VITA Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Dec. 4, 2019

ISOAG Agenda - December 2019

- Welcome and Opening Remarks - Mike Watson
- AWS Security Automation - Ted Steffan, AWS and Orchestration
- SAIC Updates - Jane Williamson, SAIC
- Security Challenge Game - Marlon Cole, VITA

Modernizing Technology Governance

Security and Compliance

Security Recognized as Stronger than On-premises

Security in the cloud is recognized as better than on-premises. Broad security certification and accreditation, data encryption at rest and in-transit, hardware security modules and strong physical security all contribute to a more secure way to manage your business' IT infrastructure.

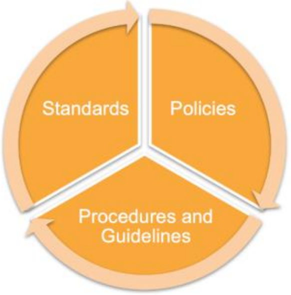
Deep Visibility into Compliance and Governance

Controlling, auditing and managing identity, configuration and usage is a crucial part of today's IT infrastructure landscape. With the AWS Cloud, these capabilities come built into the platform helping you meet your compliance, governance and regulatory requirements.

Tradition verses Cloud (Modernized) – Governance

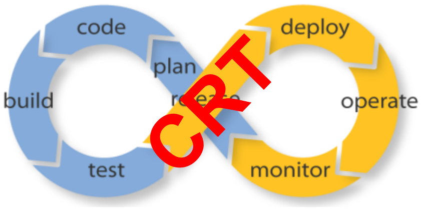
Tradition – Governance

- Information and technology (IT) governance is a subset discipline of corporate governance, focused on information and technology (IT) and its performance and risk management.
- The interest in IT governance is due to the on-going need within organizations to focus value creation efforts on an organization's strategic objectives and to better manage the performance of those responsible for creating this value in the best interest of all stakeholders.



Cloud – Governance

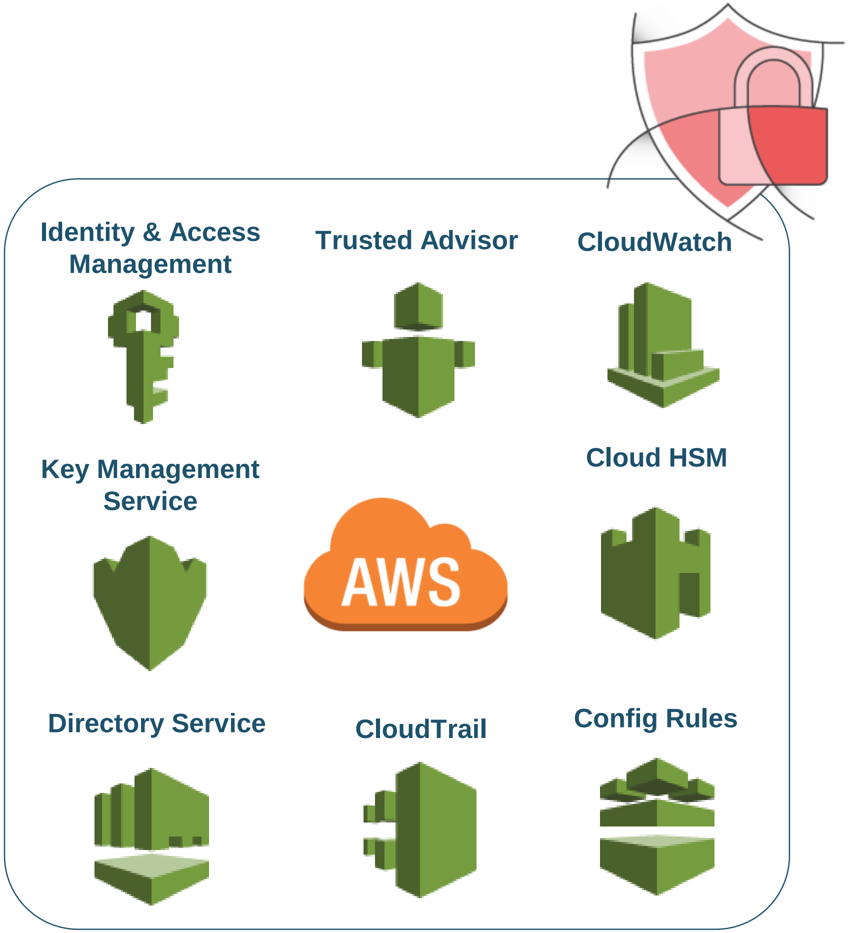
- Technology drives your governance alignment
- Governance is a "Shared Responsibility"
- Automation is the ***Key*** to successful governance
- Pre-Cloud decision making process are paramount (e.g. service selection, policies, frameworks architecture, data protections, etc.).
- Focus is on Continuous Risk Treatments (CRT)



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.



Security by Design - *Design Principles*

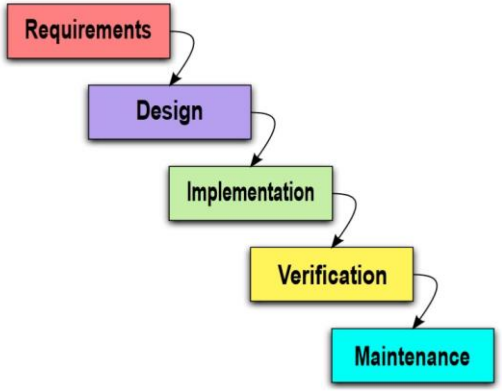
Developing new risk mitigation capabilities, which go beyond global security frameworks, by treating risks, eliminating manual processes, optimizing evidence and audit ratifications processes through rigid automation

- 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

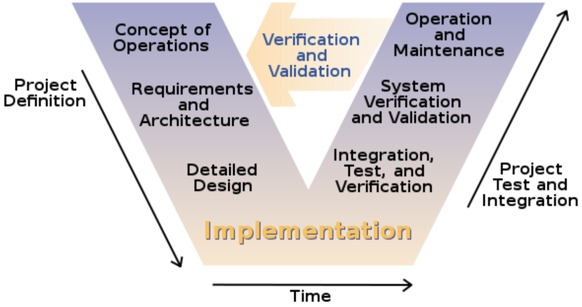
So why Security by Design…

Waterfall



- Designed for fixed requirements
- Must finish the whole before any part is usable
- Linear steps w verification gate
- Manual processes
- Infrequent system changes

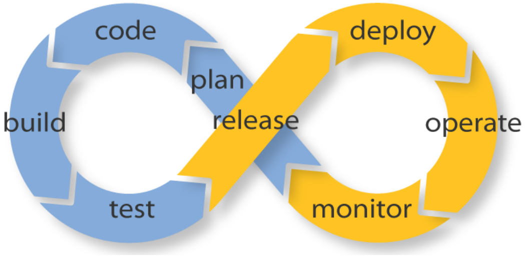
V-model



Concept of Operations
Verification and Validation
Operation and Maintenance
Project Definition
Requirements and Architecture
System Verification and Validation
Detailed Design
Integration, Test, and Verification
Project Test and Integration
Implementation
Time

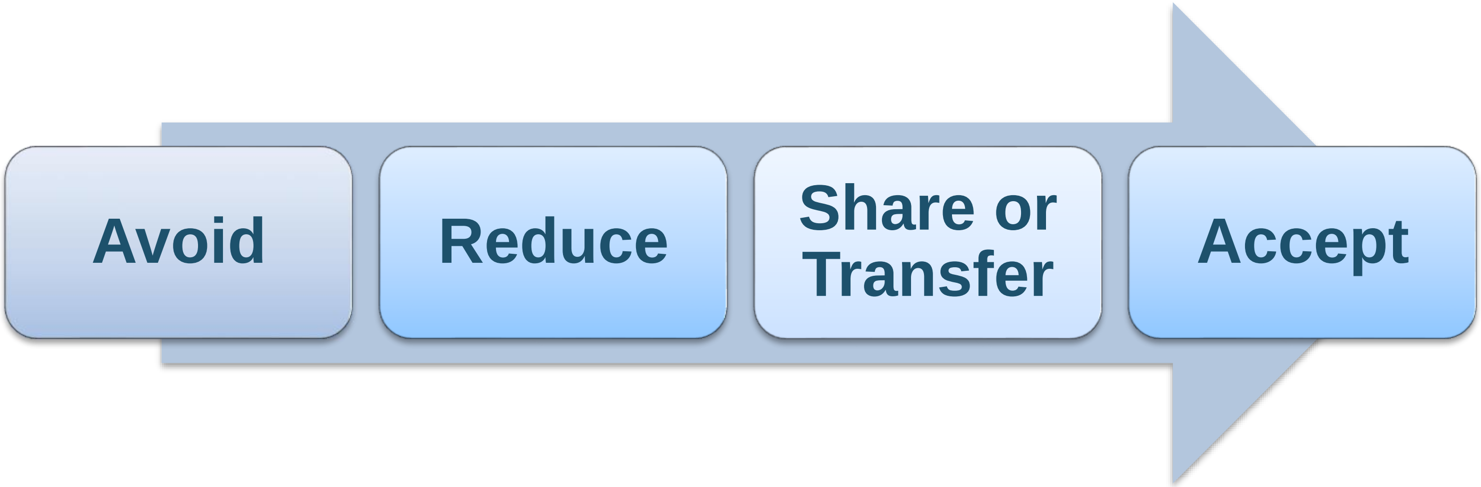
- Designed for fixed requirements
- Must finish the whole before any part is usable
- Waterfall + earlier test planning
- Manual processes + tools
- Periodic system changes

DevOps

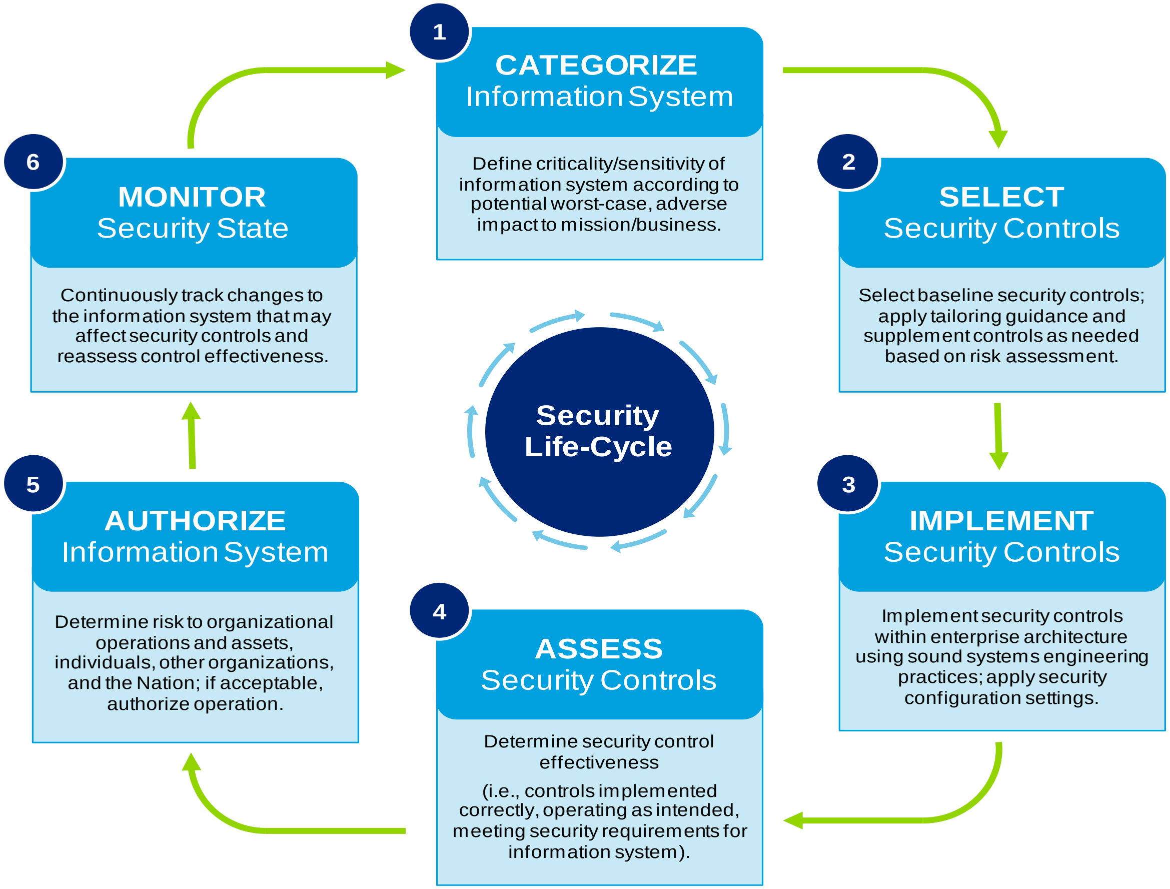


- Designed for changing requirements
- Deliver smaller parts with immediate functionality
- Iterative steps w testing in each
- Continuous deployment

Traditional Risk Treatments



Traditional Risk Management



1
CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

2
SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

3
IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

4
ASSESS
Security Controls

Determine security control effectiveness

(i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

5
AUTHORIZE
Information System

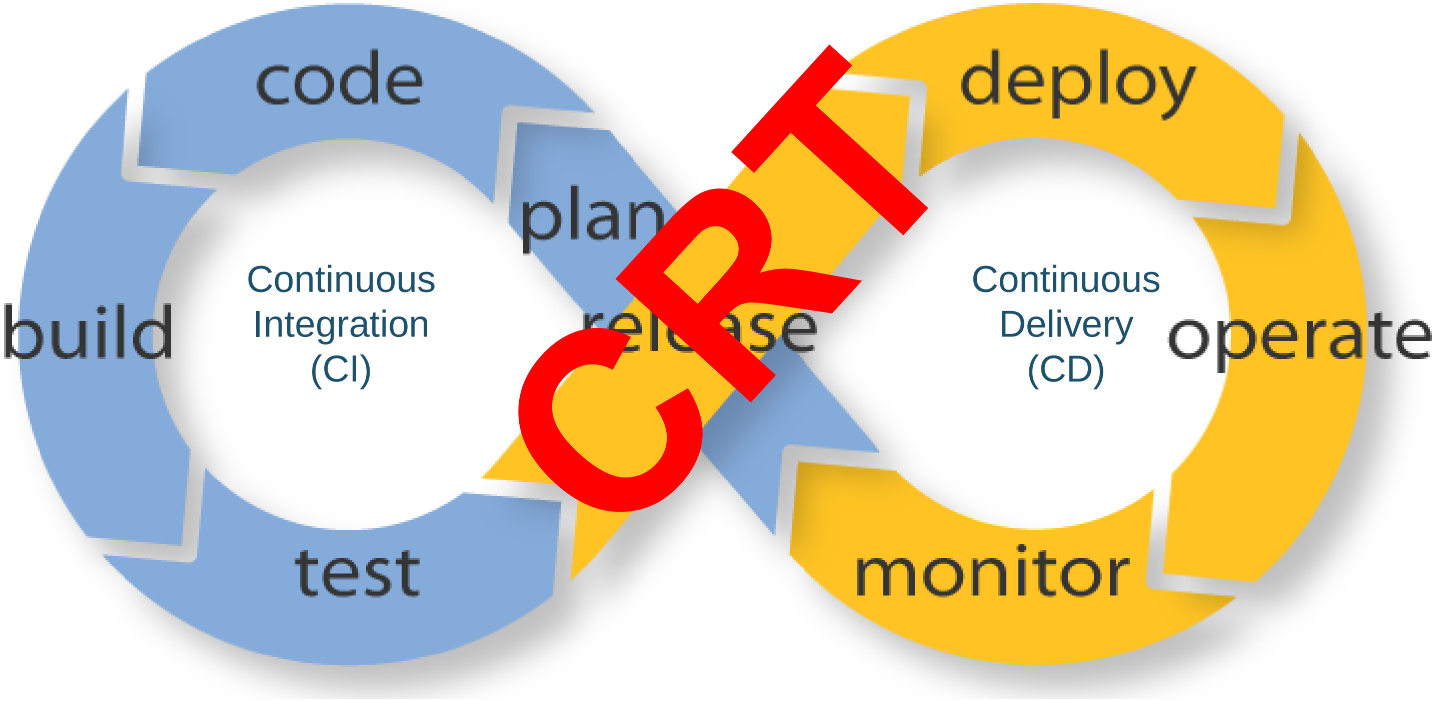
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

6
MONITOR
Security State

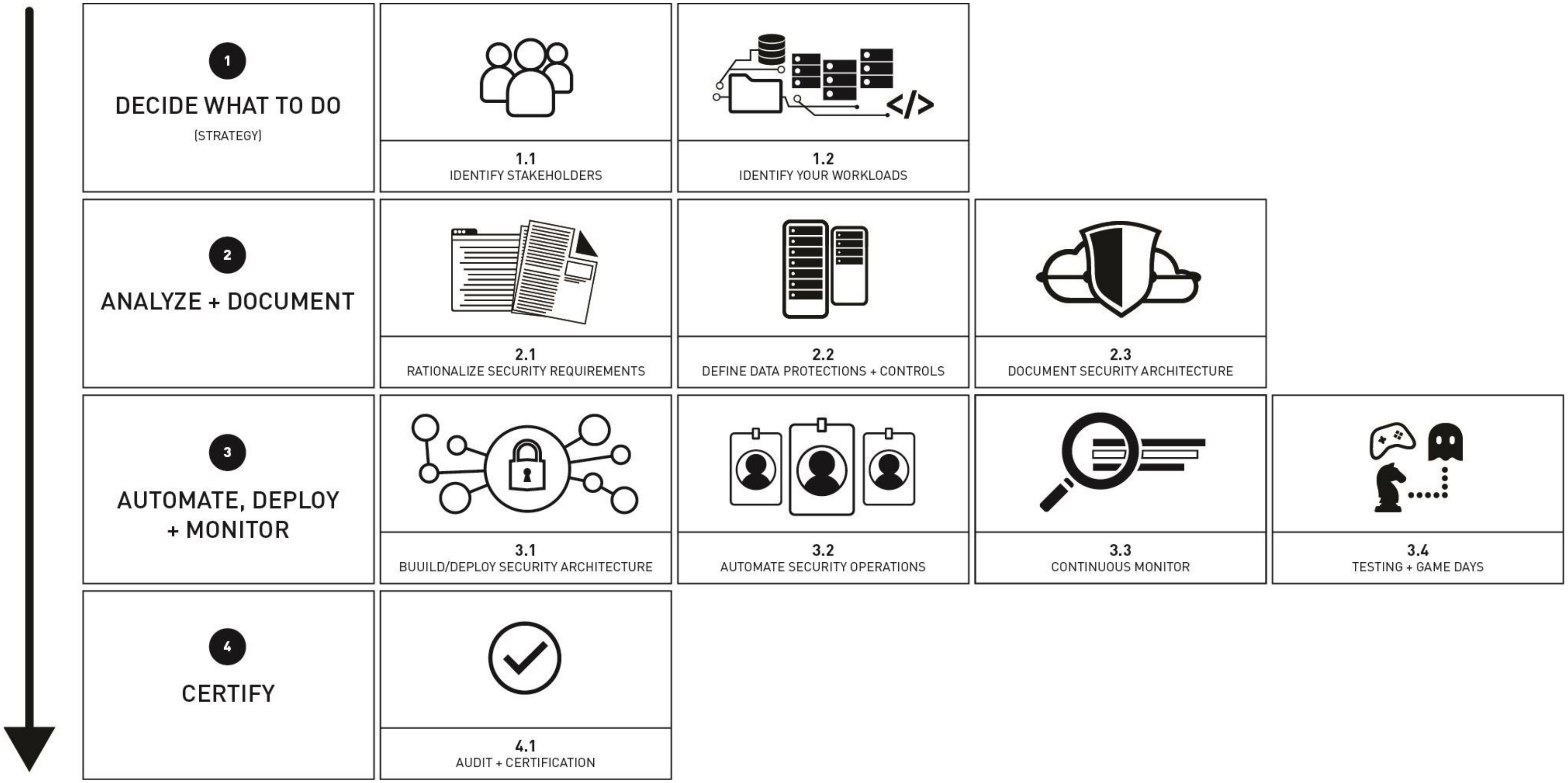
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life-Cycle

DevOps and Continuous Risk Treatment (CRT)



Modernizing Technology Governance (MTG)



1 DECIDE WHAT TO DO (STRATEGY)	1.1 IDENTIFY STAKEHOLDERS	1.2 IDENTIFY YOUR WORKLOADS		
2 ANALYZE + DOCUMENT	2.1 RATIONALIZE SECURITY REQUIREMENTS	2.2 DEFINE DATA PROTECTIONS + CONTROLS	2.3 DOCUMENT SECURITY ARCHITECTURE	
3 AUTOMATE, DEPLOY + MONITOR	3.1 BUUILD/DEPLOY SECURITY ARCHITECTURE	3.2 AUTOMATE SECURITY OPERATIONS	3.3 CONTINUOUS MONITOR	3.4 TESTING + GAME DAYS
4 CERTIFY	4.1 AUDIT + CERTIFICATION			

Step 1 - Decide what to do (Strategy)

1

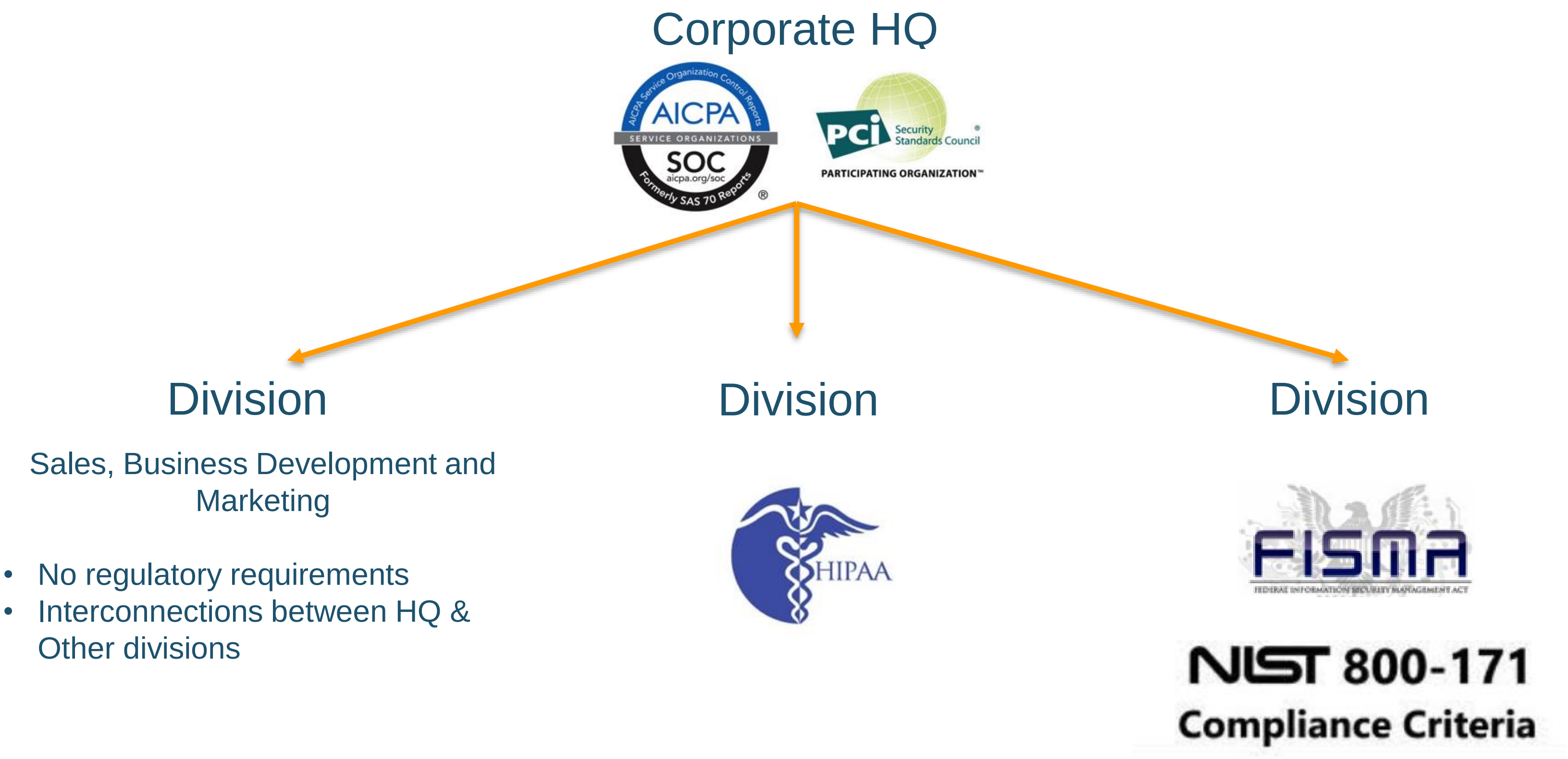
DECIDE WHAT TO DO

(STRATEGY)

1.1
IDENTIFY STAKEHOLDERS

1.2
IDENTIFY YOUR WORKLOADS

1.1 Identify Business Units



Corporate HQ

AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
AICPA Service Organization Control Reports
Formerly SAS 70 Reports
PCI Security Standards Council
PARTICIPATING ORGANIZATION

Division

Sales, Business Development and Marketing

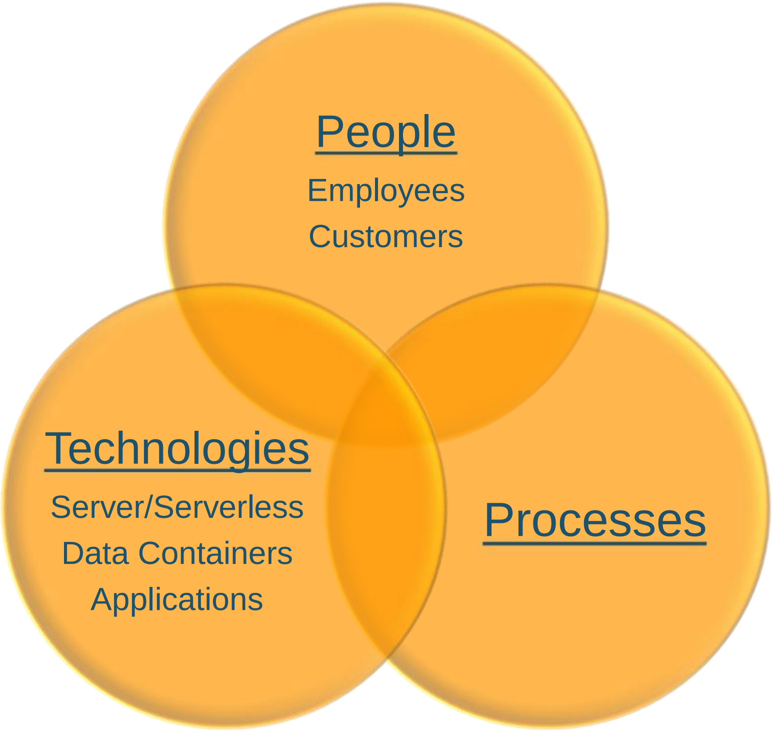
- No regulatory requirements
- Interconnections between HQ & Other divisions

Division

Division

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
NIST 800-171
Compliance Criteria

1.2 Identify your workloads



People

Employees

Customers

Technologies

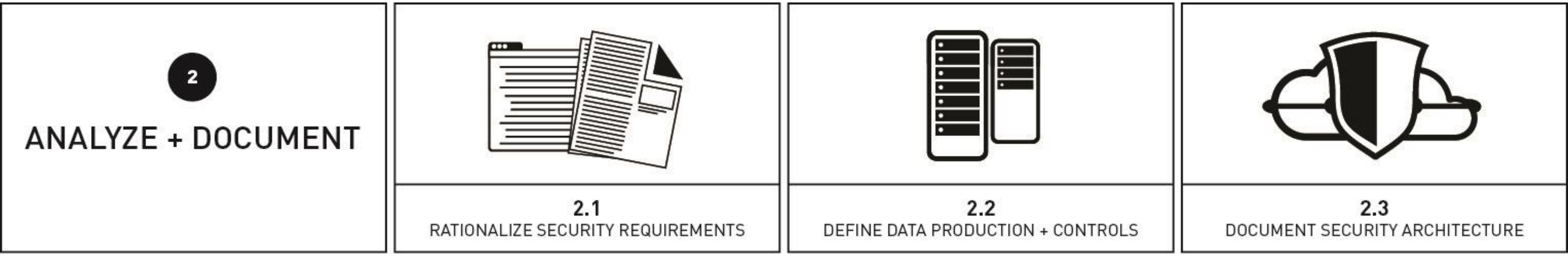
Server/Serverless

Data Containers

Applications

Processes

Phase 2 - Analyze, Define and Document



2

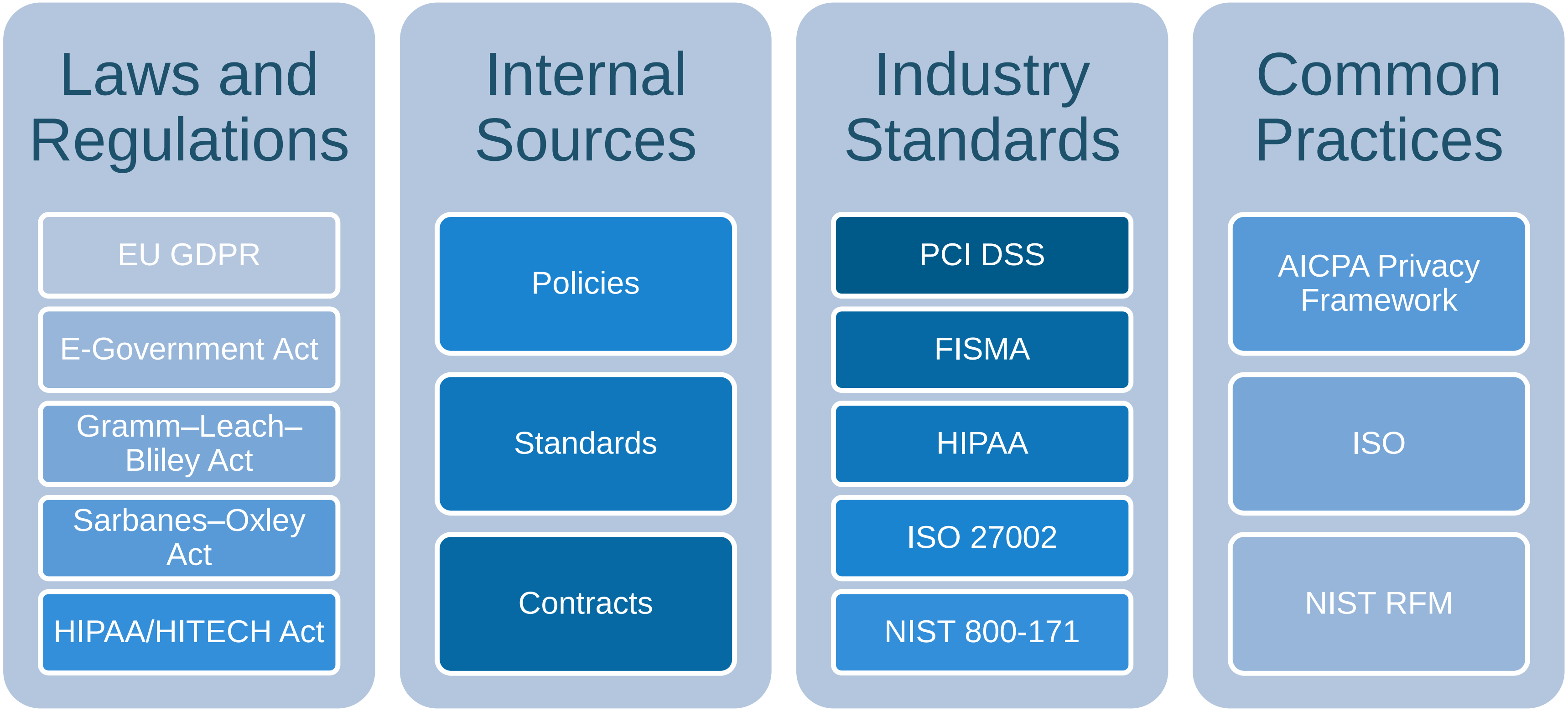
ANALYZE + DOCUMENT

2.1
RATIONALIZE SECURITY REQUIREMENTS

2.2
DEFINE DATA PRODUCTION + CONTROLS

2.3
DOCUMENT SECURITY ARCHITECTURE

Rationalizing the Security Requirements



Laws and Regulations

- EU GDPR
- E-Government Act
- Gramm–Leach–Bliley Act
- Sarbanes–Oxley Act
- HIPAA/HITECH Act

Internal Sources

- Policies
- Standards
- Contracts

Industry Standards

- PCI DSS
- FISMA
- HIPAA
- ISO 27002
- NIST 800-171

Common Practices

- AICPA Privacy Framework
- ISO
- NIST RFM

Shared Responsibility Control Types

Control Type	Description
Inherited Controls	Controls which a customer fully inherits from AWS (e.g. Data Center Controls).
Hybrid Controls	Controls for which AWS provides partial implementation of the control requirement, but require the customer to also take responsibility to fully implement the control requirement. (e.g. Access Controls and Resiliency).
Shared controls	Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure, and the customer must provide their own control implementation within their use of AWS services.
Customer Specific	Controls which are solely the responsibility of the customer, based on the application they are deploying within AWS services.

Inherited Security and Compliance

Control #	Control Name	Control #	Control Name	Control #	Control Name
A.11.1.1	Physical security perimeter	A.11.2.1	Equipment siting and protection	A.11.2.7	Equipment siting and protection
A.11.1.2	Physical entry controls	A.11.2.2	Supporting utilities	A.11.2.8	Supporting utilities
A.11.1.3	Securing offices, rooms and facilities	A.11.2.3	Cabling security	A.11.2.9	Cabling security
A.11.1.4	Protecting against external and environmental threats	A.11.2.4	Equipment maintenance	A.11.2.7	Equipment maintenance
A.11.1.5	Working in secure areas	A.11.2.5	Removal of assets	A.17.2.1	Availability of information processing facilities
A.11.1.6	Delivery and loading areas	A.11.2.6	Security of equipment and assets off-premises	A.13.1.2	Communications security

Rationalizing Controls

PCI-DSS 3.2
10.1: Implement audit trails to link all access to system components to each individual user. It is critical to have a process or system that links user access to system components accessed…
10.2: Implement automated audit trails for all system components to reconstruct the following events…

NIST 800-53 revision 4
AU-2: Audit Events - The organization: a. Determines that the information system is capable of auditing the following events…
AU-3: Content of Audit Records - The information system generates audit records containing information that establishes what type of event occurred…

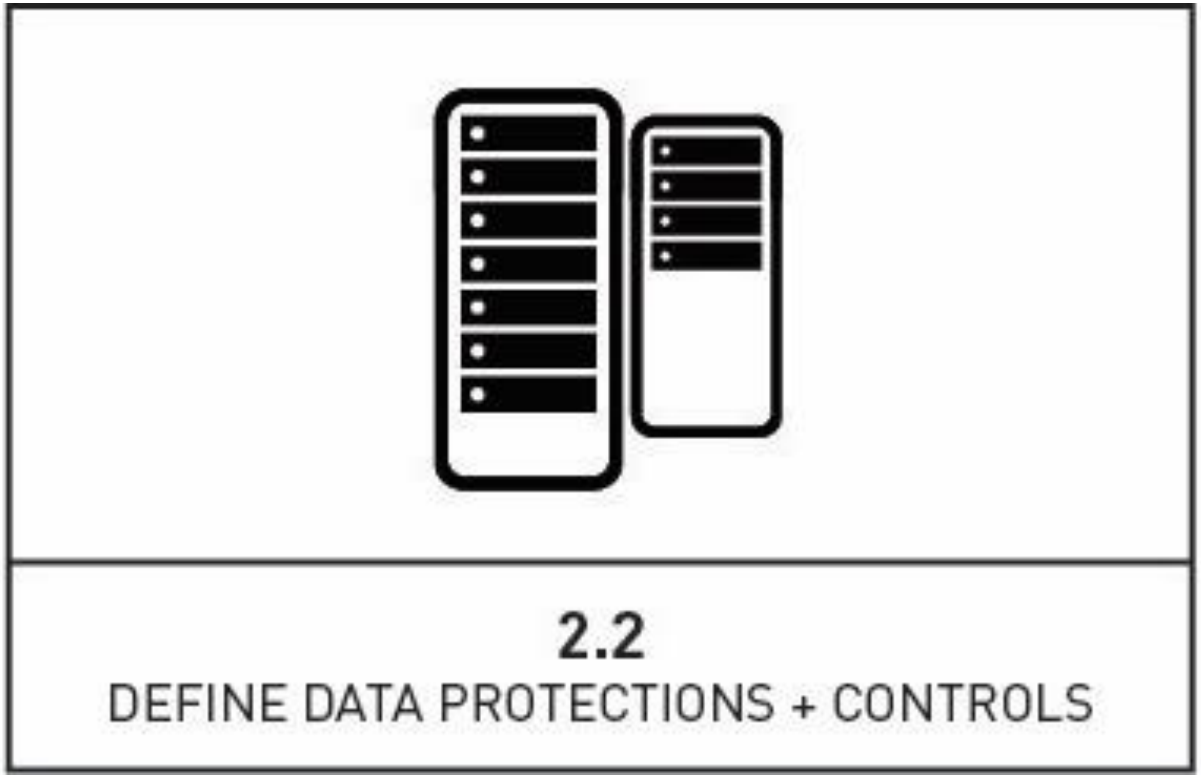
HIPAA Security Rule
164.308(a)(1)(ii)(D) - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports…
164.308(a)(5)(ii)(c) - Procedures for monitoring log-in attempts and reporting discrepancies…

Fused Control Approach

Fused Audit Trail (Control Example)

- Implement auditing for the following events (e.g. people, processes and actions) within the organizational use of cloud computing.
- Monitor for both positive and negative actions of users, system, services and applications.
- Secure, retain and automated audit trails as well as create communication paths to other security systems for analysis, reporting and investigations.

Define Data Protections



2.2

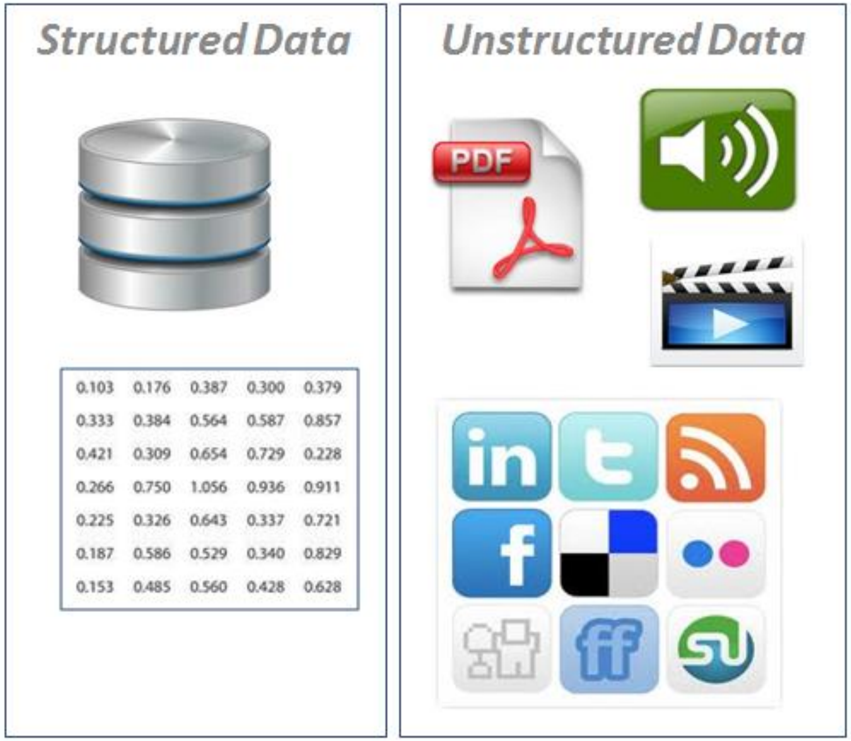
DEFINE DATA PROTECTIONS + CONTROLS

Problem Statement…

Issue #1 – The majority of organization do not have a mature “Data Classification” policy, process or user education schemes for internal use of data.

Issue #2 – Most organizations do not have a clean single source of “Truth” for what is their authoritive source for data. (Structured or Unstructured).

Issue #3 – Most organizations do not have an “Data Lifecycle” policy, procedure and/or operational processes for how data should be derived, protected, used, secured, transferred, achieved and destroyed when no longer relevant.



0.103	0.176	0.387	0.300	0.379
0.333	0.384	0.564	0.587	0.857
0.421	0.309	0.654	0.729	0.228
0.266	0.750	1.056	0.936	0.911
0.225	0.326	0.643	0.337	0.721
0.187	0.586	0.529	0.340	0.829
0.153	0.485	0.560	0.428	0.628

Data Protection Requirements

There are a number of regulatory, standards and frameworks which can impact data cloud computing.

- US - Health Insurance Portability and Accountability Act (HIPAA)
- US - Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- US - Consumer Data Security and Notification Act (Amendment to Gramm-Leach-Bliley Act)
- EU - Directive 95/46/EC of the European Parliament and of the Council
- EU - Directive 2002/58 on Privacy and Electronic Communications (e.g.-Privacy Directive)
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- Canada - The Personal Information Protection and Electronic Documents Act (PIPEDA)
- Canada – Protection B
- UK - Data Protection Act 1998 (DPA)
- Australian - The Federal Privacy Act 1988
- Japan - The Act on the Protection of Personal Information (“APPI”)
- Singapore - Personal Data Protection Act 2012
- Philippines - Data Privacy Act of 2012
- South Korea - Personal Information Protection Act (“PIPA”)
- Hong Kong - The Personal Data (Privacy) Ordinance (Cap. 486) (“Ordinance”)

Data Protection Considerations

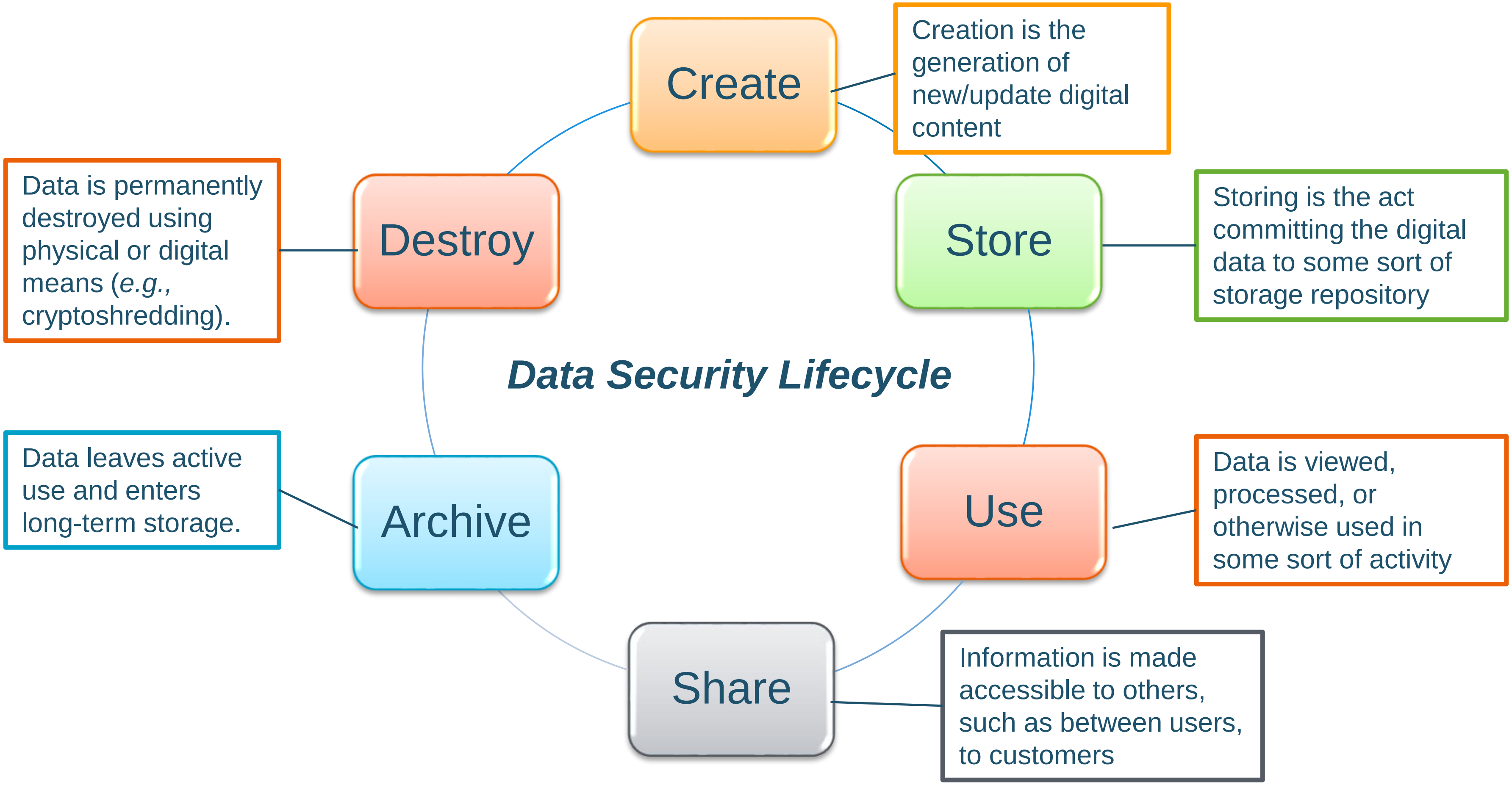
- **Access Controls**: Ensure organization can manage access to their content, services and resources independently of the cloud service provider.
    - Additionally, ensure cloud provider supports advanced set of access controls (MFA), encryption, and logging features.

- **Contractually**: Ensure the cloud providers does not access or use customer content for any purpose other than as legally required and for maintaining the cloud services.

- **Storage Locations**: Organization should be able to choose the geographic location in which their content will be stored. Cloud Providers should not move or replicate customer content outside of the customer's chosen locations.

- **Security**: Customers should choose how their customer content is secured. Through the use of various encryption of content in transit or at rest.
    - Additionally, organization should ensure they have option to manage their own encryption keys.

Define Data Protection + Controls



Data Security Lifecycle

Create

Creation is the generation of new/update digital content

Store

Storing is the act committing the digital data to some sort of storage repository

Use

Data is viewed, processed, or otherwise used in some sort of activity

Share

Information is made accessible to others, such as between users, to customers

Archive

Data leaves active use and enters long-term storage.

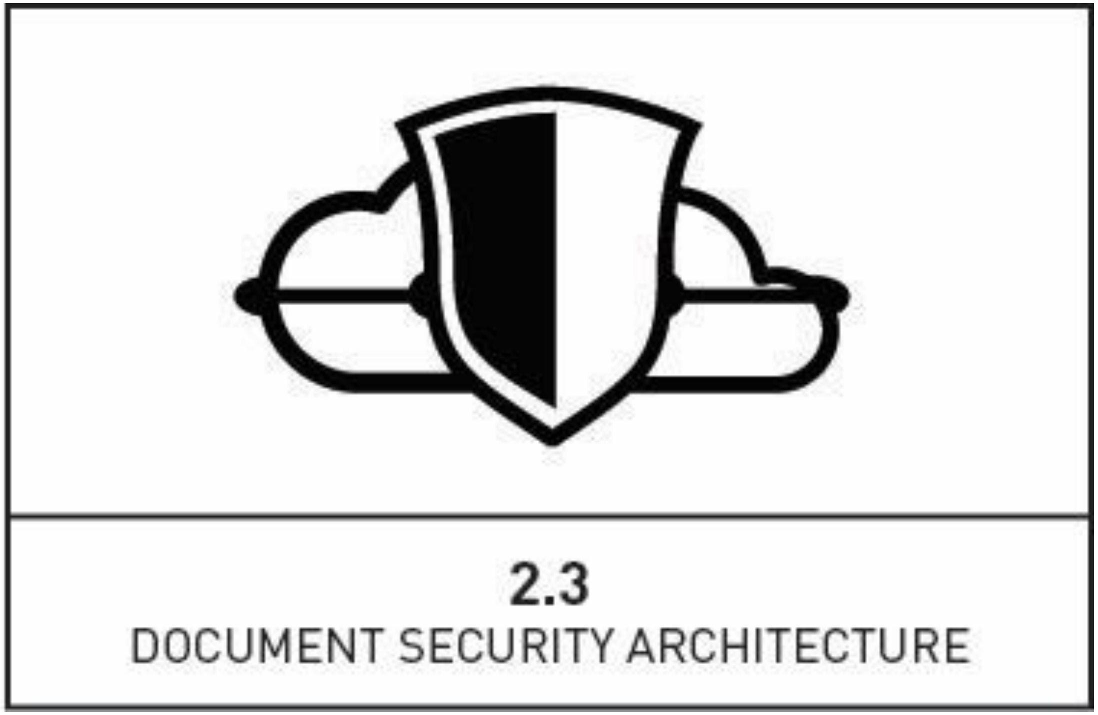
Destroy

Data is permanently destroyed using physical or digital means (*e.g.*, cryptoshredding).

(Security Controls + Data Protections)

- Define your architecture elasticity in advance
- Automate your Architecture
- Align your Test/Dev systems to Production
- Enable Continuous Integration and Continuous Deployment
- Enable a Data Protection architecture
- Test and Game Days

Security Architecture



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?

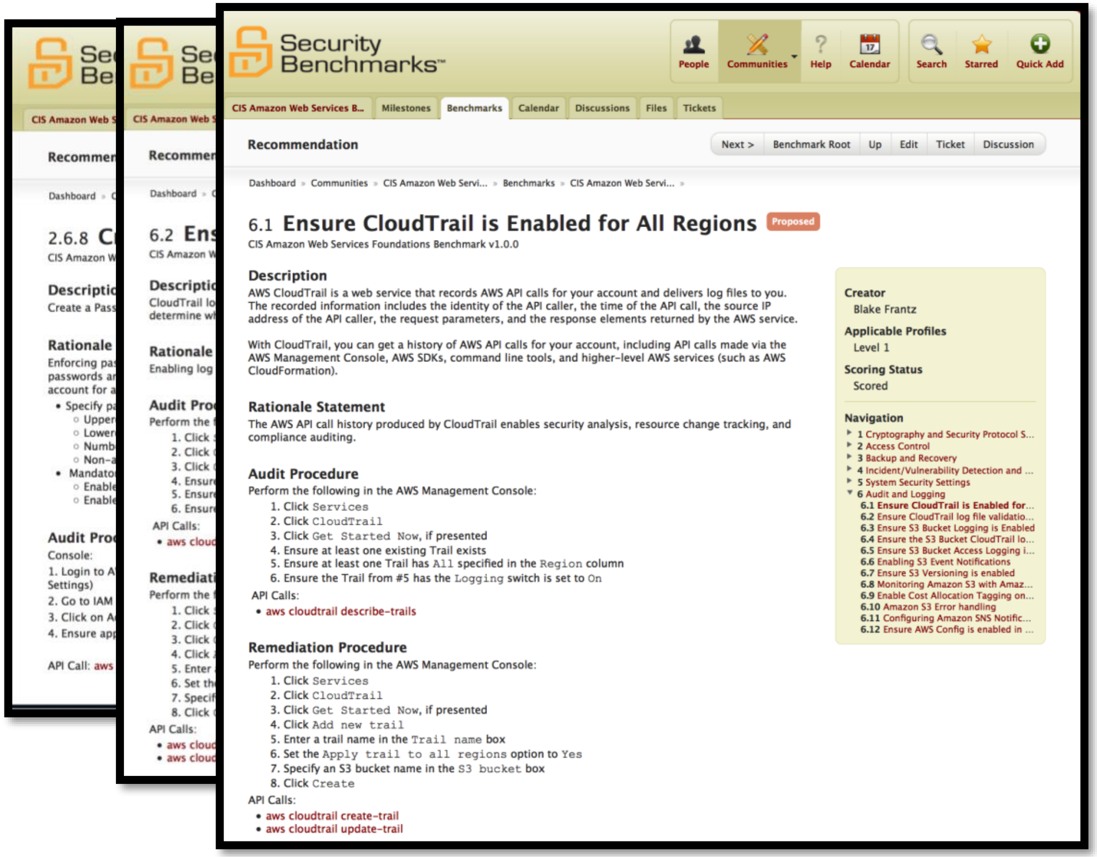
How to verify the standards are met?

AWS Security Architecture Recipes

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



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

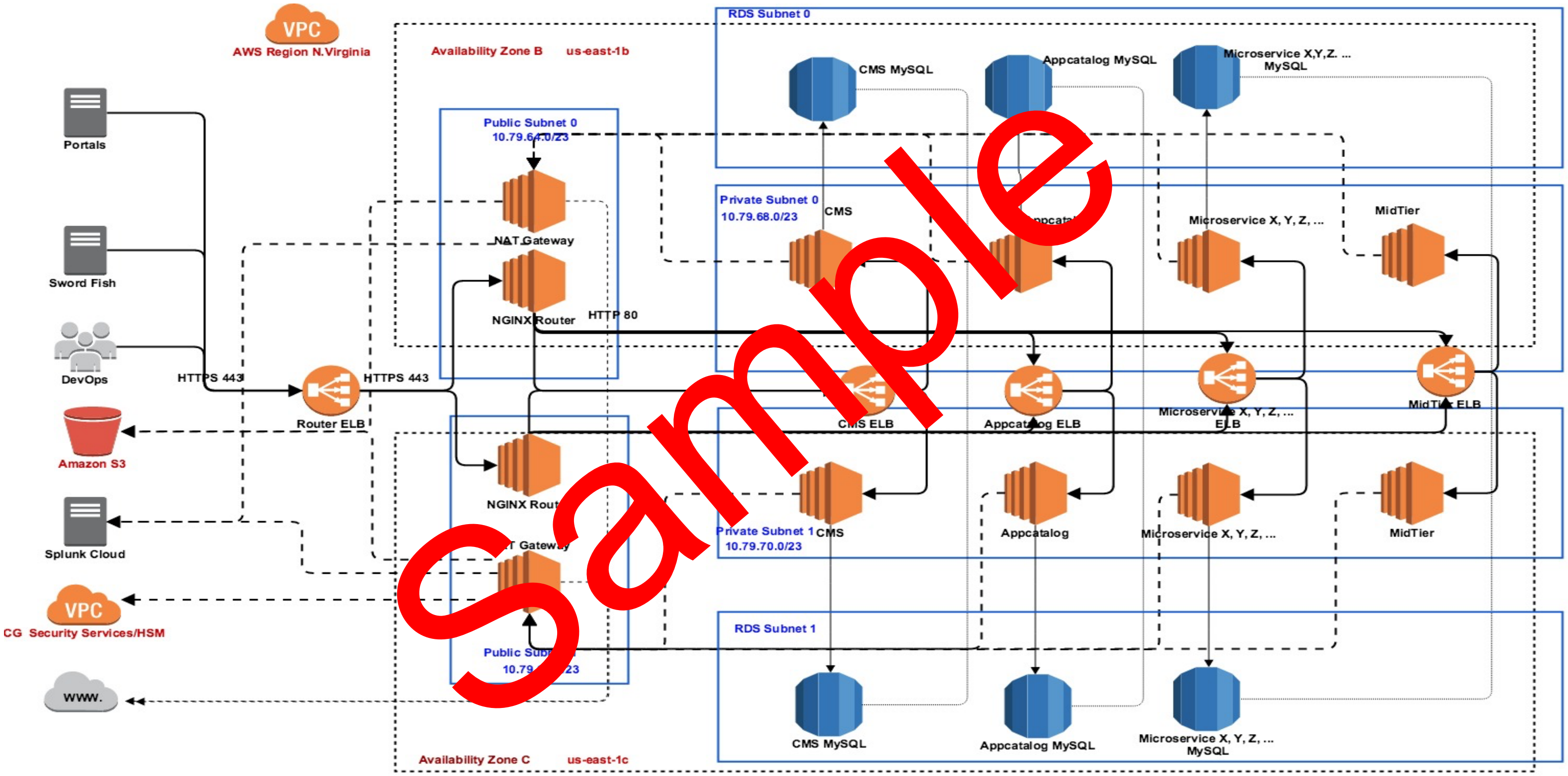
Scoring Status
Scored

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 lo...
  - 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 SNS Notific...
  - 6.12 Ensure AWS Config is enabled in ...

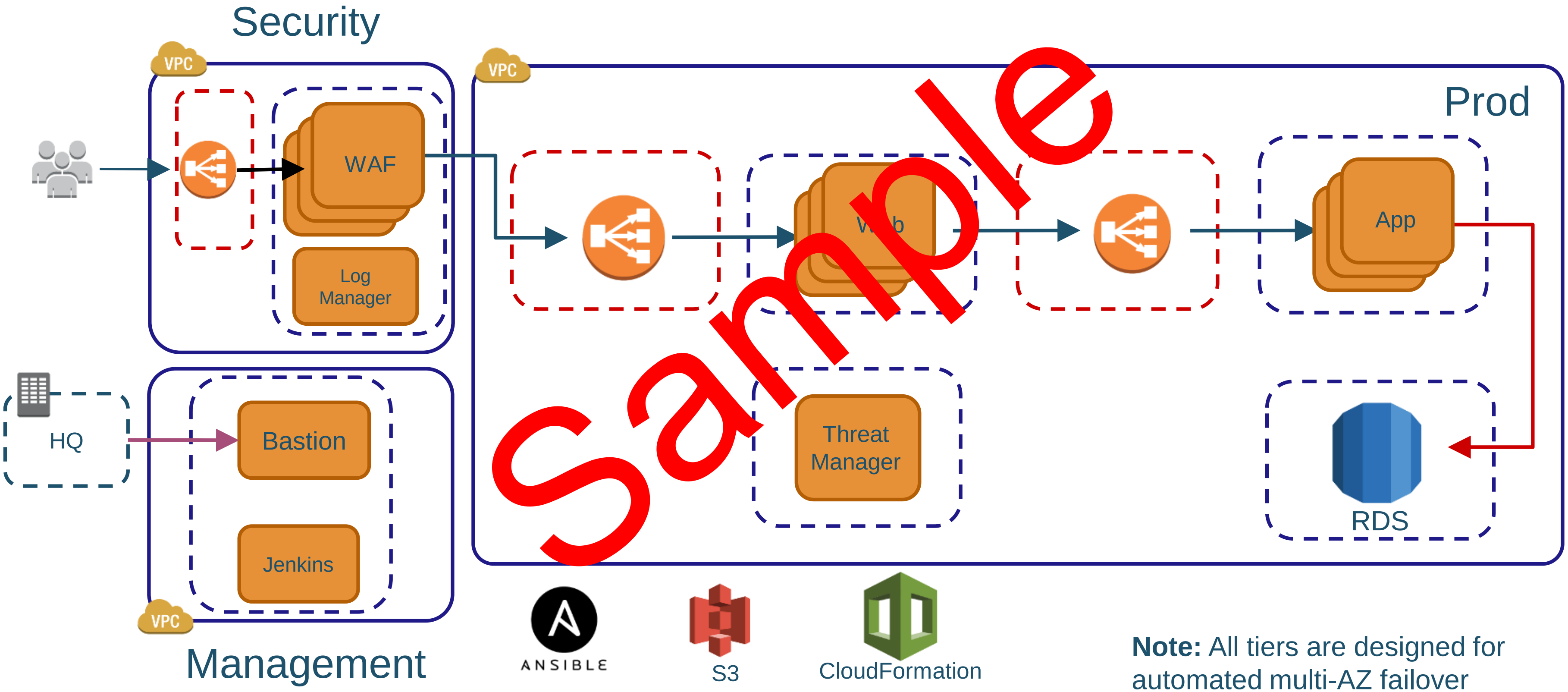
https://www.cisecurity.org/

Document your Security Architecture



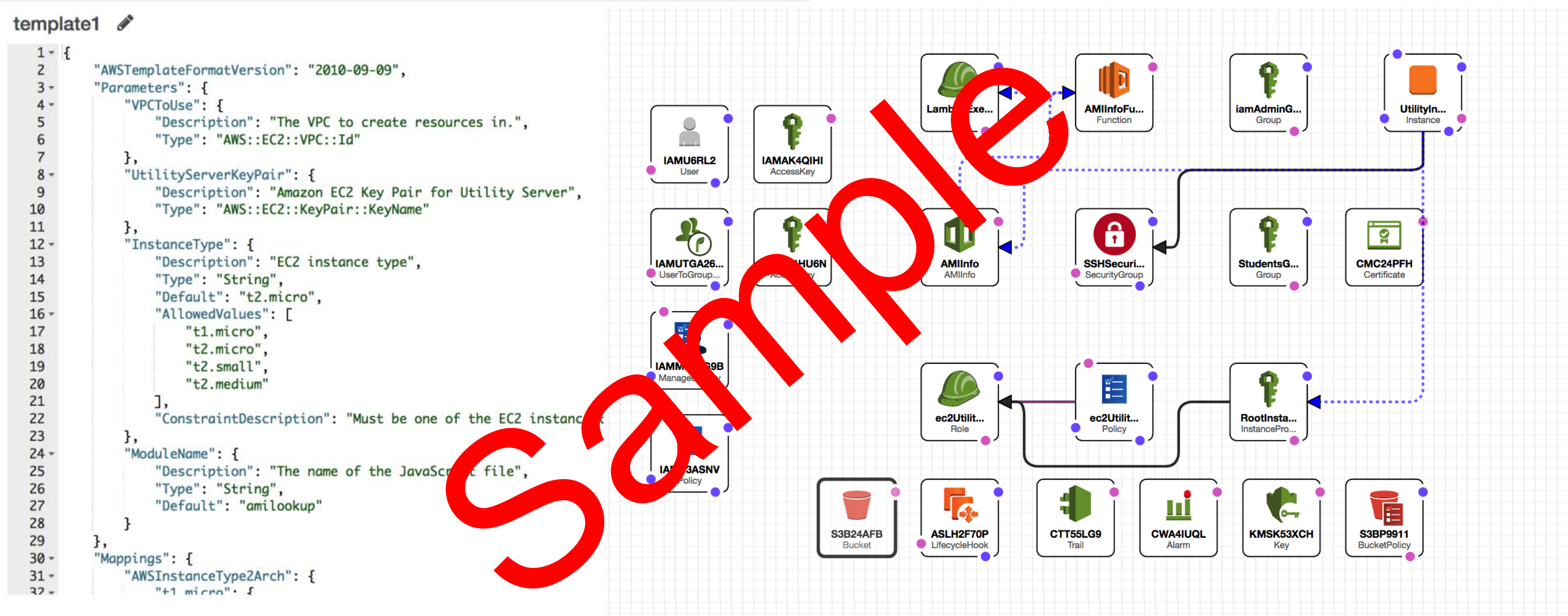
S3 KMS CodeDeploy Cloud Formation CloudTrail

Automated multi-AZ failover



Note: All tiers are designed for automated multi-AZ failover

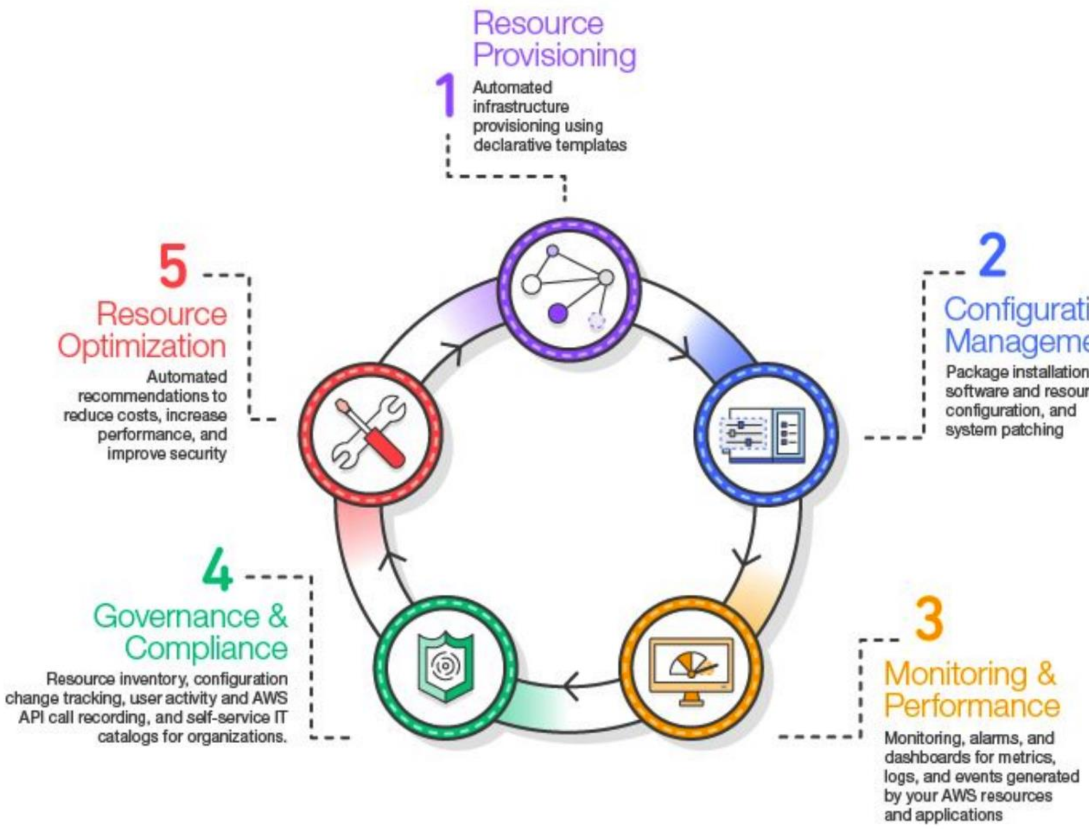
Cloud Security Automation w/DevOps (CI/CD)



template1

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Parameters": {
        "VPCToUse": {
            "Description": "The VPC to create resources in.",
            "Type": "AWS::EC2::VPC::Id"
        },
        "UtilityServerKeyPair": {
            "Description": "Amazon EC2 Key Pair for Utility Server",
            "Type": "AWS::EC2::KeyPair::KeyName"
        },
        "InstanceType": {
            "Description": "EC2 instance type",
            "Type": "String",
            "Default": "t2.micro",
            "AllowedValues": [
                "t1.micro",
                "t2.micro",
                "t2.small",
                "t2.medium"
            ],
            "ConstraintDescription": "Must be one of the EC2 instanc
        },
        "ModuleName": {
            "Description": "The name of the JavaScript file",
            "Type": "String",
            "Default": "amilookup"
        }
    },
    "Mappings": {
        "AWSInstanceType2Arch": {
            "t1.micro": {
```

Cloud Risk Management – Optimized



1 Resource Provisioning

Automated infrastructure provisioning using declarative templates

2 Configuration Management

Package installation, software and resource configuration, and system patching

3 Monitoring & Performance

Monitoring, alarms, and dashboards for metrics, logs, and events generated by your AWS resources and applications

4 Governance & Compliance

Resource inventory, configuration change tracking, user activity and AWS API call recording, and self-service IT catalogs for organizations.

5 Resource Optimization

Automated recommendations to reduce costs, increase performance, and improve security

Governance as Code – *Alignments*

Modernizing Technology Governance *in the Cloud*

Risk Management

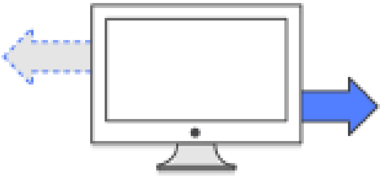
Security & Compliance lifecycle

Human Governance

Policy, Procedure and System Security Plans

Incident Response

(Protect, Detect, Respond, Identify, Recover, Report)



Configuration& Cost Management

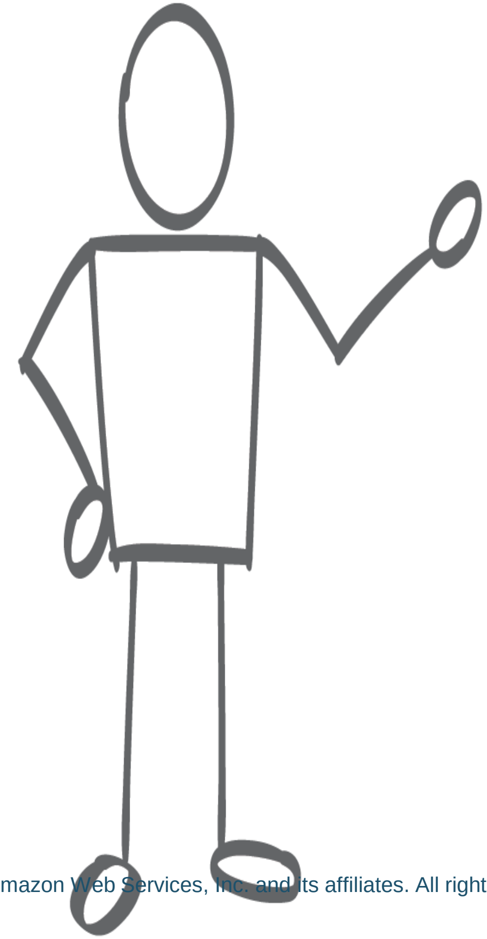
(Packaging, Configuration and Continuous Delivery)

Governance as Code

Is the process of managing and provisioning machine-readable definition files, templates, scripts and recipes for regulatory workload configurations.

GaC interacts with Continuous Configuration Automation (CCA) tools (e.g., Chef, Puppet, Ansible etc.) and can be thought of as an extension of traditional Infrastructure of Code frameworks.

The goal of GaC is to version control solutions as scripts or declarative definitions which meet regulatory requirements and adherence with audit frameworks.



Questions

SailPoint IdentityIQ

Dec. 4, 2019

SailPoint IdentityIQ (IIQ)

- Governs an identity's access across applications
  - Identity = person (usually)
  - True role-based access control
  - Birthright roles for all agency users
  - Business manager can assign roles
  - Business/application owner can approve roles (or automated)
  - Break glass account disables for agency ISOs
  - Access recertification and reconciliation at business/application owner and/or ISO level
  - Automatic separation of duties violation detection

SailPoint IdentityIQ applications

Three types of applications in IIQ:

- Connected application with provisioning (Keystone Edge/KSE)
- Connected application, read-only (COV Active Directory (AD)*)
- Disconnected application (ITFM/Digital Fuel)

Active Directory is an application to IdentityIQ

*COV AD is being converted to provisioning

Connected application with provisioning

- Application provisioning?
  - Create and delete accounts
  - Change entitlements for that account based on IT or business role assignments
  - IIQ does this *in* the application itself
  - Aggregates info into IIQ
- How?
  - Connector is needed
  - IIQ must have account management permissions in application

Connected application, read-only

- Application read-only?
  - IIQ monitors accounts and entitlements in application
  - Aggregates info into IIQ
  - Separate process must exist for account management
- How?
  - Connector is needed
  - IIQ must have view account permissions in application

Disconnected application

- Disconnected application?
  - IIQ has no connection to application
  - Separate process must exist for account management
  - IIQ tracks access that a person *should* have, not the actual account access

- How?
  - No connector is needed
  - Business roles maintained and defined by agency (application owner)
  - Verify access is correct in application (manual reconciliation)

Reasons

- Why use IIQ?
  - Good practice
  - Least privilege
  - Separation of duties
  - **Access management related audit findings**
  - *People with COV accounts are already licensed!*

Begin ~~at the beginning~~ with the easy wins

- Where to start?
  - Identify basic IT and business roles
    - Remember IT role ≠ technical roles
  - Define basic separation of duty violations with AD groups (e.g., Workstation Admin / Server Admin)
  - Submit KSE general service request:
    - With Role and/or SoD definitions
    - To request onboard applications that use COV AD groups
    - For help with account / group / identity reports
  - Contact MSI identity and access management to discuss non-AD application onboarding (pre-RFS)

Roles definition: new stuff

Define roles as new things* are rolled out:

- Already doing work needed for role definition
  - Defining user roles and access levels
  - Defining separation of duties
- Easy to assign AD groups to roles at creation

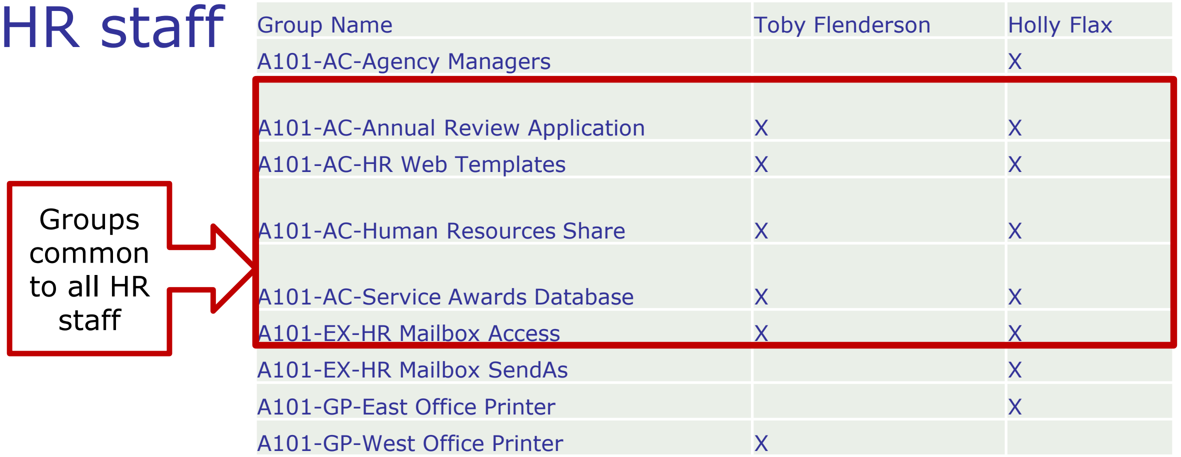
Example: Cardinal expansion

*things could be new additions or changes to existing: AD groups, applications, systems, organizational structure, etc.

Roles definition: start with small user sample

- Start with short list of accounts
- Identify AD groups common to those accounts

Example: List of HR staff



Group Name	Toby Flenderson	Holly Flax
A101-AC-Agency Managers		X
A101-AC-Annual Review Application	X	X
A101-AC-HR Web Templates	X	X
A101-AC-Human Resources Share	X	X
A101-AC-Service Awards Database	X	X
A101-EX-HR Mailbox Access	X	X
A101-EX-HR Mailbox SendAs		X
A101-GP-East Office Printer		X
A101-GP-West Office Printer	X	

Groups common to all HR staff

Roles definition: start with user account

- Use a specific individual’s account access
  - *Must understand normal vs. special access for the individual and the role*

Example: Donna Meagle is a member of these AD groups:

A101-AC-Constituent Services Share	Grants full access to Constituent Services share	AD Group
A101-AC-TimeCard Access	Grants access to submit time cards	AD Group
A101-AC-Authorized Buyers	Users authorized to make purchases	AD Group
A101-AC-Parks Anniversary Planning Committee	Committee members access to planning database	AD Group
A101-AC-Agency JKL Staff Association Committee	Committee members access to staff association events calendar	AD Group

Groups common to all Parks staff

Specific to Donna

Roles definition: one more thing…

You don’t need to have all AD groups in place to define a role.

An IT Role can be created with just one AD group and others added later.

A business role can be created with just one IT role and others added later.

What’s next? High level

- Upgrade to IdentityIQ v8
- Convert COV and Auth AD to provisioning (currently read only)
- Work with agencies to define roles
  - Workshops / small group training

- Onboard more applications for agencies:
  - If application uses COV AD groups -> submit KSE general service request
  - Application doesn’t use COV AD groups -> submit request for solution (RFS)

What's next? Service catalog

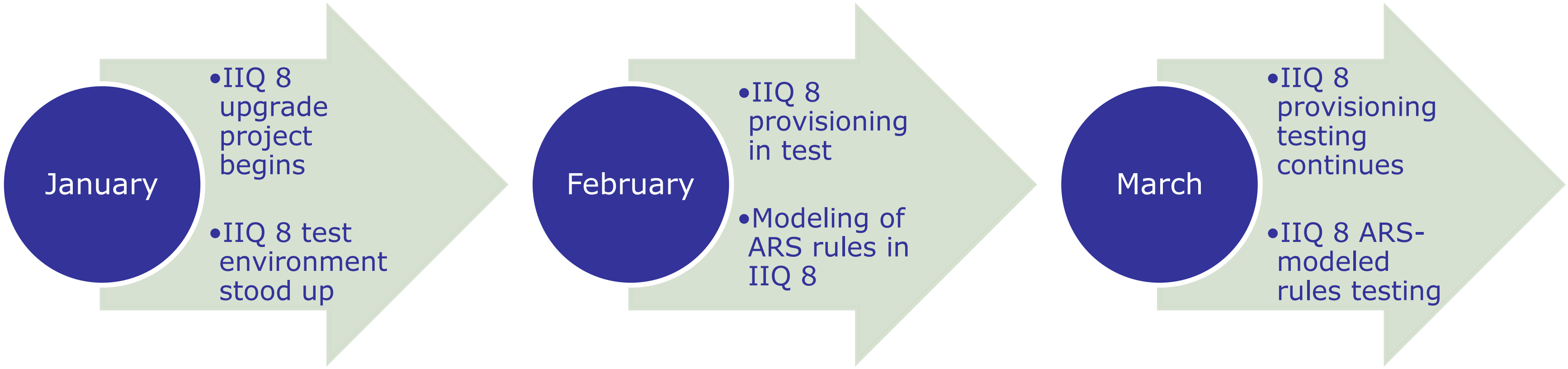
Catalog items:

- COV account request: update, to reflect identity focus
- Group / role request: create, link AD groups to roles

Knowledge base articles

- Role creation guide with template
- Additional IIQ-related KBs

SailPoint IdentityIQ v8 upgrade timeline



January

- IIQ 8 upgrade project begins
- IIQ 8 test environment stood up

February

- IIQ 8 provisioning in test
- Modeling of ARS rules in IIQ 8

March

- IIQ 8 provisioning testing continues
- IIQ 8 ARS-modeled rules testing

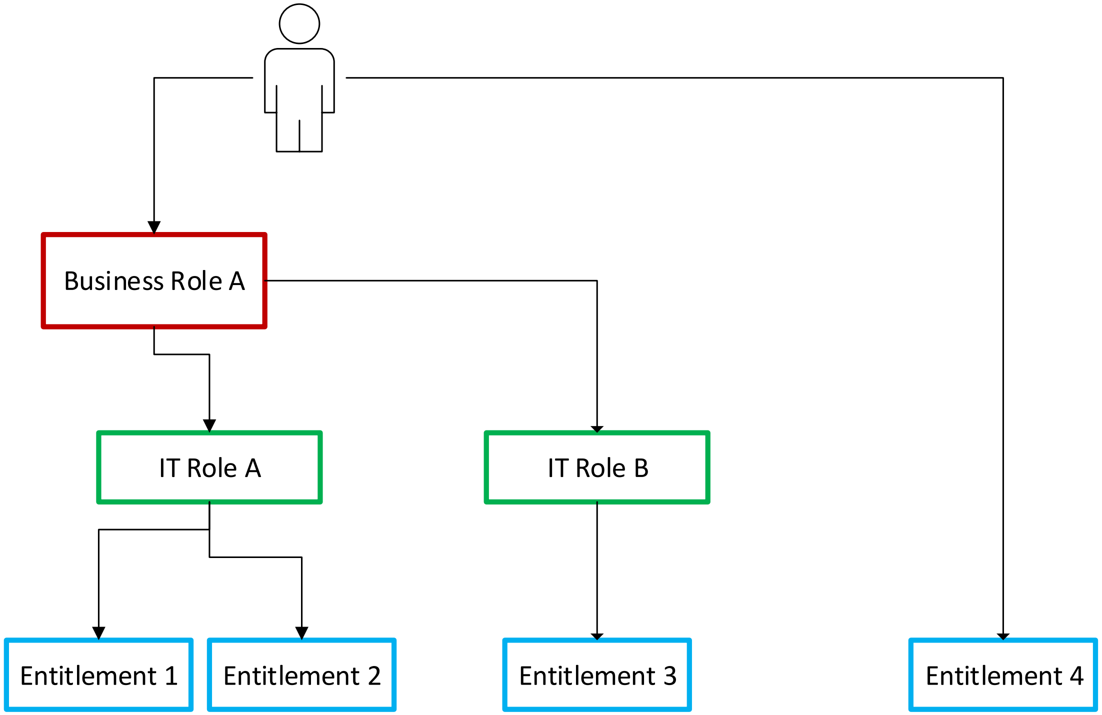
*Schedule is tentative and subject to change

Questions?

Reference: points of contact

	Role	Contact	
SAIC	MSI Identity and Access Management	**MSI IAM Team**	MSI-IdentityandAccess-Management@saic.com
SAIC	MSI Information Security Manager / ISO	**Jane Williamson**	jane.a.williamson@saic.com
SAIC	MSI Chief Security Architect	**Grayson Walters**	grayson.L.walters@saic.com

Reference: IIQ hierarchy and glossary



Business role: A position or higher level business function. Can be one or more IT roles.

IT role: Access needed to perform specific tasks or functions. Can be one or more entitlements.

Entitlement: Specific access granted to a user in an application. (e.g., AD group)

Security Challenge Game

Upcoming Events

IS orientation

Dec. 10, 2019

1-3 p.m.

Room 1221

Register @:

http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Future ISOAG

Jan. 8, 2020 @ CESC 1-4 p.m.

Speakers: Chris Atha, White Collar Crimes Center
Ira Winkler, Secure Mentem
Benjamin Sady, Dixon Hughes Goodman
Stephanie Deichman, VITA

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk