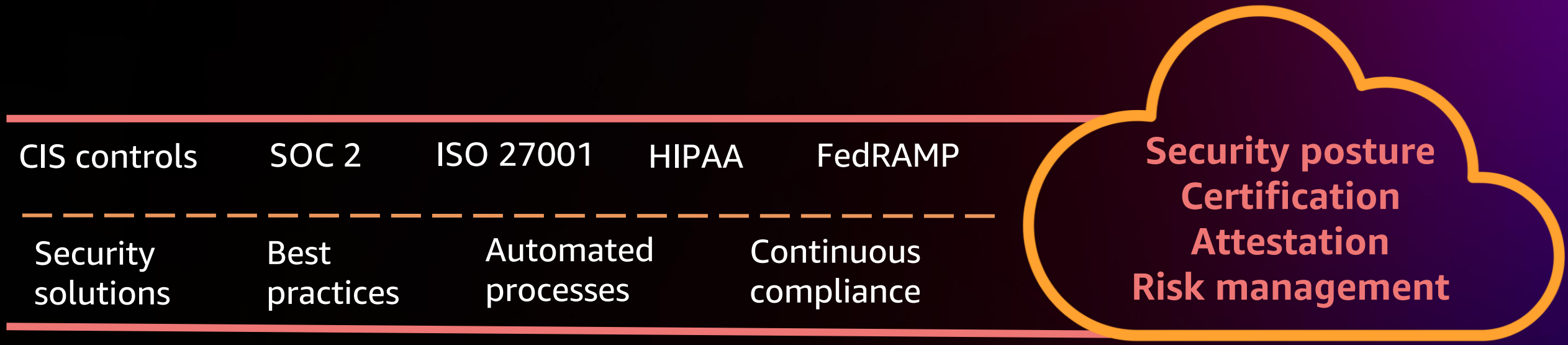
- https://aws.amazon.com/partners/foundational-technical-review/

CIS AWS Cloud benchmarks – Best practices integrated into AWS services (Amazon Inspector, AWS Audit Manager, AWS Config, AWS Security Hub)

- https://www.cisecurity.org/benchmark

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compliance – Building your roadmap



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS and our partner environment

Global Security and Compliance Acceleration (GSCA) initiative (formerly ATO on AWS)
Helps AWS Partners meet their customers' authorization needs, whether it be architecting, configuring, deploying, or integrating tools and controls to meet security, privacy, and compliance requirements for healthcare, privacy, national security, and financial sectors.
Partners – https://aws.amazon.com/partners/programs/ato/partners/

SaaS Factory Program
Helps AWS Partners at any stage of the software-as-a-service (SaaS) journey. Whether you are looking to build new products, migrate existing applications, or optimize SaaS solutions on AWS, the AWS SaaS Factory Program can help – https://aws.amazon.com/partners/programs/saas-factory

SaaS Competency Partners
https://aws.amazon.com/partners/saas-on-aws/partner-solutions

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GSCA on AWS?

GOALS AND BENEFITS















Goal

- **Help** customers, partners, independent solution vendors (ISVs)

Outcomes

- **Accelerates** security and compliance authorization processes
- **Reduces** cost and time
- **Provides** reusable artifacts including guidance, templates, tools, and prebuilt templates from AWS and Amazon Partner Solutions
- **Builds and optimizes** DevOps, SecOps, continuous integration/ continuous delivery (CI/CD), continuous risk treatments (CRT)
- **Develops** proven techniques using AWS Security Automation and Orchestration (SAO) methodologies

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

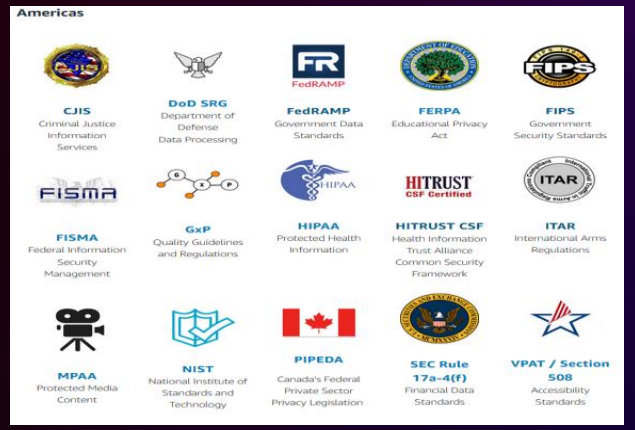
GSCA initiative

- Scale to meet regulatory and compliance-specific support globally
- Many regional and country-specific requirements leading to confusion/concerns about cloud usage
- Customers require support to understand how to meet these requirements on AWS
- Scale through partner engagement and support









© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GSCA 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

Collaborate in joint partner programs supported by AWS to develop and deliver unique capabilities and solutions

Works with qualified system integrators

- ✓ To build and support environments that meet compliance standards and requirements
- ✓ To minimize and simplify ISV's area of responsibility by offloading hosting and compliance management

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Tim Sandage
sandaget@amazon.com

Bill Tarr
billtarr@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.