
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

TATA CONSULTANCY SERVICES

SEC333

Designing compliance as a code with AWS security services

Raji Krishnamoorthy

Head, Security Platform Services
TCS

Karthik Thirugnanasambandam

Sr. Partner Solutions Architect
AWS

aws

Agenda

1. Challenges faced by organizations
2. Capabilities that AWS Cloud has
3. TCS approach to automating regulatory compliance
4. Sample customer scenario
5. Demo
6. Customer benefits

Challenges with regulatory compliance

On average, organizations must comply with

13 different IT security and privacy regulations

The greatest compliance challenge expected in 2022 is

volume and implementation of regulatory change

Source: THOMSON REUTERS

The cost of compliance

- Large organizations spend
  $700 per person
- Smaller organizations spend
  $2,000 per person

Average cost of noncompliance

exceeds **$14 million**

Source: SAVIYNT

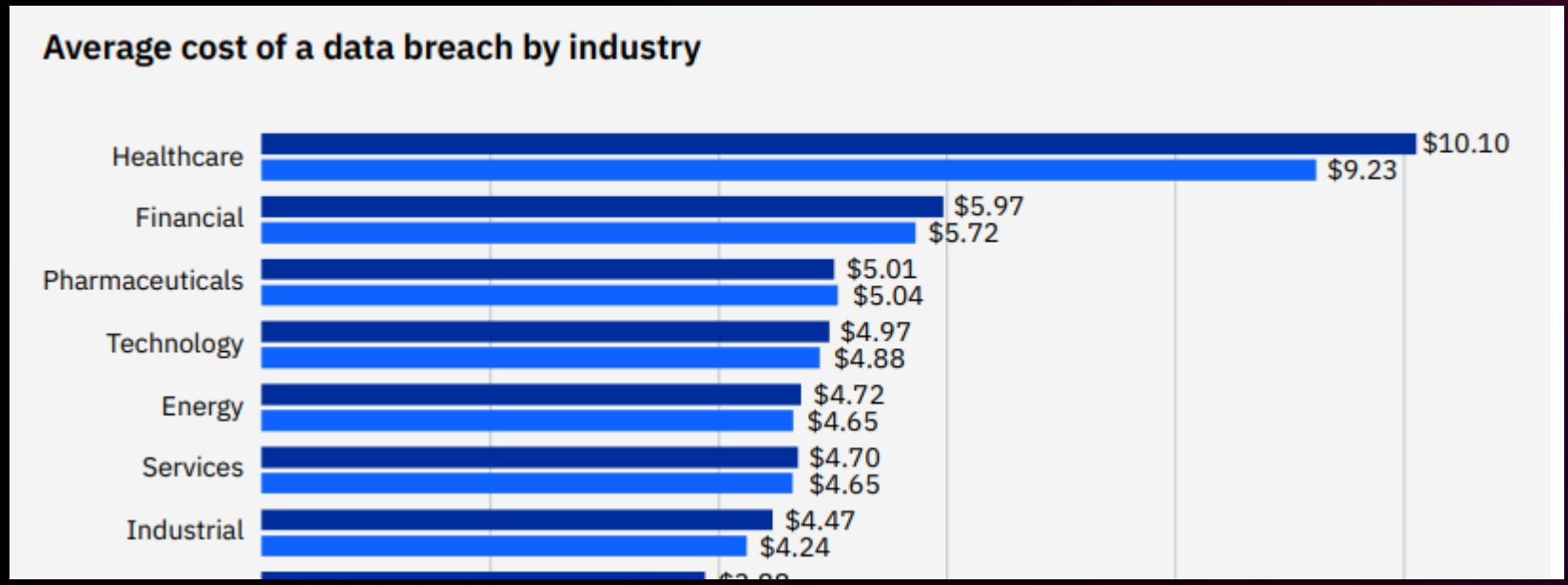
TATA CONSULTANCY SERVICES

Cost of a data breach

$4.35 million
Average total cost of a
data breach

$4.54 million
Average cost of a
ransomware event

$4.82 million
Average cost of a
critical infrastructure data breach



* Measured in USD millions

Source: IBM

Ideal compliance function

"Making good use of technology to automate processes and simple tasks to free up time for compliance teams to focus on more complex issues and forward planning."

Survey respondent
https://mco.mycomplianceoffice.com/blog/cost-of-compliance-2022

Source: THOMSON REUTERS

AWS services that support compliance


AWS Config


AWS Lambda


AWS KMS


AWS Control Tower


Amazon Inspector


Amazon GuardDuty


AWS Identity and Access Management (IAM)


Amazon Macie


AWS Audit Manager


AWS Artifact


AWS CloudHSM


AWS Security Hub

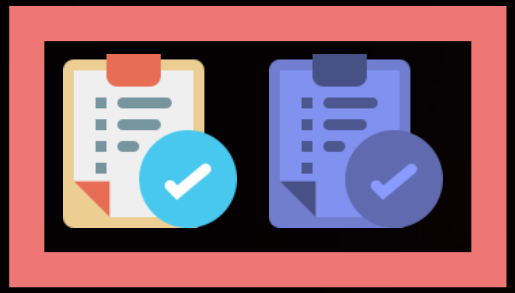
And many more

TCS approach to automating regulatory compliance

1

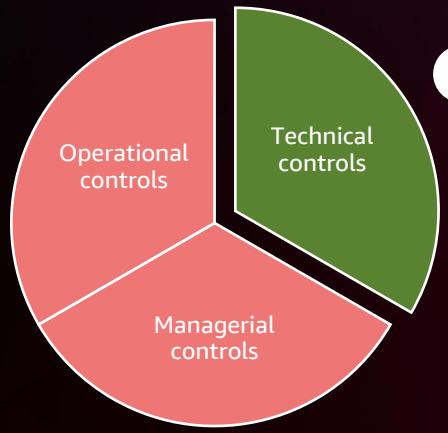
Team of domain and cybersecurity experts

2



Arrive at a baseline of applicable business and geographical regulatory frameworks

3



Consolidate all the technical compliance controls

4

Map technical controls to compliance rules

5

Single source of truth for all compliance rules across regulatory frameworks

Sample customer scenario: Financial services business in ANZ region

Controls layer

ACSC Australian Cyber Security Centre

GDPR

NIST

APRA Australian Prudential Regulation Authority

PCI DSS COMPLIANT

CIS

Baseline layer

- Asset inventory and controls
- Data privacy controls
- Identity and access management
- Workload protection
- Network security
- Secure software development
- Monitoring controls
- Incident management
- Security operations
- Threat management

Implementation layer

Mapping from controls to security guardrails

Collective control catalog enables traceability and automation

Assessment layer

Scan adherence of the cloud platform against the security guardrails

Visualization layer

Dashboard for compliance posture

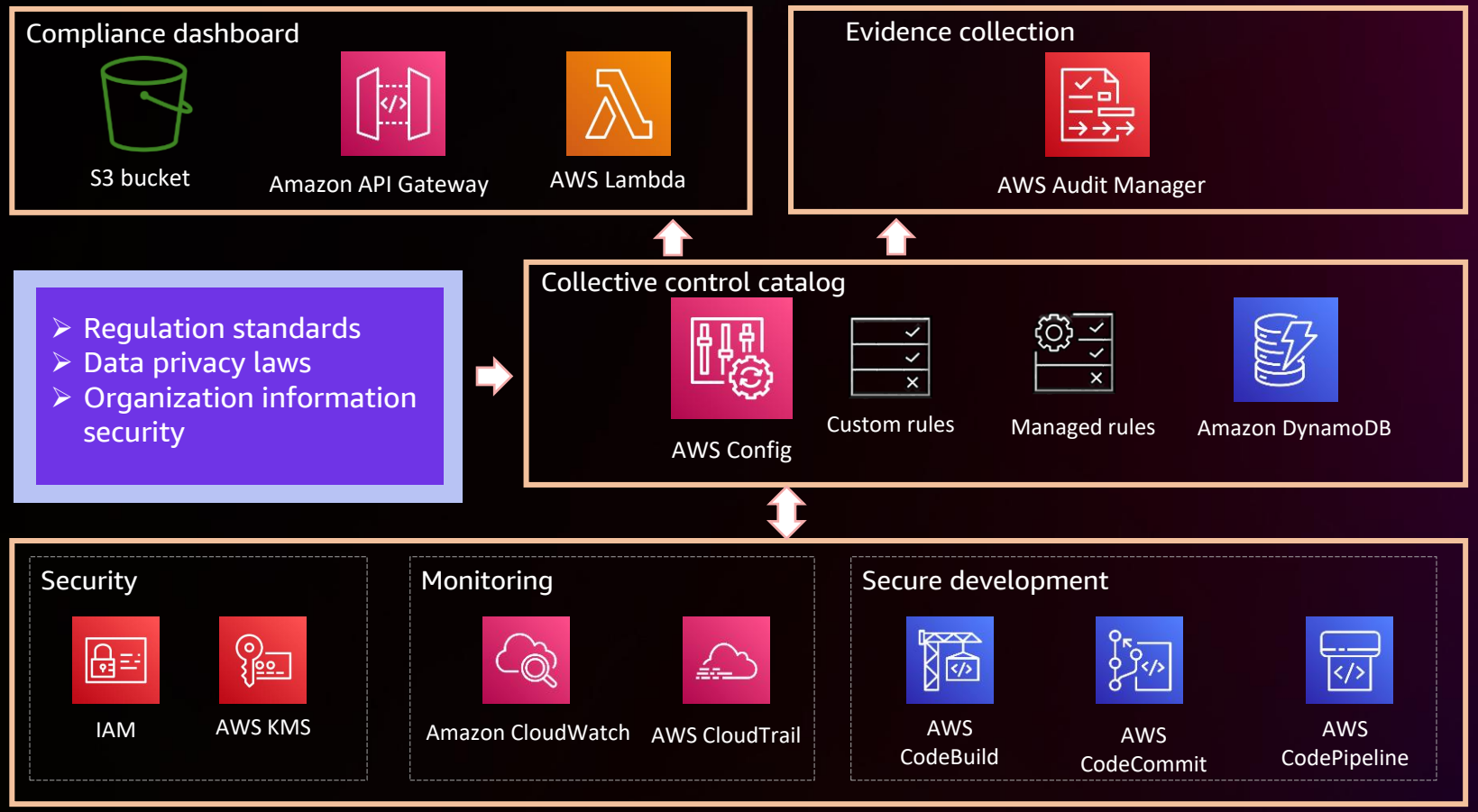
Evidence collection

Sample customer scenario: Creating security standards baseline

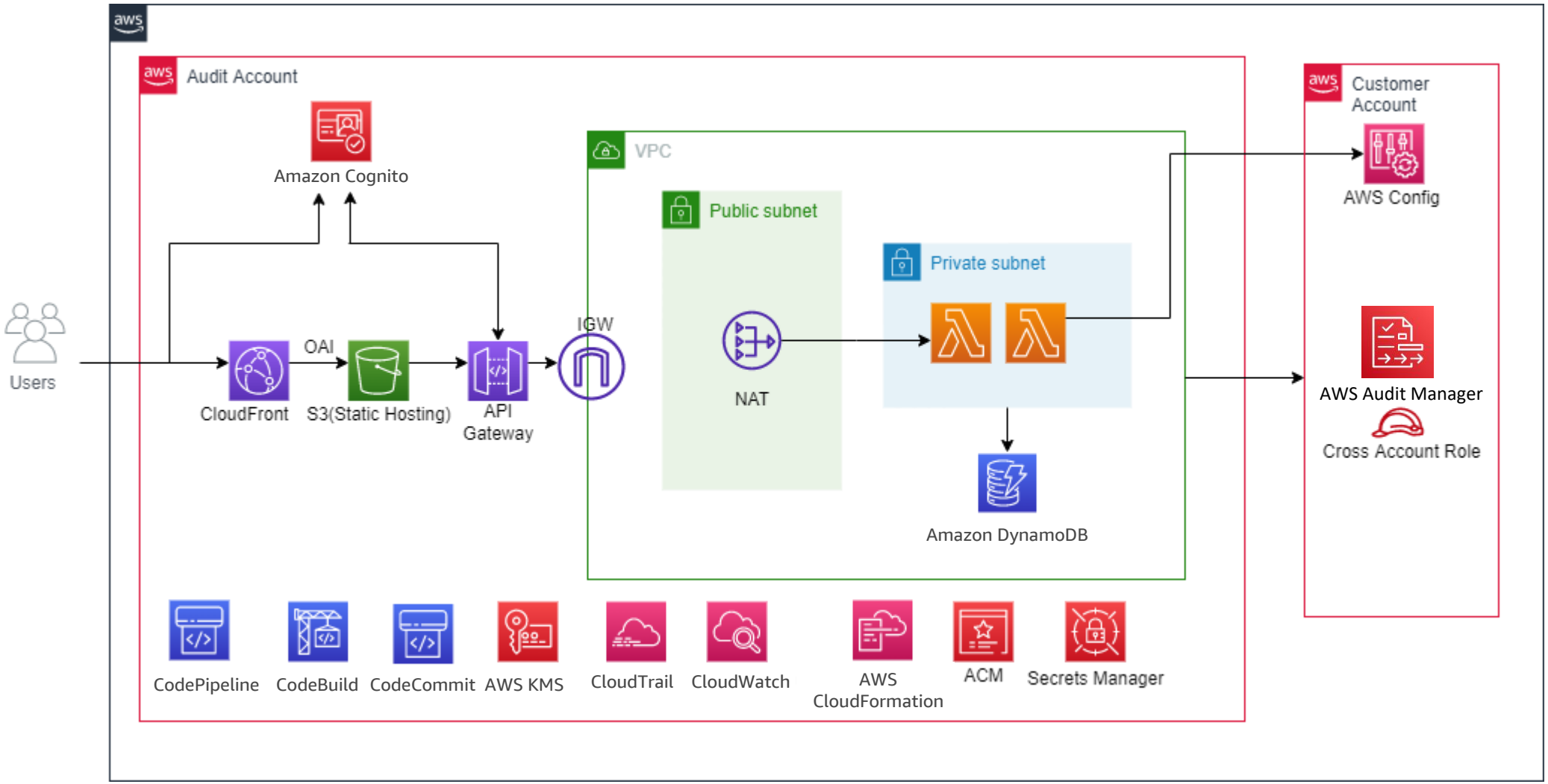
Framework	Control ID	Control description	Security policies to be applied	AWS Config rules
NIST CSF	**DE.AE-1**	A baseline of network operations and expected data flows for users and systems is established and managed	1. Ensure logging is enabled for Amazon OpenSearch Service, AWS WAF, API Gateway, ELB, Amazon RDS, Amazon Redshift, S3 bucket, VPC Flow Logs 2. Enable AWS CloudTrail in all regions 3. Ensure EC2 route tables do not have unrestricted routes to internet gateway 4. Use Amazon CloudWatch to centrally collect and manage log events 5. Do not allow ingress traffic from 0.0.0.0/0 to common ports	elasticsearch-logs-to-cloudwatch multi-region-cloudtrail-enabled wafv2-logging-enabled api-gw-execution-logging-enabled cloud-trail-cloud-watch-logs-enabled cloudtrail-enabled elb-logging-enabled rds-logging-enabled **lambda-tracing-enabled ***
CPG 234	**67 a**	Network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity	1. Ensure logging is enabled for API Gateway, ELB, AWS WAF, Amazon RDS, S3 bucket, VPC Flow Logs 2. Enable AWS CloudTrail in all regions 3. Use Amazon CloudWatch to centrally collect and manage log events	wafv2-logging-enabled api-gw-execution-logging-enabled cloudtrail-enabled elb-logging-enabled
CIS	**CIS 6**	Maintenance, monitoring, and analysis of audit logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an event	securityhub-enabled vpc-flow-logs-enabled cloudtrail-enabled multi-region-cloudtrail-enabled

* AWS Config Custom rule

Building blocks of TCS Industry Regulatory Auditor solution



Solution architecture



Customer benefits

Proactive audits

Conduct on-demand internal audits; enables proactive security risk identification

Compliance team–friendly

Compliance posture dashboard is against the compliance standards rather than security controls

Standards to practice

Compliance standards are translated and put into security practice

Reusable

Can be tailored for any combination of compliance standards

Capabilities offered

1

Translate

Translate compliance controls to security rules

2

Traceability

Ability to trace the security policies back to the compliance standards

3

Assess

Assess in real time the compliance status of the target AWS environment against the security controls

4

Monitor

Continuously monitor the compliance posture; alert on deviations

5

Remediate

Implement corrective actions to remediate the security deviations observed

TATA CONSULTANCY SERVICES

Thank you!

Raji Krishnamoorthy
raji.krishnamoorthy@tcs.com

Karthik Thirugnanasambandam
thirugk@amazon.com

Please complete the session survey in the **mobile app**