aws professional services

Secure by Design

AWS Security Workshop

Agenda

- Modernize Technical Governance
- Defining your control environment
- AWS Control Tower
- DevSecOps
- Automate Security Operations
- Continuous Compliance

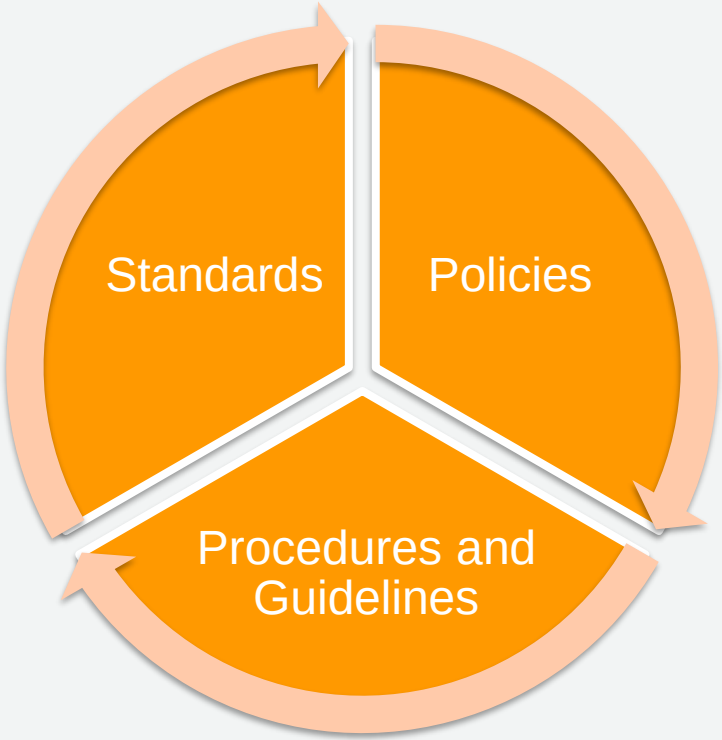
Goals

- Learn how to mitigate risk
- Understand security design principles
- Discover tools to automate security enforcement at scale
- Realize that scale does not sacrifice granular security

Modernize Technology Governance

aws professional services

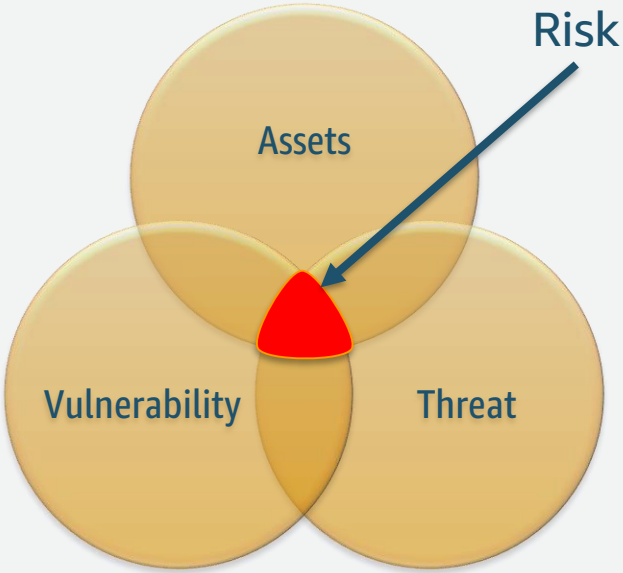
Current State – Technology Governance



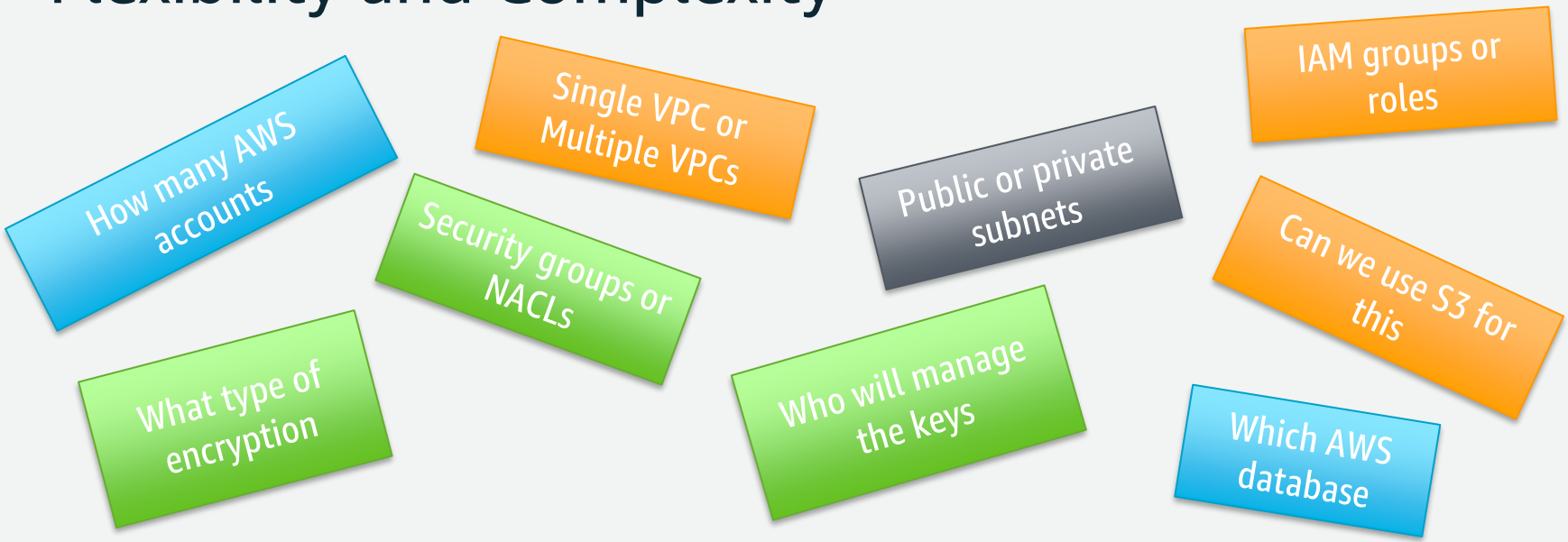
Issues – Technology Governance

The majority of technology governance processes relies predominantly on administrative and operational security controls with ***limited*** technology enforcement.

AWS has an opportunity to innovate and advance ***Technology Governance Services***.



Flexibility and Complexity

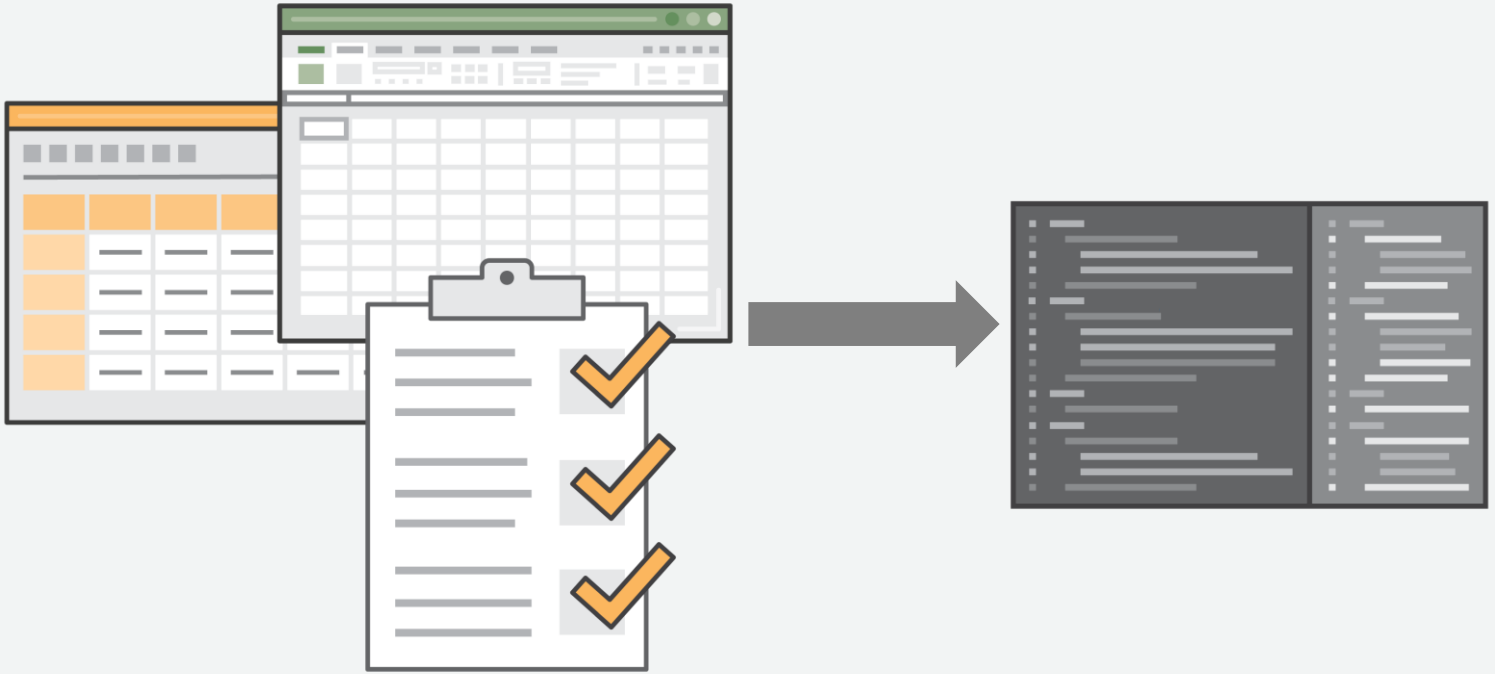


What is the regulatory requirement?

What's in-scope or out-of-scope?

How to verify the standards are met?

Security & Compliance then and now



Security by Design

Security by Design (SbD) is a security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing.

Instead of relying on auditing security retroactively, SbD provides security control built in throughout the AWS IT management process.

AWS Security Hub

AWS Identity and Access Management

Amazon CloudWatch

AWS Trusted Advisor

AWS CloudTrail

AWS Directory Service

AWS Key Management Service

AWS Config

Security by Design - Design Principles

Developing new risk mitigation capabilities, which go beyond global security frameworks, by treating risks, eliminating manual processes, optimizing evidence and audit ratifications processes through rigid automation

- Build security in every layer
- Design for failures
- Implement auto-healing
- Think parallel
- Plan for Breach

- Don't fear constraints
- Leverage different storage options
- Design for cost
- Treat Infrastructure as Code
  - Modular
  - Versioned
  - Constrained

SbD - Modernize Tech Governance (MTG)

Why?

Complexity is growing, making the old way to govern technology obsolete

You need automation that AWS offers to manage security

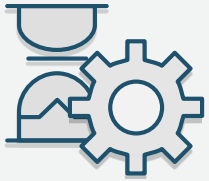
Goal - Modernize Tech Governance (MTG)

Adopting "***Prevent***" controls, making "***Detect***" controls more powerful and comprehensive

AWS Control Tower

aws professional services

AWS Control Tower



Automated AWS Setup

Launch an automated landing zone with best-practices blueprints

Policy Enforcement

Pre-packaged guardrails to enforce policies or detect violations

Dashboard for Oversight

Continuous visibility into workload compliance with controls

AWS Control Tower – Key Features

Automated landing zone with best practice blueprints

Guardrails for policy management

Account factory for account provisioning

Dashboard for visibility and actions

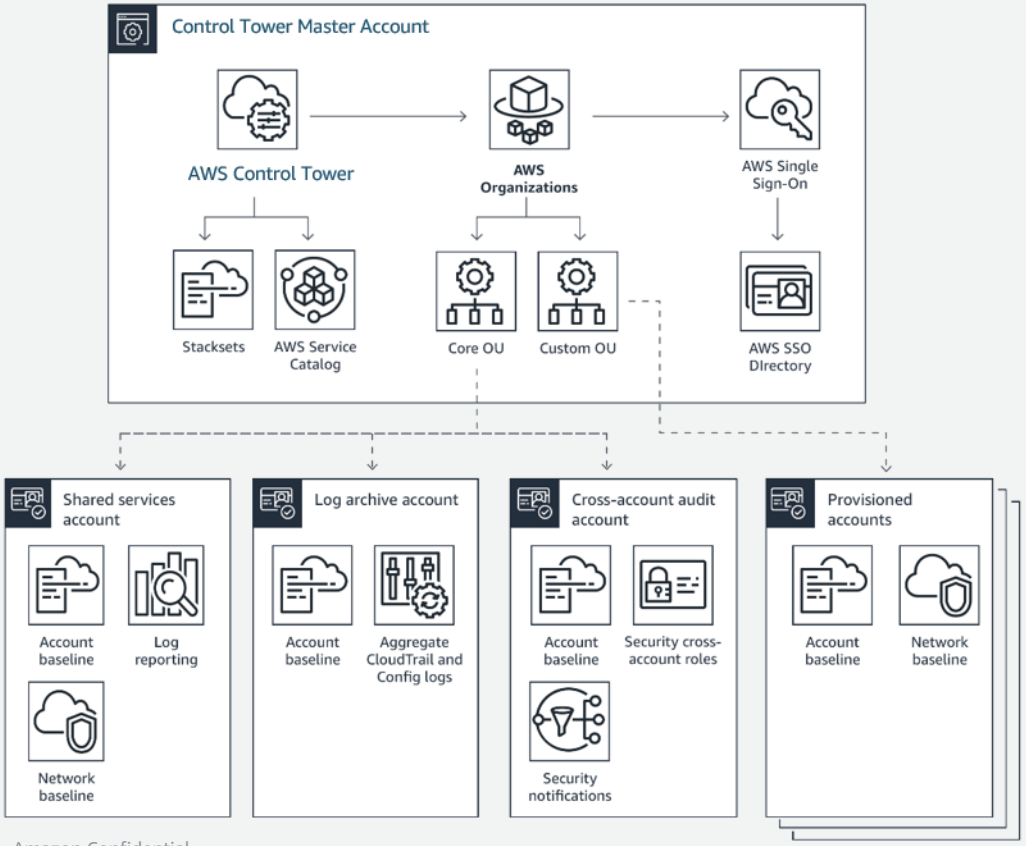
Built-in identity and access management

Preconfigured log archive and audit access to accounts

Built-in monitoring and notifications

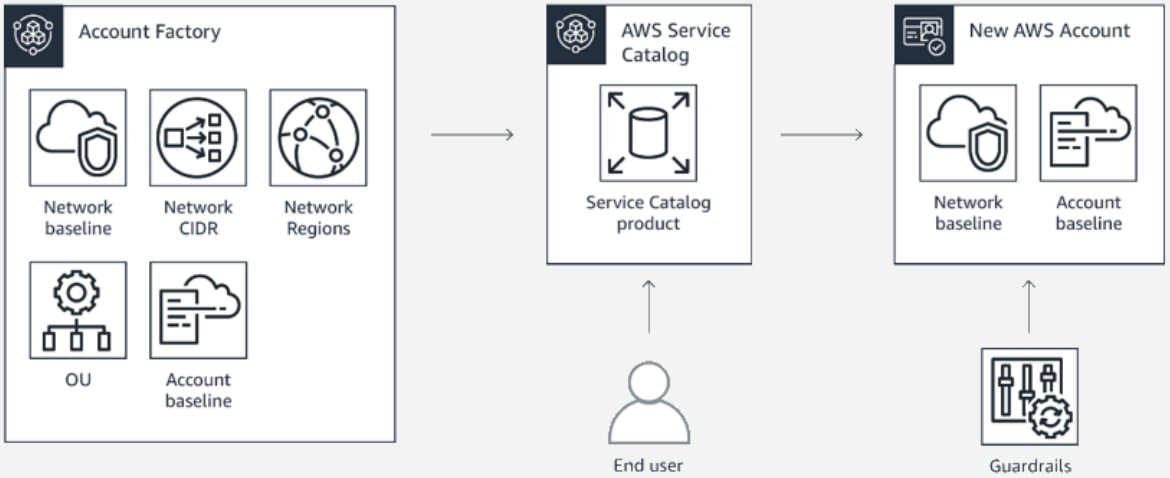
Automatic updates

AWS Control Tower – Account Overview



- AWS Organizations with a master and pre-created accounts for central log archive, cross-account audit, and shared services
- Pre-configured directory and single sign-on using AWS SSO (with Active Directory custom option)
- Centralized monitoring and alerts using AWS Config, AWS CloudTrail, and AWS CloudWatch

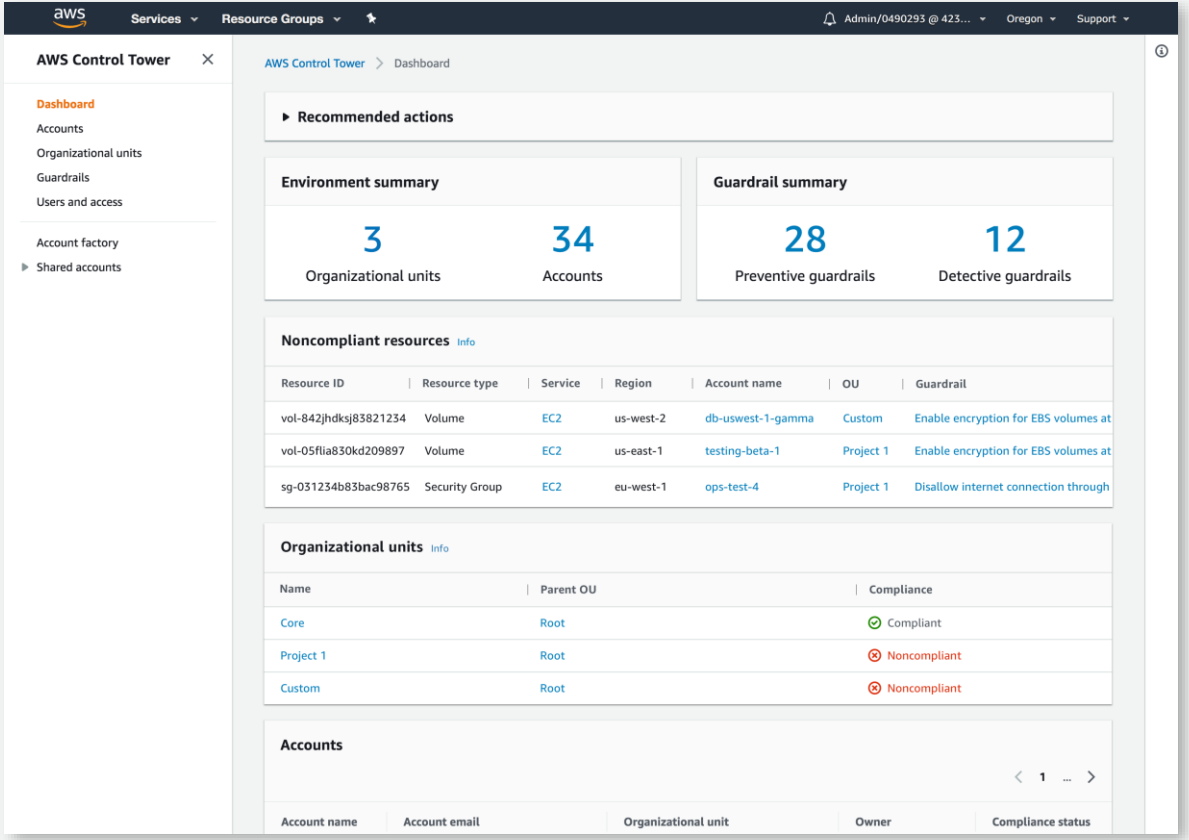
AWS Control Tower - Account Factory



- Account factory for controls on account provisioning
  - Pre-approved account baselines with VPC options
  - Pre-approved configuration options
- End user configuration and provisioning through AWS Service Catalog
- Creates/updates AWS accounts under organizational units

aws professional services

AWS Control Tower - Dashboard



aws professional services

Security Journey

aws professional services

Taking the Journey

Define a **security strategy**

Identify Stakeholders

Identify Your Workloads Moving to AWS

Deliver a **security program**

Rationalize Security Requirements

Define Data Protections and Controls

Document Security Architecture

Develop robust **security operations**

Deploy Architecture

Automation

Continuous Monitoring

Testing and Gamedays

Certify

Audit and Certification

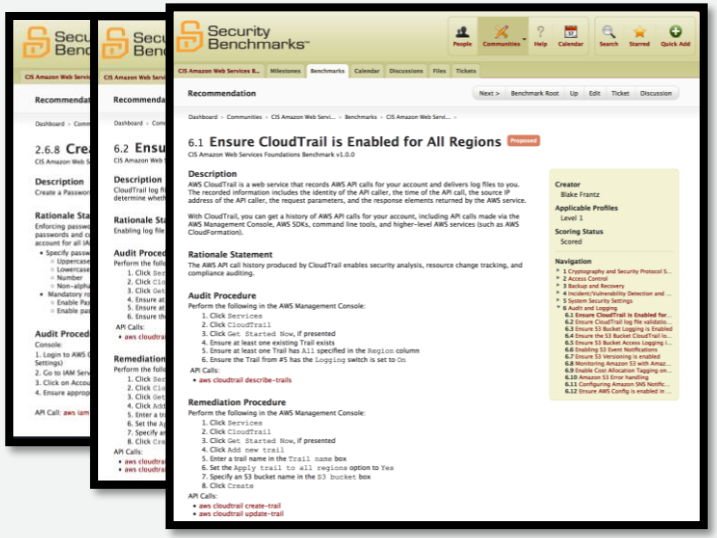
SbD – Rationalize Security Requirements

AWS has partnered with CIS Benchmarks to create consensus-based, best-practice security configuration guides that will align to multiple security frameworks globally.

The Benchmarks are:

- Recommended technical control rules/values for hardening operating systems, middle ware and software applications, and network devices
- Distributed free of charge by CIS in .PDF format
- Used by thousands of enterprises as the basis for security configuration policies and the de facto standard for IT configuration best practices.

Center for Internet Security®



https://www.cisecurity.org/

SbD – AWS CIS Benchmark Scope


AWS Identity and Access Management


AWS Security Hub


AWS Config


AWS Key Management Service


Simple Notification Service


Amazon CloudWatch


Amazon S3


AWS CloudTrail

Foundational Benchmark


Flow logs


Amazon VPC

Amazon Route 53


Amazon EC2


Amazon CloudFront


Elastic Load Balancing (ELB)


Amazon EBS

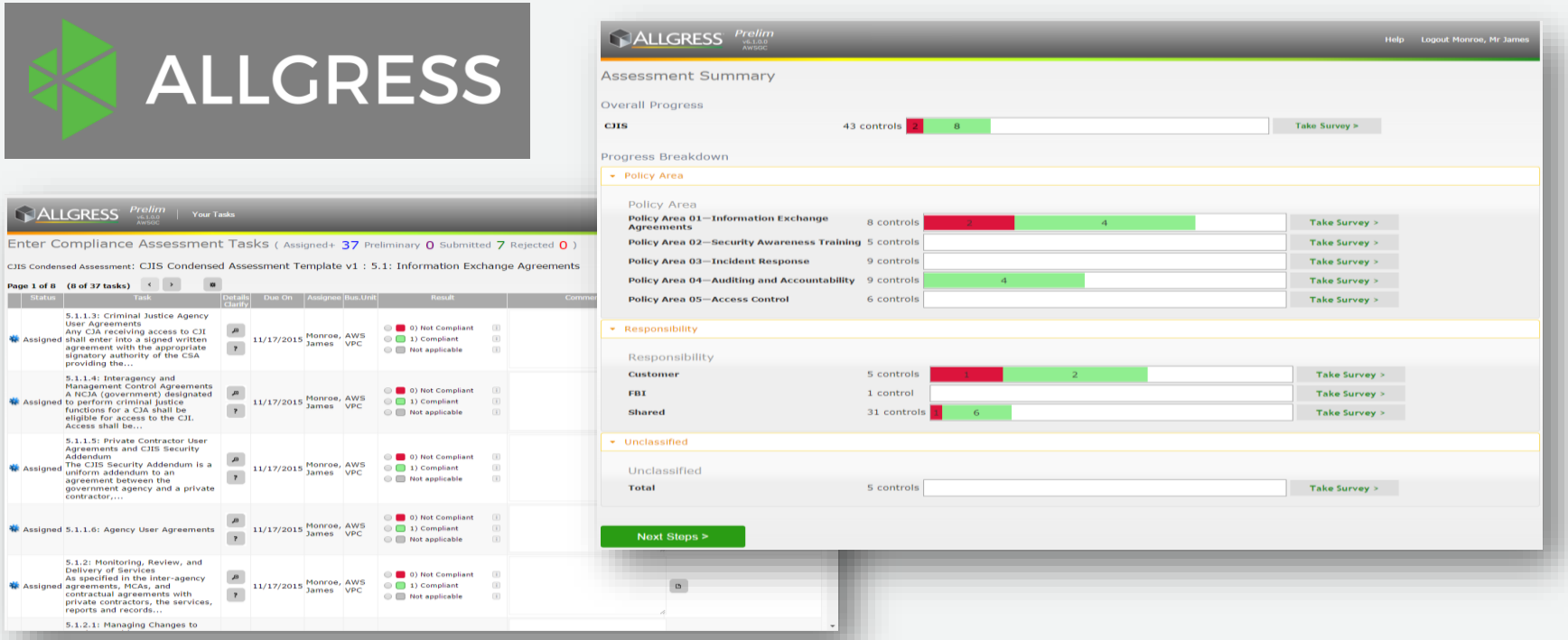

NACL

Three-tier Web Architecture

Define Data Protections and Controls

CIS AWS Foudation Benchmark Mapping									
AWS CIS Benchmark Name	Benchmark Specification	Mapping and Alignment to common Security Frameworks							
		AICPA Trust Service Criteria	BSI Germany	Canada PIPEDA	95/46/EC - European Union Data Protection Directive	FedRAMP Security Controls –MODERATE IMPACT LEVEL–	HIPAA/HITECH (Omnibus Rule)	ISO/IEC 27001:2013	PCI DSS v3.1
Define secure IAM policies	When you give permissions to a group, all users in that group get those permissions. For example, you can give the Admins group permission to perform any of the IAM actions on any of the AWS account resources. Another example: You can give the Managers group permission to describe the AWS account's Amazon EC2 instances. Permissions can be assigned in two ways: as user-based permissions or as resource-based permissions. • User-based permissions are attached to an IAM user, group, or role and let you specify what that user, group, or role can do. • Resource-based permissions are attached to a resource. You can specify resource-based permissions for Amazon S3 buckets, Amazon Glacier vaults, Amazon SNS topics, Amazon SQS queues, and AWS Key Management Service encryption keys. Resource-based permissions let you specify who has access to the resource and what actions they can perform on it. Resource-based policies are inline only, not managed.	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	35 (B) 40 (B) 41 (B) 42 (B) 44 (C+)	Schedule 1 (Section 5) Safeguards, Subs. 4.7.2 and 4.7.3	Article 17	NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-3 (3) NIST SP 800-53 R4 AC-5 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AC-6 (1) NIST SP 800-53 R4 AC-6 (2) NIST SP 800-53 R4 IA-2 NIST SP 800-53 R4 IA-2 (1) NIST SP 800-53 R4 IA-4 NIST SP 800-53 R4 IA-5 NIST SP 800-53 R4 IA-5 (1) NIST SP 800-53 R4 IA-5 (2) NIST SP 800-53 R4 IA-5 (3) NIST SP 800-53 R4 IA-5 (6) NIST SP 800-53 R4 IA-5 (7)	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	A.9.2.1, A.9.2.2 A.9.2.3 A.9.1.2 A.9.4.1	7.1 7.1.1 7.1.2 7.1.3 7.1.4 12.5.4
Attaching a Policies to an IAM Groups	User-based policies can be either inline or managed. Resource-based policies are attached to the resources (inline) only and are not managed. An AWS managed policy is a standalone policy that is created and administered by AWS. Standalone policy means that the policy has its own Amazon Resource Name (ARN) that includes the policy name. Example policies: AdministratorAccess, PowerUserAccess, and AWSCloudTrailReadOnlyAccess. Additionally, customers can create standalone policies for administering in their AWS account, which are referred to as a customer managed policies. Customers can attach the policies to multiple principal entities in your AWS account. When you attach a policy to a principal entity, you give the entity the permissions that are defined in the policy.	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for	41 (B)	Schedule 1 (Section 5), 4.7 - Safeguards	Article 17	NIST SP 800-53 R4 AC-2 NIST SP 800-53 R4 AC-2 (1) NIST SP 800-53 R4 AC-2 (2) NIST SP 800-53 R4 AC-2 (3) NIST SP 800-53 R4 AC-2 (4) NIST SP 800-53 R4 AC-2 (7) NIST SP 800-53 R4 AU-6 NIST SP 800-53 R4 AU-6 (1) NIST SP 800-53 R4 AU-6 (3) NIST SP 800-53 R4 PS-6 NIST SP 800-53 R4 PS-7	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	A.9.2.5	8.1.4
Create secure IAM accounts and enable IAM user access keys	Create access keys for programmatic access to AWS, create an IAM user and grant that user only the permissions he or she needs. Then generate an access key for that user. Users need their own access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct HTTP calls using the APIs for individual AWS services. To fill this need, you can create, modify, view, or rotate access keys (access key IDs and secret access keys) for IAM users.	(S3.2.b) b. Identification and authentication of users.	6 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	Article 17 (1), (2)	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-2 NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-11 NIST SP 800-53 R4 AC-11 (1) NIST SP 800-53 R4 AU-2 NIST SP 800-53 R4 AU-2 (3) NIST SP 800-53 R4 AU-2 (4) NIST SP 800-53 R4 AU-11 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IA-2 NIST SP 800-53 R4 IA-2 (1)	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.4 A.9.2.5 A.9.4.2	8.0 10.1, 12.3

Document Security Architecture



https://allgress.com/get-compliant

Security Considerations

Multiple AWS accounts

VPC, private subnets for application servers and RDS

Minimal network perimeter (Only SSL Terminating Reverse Proxy in DMZ)

Tightened Security Groups - fine grained rules for ports and CIDRs

Immutable Docker containers, CloudTrail, Central Log aggregation

Enable AWS Config, Config Rules, Aggregation, GuardDuty, and Security Hub

Security Considerations (Continued)

CIS-benchmarked AMIs

Hardened Linux/Software

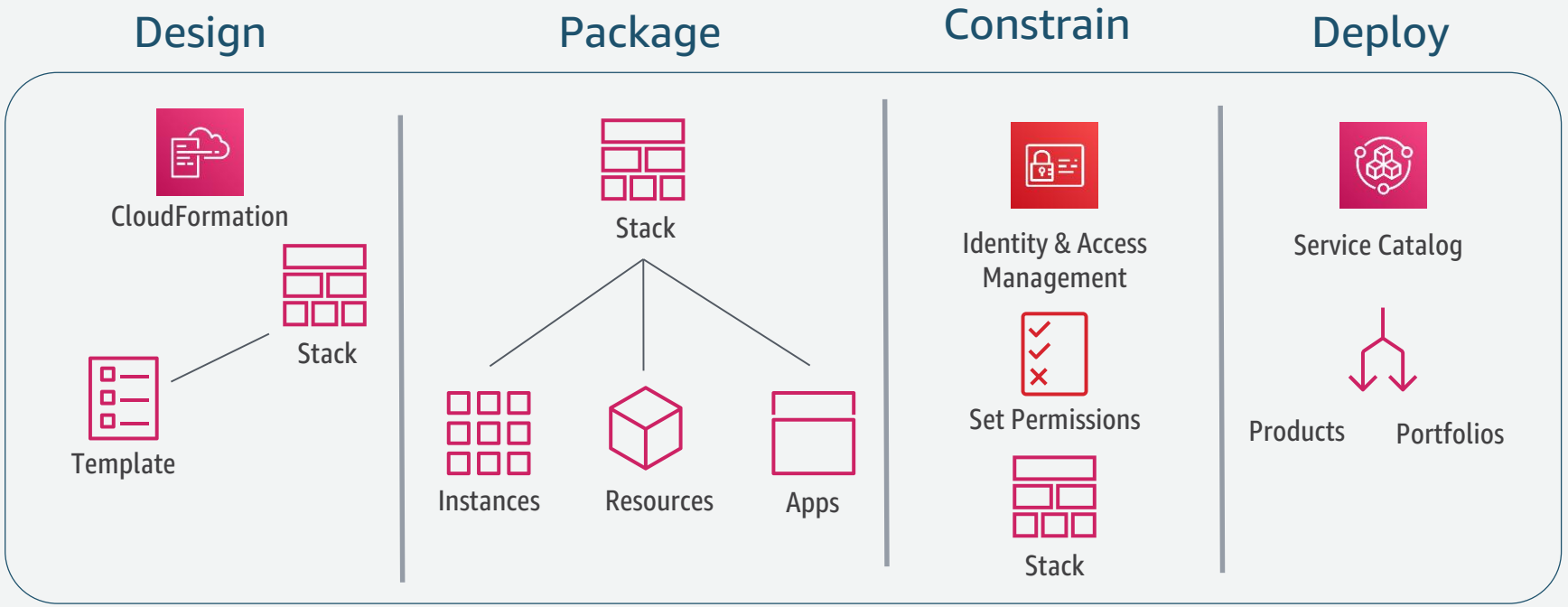
KMS-based secret management

Two-factor authentication on AMIs

Advanced user and key management using LDAP. Elimination of ec2-user

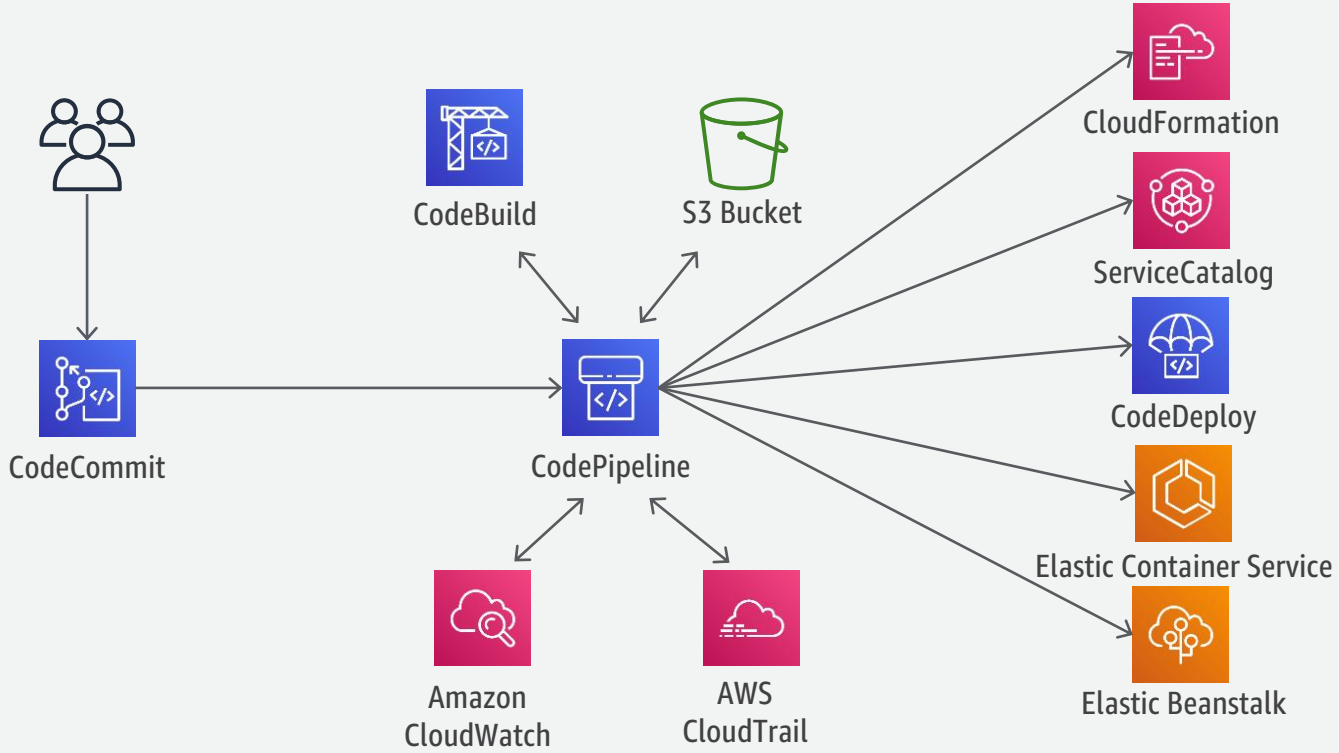
HSM for secure data/keys

SbD – Automated Deployments



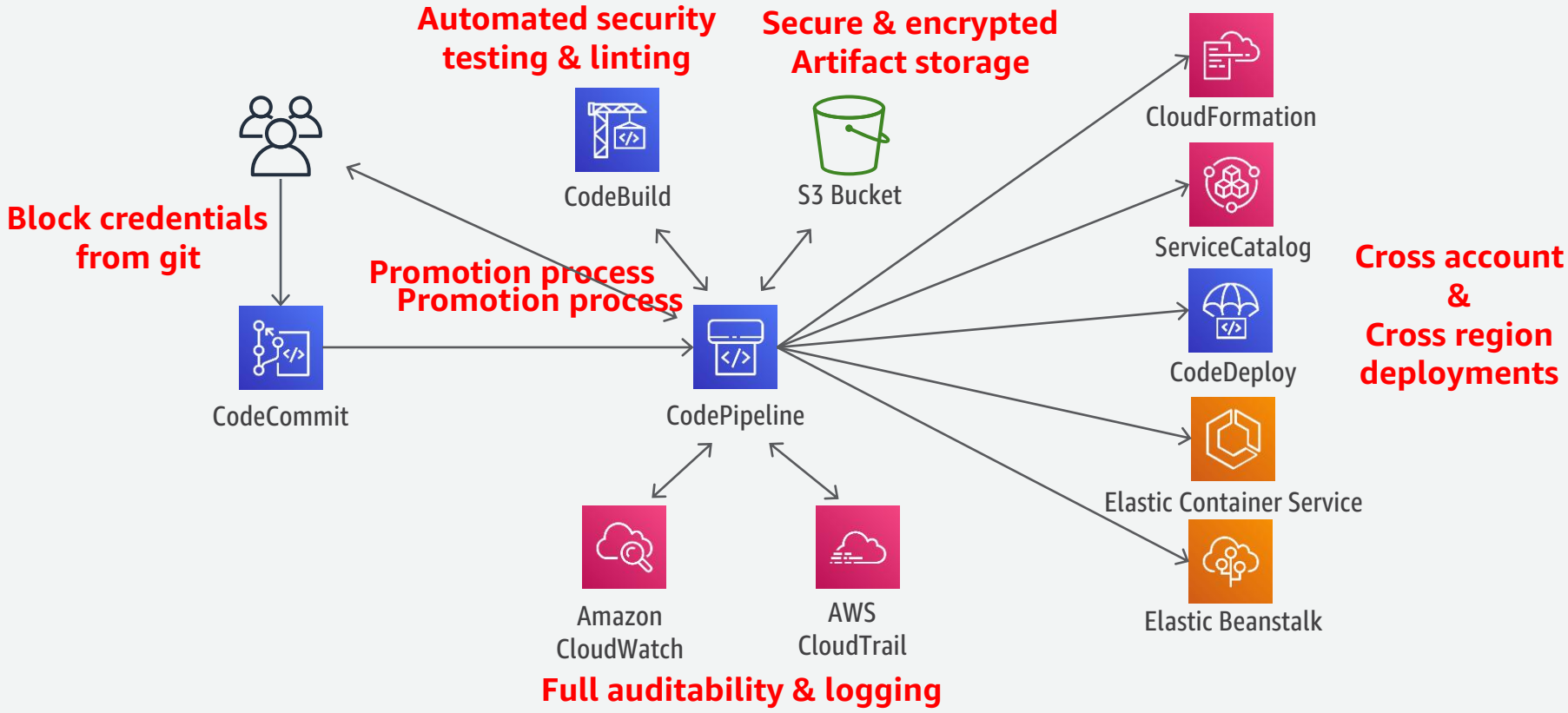
Automate deployments, provisioning, and configurations of the AWS customer environments

SbD – Continuous Deployment



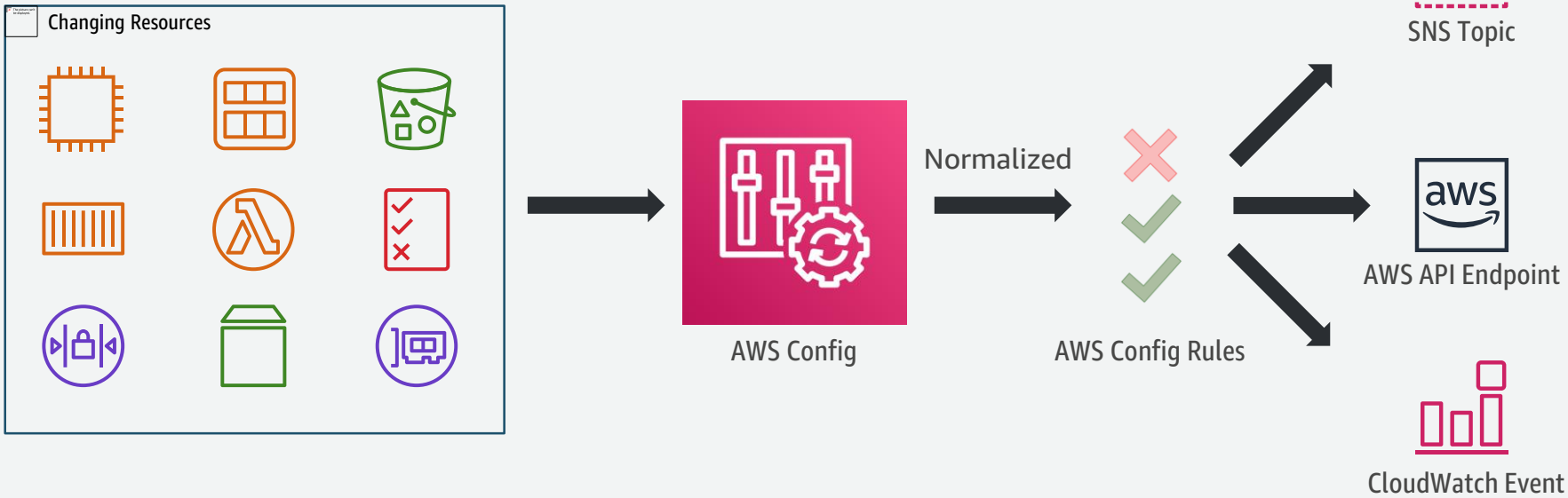
aws professional services

SbD – Continuous Deployment



Continuous Compliance

AWS Config is a continuous recording and continuous assessment service, that tracks configuration changes to AWS resources and alerts you if the configuration is non-compliant with your baseline policies.



SbD - Eco-System

Security by Design

AWS Config Rules

AWS CloudFormation

Amazon Inspector

ALLGRESS

VERIS GROUP

splunk>

ALERT LOGIC

CloudCheckr

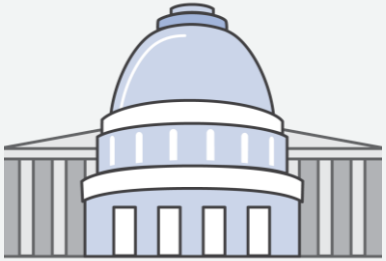
CIS Center for Internet Security

Flux7

Symantec

evident.io

SbD - Modernizing Technology Governance (MTG)



Automate Governance

Automate Deployments

Automate Security Operations

Continuous Compliance

aws professional services

AWS Resources

Amazon Web Services Cloud Compliance

- **https://aws.amazon.com/compliance/**

SbD website and whitepaper – to wrap your head around this

- **https://aws.amazon.com/compliance/security-by-design/**

Questions?

aws professional services