AWS re:Invent

SEC349-R

Establishing cloud controls for financial institutions

Mignona Cote'
Sr. Practice Manager Security Assurance & Advisory
AWS Professional Services
Amazon Web Services

AWS re:Invent

aws

Agenda

- Policy management
- Regulatory readiness
- Control mapping
- Let’s build
- Key takeaways

Related breakouts

SEC349-R Establishing cloud controls for financial institutions

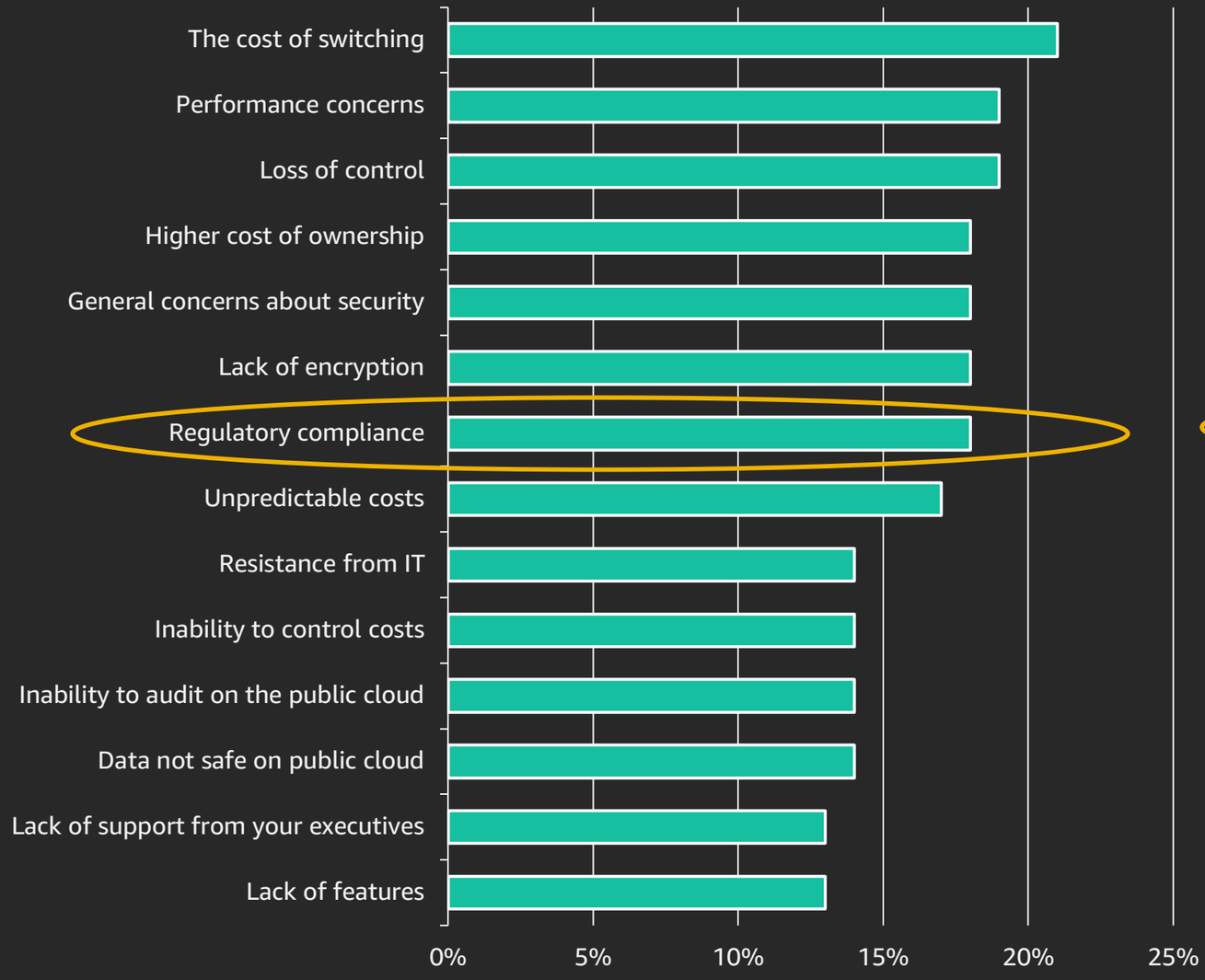
SEC349-R1 Establishing cloud controls for financial institutions

SEC349-R2 Establishing cloud controls for financial institutions

SEC349-R3 Establishing cloud controls for financial institutions

Policy management

Regulations are barriers to cloud adoption



Commonly cited potential barriers:

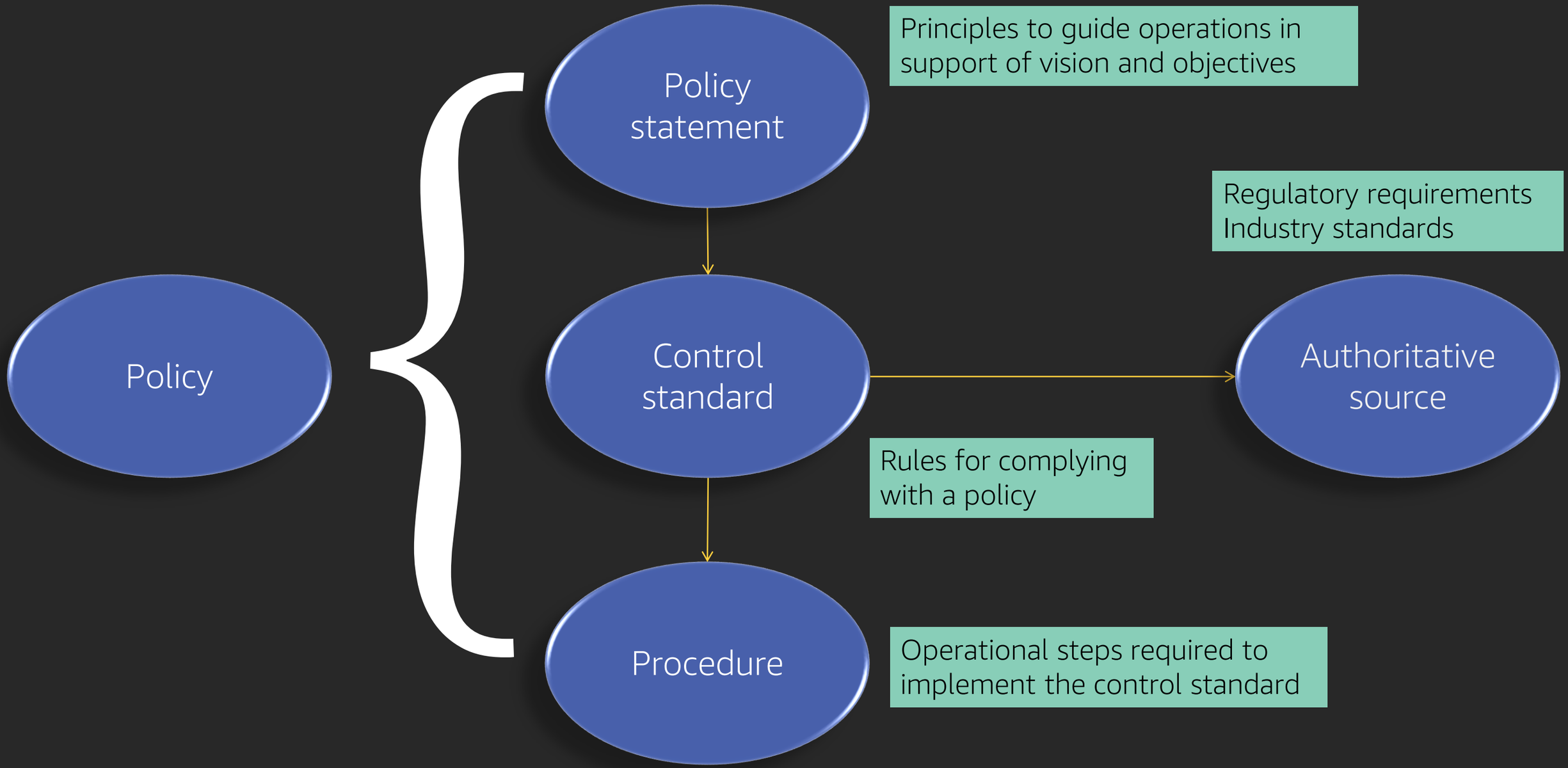
- The cost of switching (21%)
- Loss of control (19%)
- Performance concerns (19%)
- Regulatory compliance (18%)

Source: Q1 2017 global awareness, perception and purchase dynamics report – US Financial Services Industry, AWS Customer Research

Policy examples for regulatory enterprises

Security Management	Security monitoring	Business resiliency	Application development
Risk management	Communications management	Compliance and regulatory	Operations management
Personnel security	Identity and access	IT management	Privacy
Physical security	Network security	Problem management	Third-party risk governance

Translating policy into actionable controls



Regulatory readiness

Regulatory objectives

The objectives of financial regulators are:

- Financial stability – contributing to the protection and enhancement of stability of the financial system

- Market integrity – to maintain confidence in the financial system

- Consumer protection – securing the appropriate degree of protection for consumers and prevent consumer harm

Regulatory readiness areas for review

Topic	Subject area	Description
Strategy / Governance	Cloud strategy	Is there a clearly defined and documented Cloud Strategy with Board approval?
	Governance framework and operating model	How established is the governance framework overseeing the Cloud Program and the operating model that will deliver it?
	Cloud pipeline	What is the cloud pipeline of projects, activities and events, especially material workloads.
Risk management	Risk framework	Is there a risk appetite with aligned controls and what levels of 2LoD, 3LoD, and other independent reviews have and will take place.
	Data protection and Management	What is the data migration strategy and how will you ensure data is adequately protected in the cloud?
	Business Continuity, Disaster Recovery and Exit plans	What plans are in place to cope with an outage of services to ensure continuity, especially for critical and customer facing services? Is there a clear exit strategy?
People	Senior Management Accountability	Are there clear roles and responsibilities as well as accountability for the Cloud Program that are well documented and understood?
	Capability	How are you ensuring the correct levels of capability at 1st, 2nd and 3rd lines of defense within your organization to accommodate your cloud strategy?

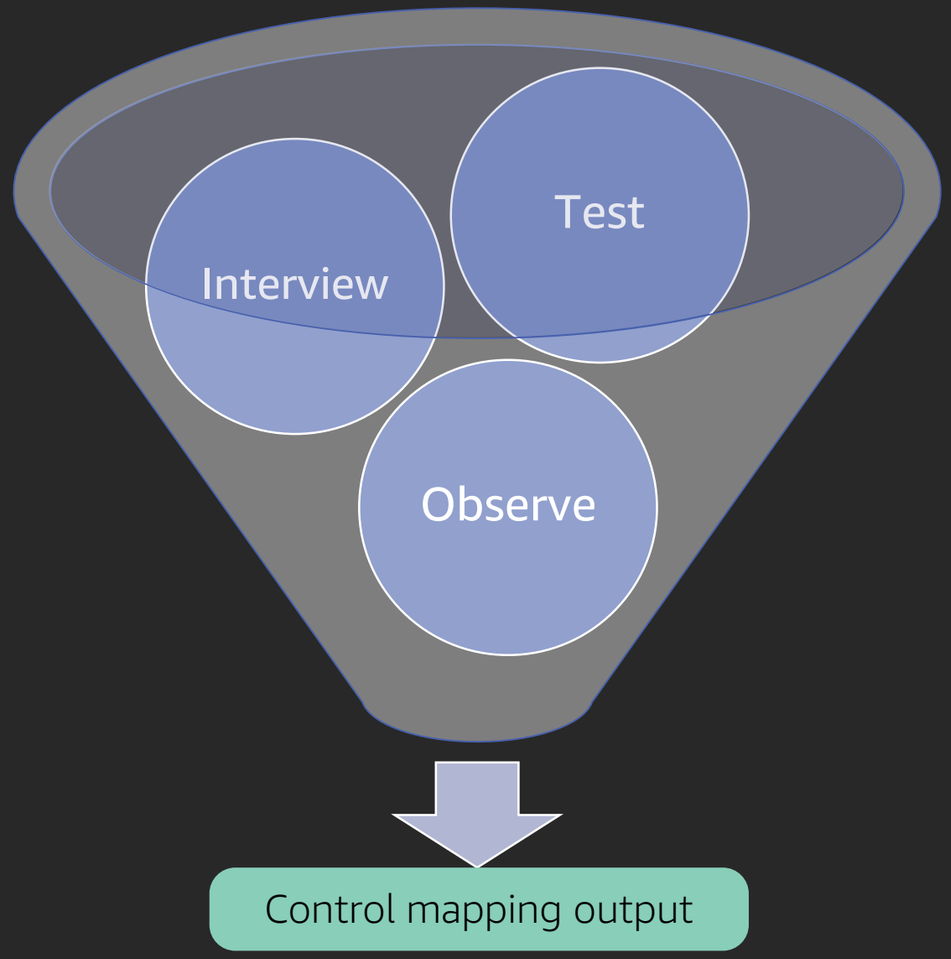
Control mapping

What is control mapping

Aligning frameworks, standards, regulation

Creating

Traceability from technical controls to business, risk, and compliance requirements



Control mapping

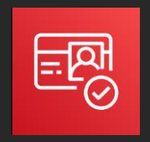
Control	Requirement	AWS Service	Monitoring
Ensure continued operations	Must have DR site	Use an alternate Availability Zone	Amazon CloudWatch
Data confidentiality	Encryption	Key Management Service	AWS CloudTrail
Only authorized users access data	Unique ID and password	IAM	AWS X-Ray

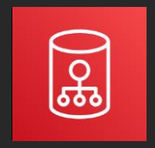
Control mapping and assessment areas

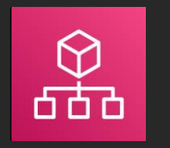
PCI	NIST CSF
12.1	ID.GV-1
12.8	IS.SC-1
12.2	ID.GV-4+
12.2	ID.RA-5
12.5.3+	PR.IP-9

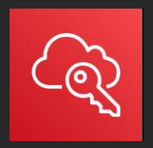
Identity


AWS IAM

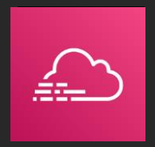

Amazon Cognito


AWS Directory Service


AWS Organizations


AWS SSO

Detective Controls


AWS CloudTrail


AWS Config


Amazon CloudWatch


Amazon GuardDuty


AWS X-Ray


Flow Logs

Infrastructure Security


Amazon Inspector


AWS Shield Advanced


Traffic Mirroring


Tag

Data Protection


Amazon Macie


AWS Trusted Advisor


AWS Security Hub

Incident Response

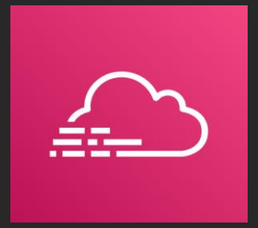

AWS Lambda


CloudWatch Alarm

Security control services

AWS Security Hub
A comprehensive view of high-priority security alerts and compliance status

Amazon GuardDuty
Intelligent threat detection and continuous monitoring for malicious activity and unauthorized behavior



AWS CloudTrail
Capture and log events related to API calls and account activity

Amazon Macie
A machine learning-powered security service to discover, classify, and protect sensitive data

AWS Config
Resource inventory, including configuration history and configuration change notification

Amazon CloudWatch
Monitoring and management service

AWS Trusted Advisor
Security configuration checks of your AWS environment

VPC Flow Logs
Log traffic flows at network interfaces in your Virtual Private Cloud (VPC)

Let’s build

AWS re:Invent

aws

Builder template

Control mapping worksheet

Business strategy:

IT strategy:

Security strategy:

Risk	Control	Requirement	AWS service	Monitoring	Control family

Key takeaways

- Enable customers to understand the controls incorporated in the AWS environment to manage risk and compliance in the Cloud
- Evaluate applicable controls that are required for regulatory compliance
- Assist our customers in implementing the controls in AWS
- Test the effectiveness of the control
- Enable customers to provide evidence based reporting for each control objective required by audit/regulator

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security

Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

Mignona Cote’

cotemign@amazon.com

Please complete the session survey in the mobile app.