Security In The Cloud

An Approach for Enterprises

Overview

For many enterprises moving to AWS, the security model can be different from their traditional on-premise infrastructure. While the security requirements will likely remain constant, the security controls that meet these requirements may be different. Security teams often ask the following questions:

- Do I have adequate security to protect my workloads and data?
- How ‘good’ is good enough?
- What security controls do I need?
- Do I have validation that the right controls were built?
- Do I have verification that the controls work as planned?

Path to Production

1. Identify & Engage Stakeholders

2. Capability & Enablement

3. Operational Model

4. Security of the Cloud

5. Security in the Cloud

6. Regulations

7. Legal Agreements

8. Establish Security Controls (Prevent, Detect, Respond, Recover)

9. Internal & External Assessment

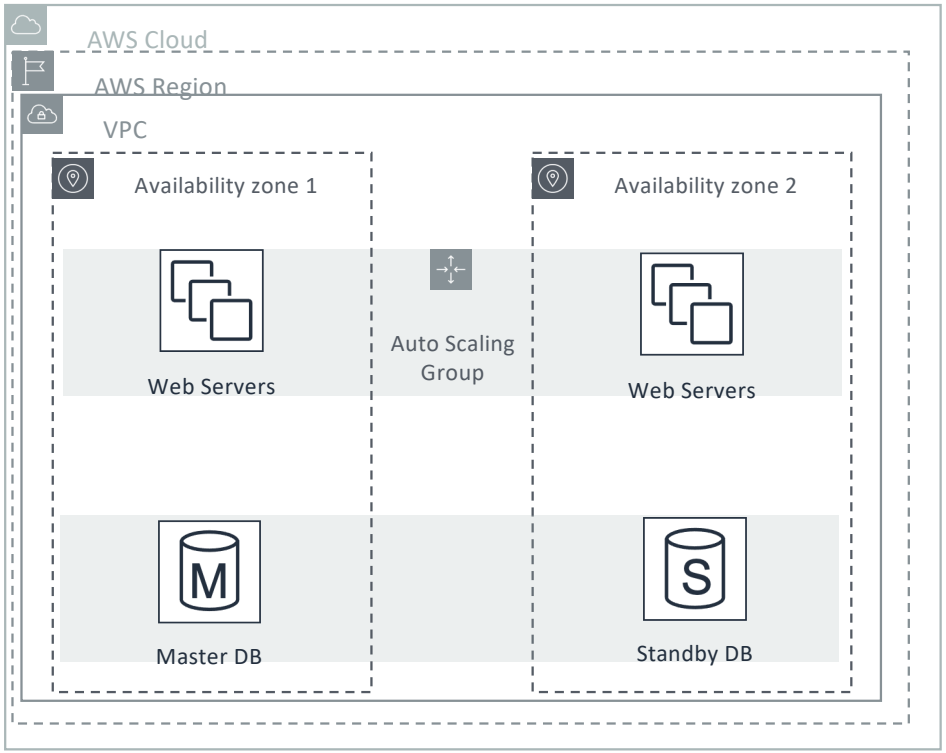
10. Regulator Approval or Notification

Overview

Individual AWS Services

Developers want to use a growing set of AWS services to deploy workloads that execute business outcomes.

Production Business Application

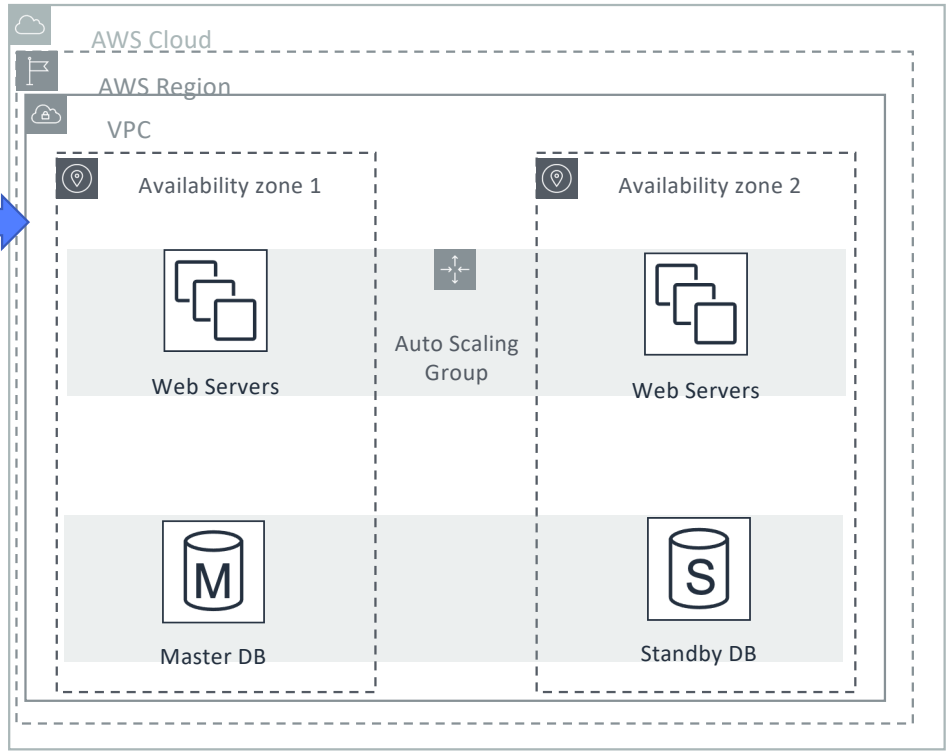


Overview

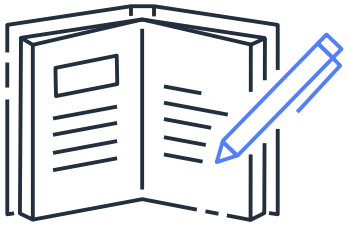
Individual AWS Services

Security, Risk & Compliance teams want to support the business outcomes in line with the organizations risk appetite.

Production Business Application

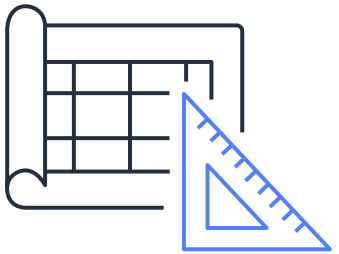


Components of a Cloud Security Strategy



Cloud Security Policy

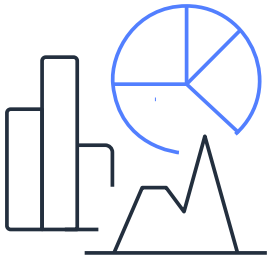
AWS Service Due-Diligence



Automated Secure Patterns

Security Assessments

Continuous Compliance

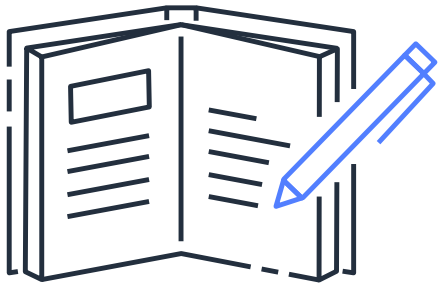


Cloud Risk Management

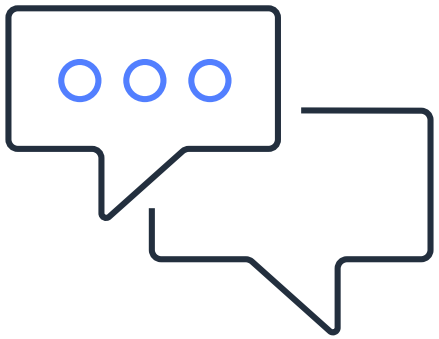
Cloud Security Policy

“How do I use AWS appropriately in line with my company policy?”

Cloud Security Policy



Create a AWS usage policy
Leverage existing where possible, create new ones where required



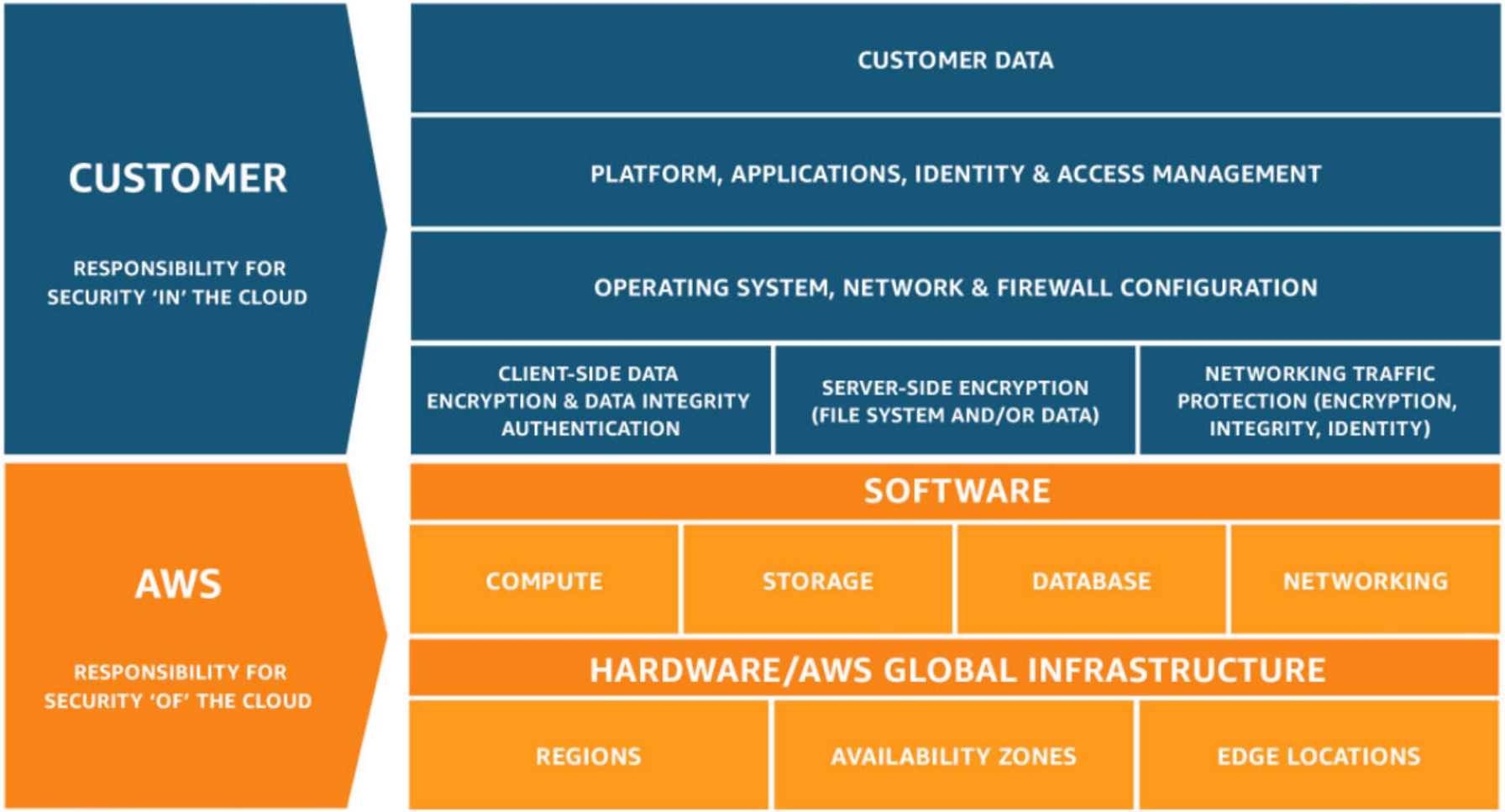
Communicate policy with AWS users and development teams that will be using AWS.

Aim for a high degree of automation for implementing policy

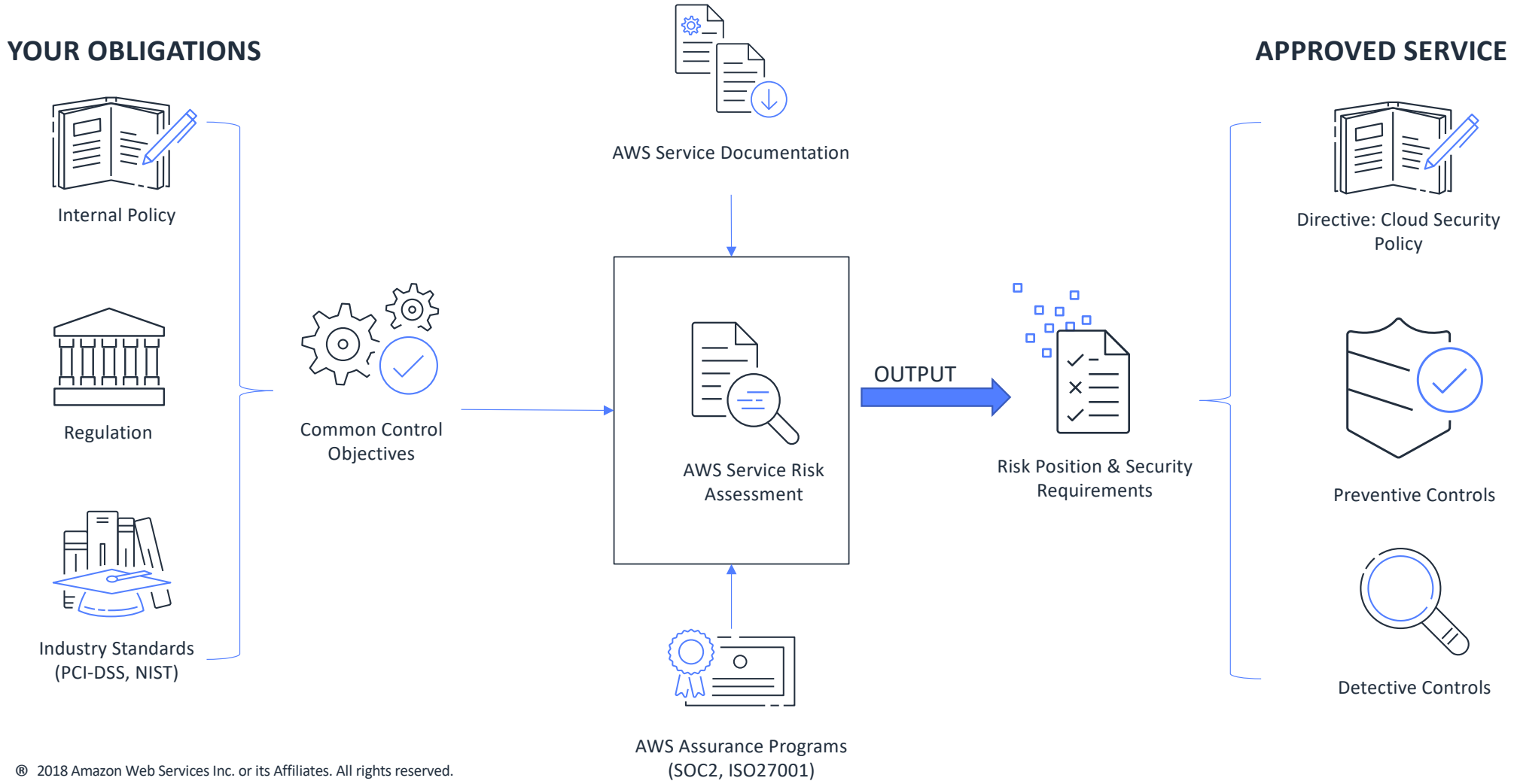
AWS Service Due-Diligence

“How do I know which AWS services my teams can use?”

Understanding the AWS Shared Responsibility Model



AWS Service Due-Diligence

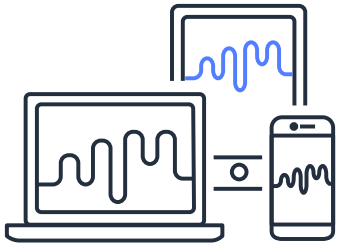


Use AWS Organizations To Enforce

AWS Organizations allows customers to segregate environments, systems and applications using AWS accounts. AWS Organizations supports different Organization Units (OUs) that can have different service control policies applied.

AWS ORGANIZATIONS

PRODUCTION OU



The production OU may only allow services that have been approved by the security team.

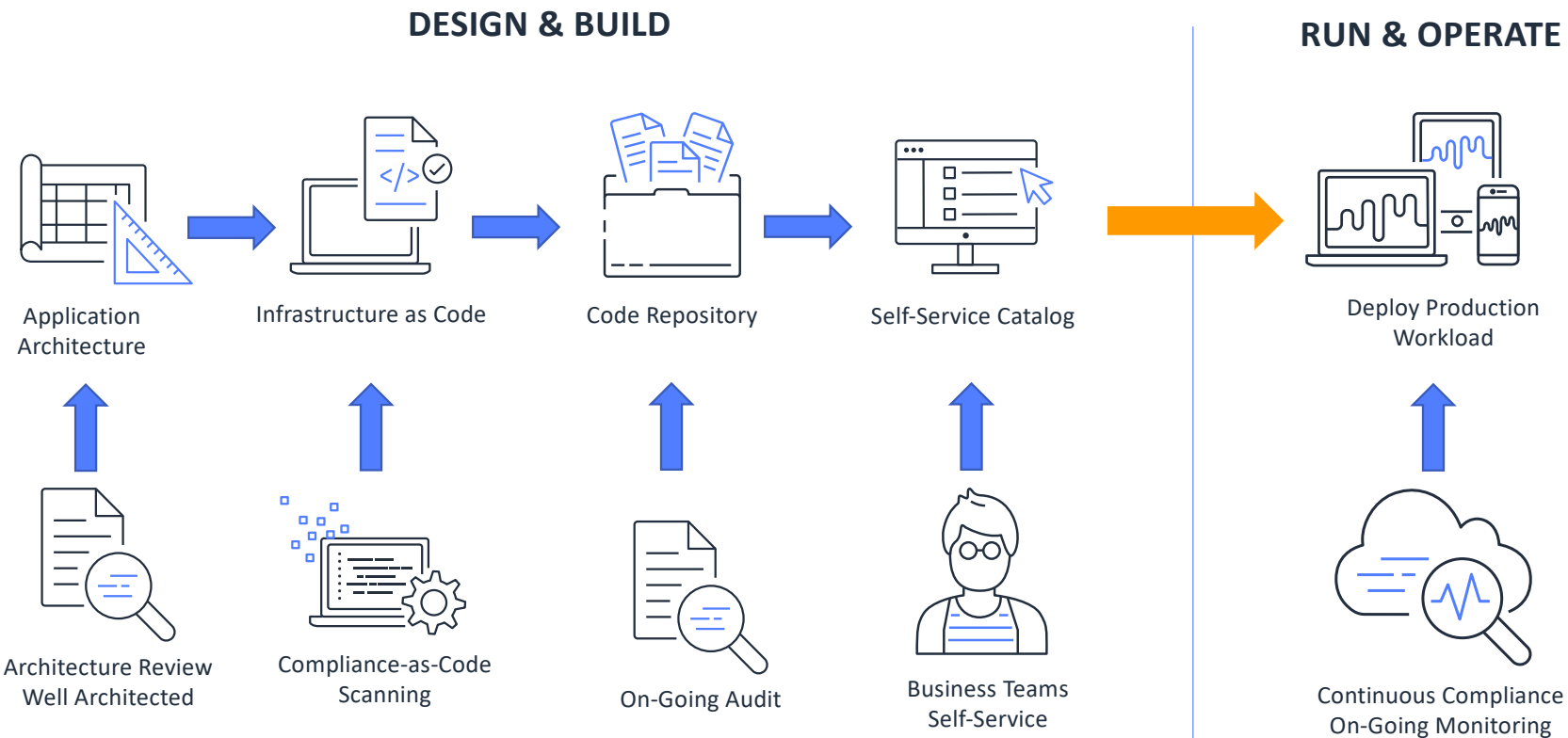
DEVELOPMENT OU

The development OU may allow all services to drive innovation & experimentation.

Self-Service Patterns

“How do I let my teams move fast and stay secure?”

Automated Secure Patterns

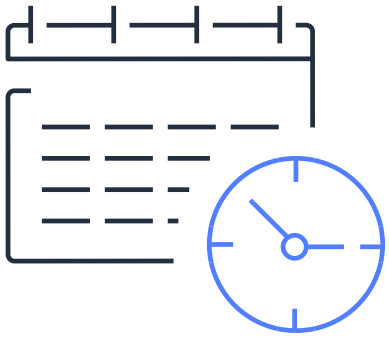


Continuous Compliance & Monitoring

“How do I perform continuous compliance and respond appropriately?”

Current Approach to Compliance

Sampling Approach

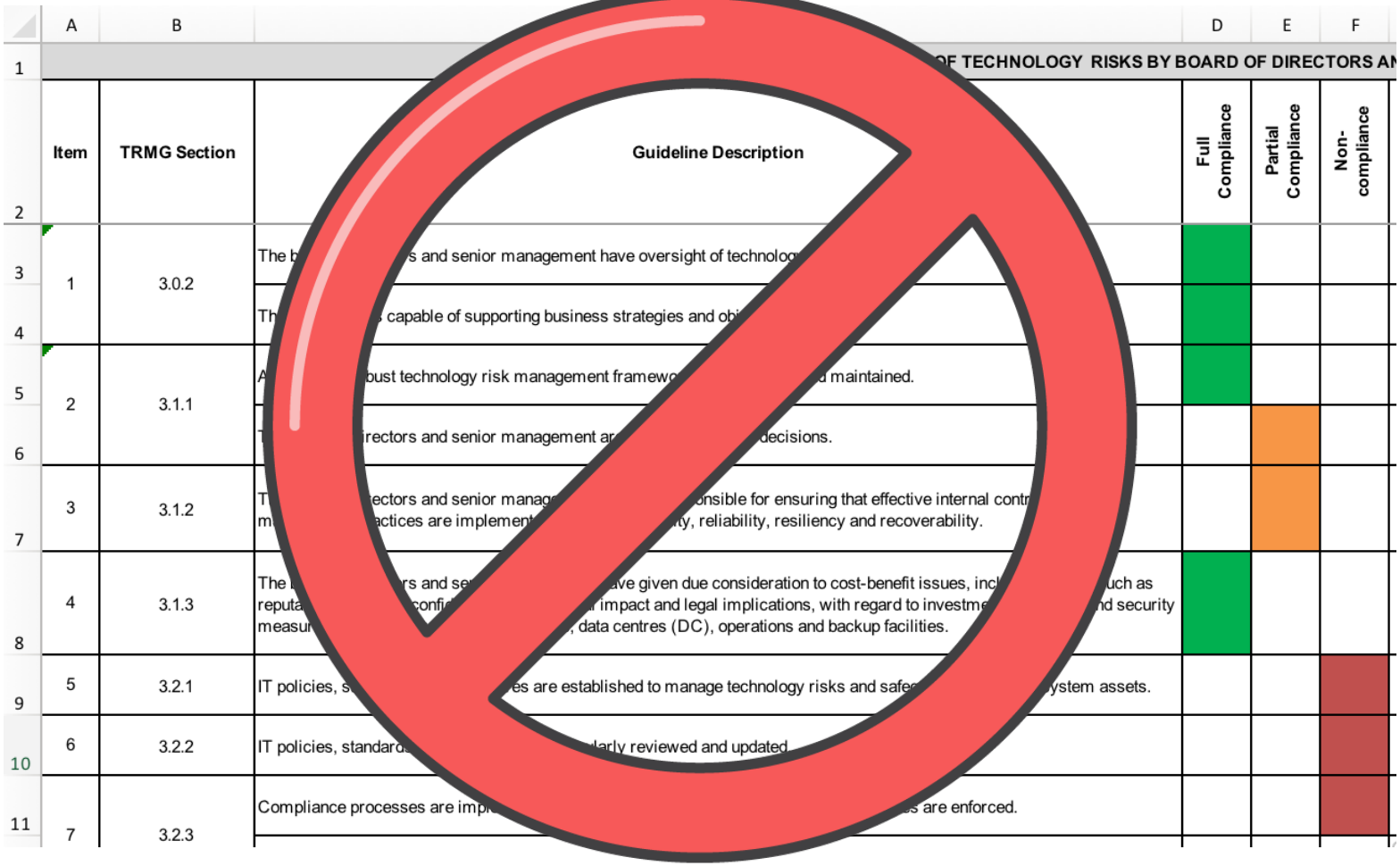


Point in Time Assessments

Spreadsheet / Checklist Driven

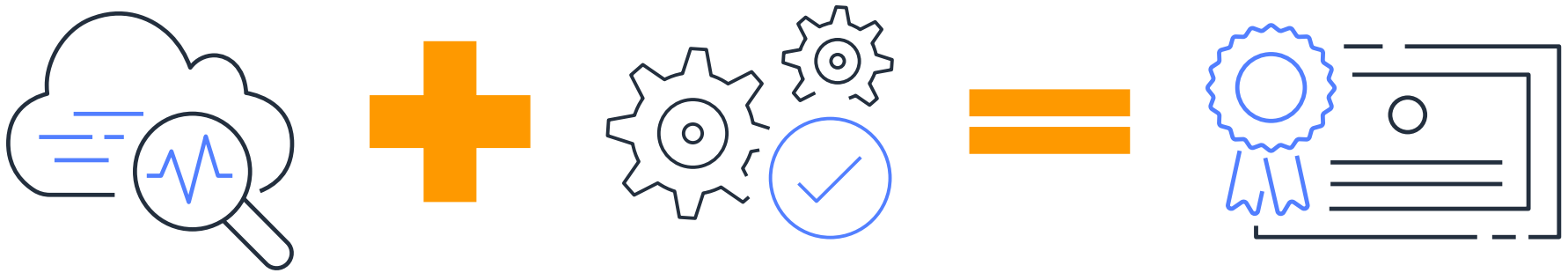
Inaccurate Evidence Collection

Your Compliance Requirements



	A	B		D	E	F
1			OF TECHNOLOGY RISKS BY BOARD OF DIRECTORS AN			
2	Item	TRMG Section	Guideline Description	Full Compliance	Partial Compliance	Non-compliance
3	1	3.0.2	The b s and senior management have oversight of technolog			
4			Th capable of supporting business strategies and obj			
5	2	3.1.1	A bust technology risk management framewo d maintained.			
6			rectors and senior management ar decisions.			
7	3	3.1.2	T ectors and senior manag onsible for ensuring that effective internal contr m actices are implement ty, reliability, resiliency and recoverability.			
8	4	3.1.3	The rs and se ave given due consideration to cost-benefit issues, incl uch as reputa confi impact and legal implications, with regard to investme nd security measu , data centres (DC), operations and backup facilities.			
9	5	3.2.1	IT policies, s es are established to manage technology risks and safe ystem assets.			
10	6	3.2.2	IT policies, standard larly reviewed and updated			
11	7	3.2.3	Compliance processes are imp s are enforced.			

Continuous Compliance Monitoring



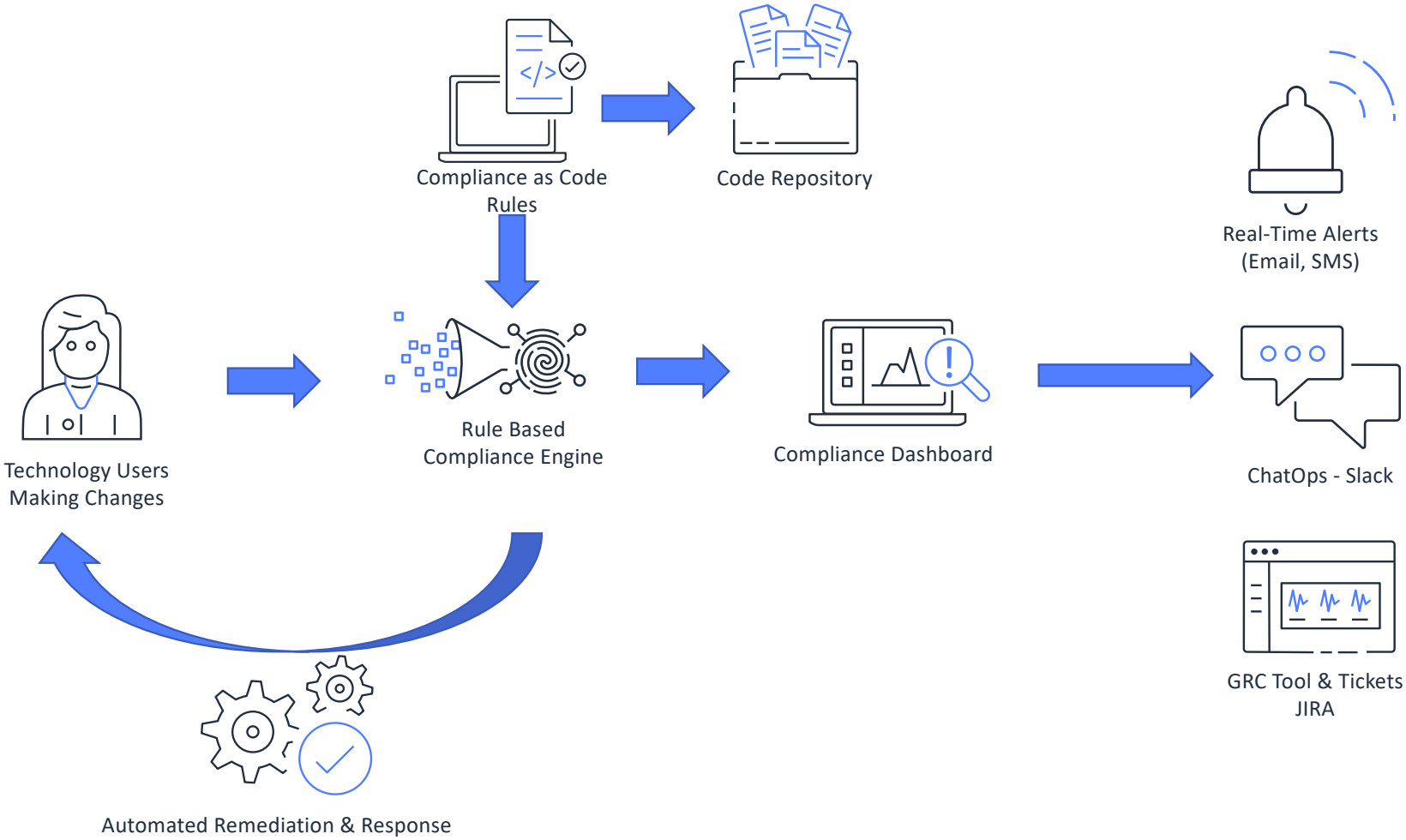
Unprecedented Visibility

Near Real-Time Automation

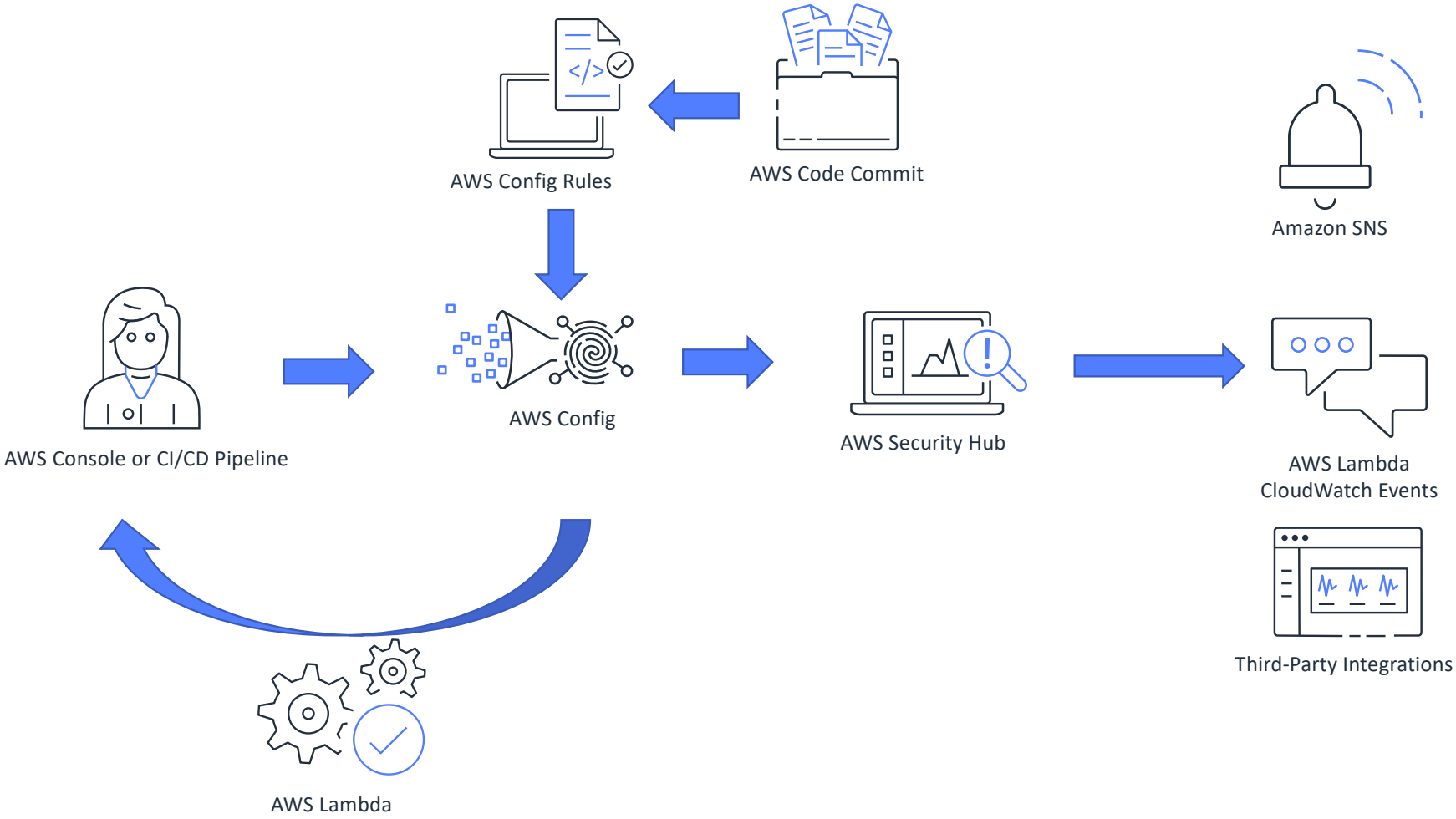
Continuous Compliance

Having the visibility into **WHO** made **WHAT** change from **WHERE** in near real-time allows enterprises to **DETECT** mis-configurations and non-compliance and **RESPOND** quickly to **PREVENT** risks from materializing.

High Level Overview

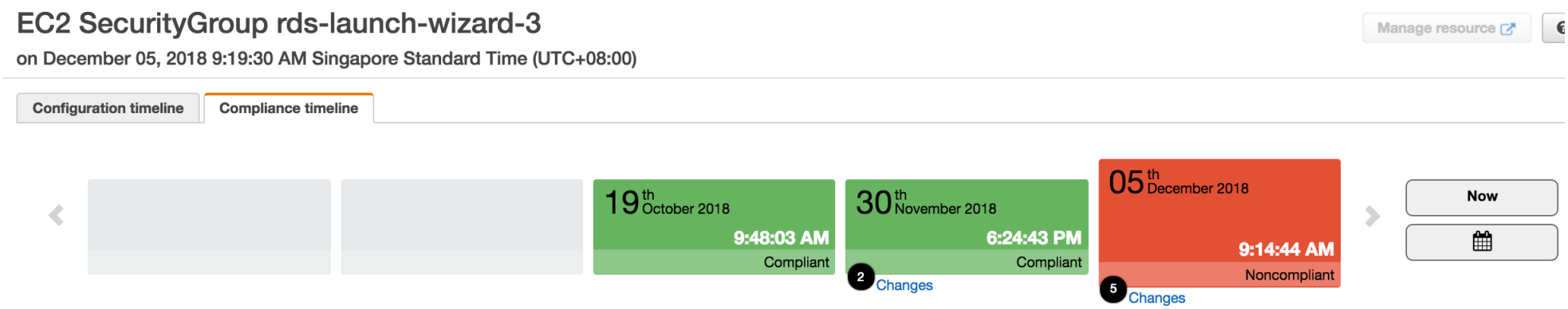


AWS Service Level Overview



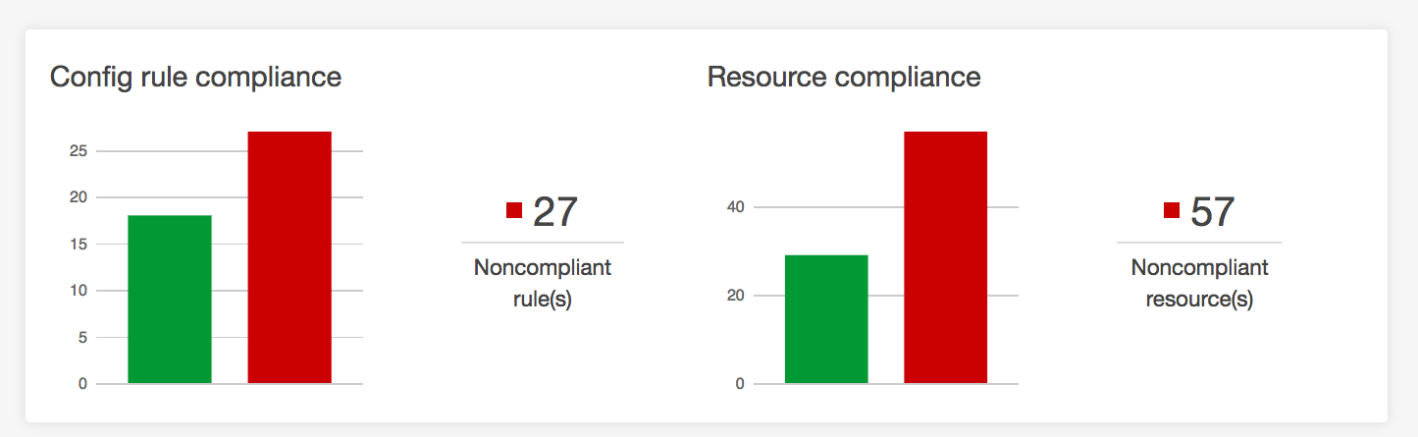
Compliance Engine: AWS Config

Compliance Timeline



AWS Config allows you to record and retrieve the compliance status of a resource over time. This allows your risk and compliance teams to determine if a resource always has been compliant or has drifted in and out of compliance with on-going changes.

Compliance Engine: AWS Config



Rule name	Compliance
APRA-001-EncryptedVolumes	5 noncompliant resource(s)
APRA-002-MultiFactorAuth	4 noncompliant resource(s)
APRA-003-Logging	1 noncompliant resource(s)

Predefined & Customizable Rules

Near Real-Time Visibility

Ability to Automatically Respond

Compliance Engine: Third-Party Partners

Third-Party Partners: Compliance Engines

Cloud Conformity is a market leading security & real-time threat detection platform.

Real-time visibility, control, governance and automation embedded within the Cloud Conformity product suite enables customers to rapidly build, deploy and monitor their AWS infrastructure, knowing their critical data and systems are secure, reliable, efficient and optimised.

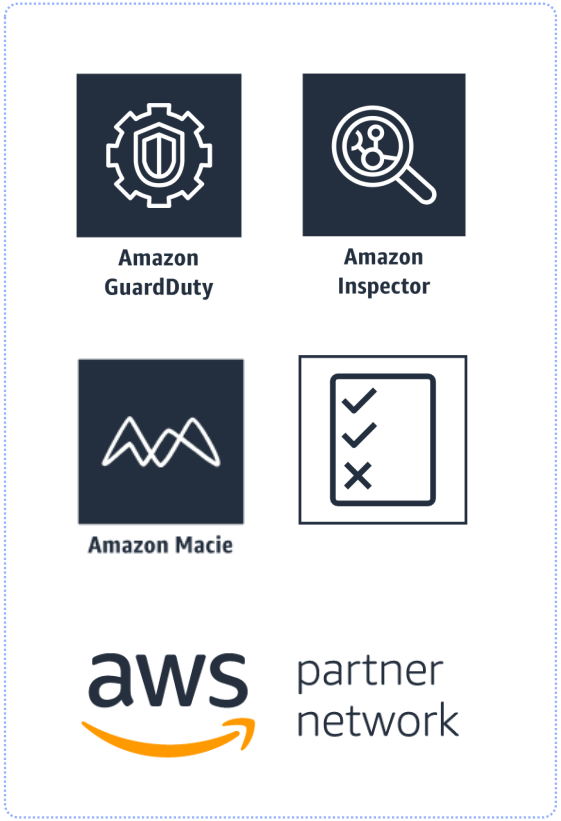
Risk prioritization helps you prioritize remediation for the riskiest resources first, with risk scores determined for every cloud resource, based on the severity of business risks, violations and anomalies.

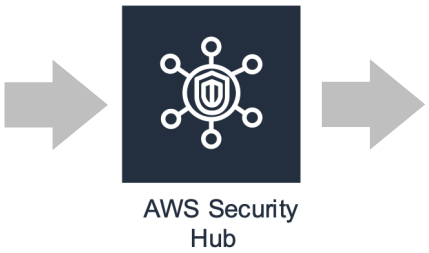
Audit trail provides you with a DVR-like capability to view time-serialized activity for any given resource. You can review the history of changes for a resource and better understand the root cause of an incident – past or present.

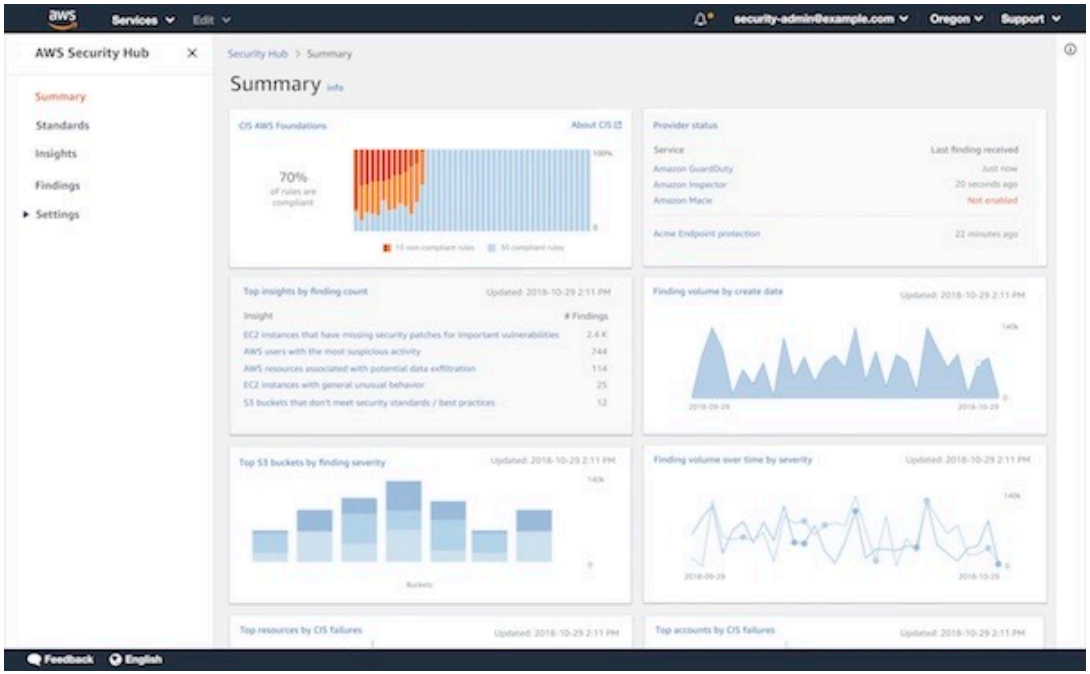
https://aws.amazon.com/products/management-tools/partner-solutions/

Compliance Engine: AWS Security Hub

AWS Security Hub





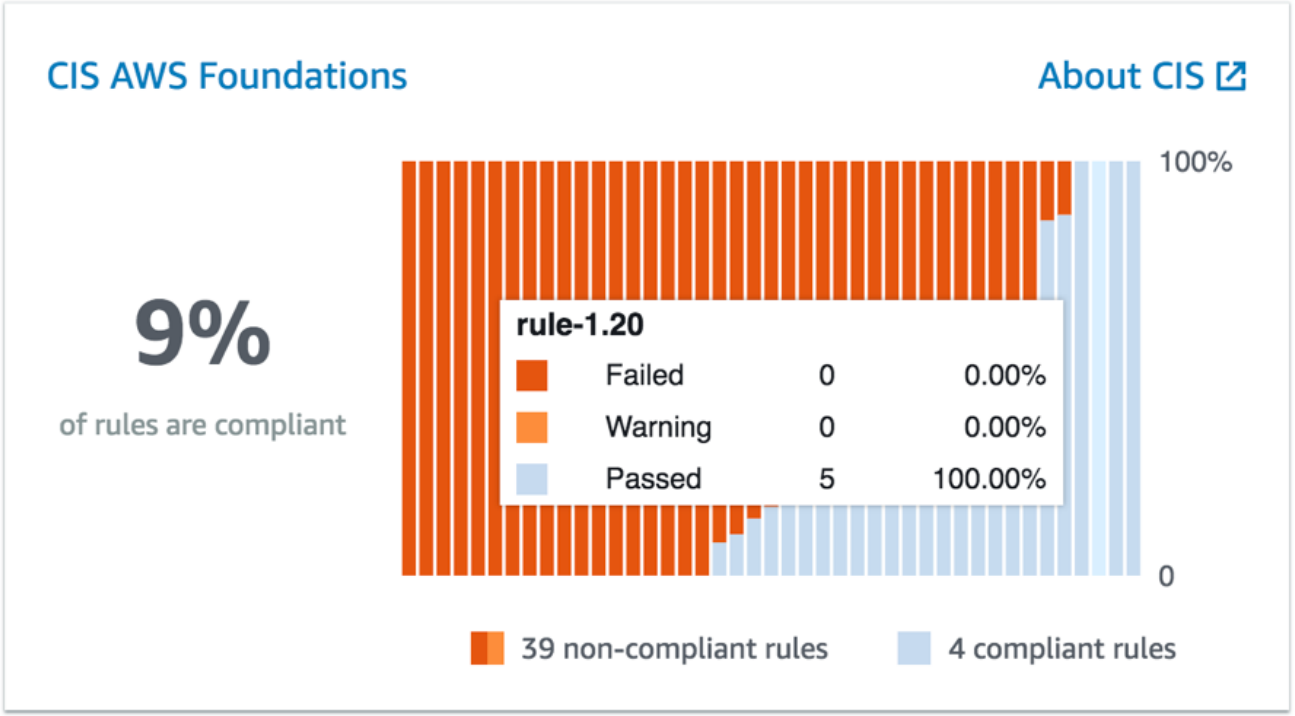


Understand your **security** and **compliance** state

AWS Security Hub: Automated Assessment Versus Standards

CIS Center for Internet Security®

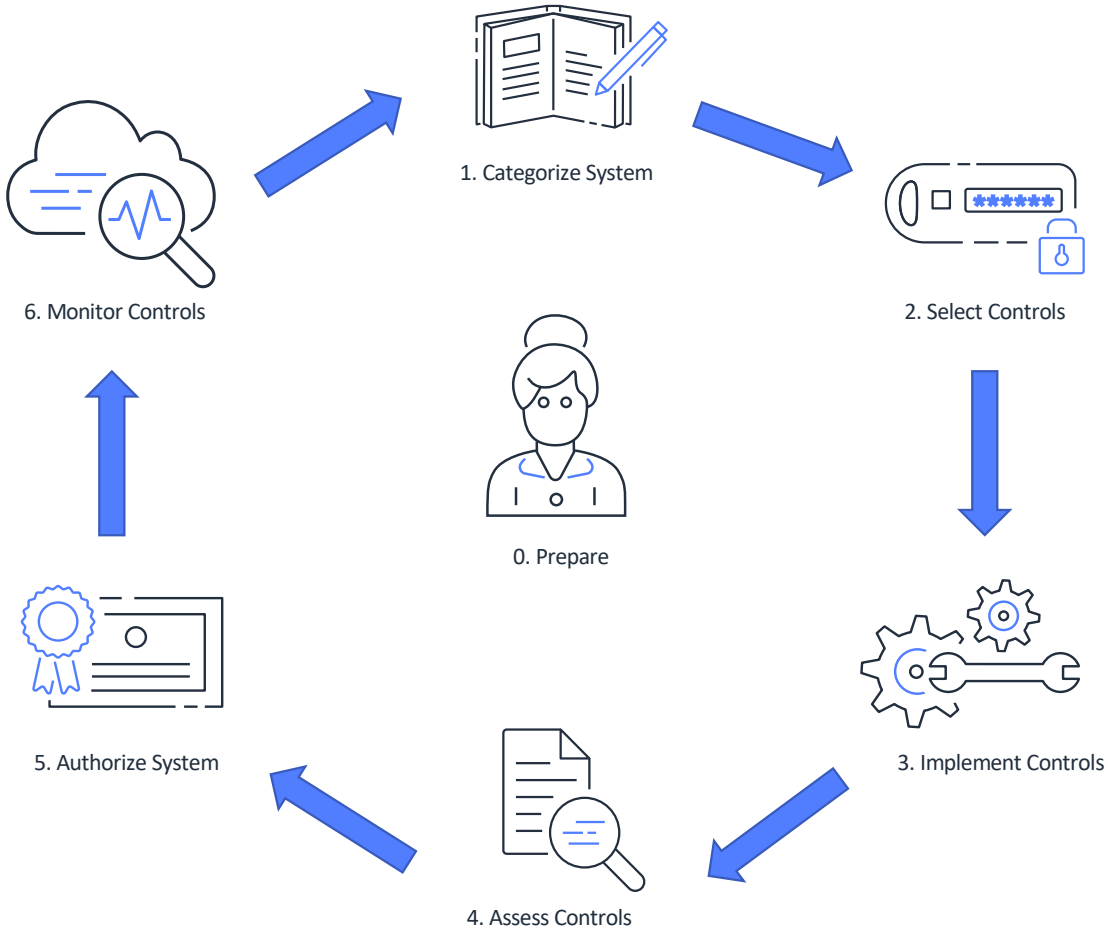
43 fully automated, nearly continuous checks



Cloud Risk Management Framework

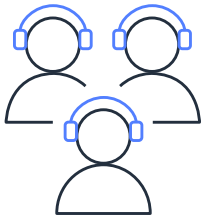
“How do I manage my risk in the cloud?”

A Risk Management Framework (NIST 800-37)



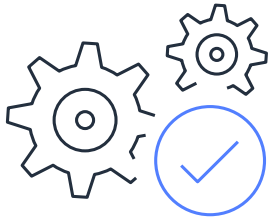
0. Prepare

The purpose of the ***Prepare*** step is to carry out essential activities at the organization and line of business levels to help prepare the organization to manage its security and privacy risks using the *Risk Management Framework*.



Roles and Responsibilities are assigned for security risk and compliance

A cloud security standard is created to dictate cloud usage



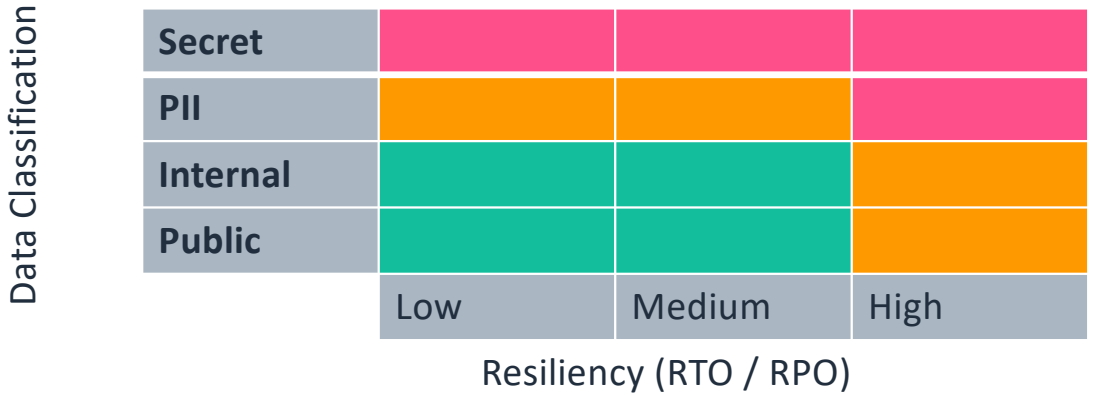
Common controls are identified, documented, and published.

An organization-wide strategy for monitoring control effectiveness is developed and implemented

1. Categorize System

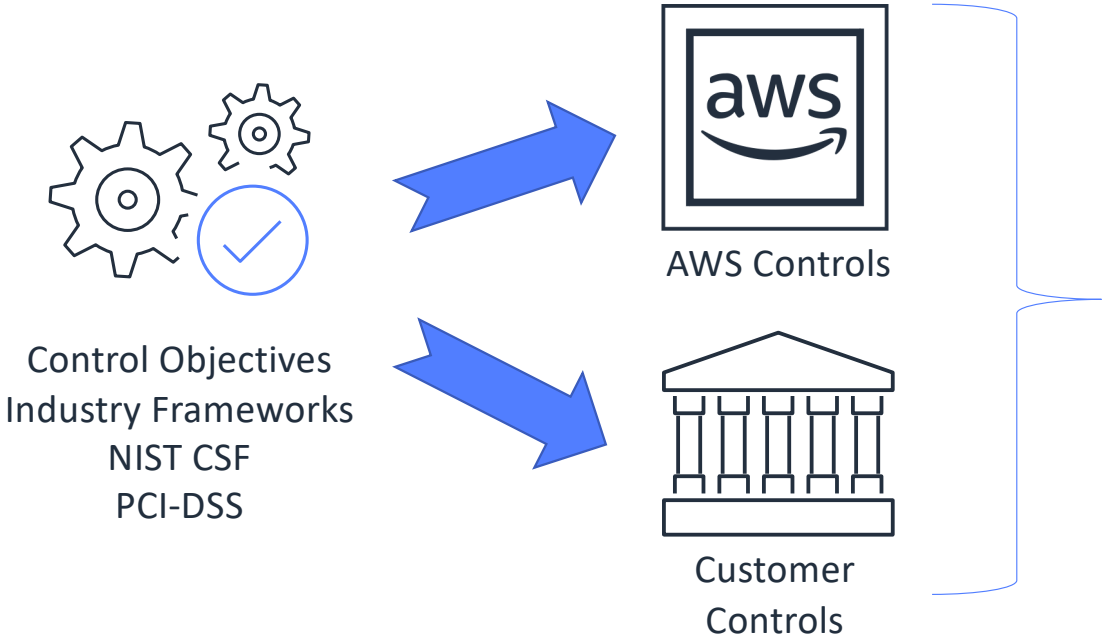
The purpose of the ***Categorize*** step is to inform risk management processes by determining the adverse impact to the with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

A security categorization of the system, including the information processed by the system represented by the organization- identified information types, is completed.

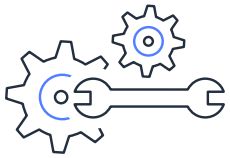


2. Select Controls

The purpose of the ***Select*** step is to select and document the controls necessary to protect the system commensurate with risk to the organization.

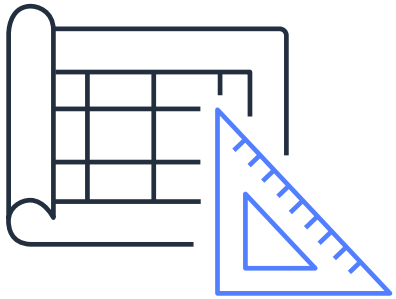


3. Implement Controls

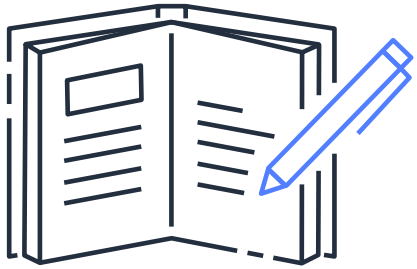


The purpose of the ***Implement*** step is to implement the controls selected for the system.

Controls specified in the security plan are implemented



Automated secure patterns are used where possible



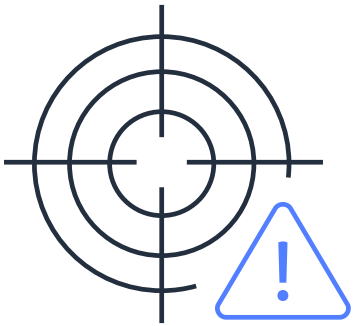
Cloud security policy updated with any learnings

4. Assess Controls

The purpose of the ***Assess*** step is to determine if the controls selected for implementation are implemented correctly and operating as intended.

AWS Well Architected

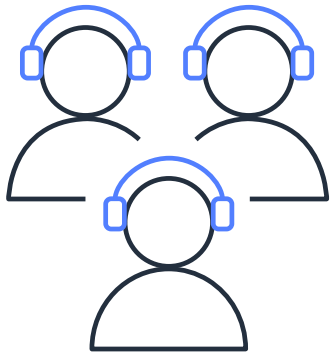
Continuous Compliance



Penetration Testing

5. Authorize System

The purpose of the ***Authorize*** step is to provide accountability by requiring a authorizing official to determine if the security risk to the organization based on the operation of a system is acceptable.



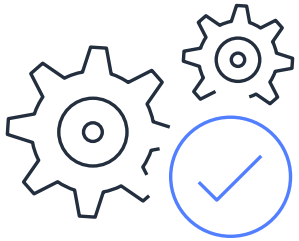
The authorizing official or authorizing process is clearly defined and established

The authorizing official or authorizing process is supplied with the authorization package, a risk decision is rendered.

6. Monitor Controls

The purpose of the ***Monitor*** step is to maintain an ongoing situational awareness about the security posture of the information system in support of risk management decisions.

The information system and changes are monitored in accordance with the organizations continuous monitoring strategy

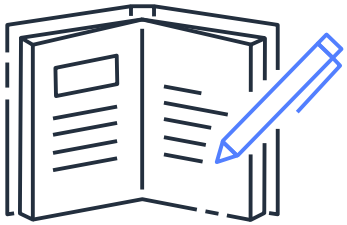


Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy

The output of the continuous monitoring activities is analyzed and responded to appropriately.

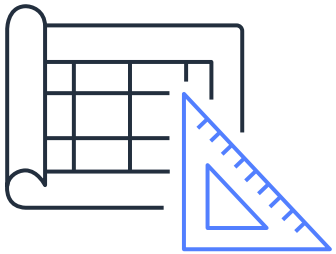
Conclusion

Call to Action: Next Steps



Create a Cloud Security Policy

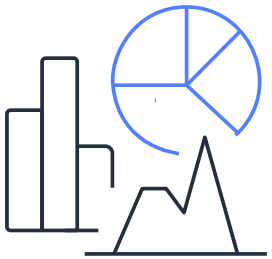
Perform AWS Service Due-Diligence



Create Automated Secure Patterns

Perform Security Assessments

Develop a Continuous Compliance Program



Establish a Cloud Risk Management Framework

Thank you!