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

ARC217-L

Building modern apps: Architecting for observability & resilience

Francessca Vasquez (she/her)
VP, Technology
Amazon Web Services

Shaown Nandi (he/him)
Director, Technology
Amazon Web Services

”Things happen in there that you don’t see, the ghosts always catch you.”

Gregory Robinson

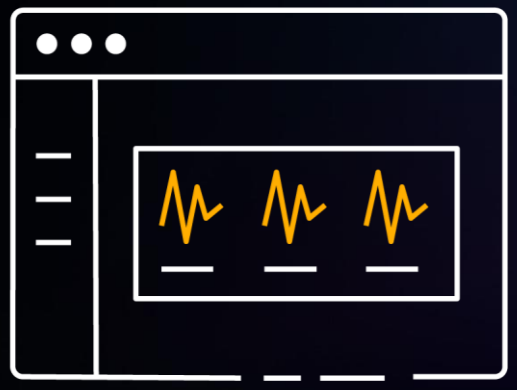
Program Director
James Webb Space Telescope


$10B
Budget
$800M
Additional costs
1M
Miles
1
Telescope


300+
Single points of failure

Agenda

- The importance of resilience and observability: Beyond the cloud
- Approaches to resilience and observability
- Continuous improvement



Observability

Resilience

AWS Well-Architected Framework

Resilience

What is resilience?

A WORKLOAD'S ABILITY TO RESPOND AND QUICKLY RECOVER FROM FAILURE

The mental model

High availability

Resistance to common failures through design and operational mechanisms

Core services, design goals to meet availability goals

Disaster recovery

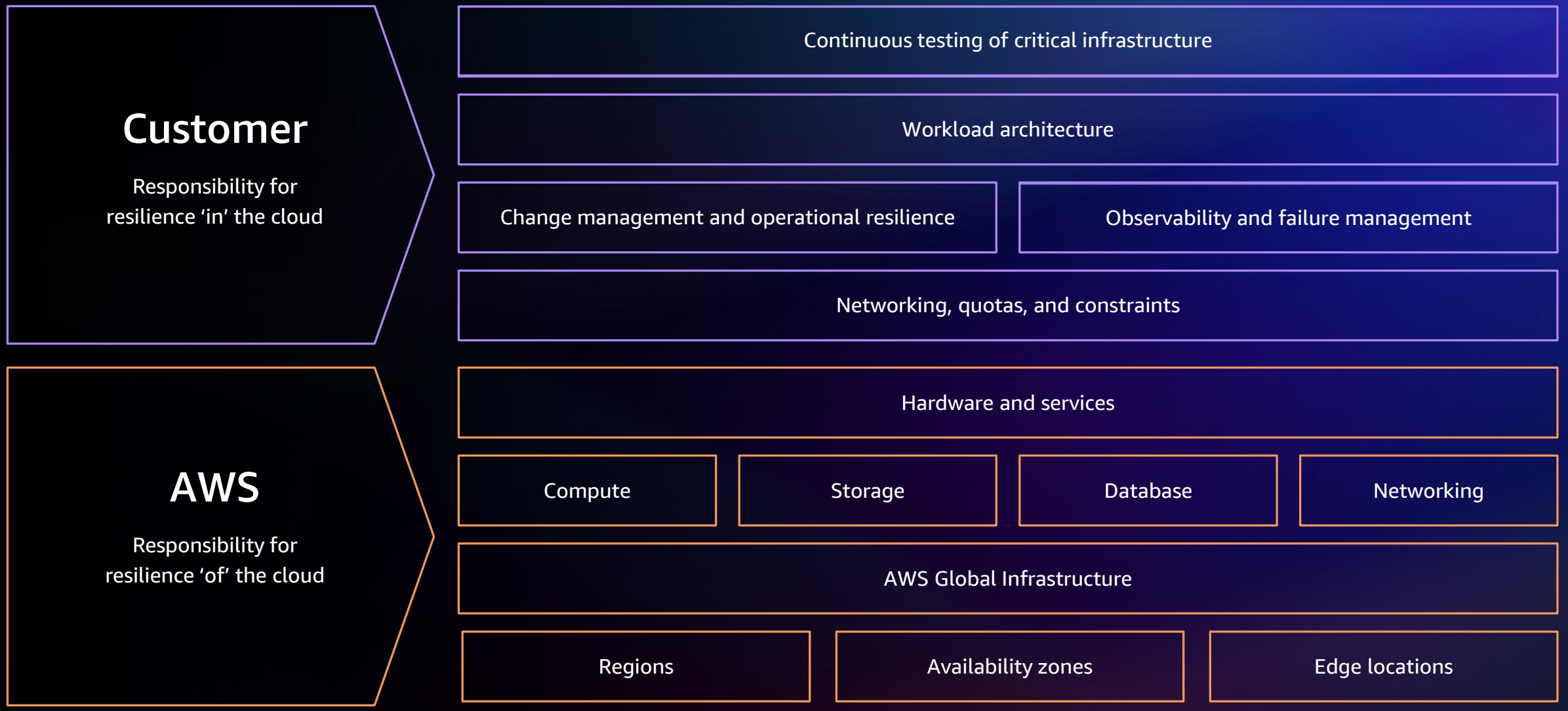
Returning to operations within specific targets for more rare but highly impactful failures

Backup and recovery, data bunkering, managed RPO/RTO

Continuous improvement

CI/CD, code refinement, operational testing, observability/monitoring

Shared responsibility model for resilience



Resilience ‘of’ the cloud

A CULTURE BUILT AROUND RESILIENCE

Service ownership model

Incentivizes continuous improvement of operations

Operational Readiness Reviews (ORR)

Ensures compliance to best practices prior to a service launch

Safe, continuous deployment

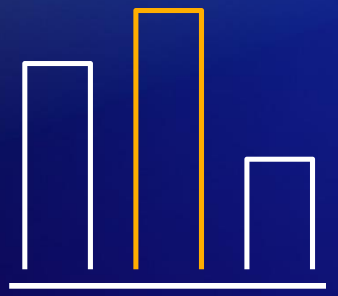
Minimizes impact on production caused by faulty deployments

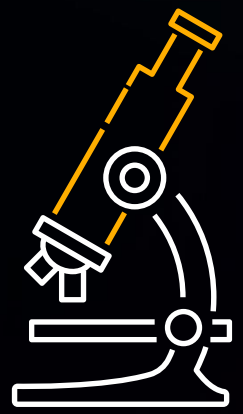
Correction of Error (CoE) processes

Helps teams understand the root cause and prevents reoccurrence

Resilience ‘in’ the cloud

ACHIEVING CONTINUOUS RESILIENCE





Categories of failure

Code deployments & configuration

e.g. bad deployment, cred expiration

Core infrastructure

e.g. data center failure, host failure

Data and state

e.g. data corruption

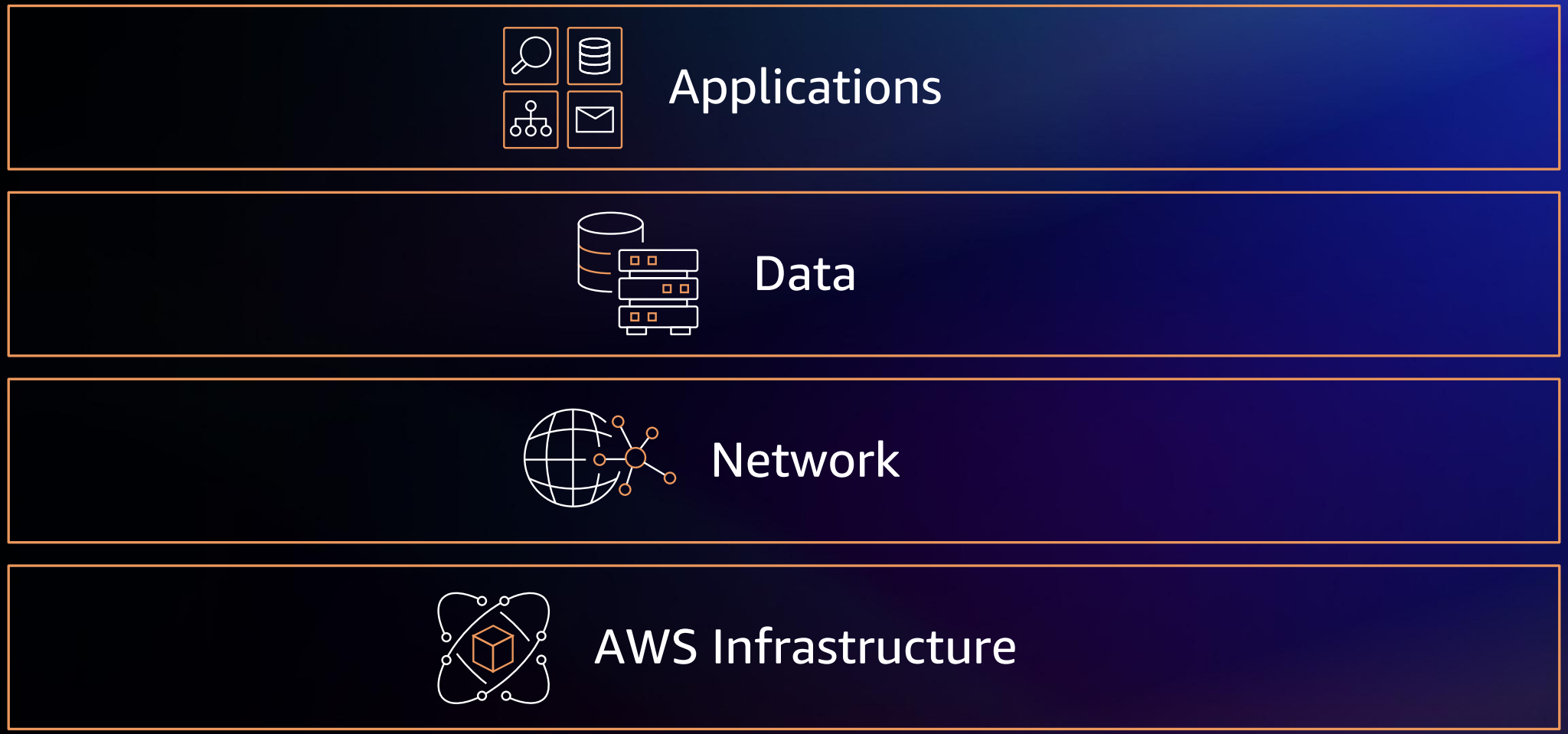
Dependencies

e.g. infrastructure, external APIs

Highly unlikely scenarios

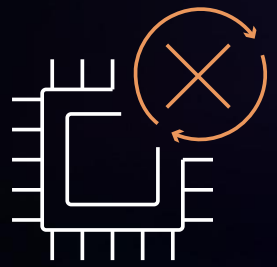
e.g. all of internet failure, environmental disasters

Building a resilient foundation



Recovery-oriented patterns

Backoff and retry



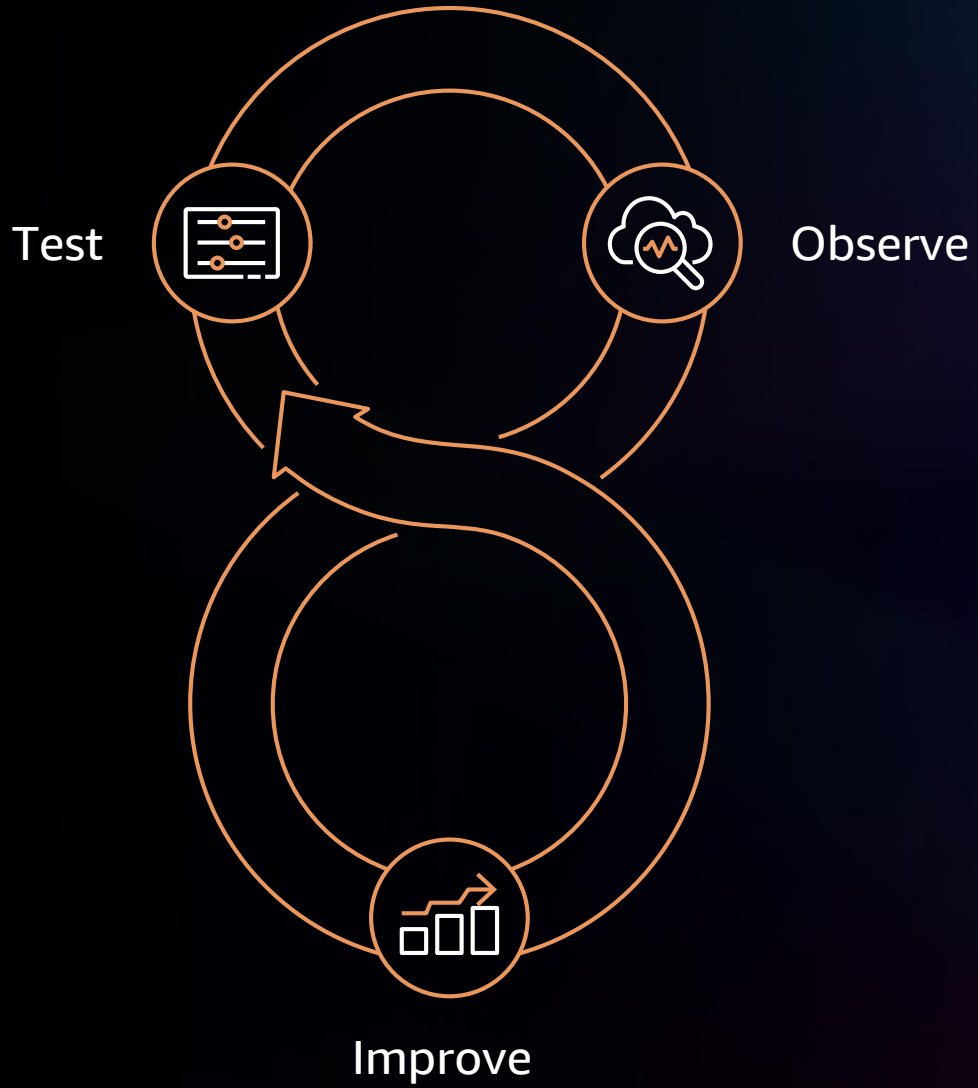
Circuit breaker

Graceful degradation

Throttling

Load shedding

Continuous testing



- Chaos engineering
- Regularly practicing failover & failback
- Game days
- And more

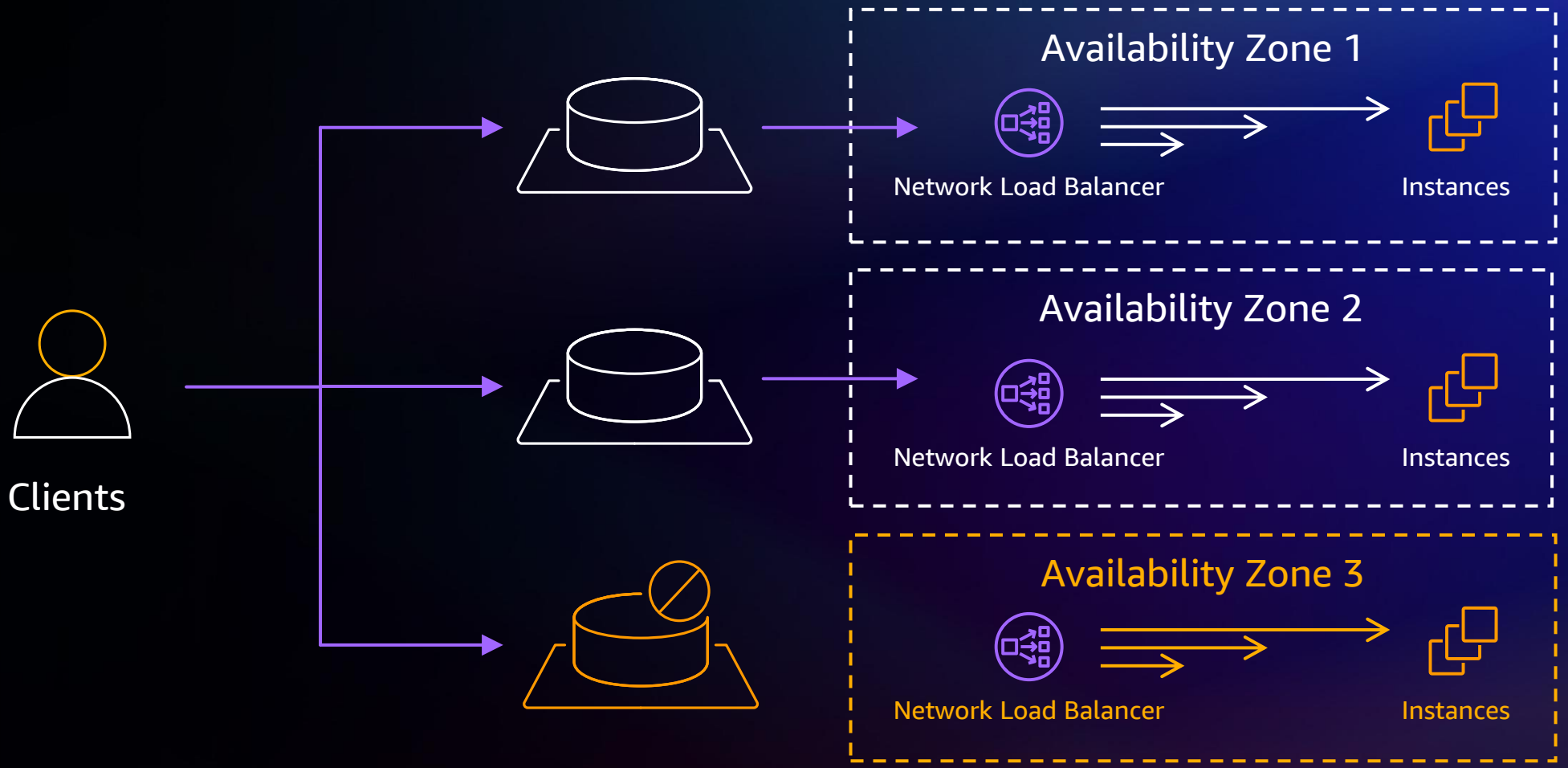
AWS investments in resilience

AWS Well-Architected

Protect	Define	Test	Monitor and manage	Recover
AWS Backup	AWS CloudFormation	AWS Fault Injection Simulator	Amazon DevOps Guru	AWS Backup
AWS Elastic Disaster Recovery	AWS Trusted Advisor	AWS Resilience Hub	AWS CloudTrail	AWS Elastic Disaster Recovery
AWS Systems Manager	AWS Service Catalog AppRegistry		AWS Resilience Hub	AWS Systems Manager
	AWS Resilience Hub		Amazon Route 53 Application Recovery Controller	
			Amazon CloudWatch	

New! Zonal Shift feature for Amazon Route53 ARC

SPEEDS RECOVERY FOR MULTI-AZ APPLICATIONS



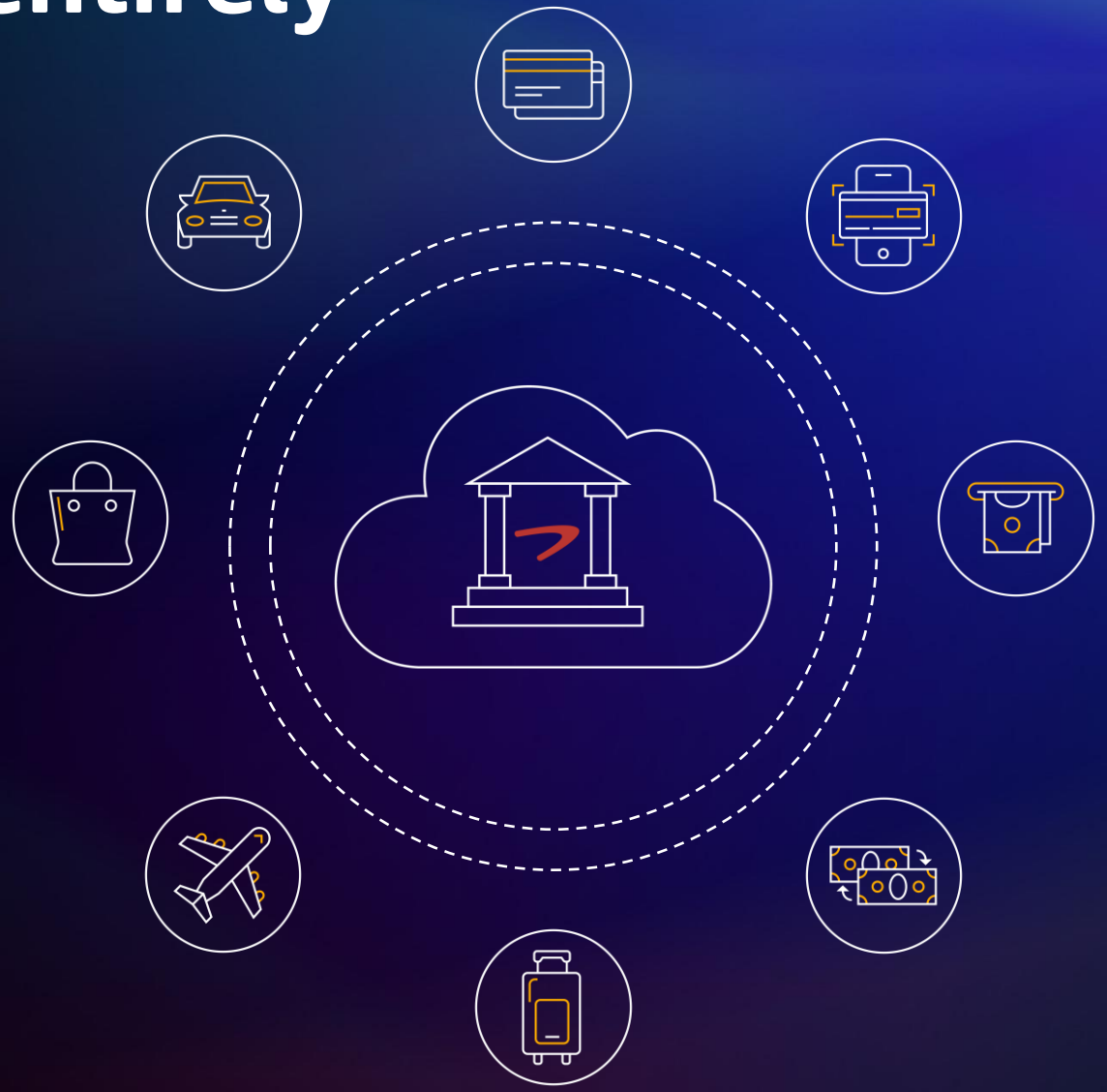
Capital One

Will Meyer

MANAGING VP, CLOUD & CONNECTIVITY

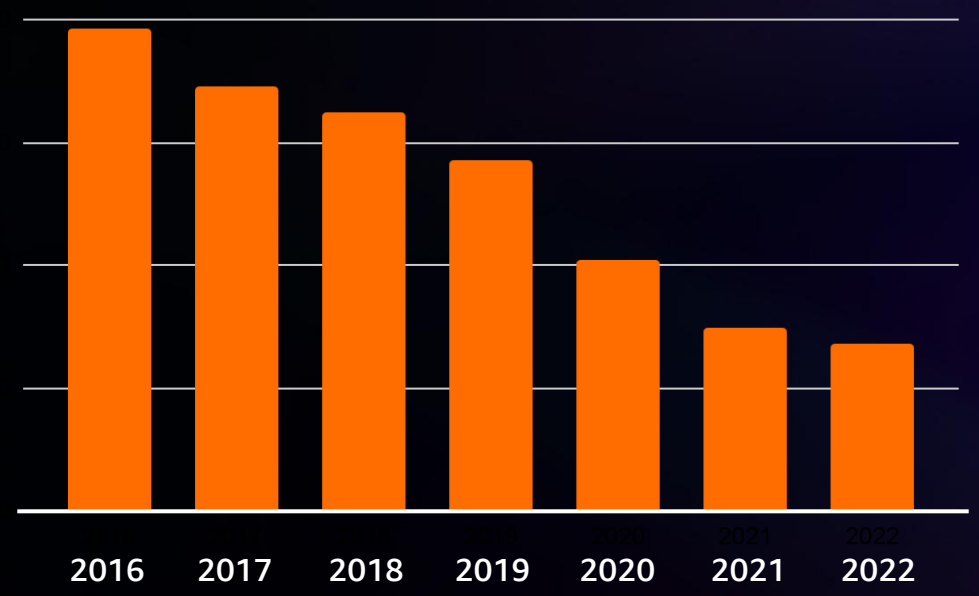
The first bank running entirely on the public cloud

- 25-year-old, founder-led public company
- Top 10 bank, credit card issuer, and auto loan originator
- 100M+ customers and 50,000 associates
- All-in in the cloud

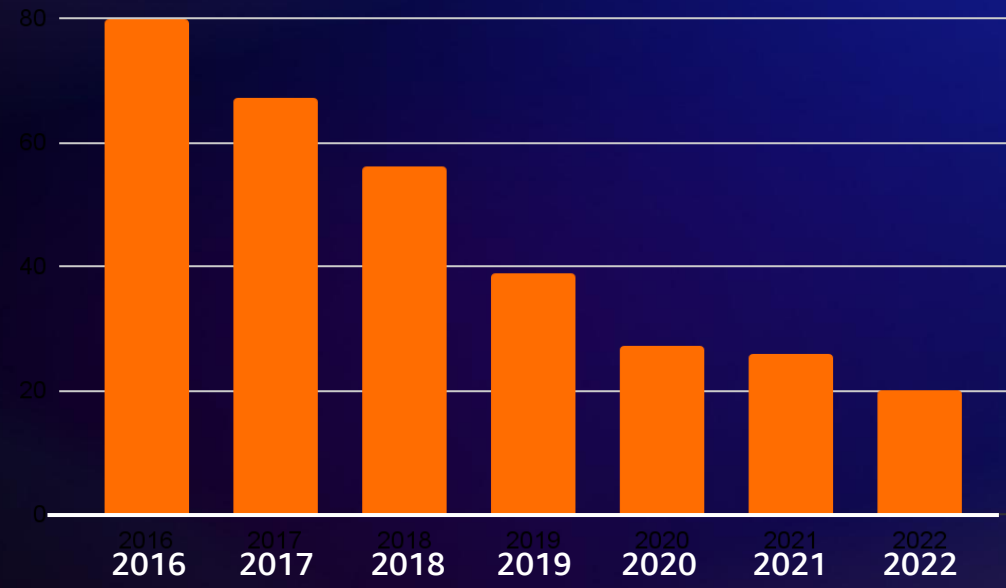


The cloud is a proven* enabler of resilient architecture

Critical impacting incidents

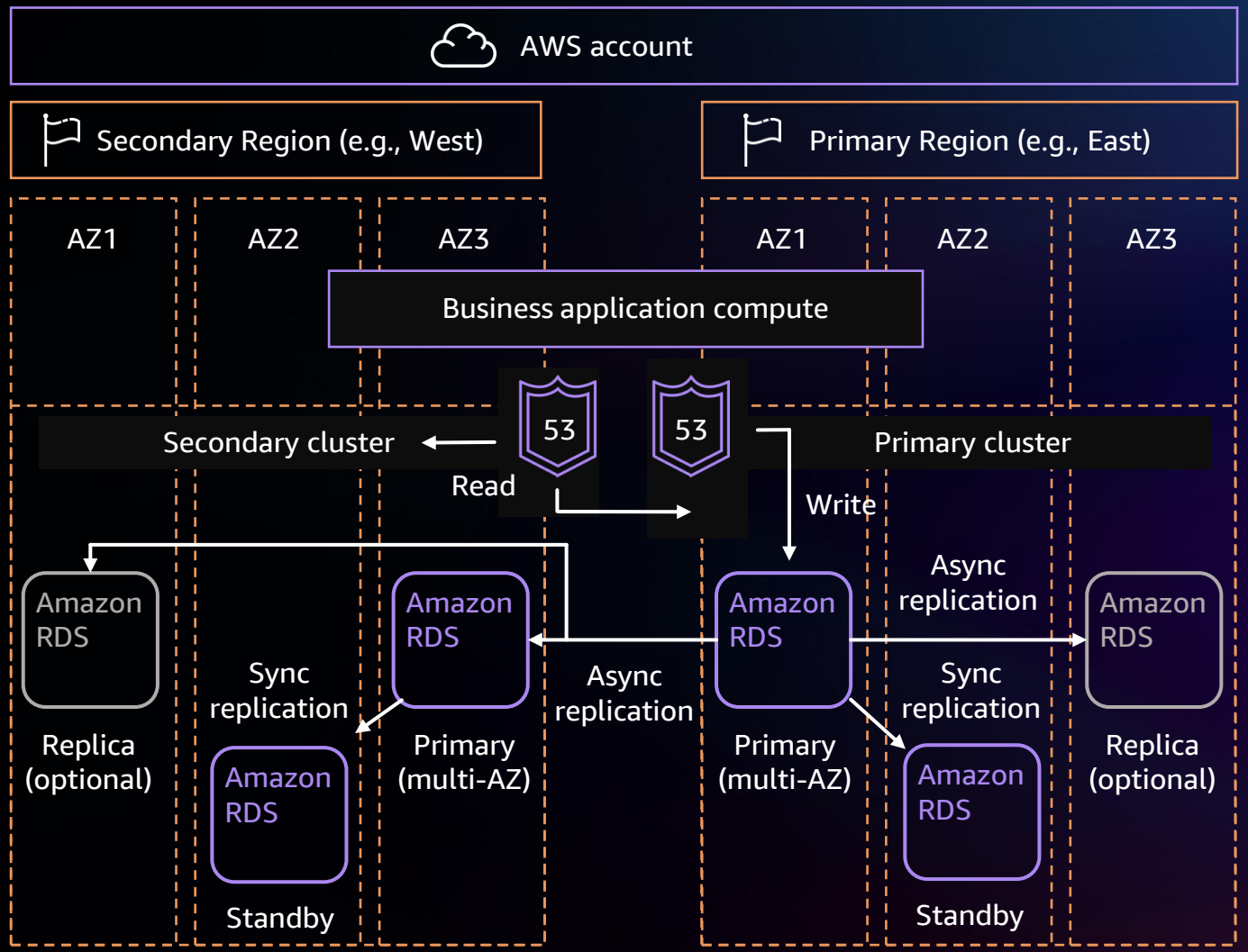


Incidents failing resolution target



*if you use it wisely

Multi-AZ and multi-Region: “Yes, and…”



Deploying across Regions and Availability Zones is just the start

Standardize resilience requirements

Focus on complex dependencies

Push toward static stability

Tool-up to fight complexity, and assume failure

Tools
(FIS, SSM, Cloud Doctor)

App layer failures

AZ failures

Regional failures

Disaster scenarios

Exercises
(Game Days, chaos, isolations)

Standardize deployment and embrace IaC

Invest in tooling to understand complex cloud state and call flows

Root out manual intervention through targeted exercises

“The real test is not whether you avoid this failure because you won’t. It’s whether you let it harden or shame you into inaction, or whether you learn from it; whether you choose to persevere.”

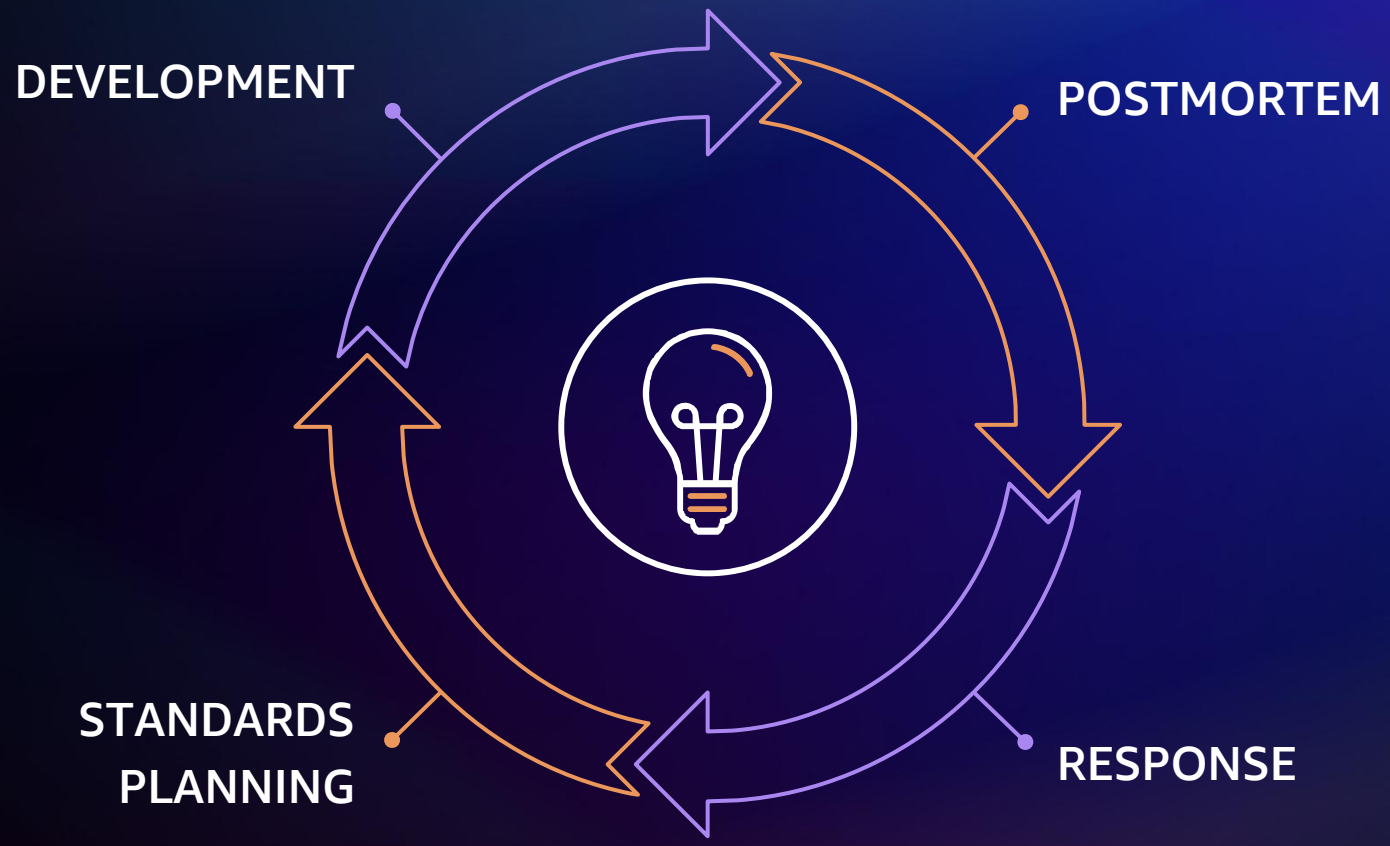
Barack Obama

Learn your way to greater resilience

Incentivize collaborative problem solving

Invest in blameless postmortems

Make your learning process a technical and organizational imperative



A serverless strategy can be a strategy for resilience

- Cost efficiency, security, productivity, and resiliency at scale still aren’t trivial, especially distributed
- Higher-level managed services do offer targeted resilience features . . .
- . . . they can also inherently change your resilience for the better as you continue to offload the undifferentiated heavy lifting

Our recipes for enterprise resilience on the cloud

Educate on patterns and continuously evolve them

Standardize and embrace left-shifted tooling

Focus relentlessly on dependencies

Practice for failure and coordinated response

Observability

“You can’t legislate against failure, focus on fast detection and response.”

Founding member, Amazon EC2

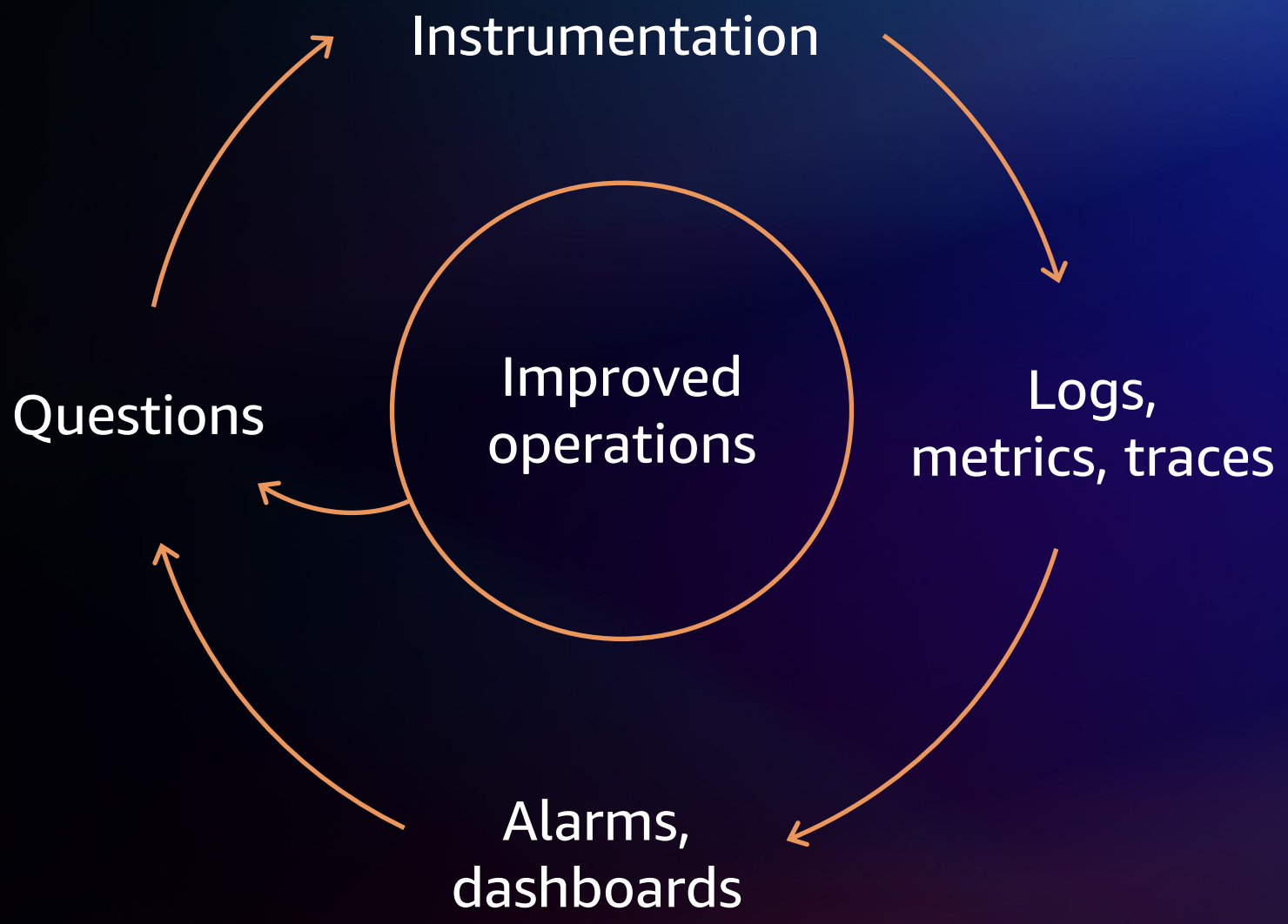
What is observability?

Our monitoring philosophy

Measure the customer experience

Detect and respond

The cycle of monitoring



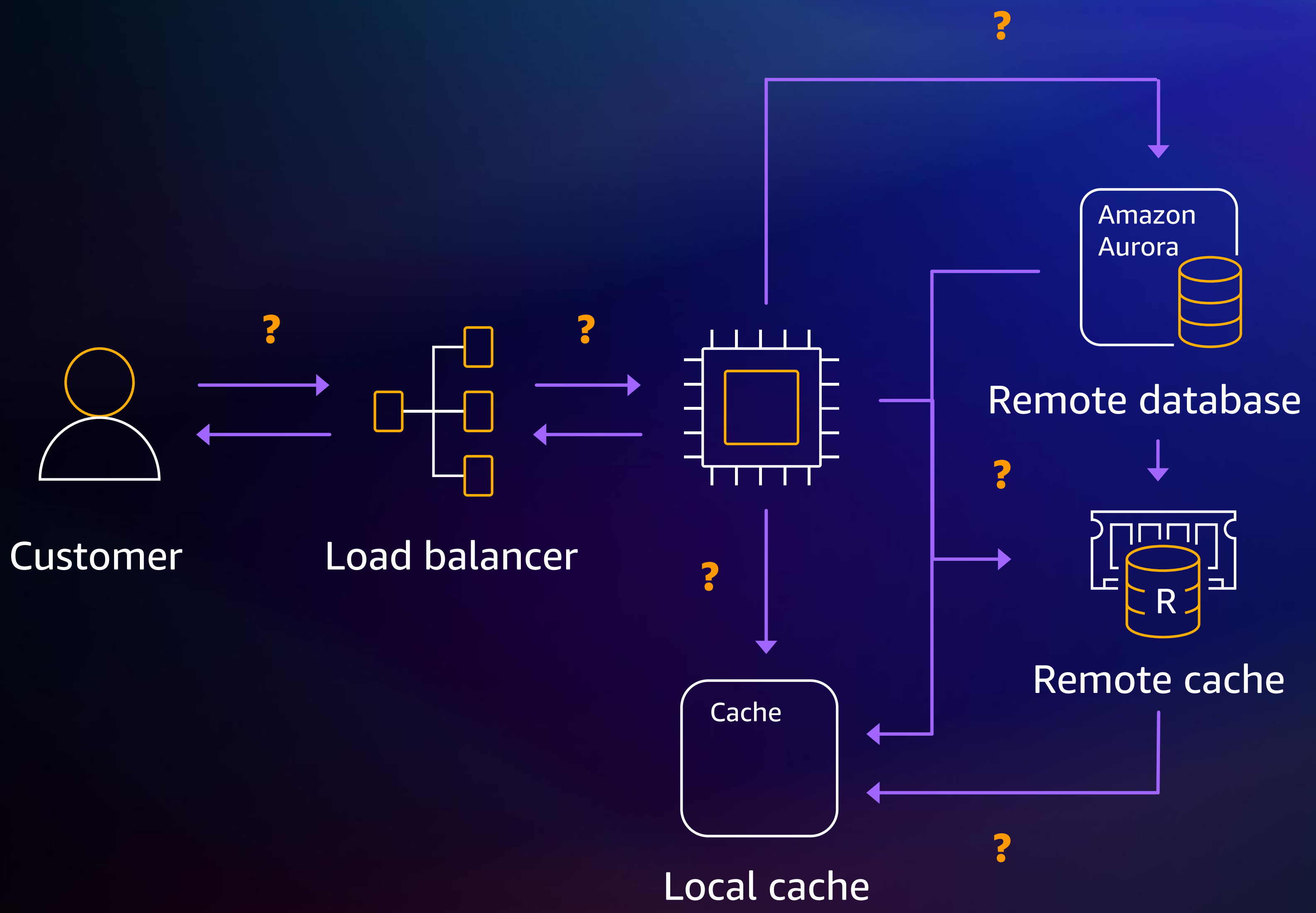
What to measure

Did we find the item in the remote cache?

GetProductInfo()

How long did it take to read from the cache?

they evict other items?



Different types of metrics

Health metrics

"Am I failing?"

Diagnostic metrics

"What is the value of this thing I measured?"

Implementing essential metrics

IN ORDER TO DETECT, INVESTIGATE, AND RESPOND TO IMPACT

Customer experience metrics

Impact assessment metrics

Operational health metrics

Monitoring in the cloud

THREE PILLARS OF OBSERVABILITY TOOLING

Metrics

Numeric data

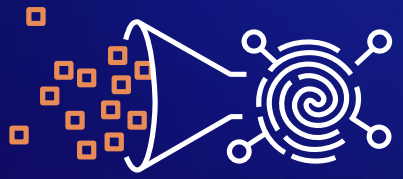
Measured at various time intervals, like 1 or 5 minutes

Logs

Time-stamped records of discrete events

One log per “unit of work”

Traces



User’s journey across multiple applications and systems

Observability

AWS Observability suite

Observability

AWS-native services

Open source managed services

CloudWatch ServiceLens

Amazon Managed Grafana

Container insights

Lambda insights

Contributor insights

Application insights

Metric insights

Do it yourself (DIY)

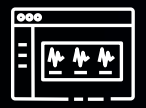
Events

Dashboards

Alarms

RUM

Evidently



Metrics

Logs

Synthetics

AWS X-Ray

Amazon OpenSearch Service

Amazon Managed Service for Prometheus

Jaeger and Zipkin tracing

Insights and ML

CloudWatch agent

AWS X-Ray agent

Collectors and SDKs

AWS Distro for OpenTelemetry

Instrumentation

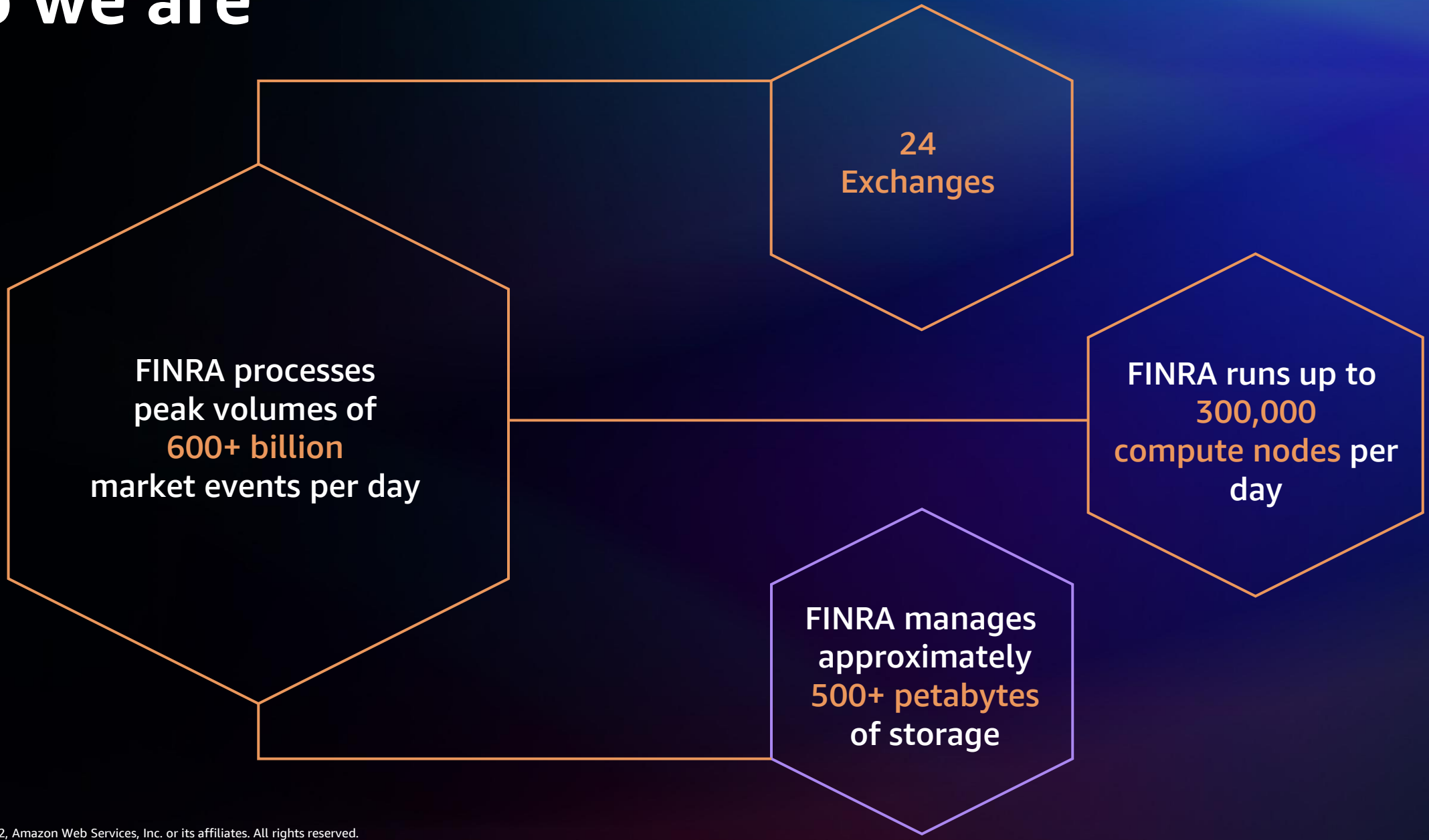
FINRA

Kym Weiland

VICE PRESIDENT, ENTERPRISE OPERATIONS
FINRA

Our mission

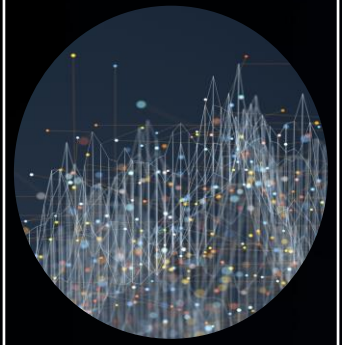
Who we are



FINRA cloud journey

	2016	2019	2022	2026
Data Intake	39B	190B	450B	600B to 1T
Storage	45 Pb	50 Pb	500 Pb+	Bigger
Average daily compute	25k	35k	150k	Bigger
RDS Instances	100	500	1200	Bigger

FINRA cloud architecture principles

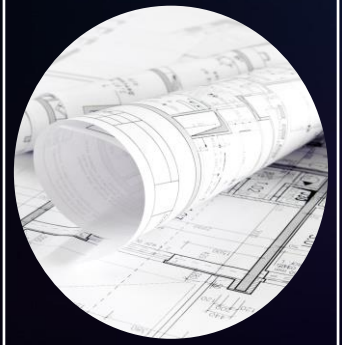


Enterprise data management

- Data registration
- Data lineage
- Data lifecycle
- Data classifications

Cloud elasticity

- Serverless
- Instance types
- Storage types
- On-demand scalability



Architecture

- Core framework services
- Supported blueprints
- Central messaging
- API-focused
- Open source preferred

Security

- Encryption
- Configuration
- Alerting
- Authorizations
- Auditable

DevOps

- Infrastructure as Code
- Continuous delivery
- Automated testing

Operations

- Resilient
- Automated monitoring
- Supportable
- Performant
- Enterprise observability

Analytics

- Compliance as Code
- Data democratization

Cloud management

Innovate

- Service evaluations
- R&D/POC environments
- Preview participation
- Informed feedback

Optimization of workloads

- Operating observability
- Capacity utilization
- Cost efficiencies

Adoption

- Delivery-focused automation
- Provisioning guardrails
- Automation at scale

Maintaining observability

System monitoring

- Platform
- Service
- Application

Compliance

- Policy enforcement
- Oversight
- Records management

Security

- Logging standards
- Control deviations

Operational scorecards

- Resilience
- Logging
- Tagging
- AWS Trusted Advisor

Application health status

- Core connectivity
- Direct dependencies
- Indirect dependencies

Enhanced disaster recovery strategic vision

Focus on services and offerings instead of custom solutions

- Amazon S3 – Cross-Region replication
- Amazon RDS – Aurora Global Database
- AWS KMS – Multi-Region Keys
- Amazon Dynamo Global Tables – Parameter Store

Continue to infuse resilience through architecture and services

Evaluate opportunities for efficiencies between regions

Ensure data security, encryption, and durability

Take advantage of AWS advances in multi-region aware services as they become available

Resilience with observability

Annual testing and verification

- IEM, planning

FINRA Canary

- Automated application health status
- Configurable region expectations
- Application direct dependencies
  - (Self)
- Downstream direct dependencies
  - (Friends)

App – Core app fail dependencies - Failed

App – Core app pass dependencies - Failed

App – Core app pass dependencies - Pass

Managing at scale

Integrated security

Hands-off operations

Automated on-boarding of fleet

Audit trail and self reporting

Self service for delivery teams

Continuous improvement

The AWS Well-Architected Framework

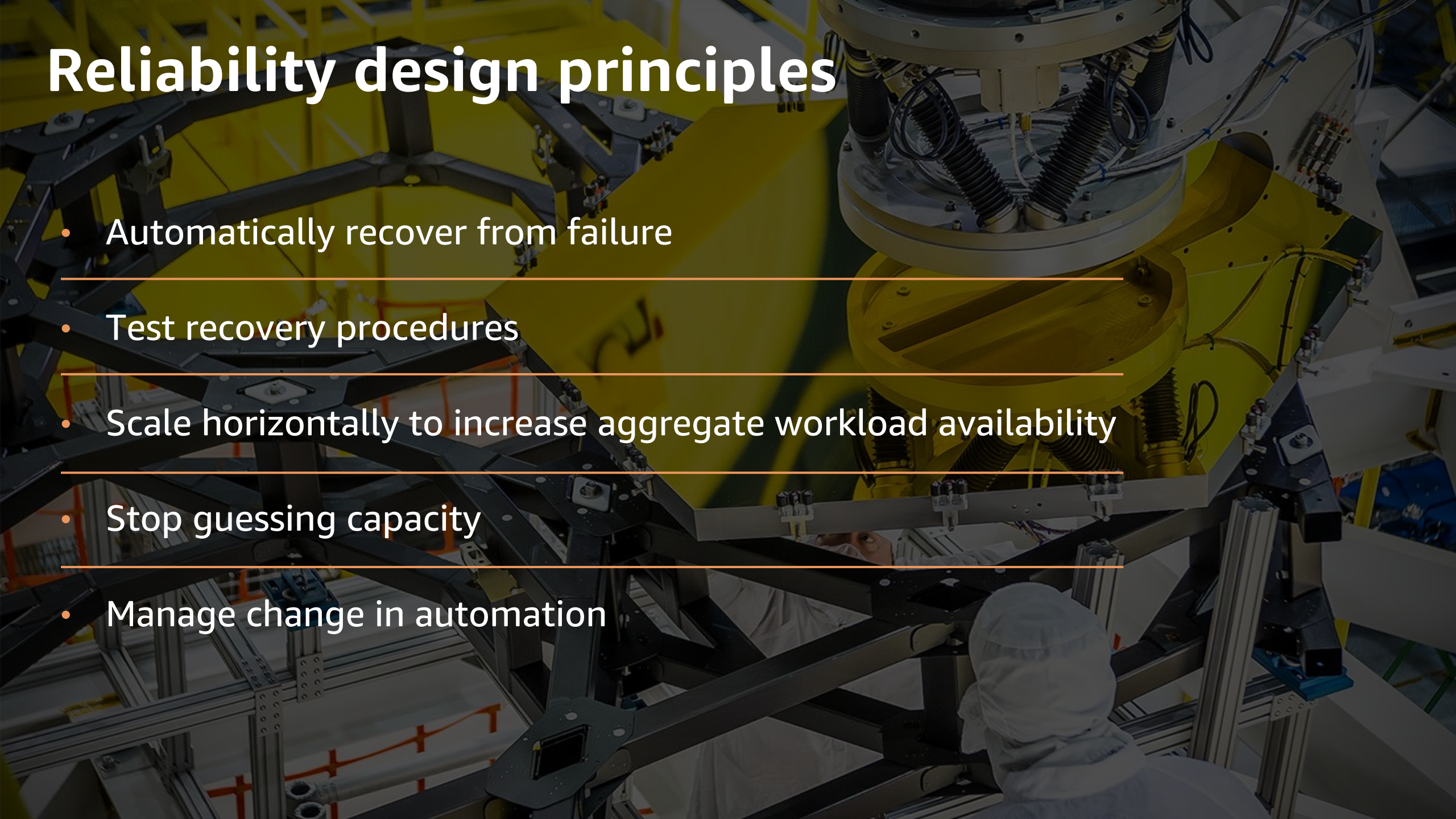
Build and deploy faster

Lower or mitigate risks

Make informed decisions

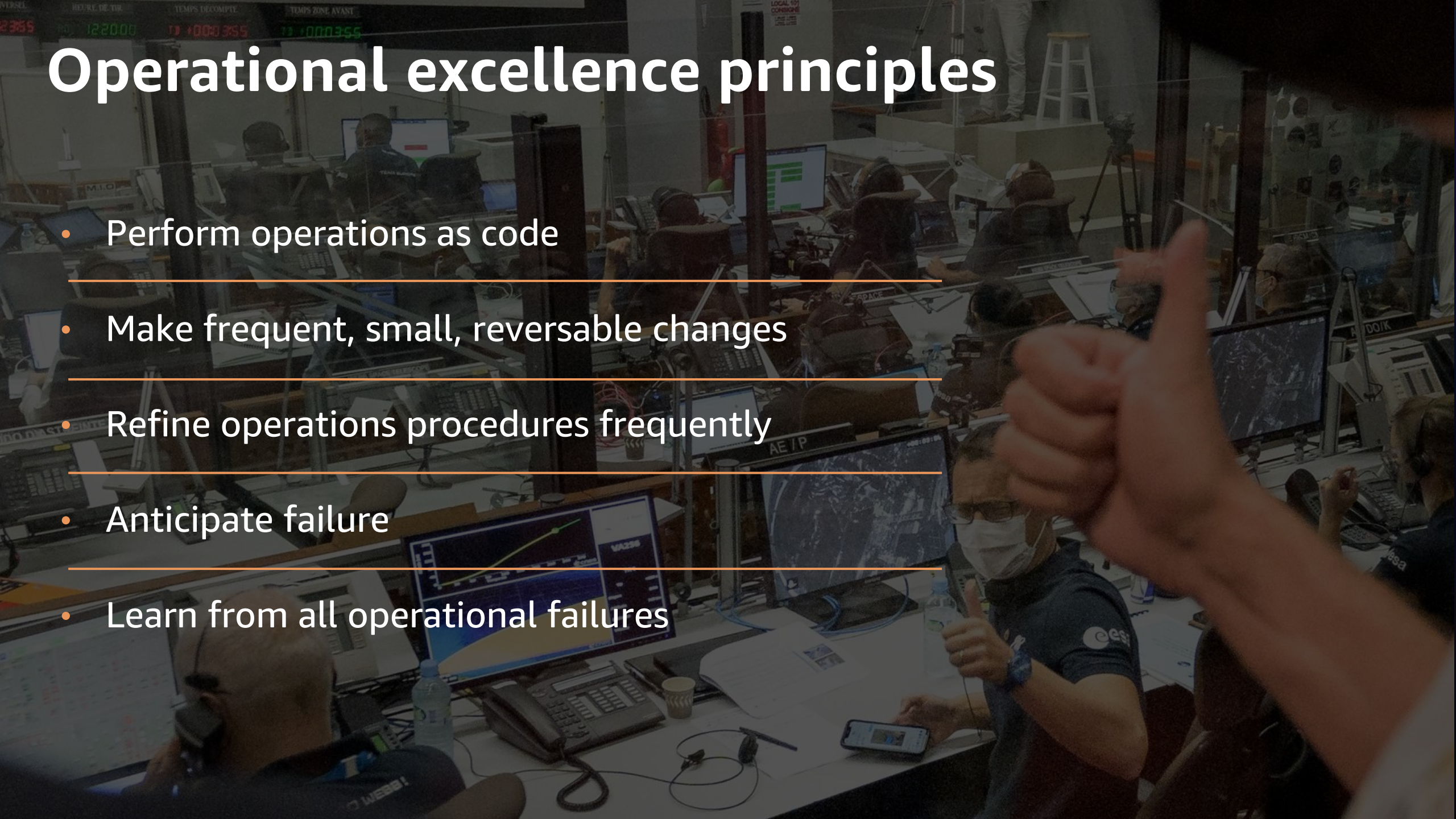
Learn AWS best practices

Reliability design principles



- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change in automation

Operational excellence principles



- Perform operations as code
- Make frequent, small, reversable changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

Game days

REGULARLY TEST YOUR PEOPLE, PROCESSES, AND SYSTEMS

Exercise your procedures

Ensure no impact to users

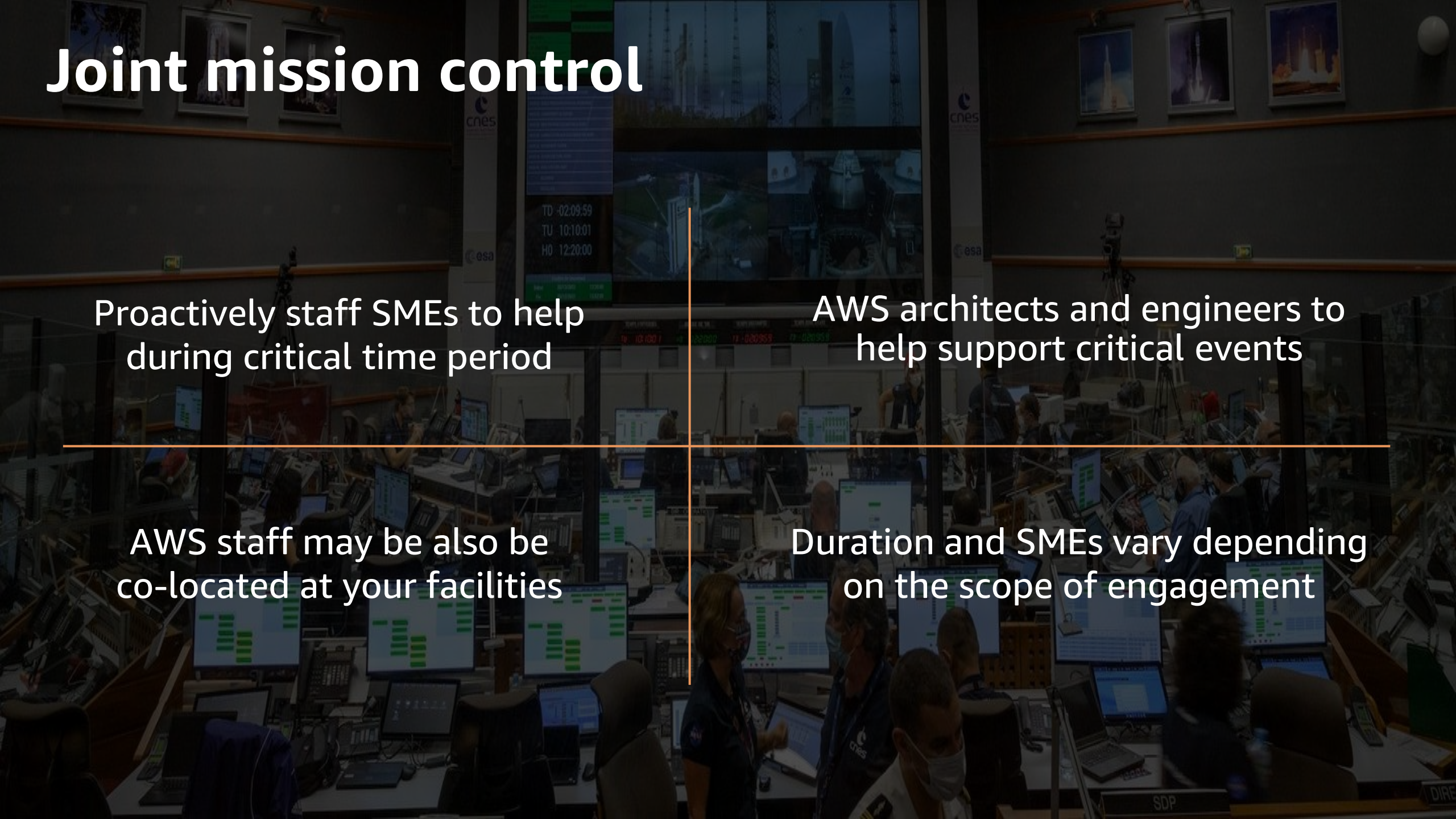
Simulate exceptional event

Infrastructure event management

- Planning for large-scale events
- Framework to ensure alignment
- Planning, review, and risk mitigation
- Post-event recap

We use this process for events like Amazon Prime Day!

Joint mission control



Proactively staff SMEs to help during critical time period

AWS architects and engineers to help support critical events

AWS staff may be also be co-located at your facilities

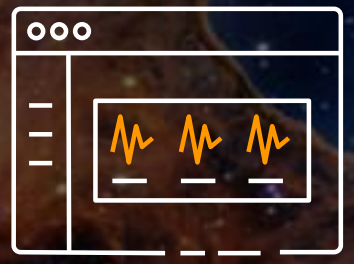
Duration and SMEs vary depending on the scope of engagement

Resources

AWS Well-Architected Framework

AWS Fault Isolation Boundaries Whitepaper

AWS Solutions Library



Observability

Strategies

Key services

Mechanisms

Building resilience together

Thank you!

Francessca Vasquez (she/her)
VP, Technology
Amazon Web Services

Shaown Nandi (he/him)
Director, Technology
Amazon Web Services

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