AWS ENTERPRISE SUMMIT

Compliance in the Cloud Using Security by Design

Modernization of Technology Governance *IN* the Cloud

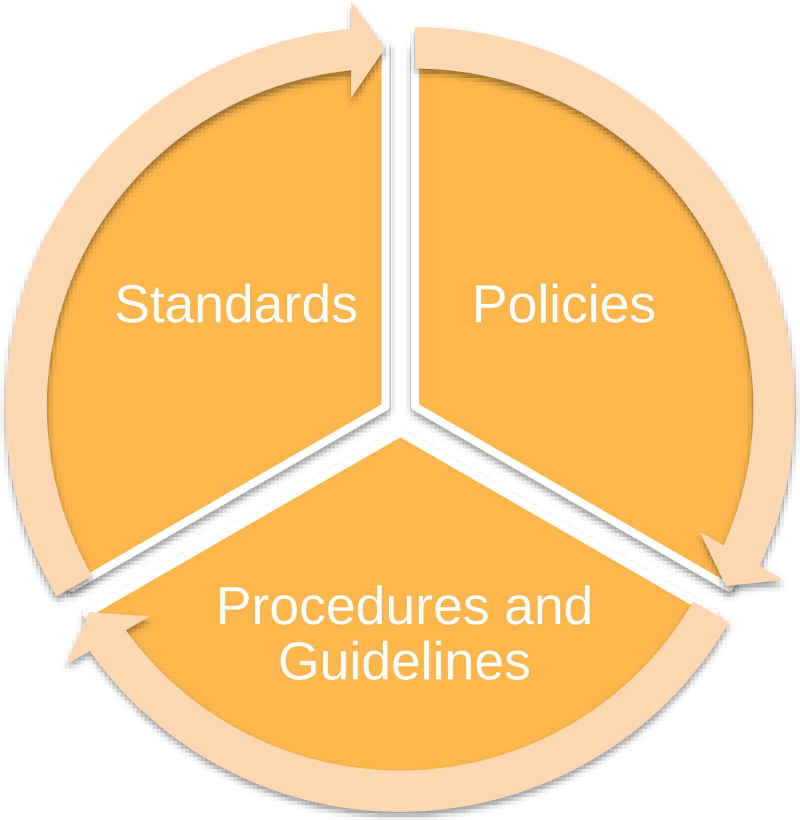
Felix Candelario, Global Solutions Architect

amazon web services

Problem Statement

Increasing complexity (mobility, system connectivity) causes increasing difficulty in managing risk and security and demonstrating compliance.

Current State – Technology Governance



Standards

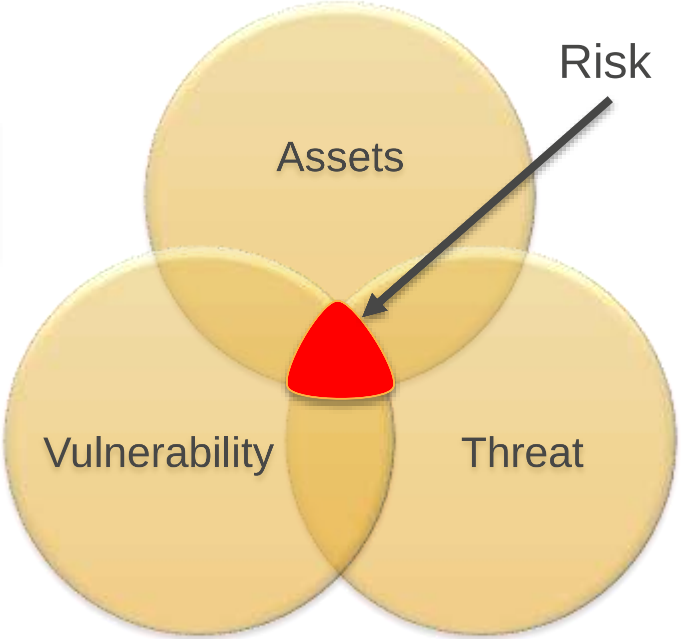
Policies

Procedures and Guidelines

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

How many AWS accounts

Single VPC or Multiple VPCs

IAM groups or roles

Public or private subnets

Security groups or NACLs

Can we use S3 for this

What type of encryption

Who will manage the keys

Which AWS database

What is the regulatory requirement?

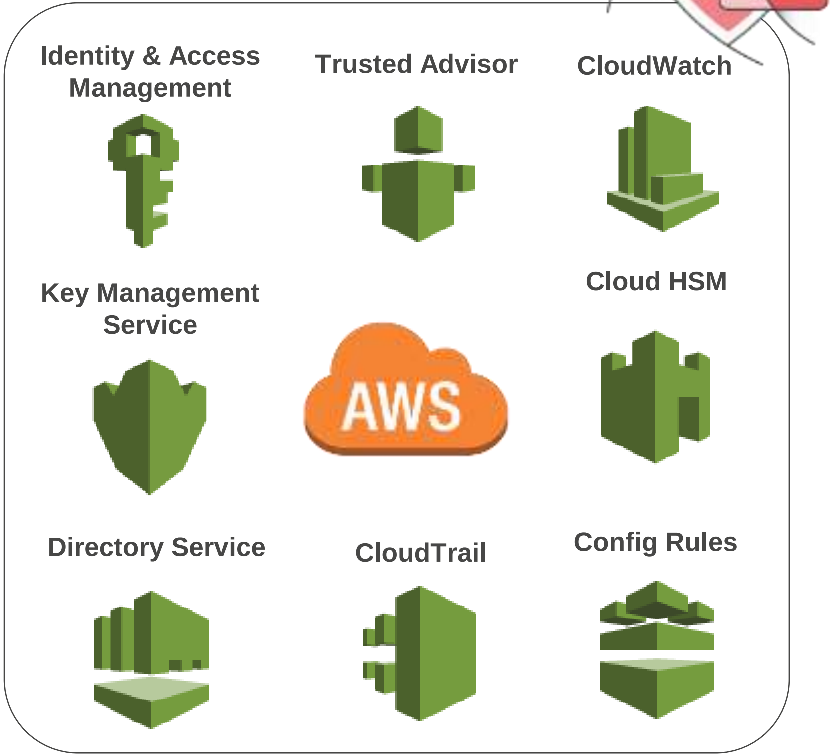
What's in-scope or out-of-scope?

How to verify the standards are met?

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.



Identity & Access Management

Trusted Advisor

CloudWatch

Key Management Service

Cloud HSM

Directory Service

CloudTrail

Config Rules

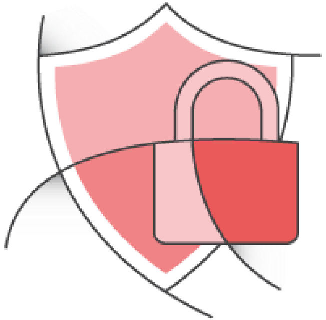
Security by Design - *Design Principles*

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

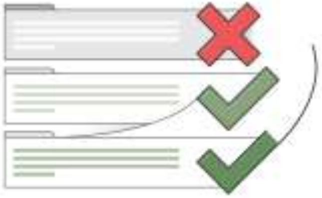
- Build security in every layer
- Design for failures
- Implement auto-healing
- Think parallel
- Plan for Breach

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

SbD - Eco-system

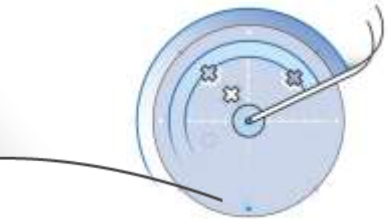


Security by Design (SbD)



AWS Config Rules

AWS CloudFormation



Amazon Inspector

splunk>

ALLGRESS

VERIS GROUP

TREND MICRO | Securing Your Journey to the Cloud

ALERT LOGIC

CloudCheckr

Flux7

the CENTER for INTERNET SECURITY

Symantec.

evident.io

SbD - Modernize Tech Governance (MTG)

Why?

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

You need automation AWS offers to manage security

Goal - Modernize Tech Governance (MTG)

Adopting “***Prevent***” controls, making “***Detect***” controls more powerful and comprehensive

SbD - Modernizing Technology Governance (MTG)

1. Decide what to do (Strategy)
   - 1.1 Identify Stakeholders
   - 1.2 Identify Your Workloads Moving to AWS

2. Analyze and Document (outside of AWS)
   - 2.1 Rationalize Security Requirements
   - 2.2 Define Data Protections and Controls
   - 2.3 Document Security Architecture

3. Automate, Deploy & Monitor
   - 3.1 Build/deploy Security Architecture
   - 3.2 Automate Security Operations
   - 3.3 Continuous Monitor
   - 3.4 Testing and Game Days

4. Certify
   - 4.1 Audit and Certification

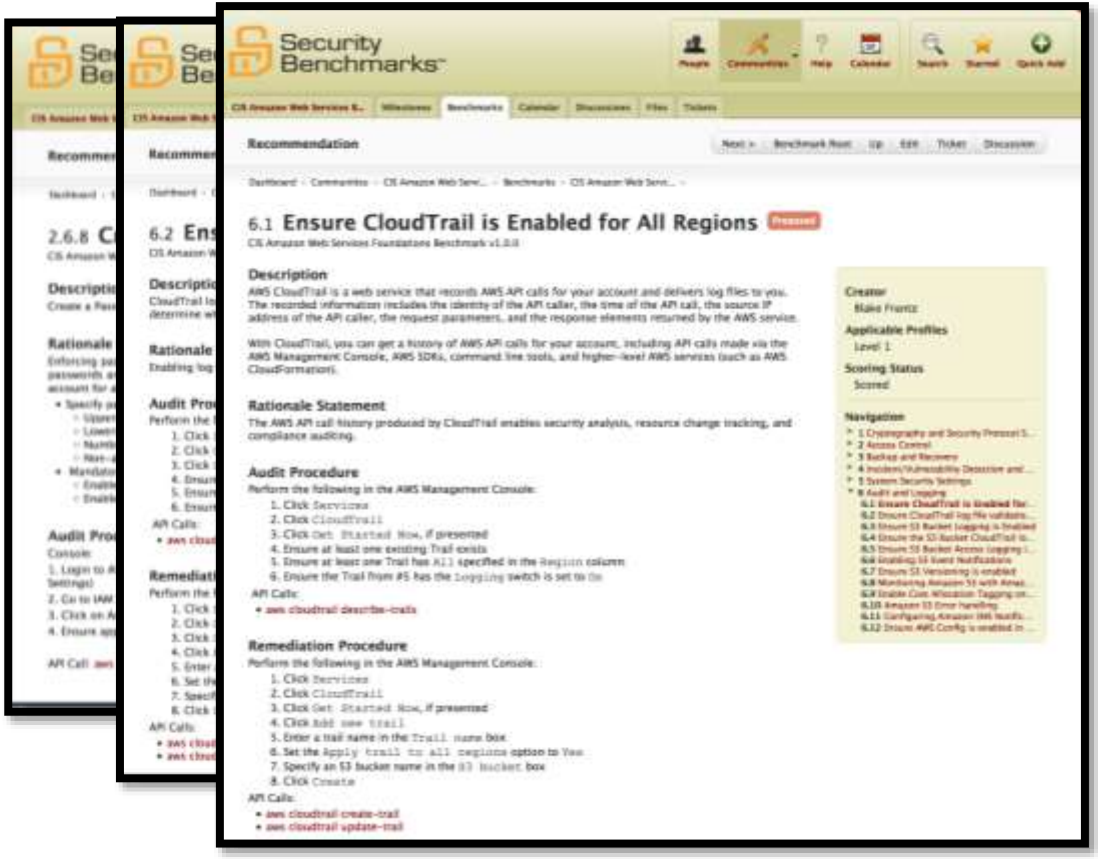
SbD – Rationalize Security Requirements

AWS has partnered with CIS Benchmarks to create consensus-based, best-practice security configuration guides which 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.

https://www.cisecurity.org/



Recommendation

6.1 Ensure CloudTrail is Enabled for All Regions

CIS Amazon Web Services Foundations Benchmark v1.0.0

Description

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

With CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation).

Rationale Statement

The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

Audit Procedure

Perform the following in the AWS Management Console:

1. Click `Services`
2. Click `CloudTrail`
3. Click `Get Started Now`, if presented
4. Ensure at least one existing Trail exists
5. Ensure at least one Trail has `All` specified in the `Region` column
6. Ensure the Trail from #5 has the `Logging` switch is set to `On`

API Calls:

- aws cloudtrail describe-trails

Remediation Procedure

Perform the following in the AWS Management Console:

1. Click `Services`
2. Click `CloudTrail`
3. Click `Get Started Now`, if presented
4. Click `Add new trail`
5. Enter a trail name in the `Trail name` box
6. Set the `Apply trail to all regions` option to `Yes`
7. Specify an S3 bucket name in the `S3 bucket` box
8. Click `Create`

API Calls:

- aws cloudtrail create-trail
- aws cloudtrail update-trail

Creator
Blake Frantz

Applicable Profiles
Level 1

Scoring Status
Scored

Navigation

- 1 Cryptography and Security Protocol S...
- 2 Access Control
- 3 Backup and Recovery
- 4 Incident/Vulnerability Detection and...
- 5 System Security Settings
- 6 Audit and Logging
  - 6.1 Ensure CloudTrail is Enabled for...
  - 6.2 Ensure CloudTrail log file validatio...
  - 6.3 Ensure S3 Bucket Logging is Enabled
  - 6.4 Ensure the S3 Bucket CloudTrail is...
  - 6.5 Ensure S3 Bucket Access Logging i...
  - 6.6 Enabling S3 Event Notifications
  - 6.7 Ensure S3 Versioning is enabled
  - 6.8 Monitoring Amazon S3 with Amaz...
  - 6.9 Enable Cost Allocation Tagging on...
  - 6.10 Amazon S3 Error handling
  - 6.11 Configuring Amazon IAM Notifi...
  - 6.12 Ensure AWS Config is enabled in ...

SbD – AWS CIS Benchmark Scope

Identity & Access Management

CloudTrail

CloudWatch

Cloud HSM

S3

Glacier

Key Management Service

SNS

Config & Config Rules

Foundational Benchmark

EC2

VPC

Elastic Load Balancing

Direct Connect

VPN Gateway

Route 53

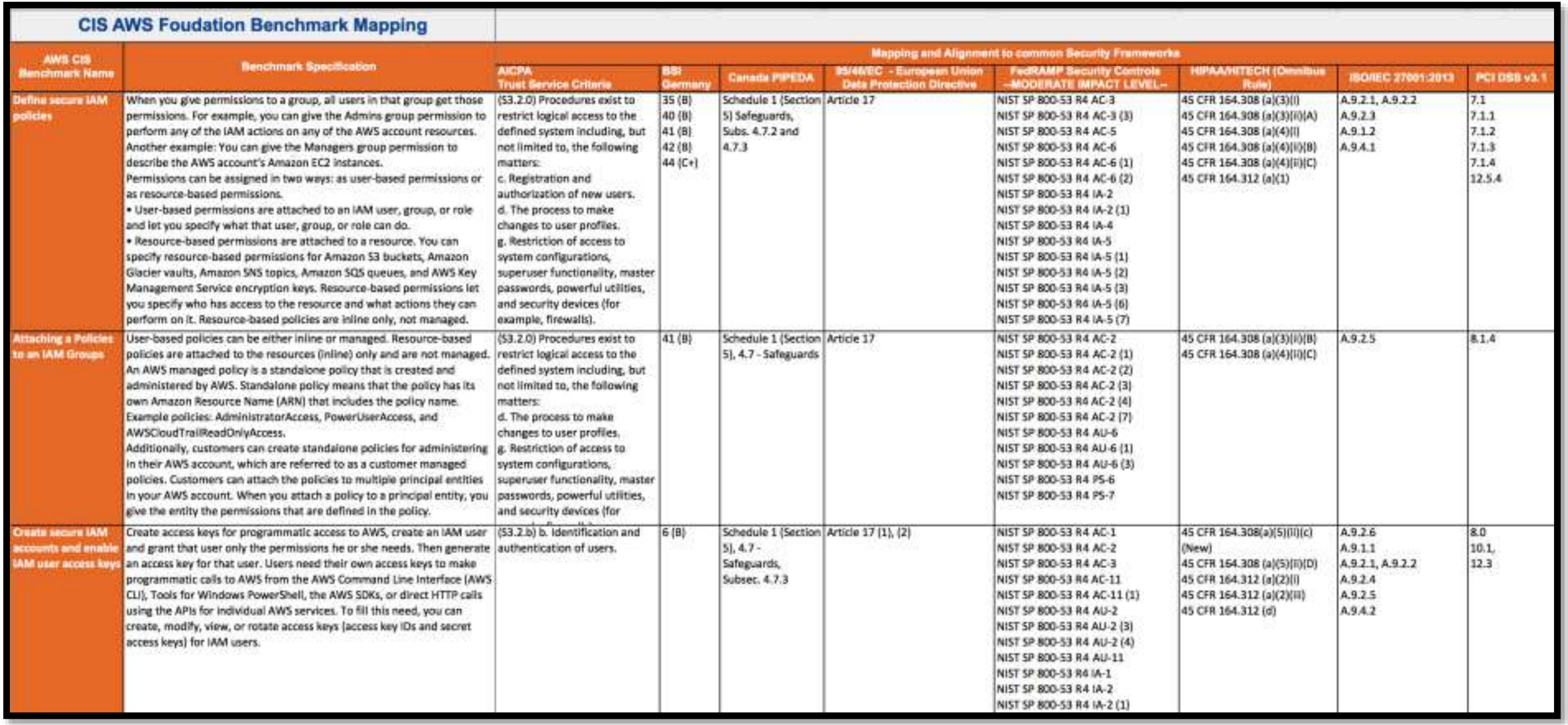
Amazon Elastic Block Store

CloudFront

Three-tier Web Architecture

the CENTER for INTERNET SECURITY

Define Data Protections and Controls

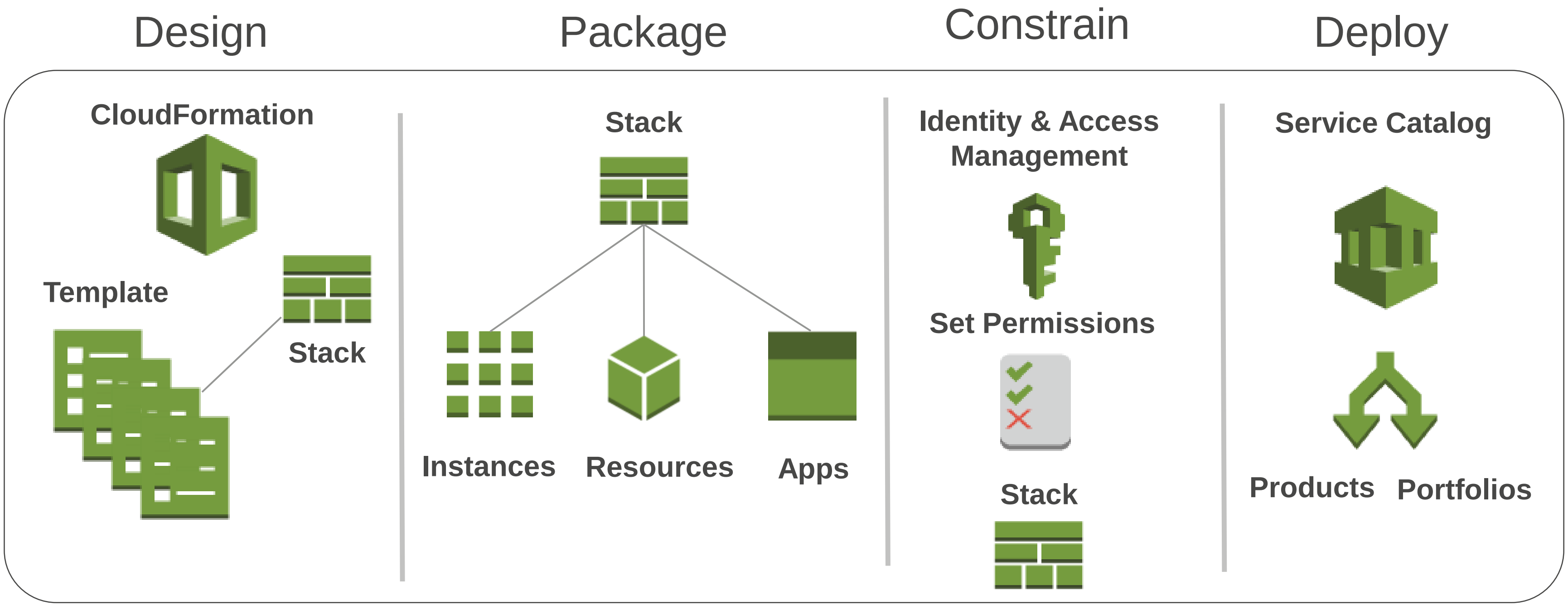


CIS AWS Foudation Benchmark Mapping

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

SbD – Automate Security Operations

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



SbD - Modernizing Technology Governance (MTG)

Automate Governance

Automate Deployments

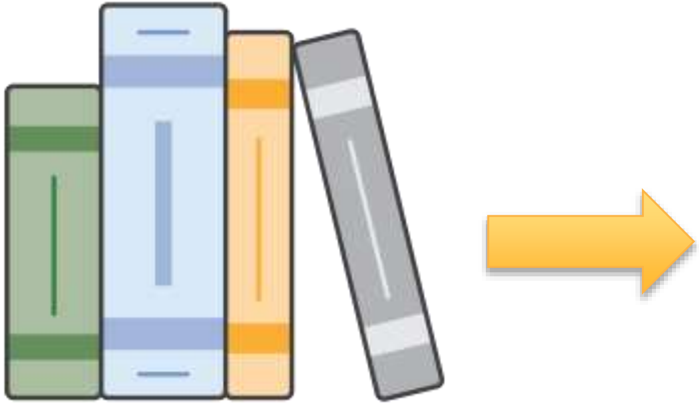
Automate Security Operations

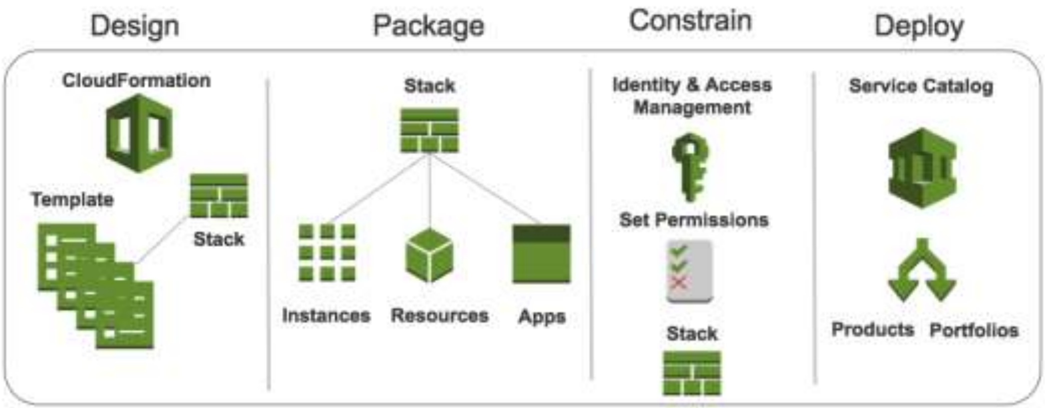
Continuous Compliance

Closing the loop -

SbD - Modernizing Technology Governance

Result: Reliable technical implementation and enforcement of operational and administrative controls





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/

AWS

ENTERPRISE

SUMMIT

amazon
web services