
AWS
re:Invent

SEC402

Trusted connects for government workloads

Brad Dispensa

Pr. Security and Compliance Specialist SA, WWPS

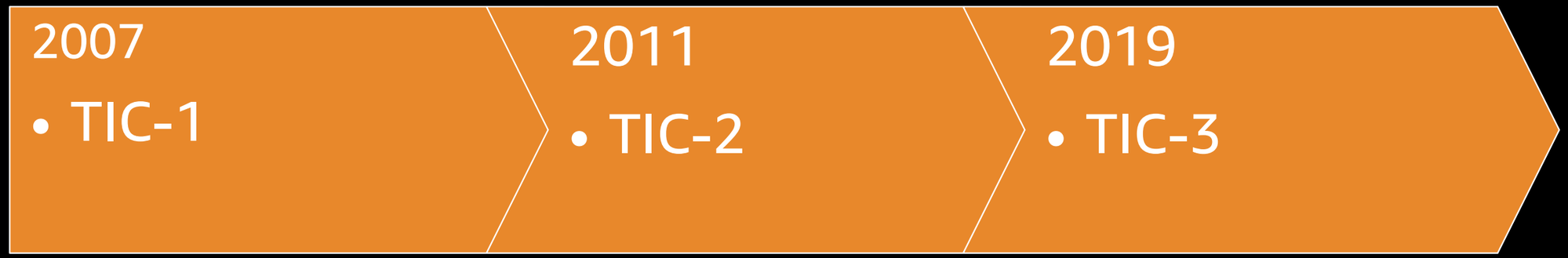
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is TIC?

Cybersecurity & Infrastructure Security Agency



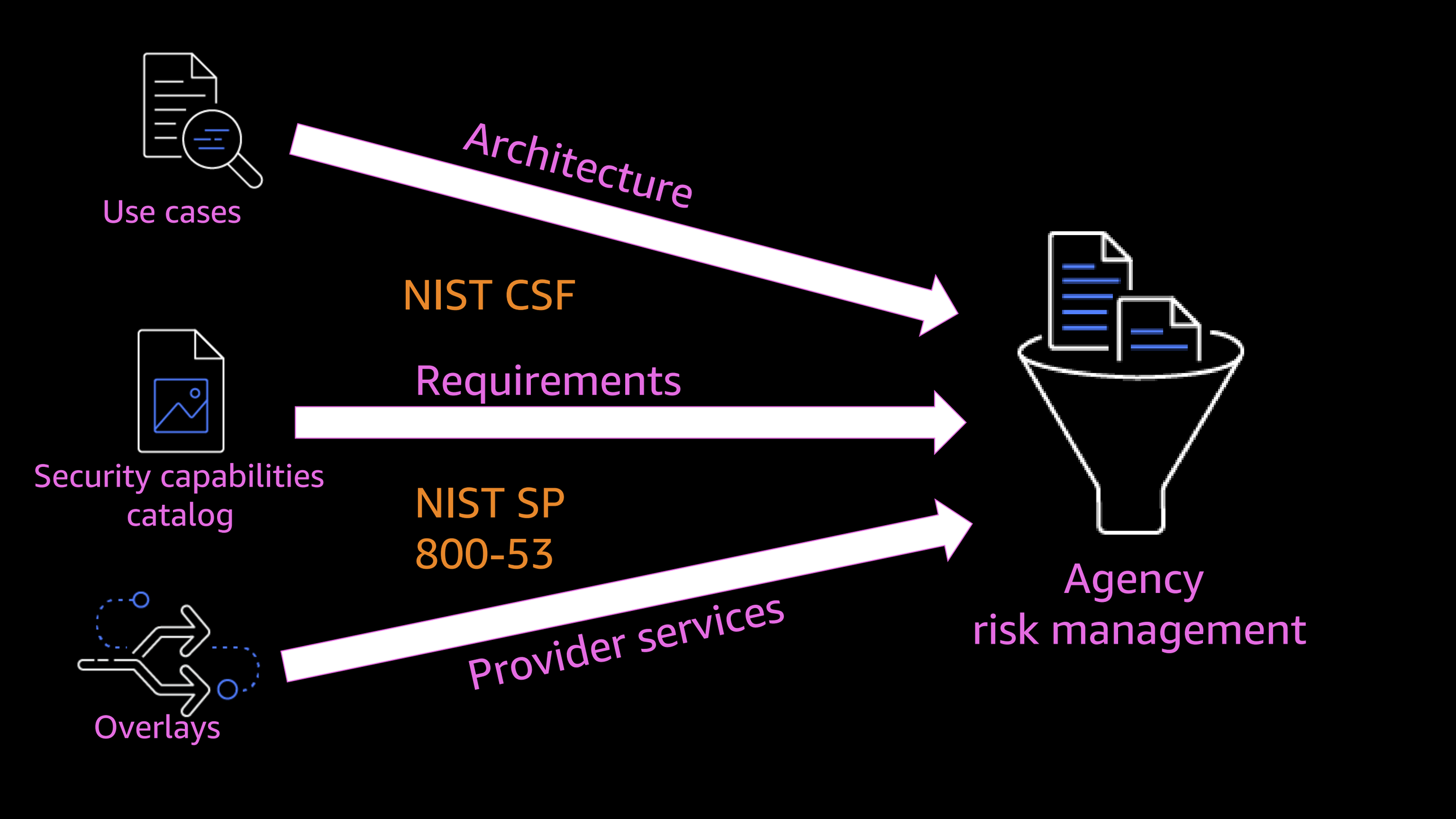
So, what's the difference?



Wait, where are the controls??



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Use cases
Architecture
NIST CSF
Security capabilities catalog
Requirements
NIST SP 800-53
Overlays
Provider services
Agency risk management

So, how do I develop for compliance?

Security objectives

Objective	Description
Manage traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny
Protect traffic confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement
Protect traffic integrity	Prevent alteration of data in transit; detect altered data in transit
Ensure service resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscapes evolve
Ensure effective response	Promote timely reaction and adapt future response to discovered threats; policies define and implemented; simplified adoption of new countermeasures

Source: *TIC 3.0 Security Capabilities Handbook*, 3–4, www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

Example:

Security objective solutions[1]

Objective	AWS solution	Draft solution
Manage traffic	Amazon VPC Flow Logs, security groups, AWS Network Firewall	Log delivery of filtered inbound external IP deny
Ensure effective response	Lambda	Event-driven automation

1 – *TIC 3.0 Security Capabilities Handbook*, 3, www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

Example:

Universal security capabilities[1]

Objective	AWS solution	Draft solution
Backup and recovery	AWS Config, CloudTrail logs	Centralized log delivery, AWS Config log data for resources
Least privilege	IAM Access Analyzer, AWS Config	Automated policy scans, alerting for external role access

1 – *TIC 3.0 Security Capabilities Handbook*, 6, www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

Example:

Universal security capabilities[1]

Objective	AWS solution	Draft solution
Inventory	AWS Config, Systems Manager	Gather inventory on premises and on AWS using SSM
Central log management with analysis	S3, CloudTrail, Amazon ES	Log storage in S3, analysis with Amazon ES

1 – *TIC 3.0 Security Capabilities Handbook*, 6, www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

Example:

Policy enforcement point capabilities[1]

Objective	AWS solution	Draft solution
DDoS protections	AWS Shield, AWS WAF	Deployment of Shield and AWS WAF rules
DNS sinkholing	AWS Network Firewall	Deployment of DNS deny lists

1 – *TIC 3.0 Security Capabilities Handbook*, 13, www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

Example:

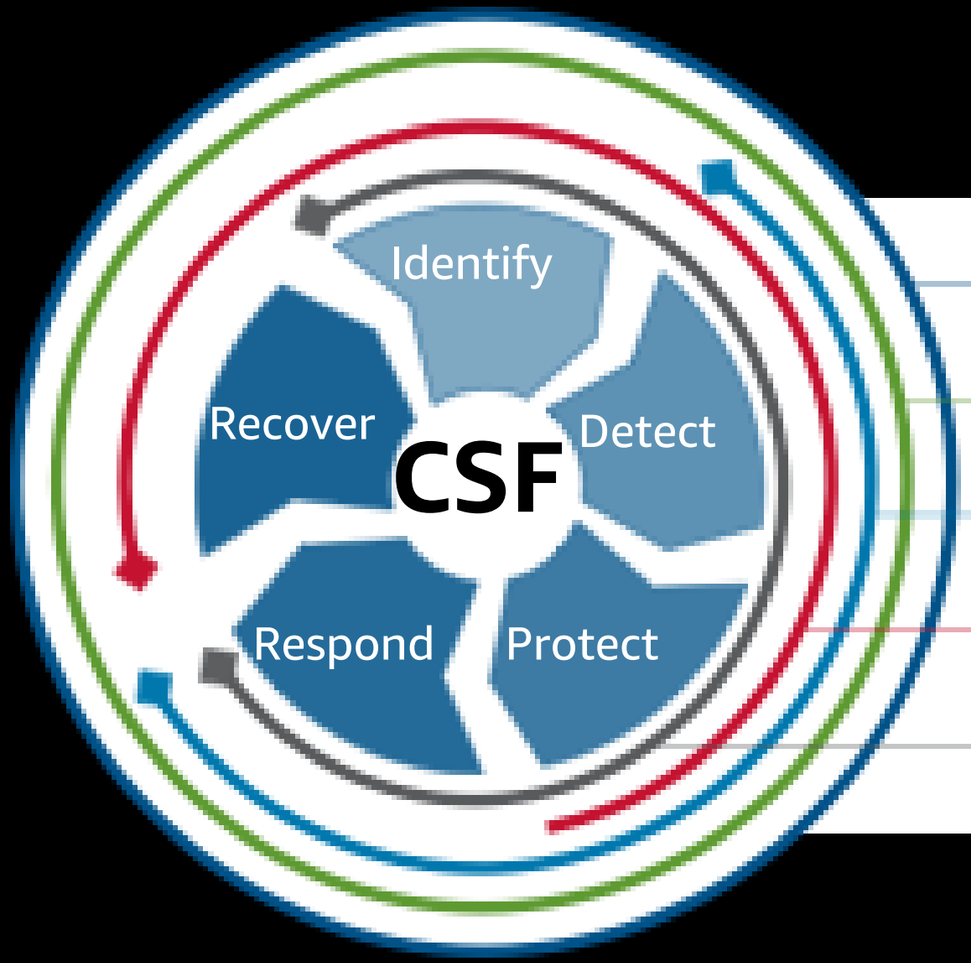
Policy enforcement point capabilities[1]

Objective	AWS solution	Draft solution
Dynamic threat discovery	Amazon GuardDuty, AWS Security Hub, Amazon Detective	Enable GuardDuty and review findings
Patch management	AWS Systems Manager	Deployment patch baselines

1 – *TIC 3.0 Security Capabilities Handbook*, 13, www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

Trust zones


High trust zone examples
• CSP environments
• Agency internal network
• Branch office
Medium trust zone examples
• CSP environments
• External partner
• Branch office
Low trust zone examples
• CSP environments
• Open internet
• Research network
• External partner

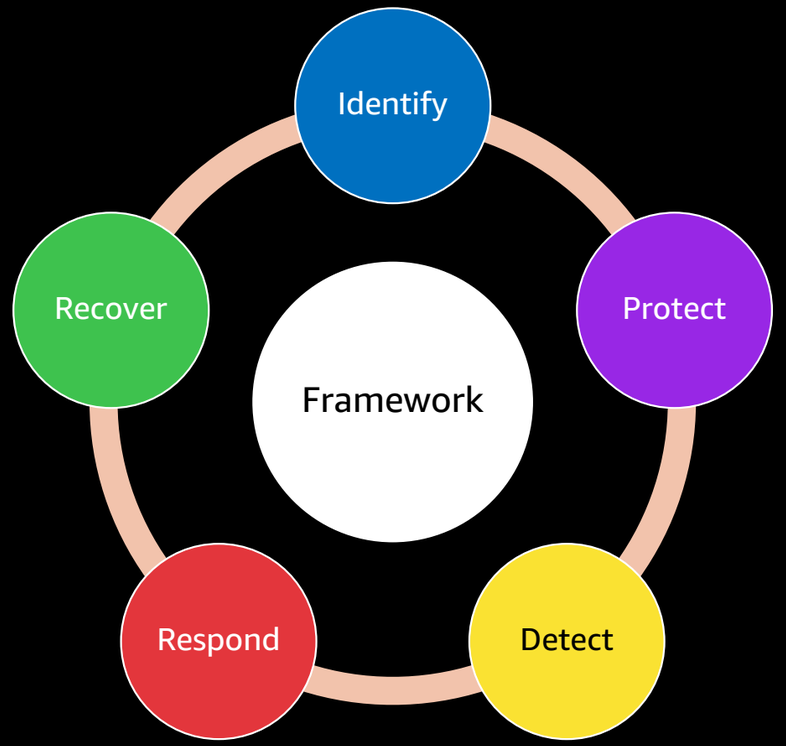


TIC objectives

- Manage traffic
- Protect traffic confidentiality
- Protect traffic integrity
- Ensure service resiliency
- Ensure effective response

NIST CSF

Identify	Protect	Detect	Respond	Recover
Asset management	Access control	Anomalies and events	Response planning	Recovery planning
Business environment	Awareness and training	Security continuous monitoring	Communications	Improvements
Governance	Data security	Detection processes	Analysis	Communications
Risk assessment	Information protection processes and procedures		Mitigation	
Risk assessment strategy	Maintenance		Improvements	
Supply chain risk management	Protective technology			



NIST CSF | Identify

Asset management (ID.AM)


AWS Management Console


AWS Identity and Access Management


AWS Systems Manager


AWS IoT Device Management


Inventory


Amazon Macie


AWS CodeCommit

Business environment (ID.BE)


Amazon CloudWatch


Event (event-based)


AWS Lambda


Lambda Function

Governance (ID.GV)


AWS Service Catalog


AWS Identity and Access Management


AWS CloudFormation


AWS Key Management Service


AWS Config


AWS Budgets


AWS OpsWorks


AWS Secrets Manager

Risk assessment (ID.RA)


Amazon Inspector


AWS X-Ray


Amazon GuardDuty

Risk management strategy (ID.RM)


Amazon CloudWatch


Event (event-based)


AWS Lambda


Lambda Function

Supply chain risk management (ID.SC)


Enterprise agreement


AWS Artifact


AWS Marketplace

NIST CSF | Protect

Identity management, authentication, and access control (PR.AC)

- AWS Identity and Access Management
- AWS Directory Service
- AWS Security Token Service (AWS STS)
- Amazon Cognito
- MFA token
- AWS Single Sign-On
- Role
- AWS Certificate Manager
- Permissions

Awareness and training (PR.AT)



AWS & partner online and classroom training



Data security (PR.DS)

- Amazon S3
- AWS Config
- Amazon S3 Glacier
- Amazon Macie
- AWS Key Management Service
- AWS Certificate Manager
- AWS CodePipeline
- AWS PrivateLink

Information protection processes and procedures (PR.IP)

- AWS Config
- AWS Service Catalog
- AWS CloudFormation
- AWS OpsWorks
- AWS Lambda
- AWS Storage Gateway
- Amazon Inspector
- AWS X-Ray

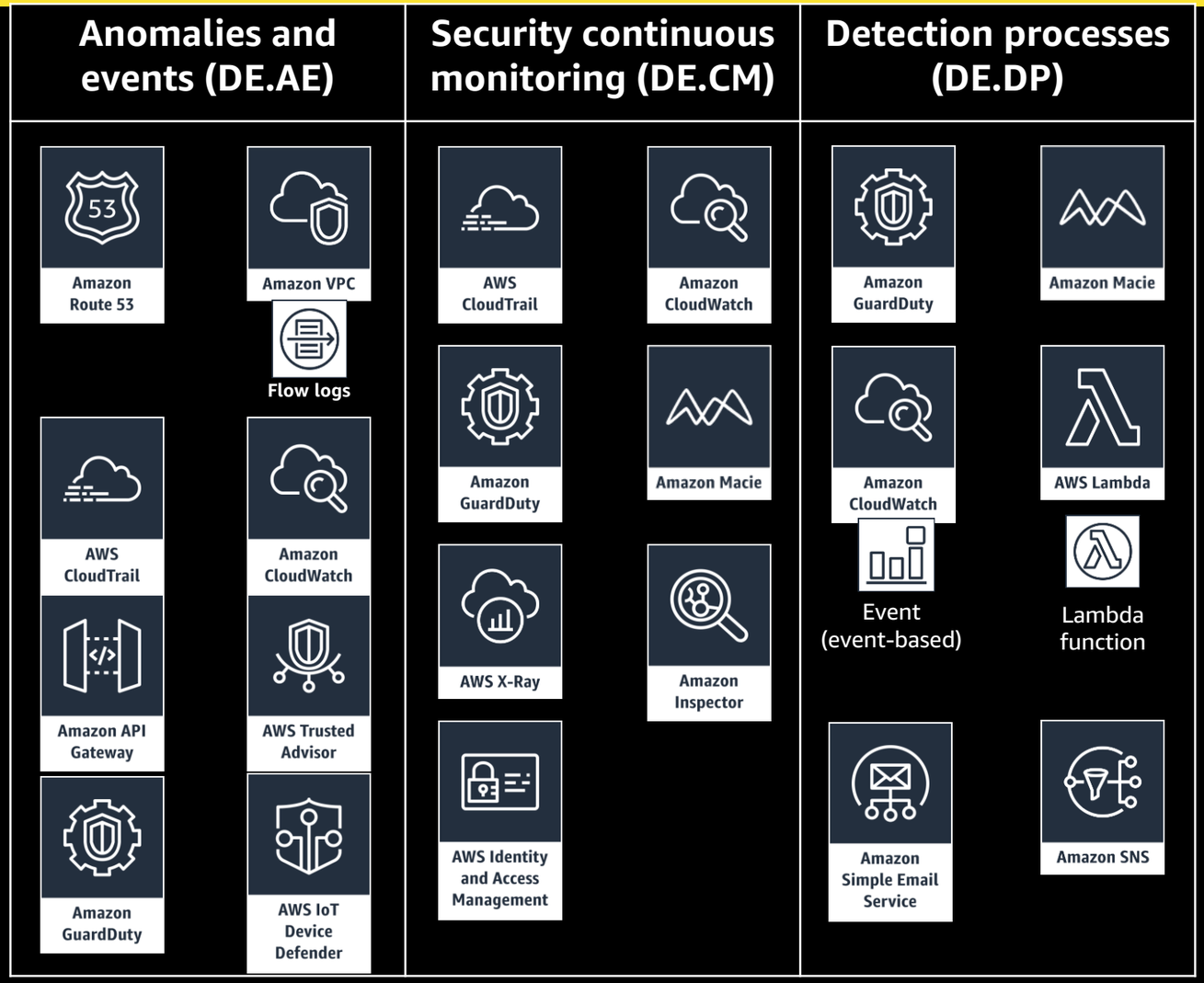
Maintenance (PR.MA)

- AWS Config
- AWS CloudTrail
- AWS Secrets Manager
- Amazon CloudWatch
- AWS OpsWorks
- AWS Managed Services
- AWS Command Line Interface
- AWS Identity and Access Management

Protective technology (PR.PT)

- AWS CloudTrail
- Amazon CloudWatch
- AWS Trusted Advisor
- Elastic Load Balancing
- Amazon GuardDuty
- AWS Application Auto Scaling
- AWS WAF
- Availability Zones

NIST CSF | Detection



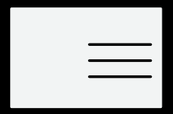
NIST CSF | Respond

Response planning (RS.RP)	Communications (RS.CO)	Analysis (RS.AN)	Mitigation (RS.MI)	Improvements (RS.IM)
AWS Config Amazon GuardDuty Amazon CloudWatch AWS Lambda AWS ProServ Zipline AWS Partners	Amazon Simple Email Service Amazon SNS AWS Lambda Amazon SQS Amazon Connect Amazon Pinpoint Amazon QuickSight Amazon Chime	Amazon GuardDuty Amazon Macie Amazon CloudSearch AWS Data Pipeline Amazon QuickSight Amazon SageMaker Amazon Elasticsearch Service Amazon Athena	Amazon GuardDuty AWS Lambda AWS WAF Filtering rule AWS Config Rule Subnet 172.16.0.0 172.16.1.0 172.16.2.0 ACL	Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities AWS service configurations and security automation are updated / improved

NIST CSF | Recover

Recovery planning (RC.RP)	Improvements (RC.IM)	Communications (RC.CO)
  	Organizational recover activities are improved by incorporating lessons learned from current and previous detection and response activities AWS service configurations and security automation are updated / improved	       

AWS security solutions



Identity and access management

AWS Identity and Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Secrets Manager

AWS Resource Access Manager



Detective controls

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

Amazon VPC Flow Logs



Infrastructure protection

AWS Systems Manager

AWS Shield

AWS WAF – Web application firewall

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (Amazon VPC)

AWS Network Firewall



Data protection

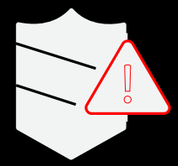
AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS Certificate Manager (ACM)

Amazon Macie

Server-side encryption



Incident response

AWS Config rules

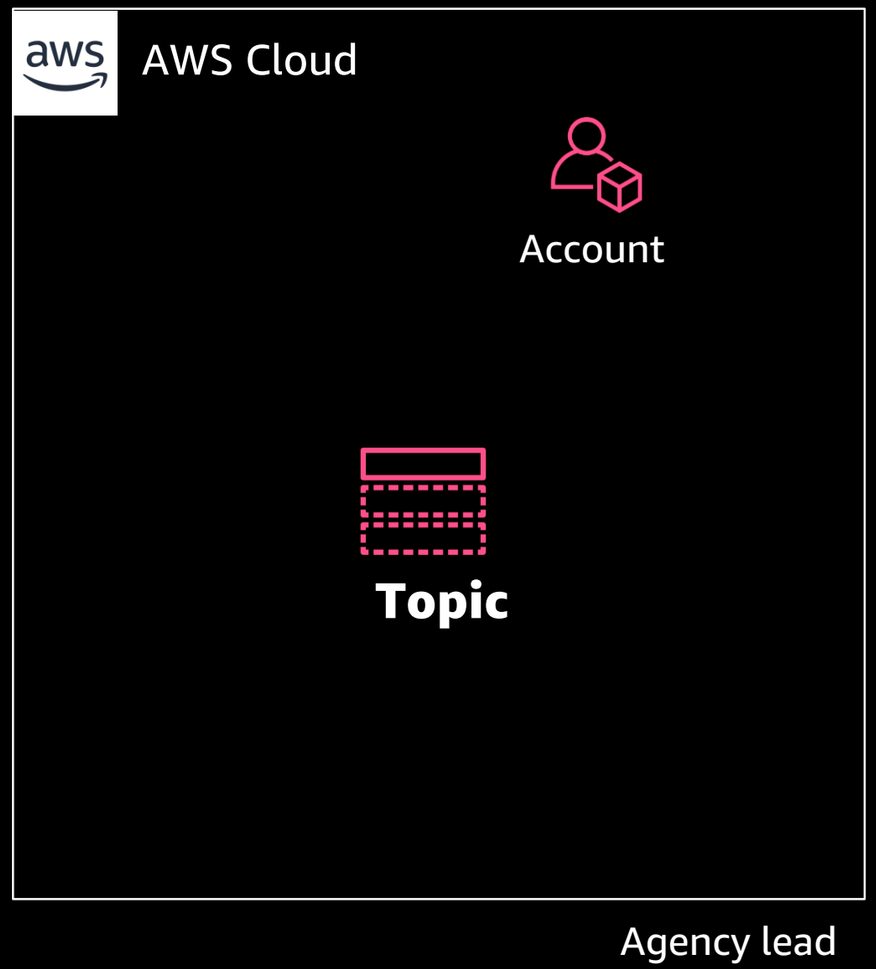
AWS Lambda

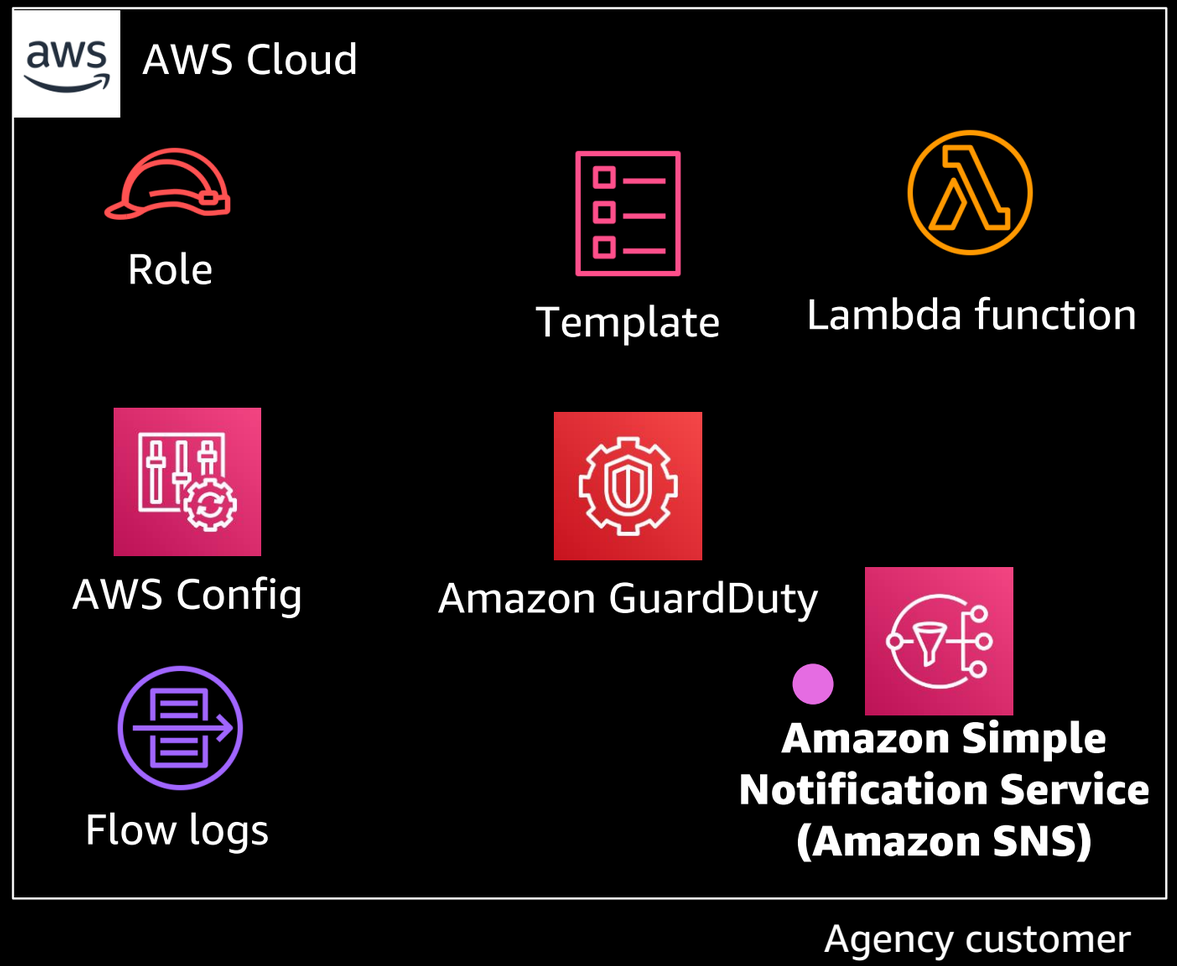
Compliance as code



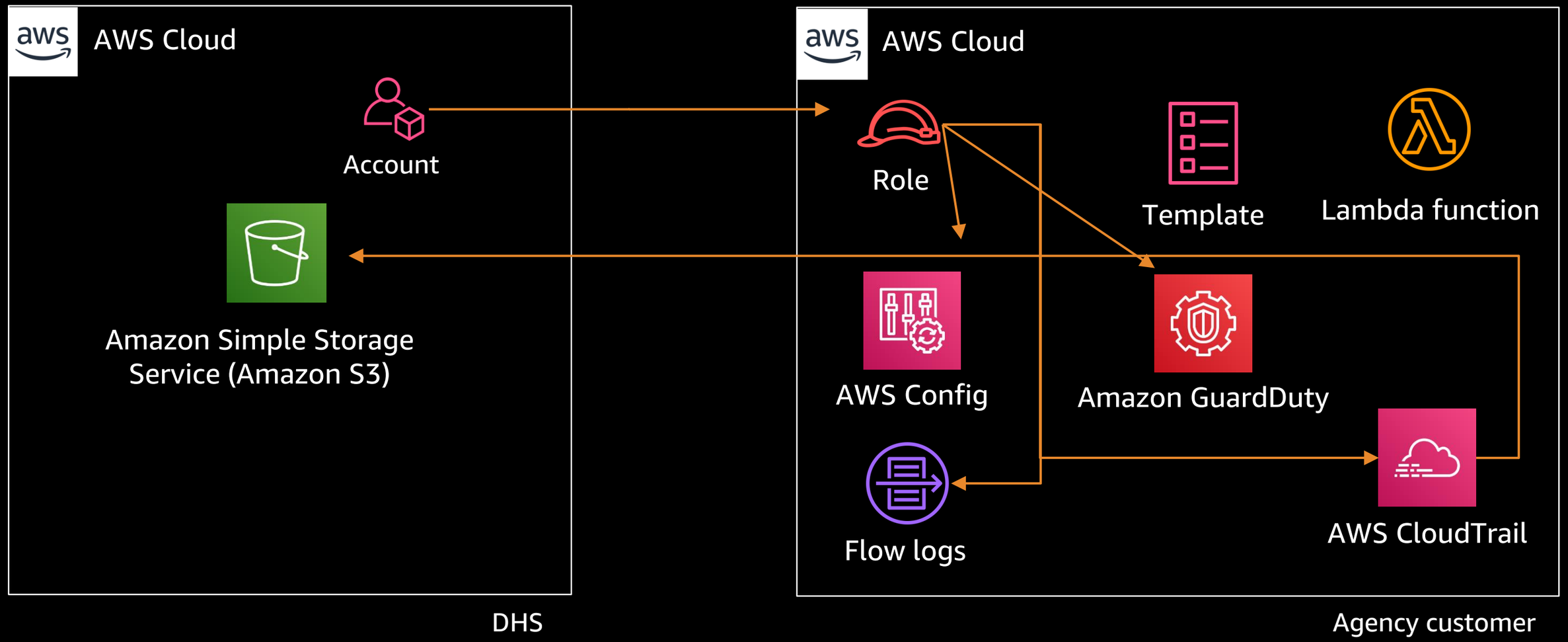
- Audit role
  - Read-only access to logs
- Approved checks
  - Pre-populated rules
- Pub / Sub lists
  - URL deny list
  - IP deny list
- Pre-made compliance checks
  - e.g., enable these to comply with PEP X

TIC 3 – Agency

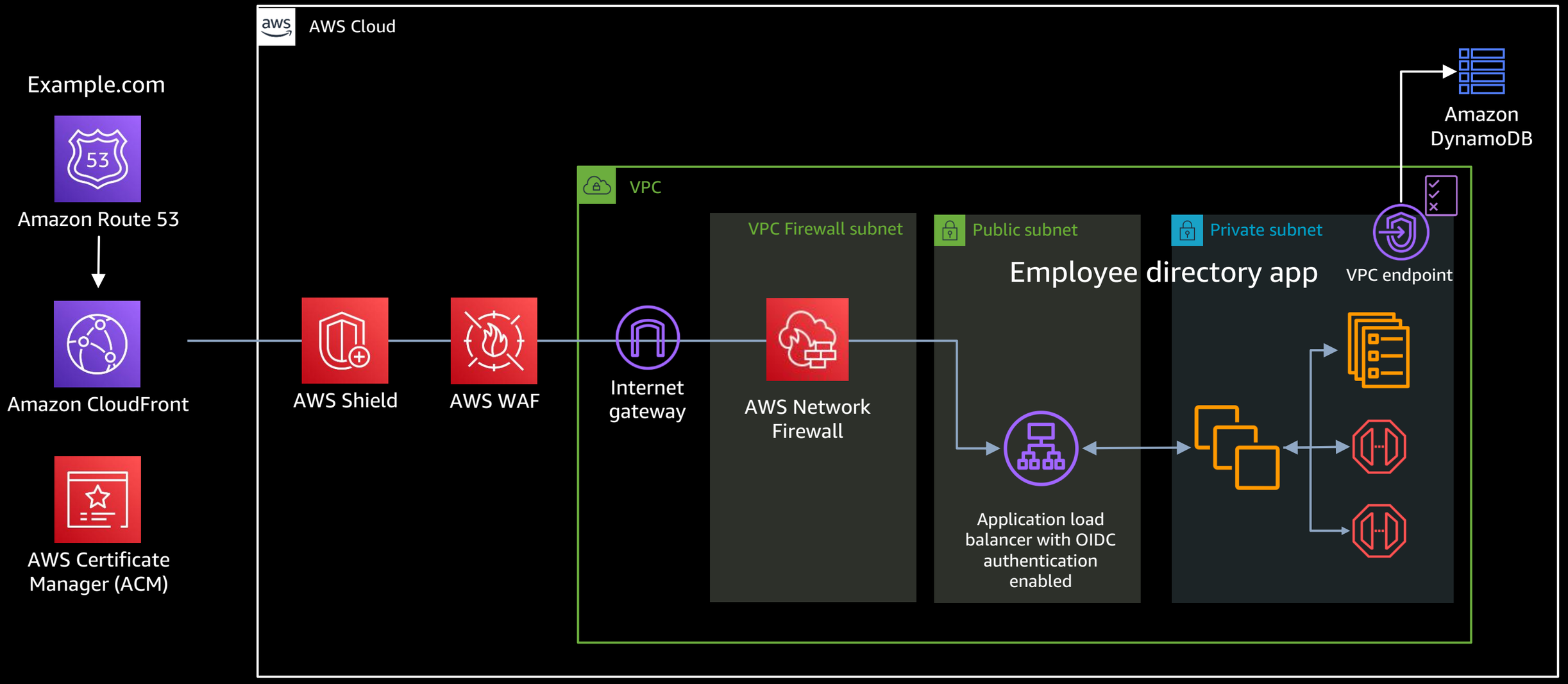

AWS Cloud
Account
Topic
Agency lead


AWS Cloud
Role
Template
Lambda function
AWS Config
Amazon GuardDuty
Flow logs
Amazon Simple Notification Service (Amazon SNS)
Agency customer

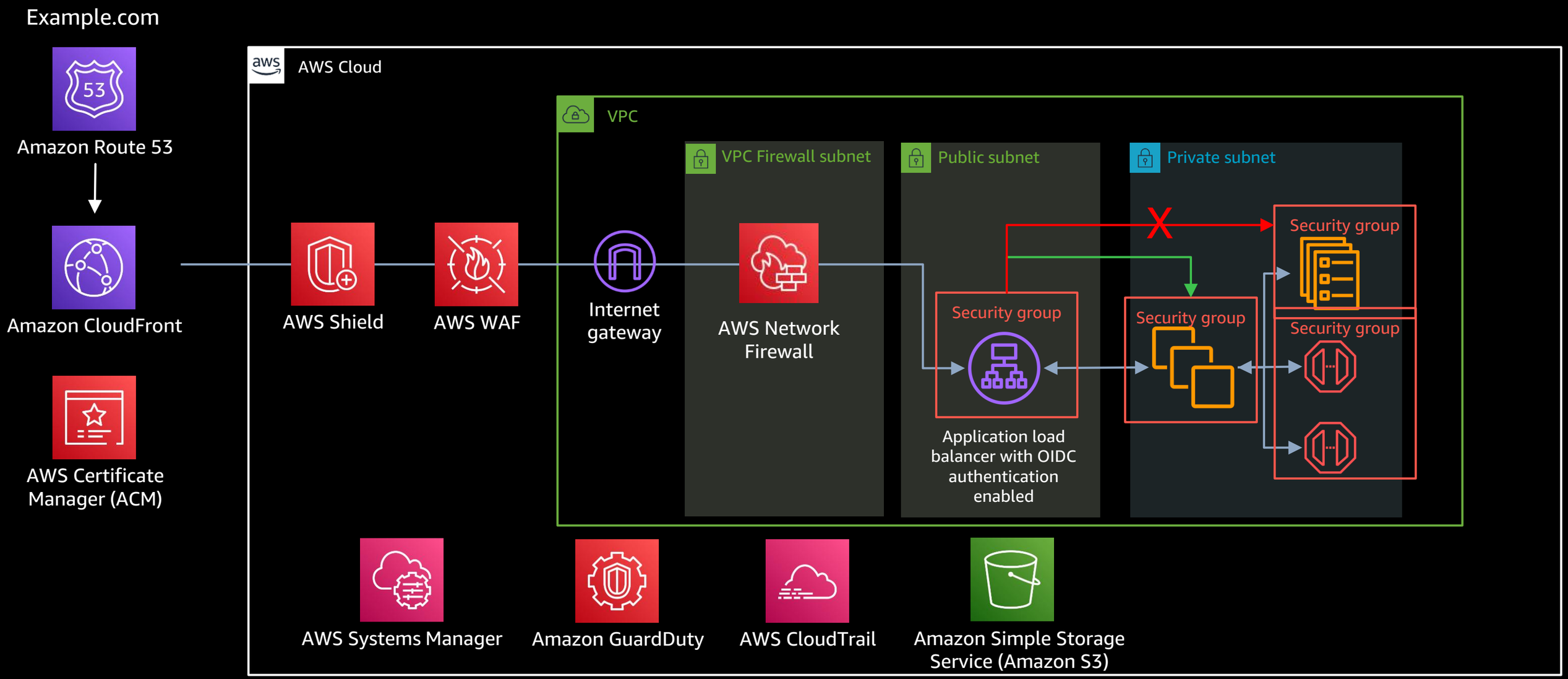
TIC 3 – CLAW


AWS Cloud
Account
Amazon Simple Storage Service (Amazon S3)
DHS
AWS Cloud
Role
Template
Lambda function
AWS Config
Amazon GuardDuty
Flow logs
AWS CloudTrail
Agency customer

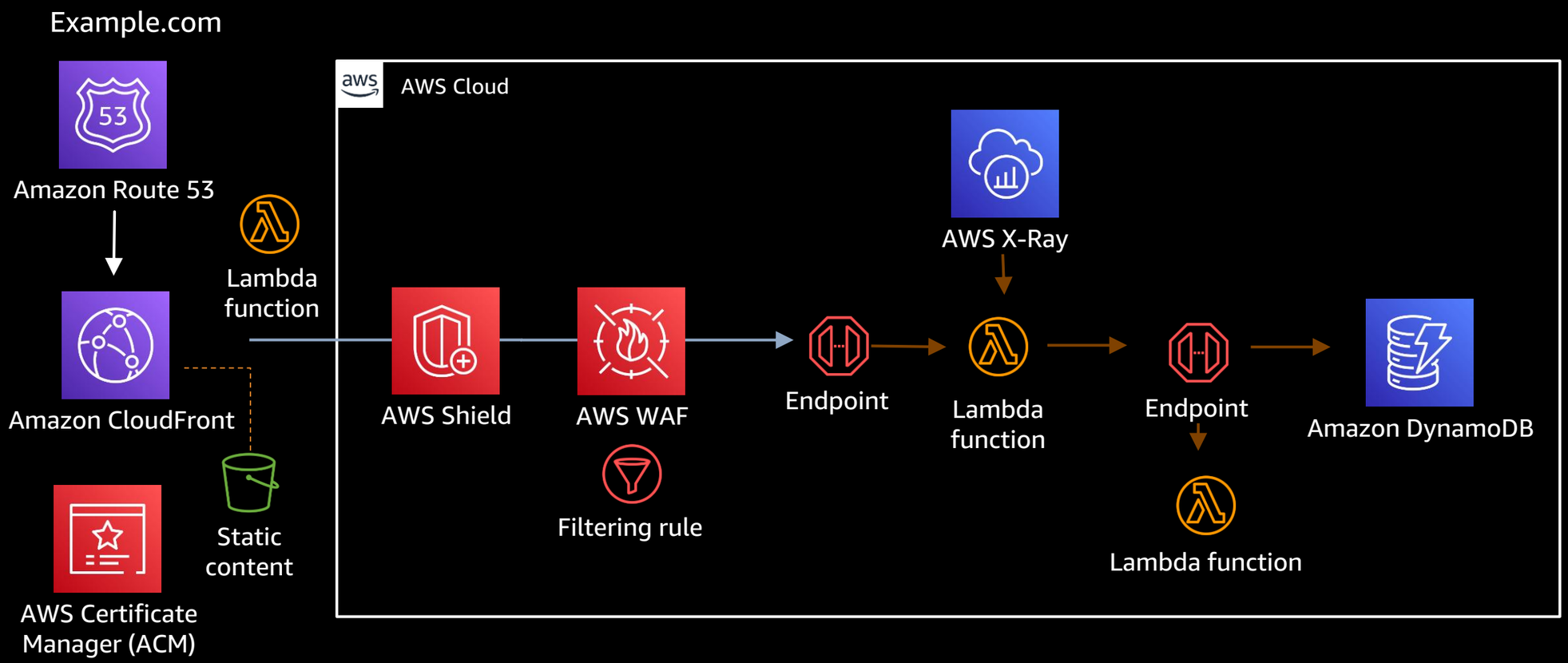
3-tier web application (generic)



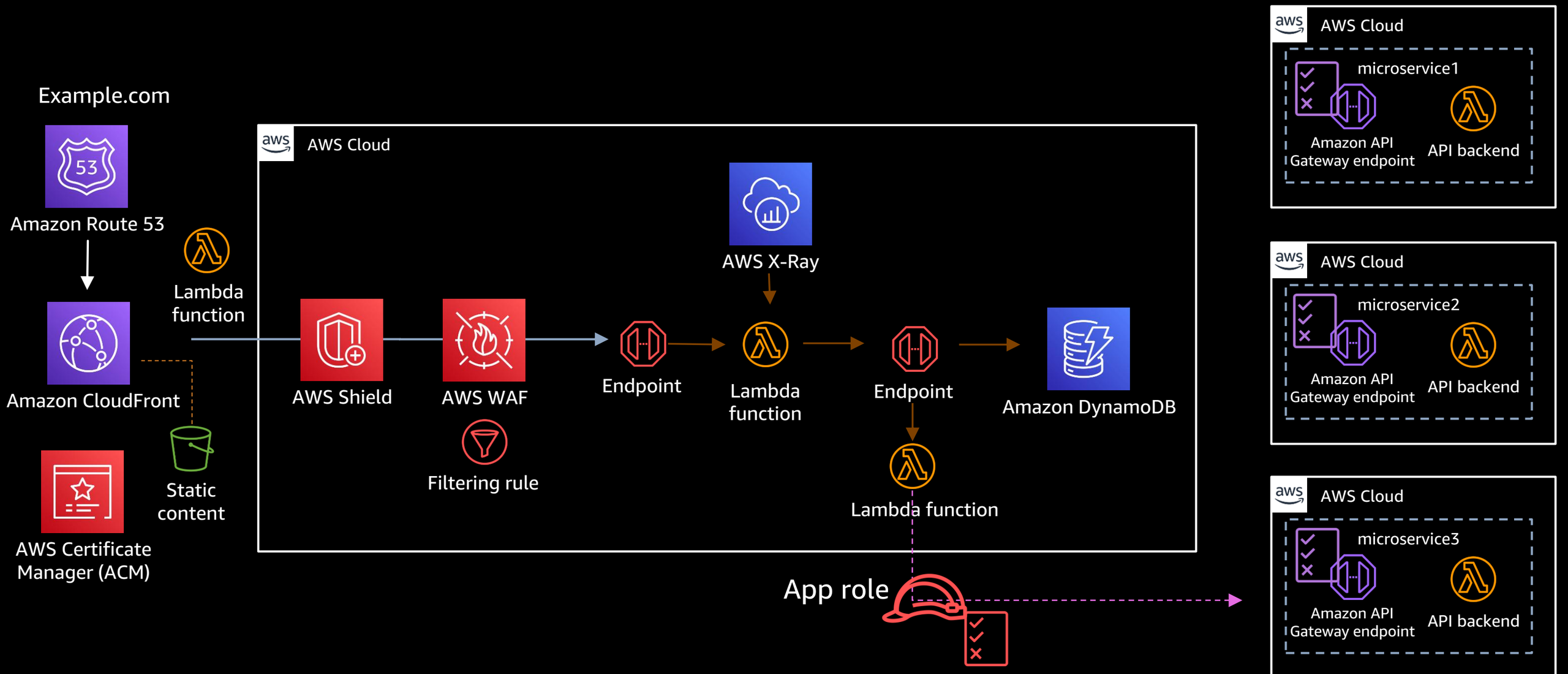
3-tier web application (generic)



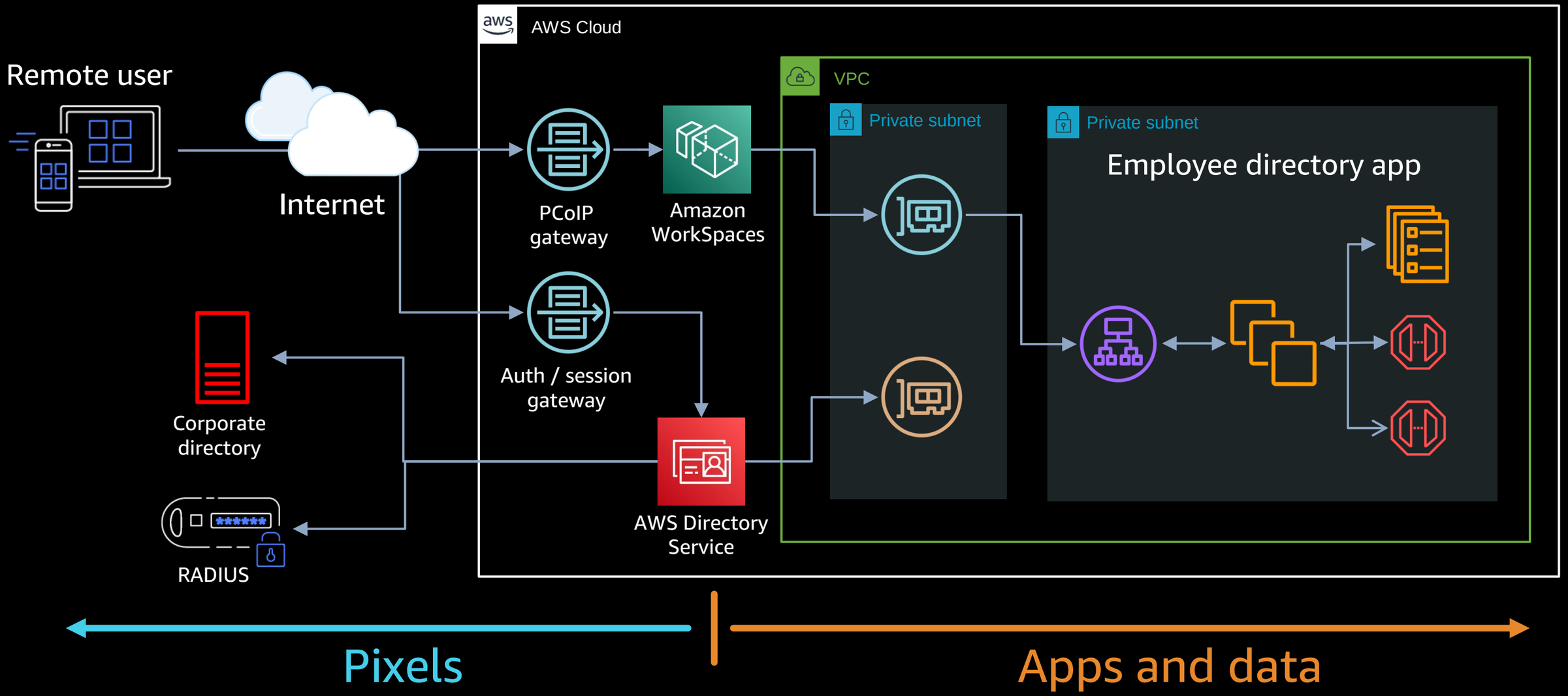
Serverless application



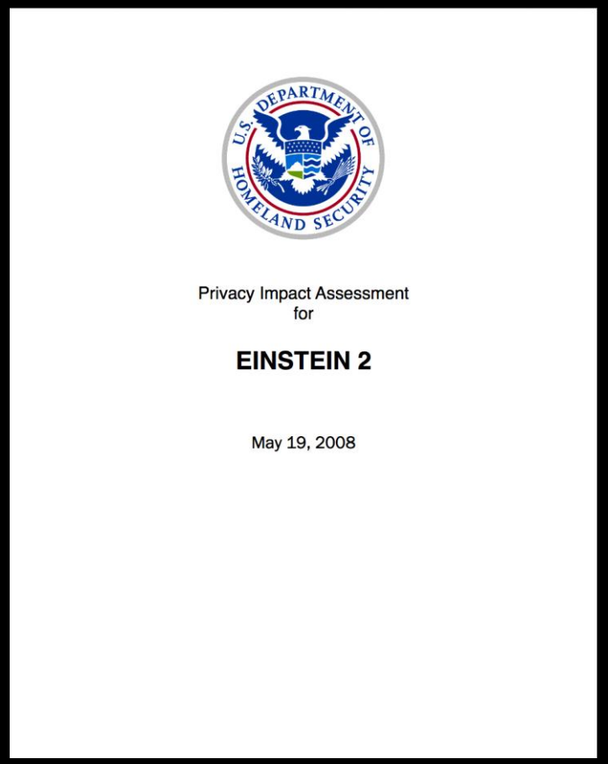
Serverless application

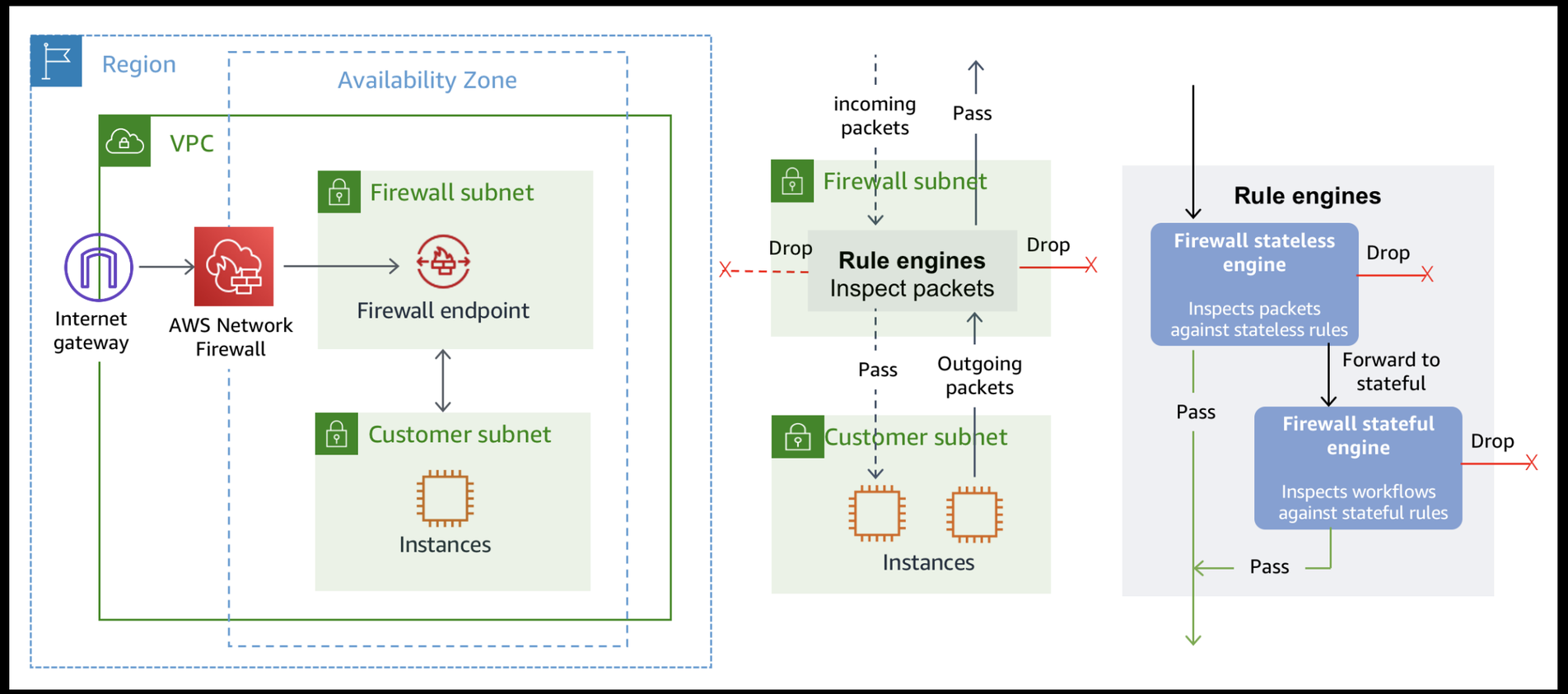


OMB-20-19


Remote user
Internet
AWS Cloud
VPC
Private subnet
Private subnet
Employee directory app
PCoIP gateway
Amazon WorkSpaces
Auth / session gateway
Corporate directory
AWS Directory Service
RADIUS
Pixels
Apps and data

AWS Network Firewall





Aligning to the NIST CSF in the AWS Cloud

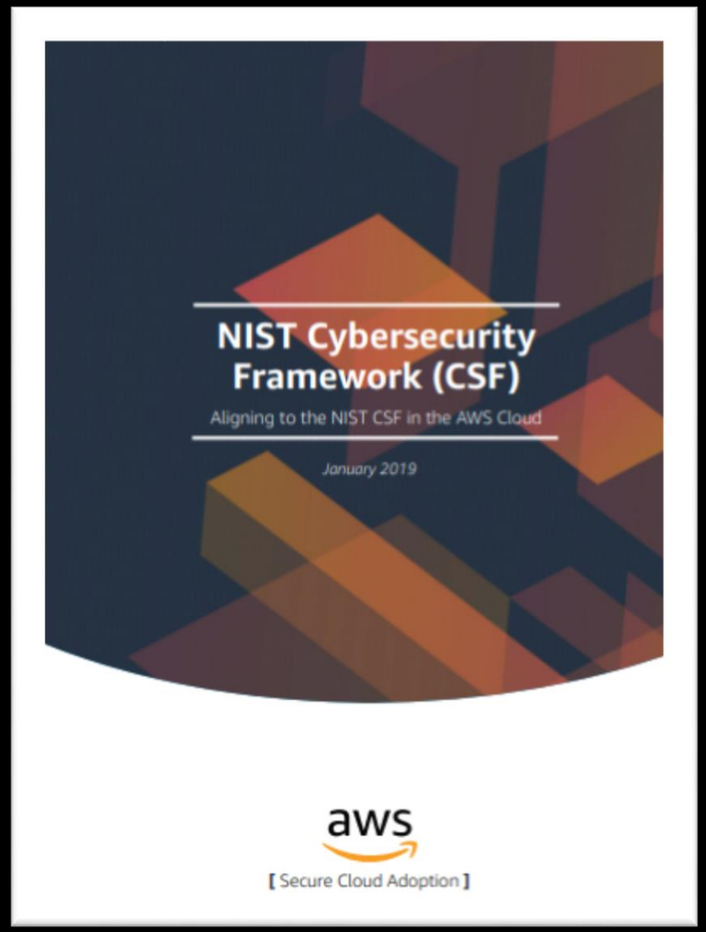
Two objectives with the whitepaper:

Security *of* the cloud

- Third-party attestation that AWS infrastructure and services conform to NIST CSF risk-management practices based on FedRAMP and ISO 27001 accreditations

Security *in* the cloud

- Detailed mapping of AWS services and resources (beyond FedRAMP and ISO 27001)
- Customer responsibilities
- AWS responsibilities



https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Session to watch: SEC303 – Zero Trust:
An AWS perspective



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.