

The background features a dark blue gradient on the left, transitioning into a large, abstract, curved shape on the right. This shape is composed of various shades of purple and blue, with a bright orange-yellow highlight along its bottom edge. The overall design is modern and dynamic.

aws SUMMIT

OTTAWA | SEPTEMBER 8, 2022

SEC201

Disaster recovery and data residency in Canada

Scott Levac

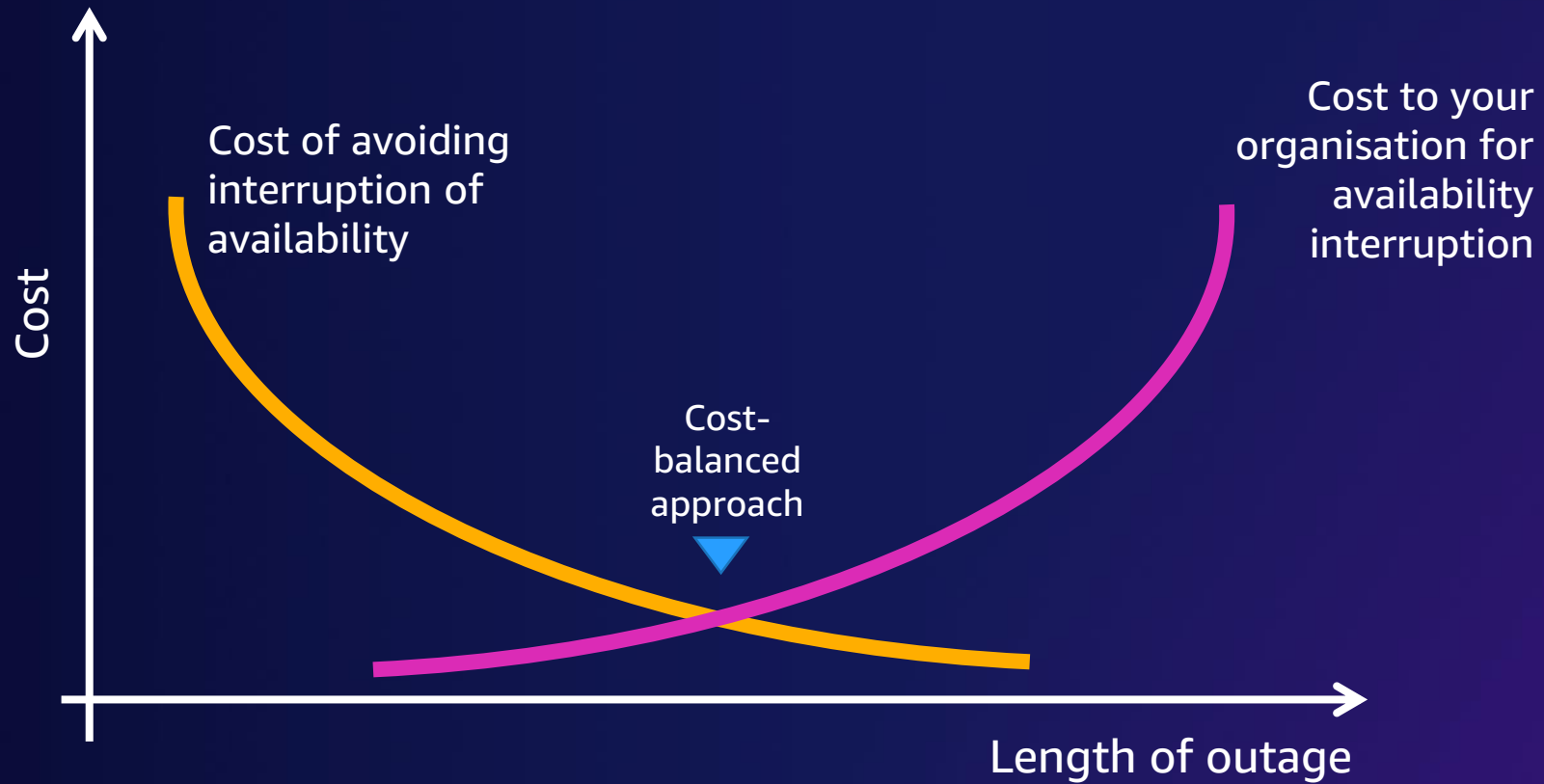
Office of the Chief Information Officer
Treasury Board of Canada Secretariat

Bill Ohlson

Principal Security Leader
AWS WWPS LCC SA



Availability is not free



Focus on outcomes

Daily tape backups on magnetic tape stored offsite in two locations at least 10 km apart. Redundant servers hosted in data centres 50 km apart.



The business cannot tolerate more than one hour of lost services and should never lose more than 20 minutes of data. The service needs to be available 24 hours per day, seven days per week, with no more than one hour of lost productivity per month.



Myth: For cloud providers, we must specify how recovery is implemented.

Busted: Policy wants an outcomes-based approach.

Clouds are made of cells



Myth: Availability Zones (AZs), or Zones, are all created equal across cloud providers

Busted: Understand each cloud provider's SLAs and design for AZs; look beyond the name



Tip: In Canada, AZ is pronounced “eh zed,” not “a zee”

Oh Canada



Myth: Government of Canada (GC) policy does not allow Protected B data to be stored outside of Canada

Busted: GC policy states Canada is the preferred location, but departmental CIOs can decide otherwise

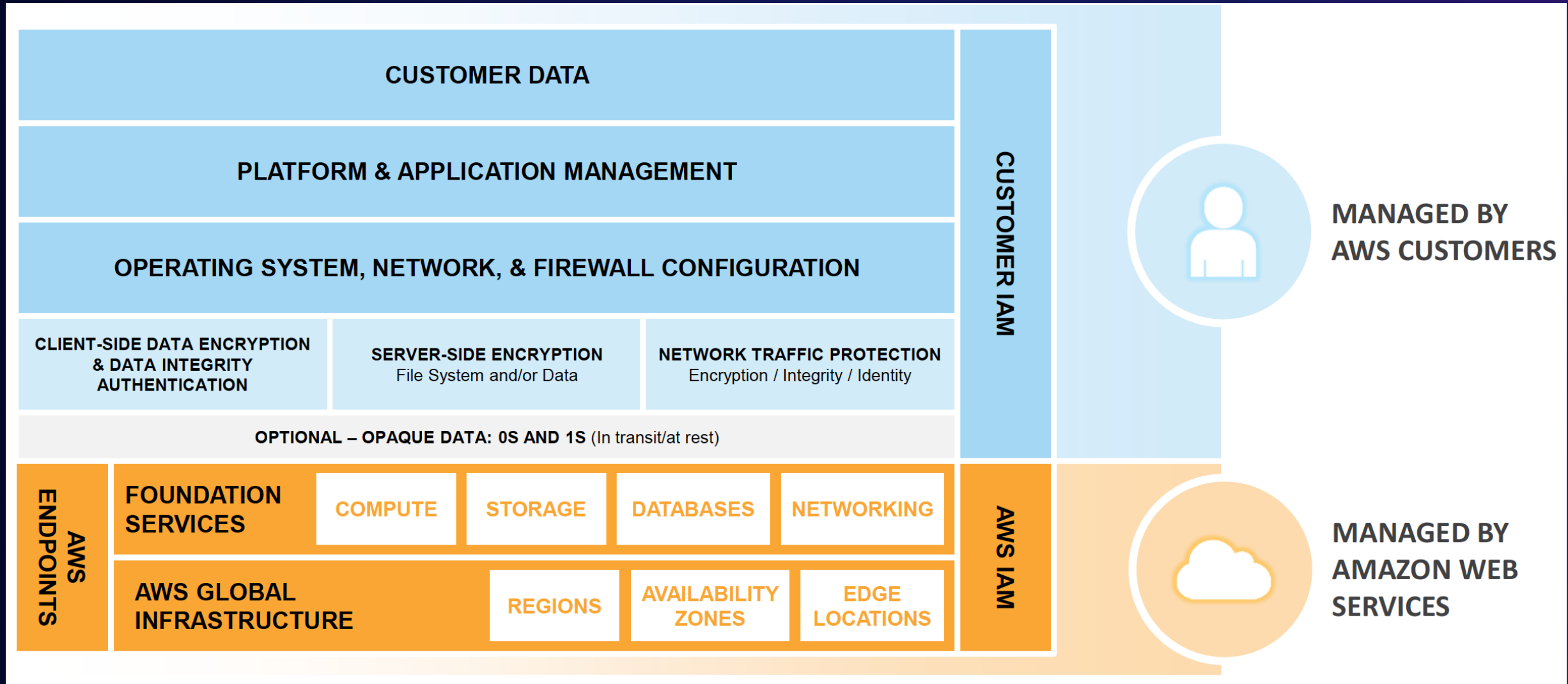
What is resiliency?

“The ability for a system to **continue operating during a failure induced by **load, attacks,** and **failures**, and **recover quickly**.”**

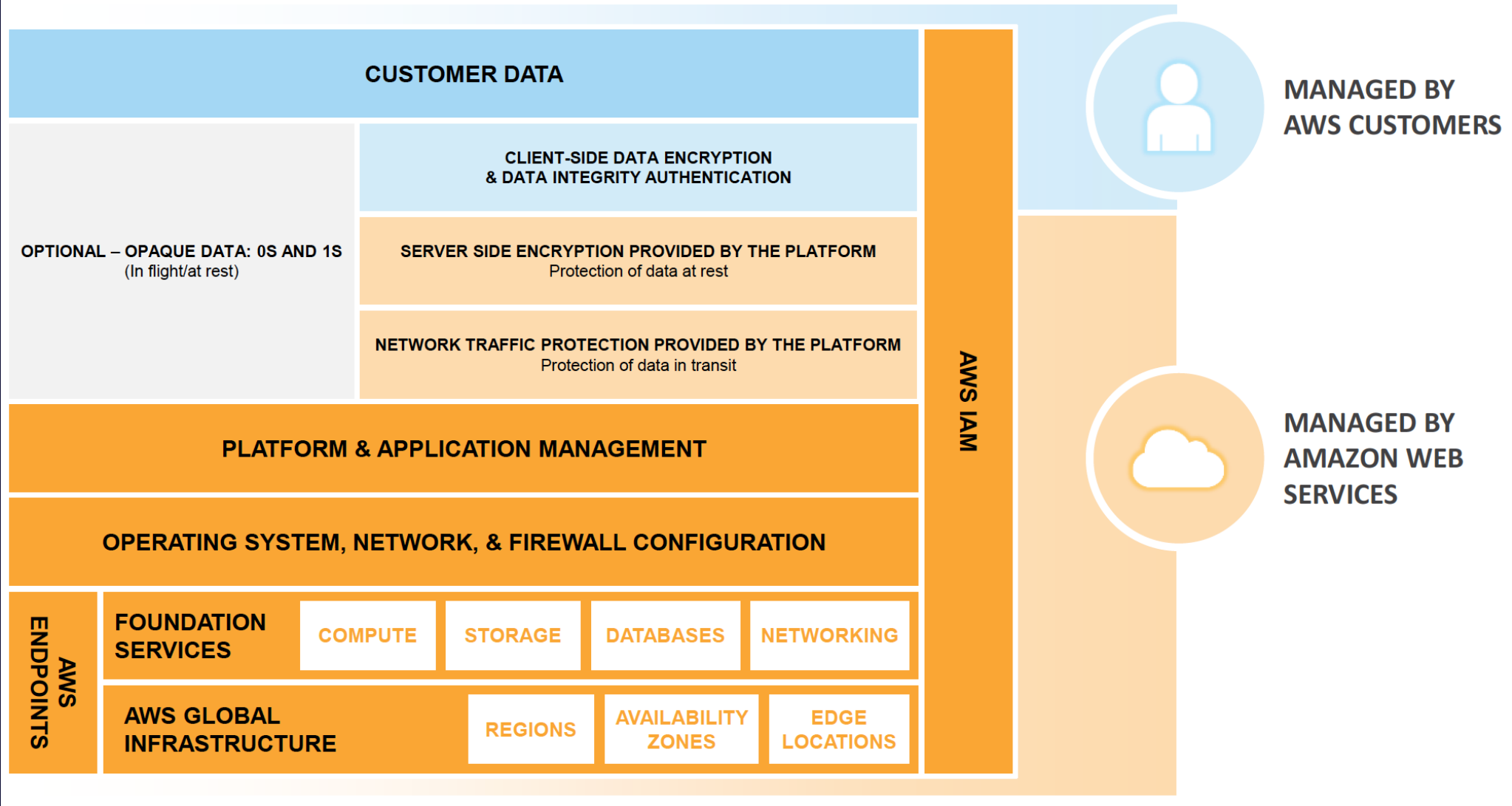
Resiliency Pillar

AWS Well-Architected Framework

Understand the Shared Responsibility Model



Shared Responsibility Model is not static



AWS Region design

AWS Regions are comprised of multiple Availability Zones (AZs) for **high availability**, **high scalability**, and **high fault tolerance**. Applications and data are replicated in real time and consistent in the different AZs.

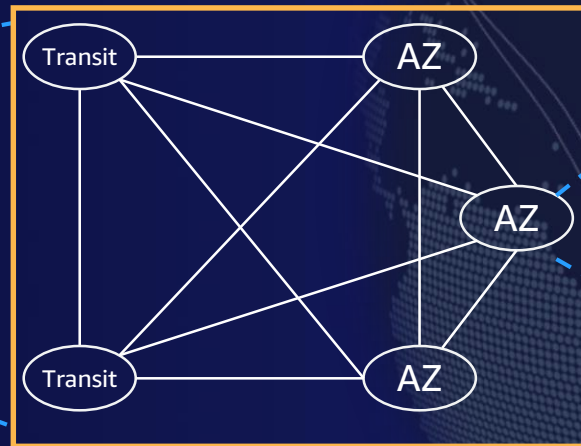


26 geographic Regions

84 AZs

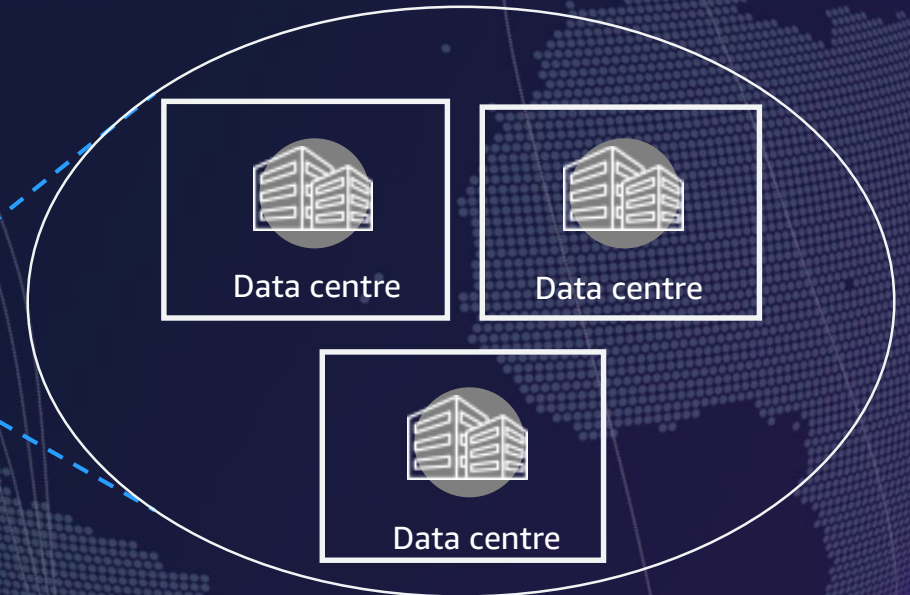
230+ points of presence

AWS **Canada** Region



A **Region** is a physical location in the world where we have multiple **AZs**.

AWS AZ



AZs consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities.

Canada West coming in 2023/2024!

Calgary Region – On track for Q4 2023

FULL REGION – 3 AVAILABILITY ZONES

CA\$21 billion

data centre investment in
Canada by 2037

CA\$39 billion

increase in GDP due to
construction and operation
of our data centres by 2037

5,195

full-time equivalent (FTE)
jobs supported through
construction and operation
of data centres by 2037

AWS locations in Canada



Amazon Offices

Vancouver, Winnipeg,
and Toronto



AWS Regions

Montreal
Calgary (Coming Soon)



Amazon CloudFront Edge Locations

Vancouver, Toronto, and
Montreal



Amazon Solar Farms

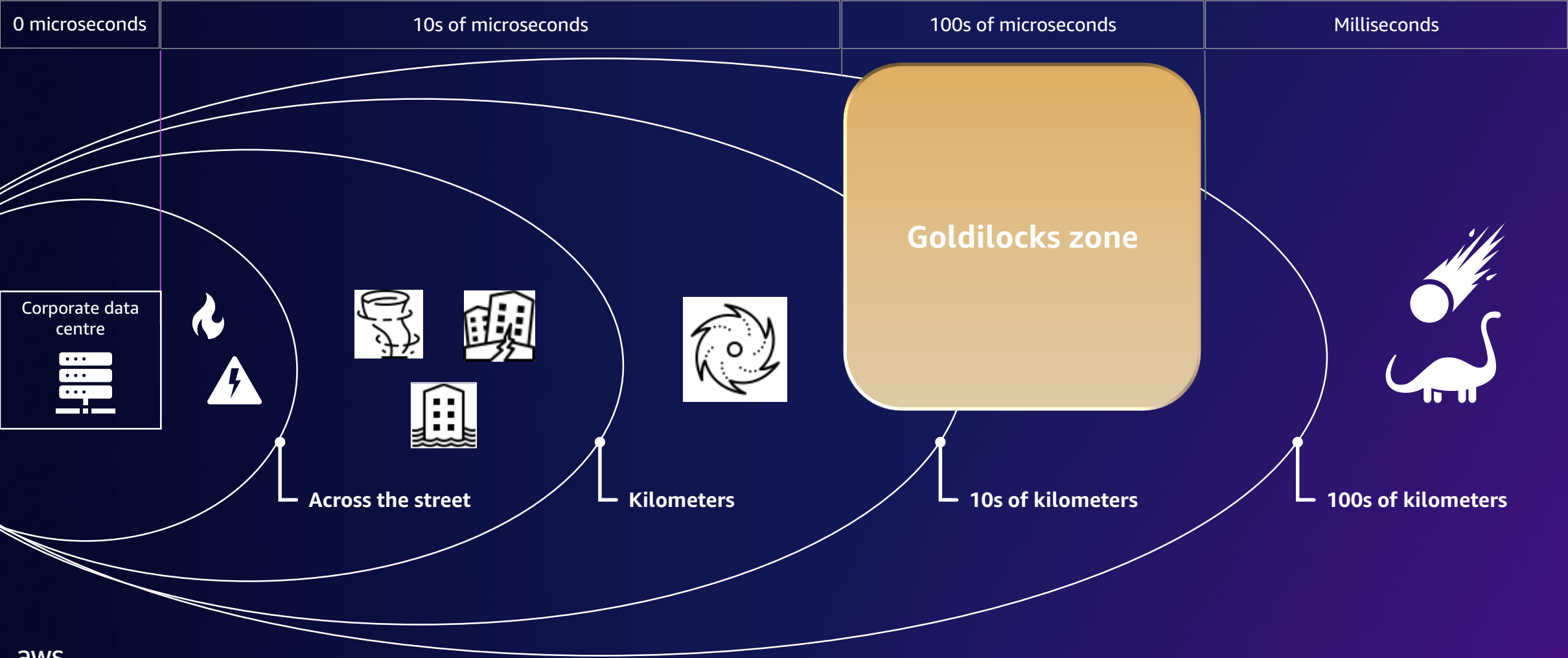
Newell, AB
Vulcan, AB



Goldilocks zone

NOT TOO CLOSE, AND NOT TOO FAR, BUT JUST RIGHT

Distance between data centres



Inherit global security and compliance controls



High-compliance environments

aws

Contact UsSupport▼My Account▼S▼

Products

Solutions

Pricing

Documentation

Learn

Partner Network

AWS Marketplace

Customer Enablement

Events

Explore More

Q

Blog Home

Category ▼

Edition ▼

Follow ▼

AWS Public Sector Blog

Canadian Centre for Cyber Security adds additional AWS services to its assessment of the AWS Canada (Central) Region

by James Kierstead and Brian Mycroft | on 19 NOV 2021 | in Announcements, AWS Artifact, Compliance, Federal, Government, Public Sector, Security, Security, Identity, & Compliance, State Or Local Government | Permalink | Comments | Share



The Canadian Centre for Cyber Security (CCCS) is Canada's authoritative source of cyber security expert guidance, services, and support. CCCS provides this expertise to Canadian governments, industry, and the general public. Their rigorous assessments of cloud service providers are relied on by Canadian public sector organizations across the country, to make informed cloud procurement decisions. In September 2021, CCCS added more Amazon Web Services (AWS) services to its assessment of the AWS Canada (Central) Region, bringing the total number of assessed AWS services to 120. This provides Canadian public sector customers additional confidence that AWS Cloud services meet the Government of Canada's security control requirements.

Resources

AWS in the Public Sector

AWS for Government

AWS for Education

AWS for Nonprofits

AWS for Public Sector Health

AWS for Aerospace and Satellite Solutions

Case Studies

Fix This Podcast

Additional Resources

Contact Us

Follow

☒ AWS for Government

☒ AWS Education

☒ AWS Nonprofits

☒ Newsletter Subscription



Cloud disaster recovery benefits



Traditional disaster recovery

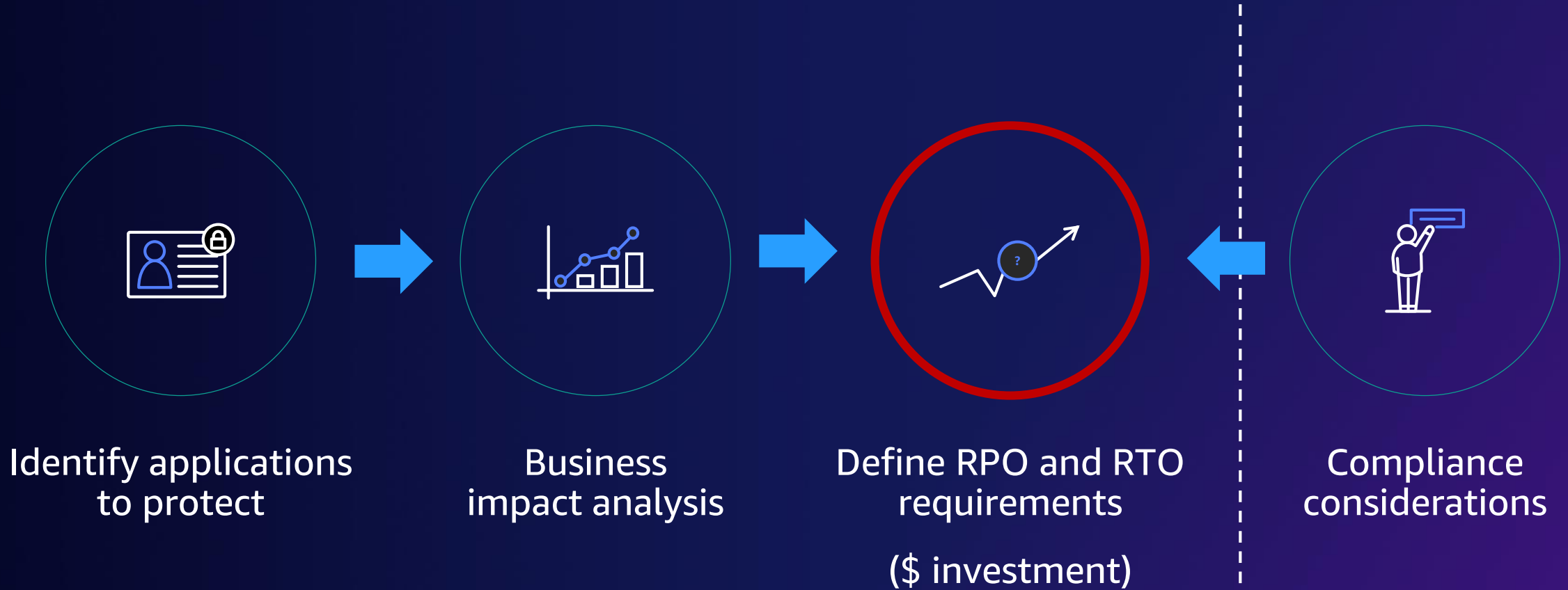
- Massive upfront investment in hardware and high ongoing costs
- Data growth increases hardware and operational costs
- Hard to actually test without business disruption
- Management and infrastructure overhead for globally distributed businesses
- Vulnerable to cyber threats/hacking



Disaster recovery in the cloud

- No upfront hardware investment needed
- Only pay for rightsized compute/storage when actually needed
- Lower IT management overhead
- **(Much)** More automation
- Easy and repeatable testing
- Systems up in minutes (not hours/days)

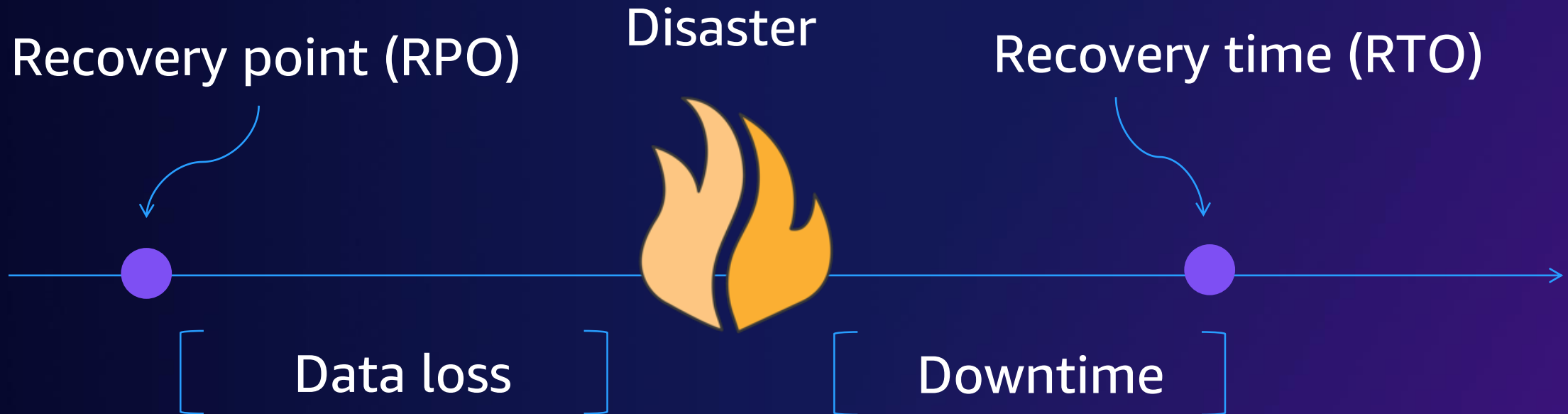
Start with requirements



Objectives and impacts

How much data can you afford to recreate or lose?

How quickly must you recover?
What is the cost of downtime?

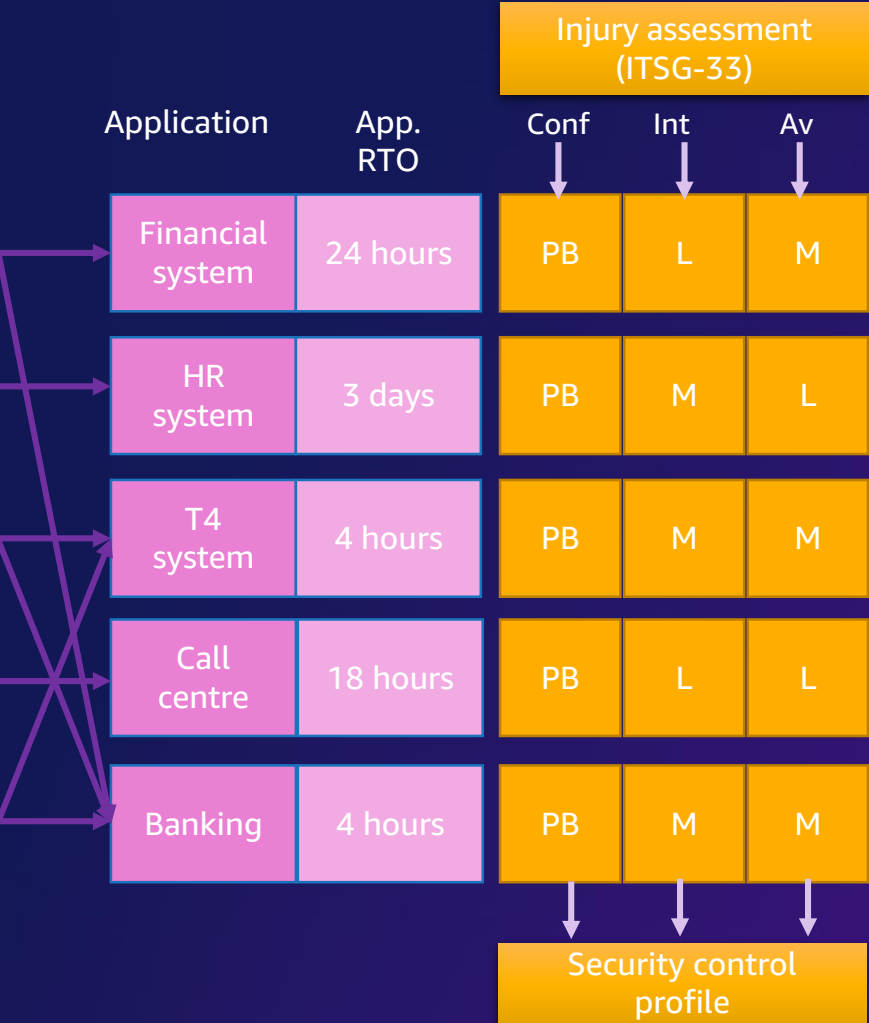


What does policy tell us?

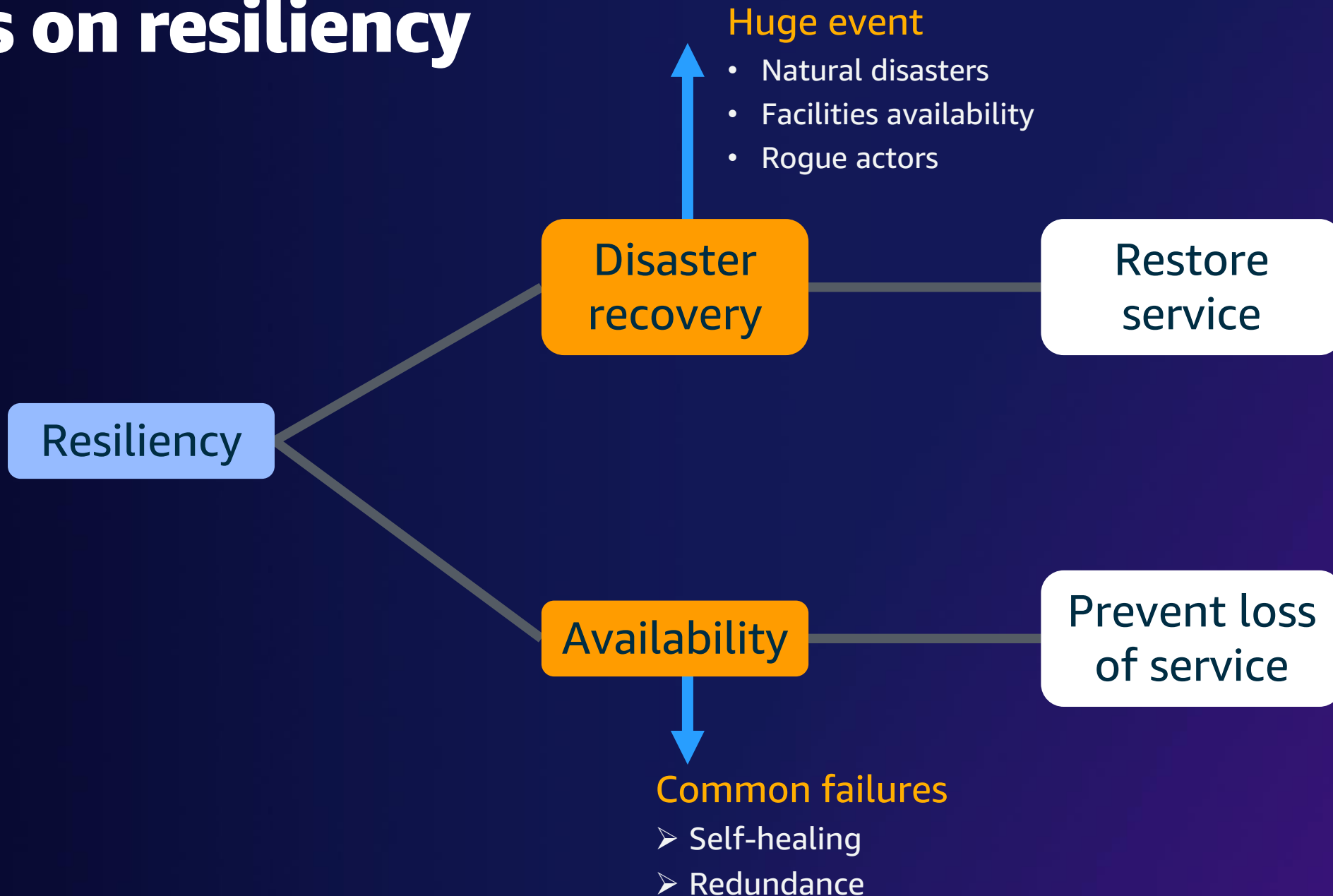
Business impact assessment
(Appendix D: Mandatory Procedures for Business Continuity Planning)

Service	Potential impacts	Service RTO
Payroll	Operations – Cannot pay employees. Emergency checks can be issued for a period.	24 hours
Staffing	Operations – Emergency staffing only. Letters of offer issued ad hoc.	3 days
Personal tax processing	Reputation – Inability to perform core function of organization. 30,000 taxes processed daily.	12 hours
Inquiries	Reputation – Public-facing service will be unavailable. 1,000 calls per day unanswered.	24 hours
Payments	Operations – Inability to pay out \$5M daily to small and medium businesses.	8 hours

Data categorization
(Appendix J: Standard on Security Categorization)



Focus on resiliency



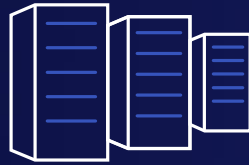
Categories of failures

WHEN TO CHOOSE SINGLE REGION VS. MULTI-REGION



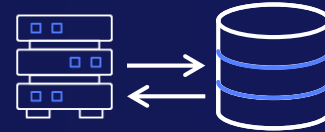
Code deployments and configuration

(e.g., bad deployment, cred expiration)



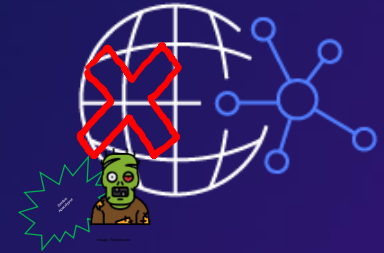
Core infrastructure

(e.g., data centre failure, host failure)



Data and state

(e.g., data corruption)

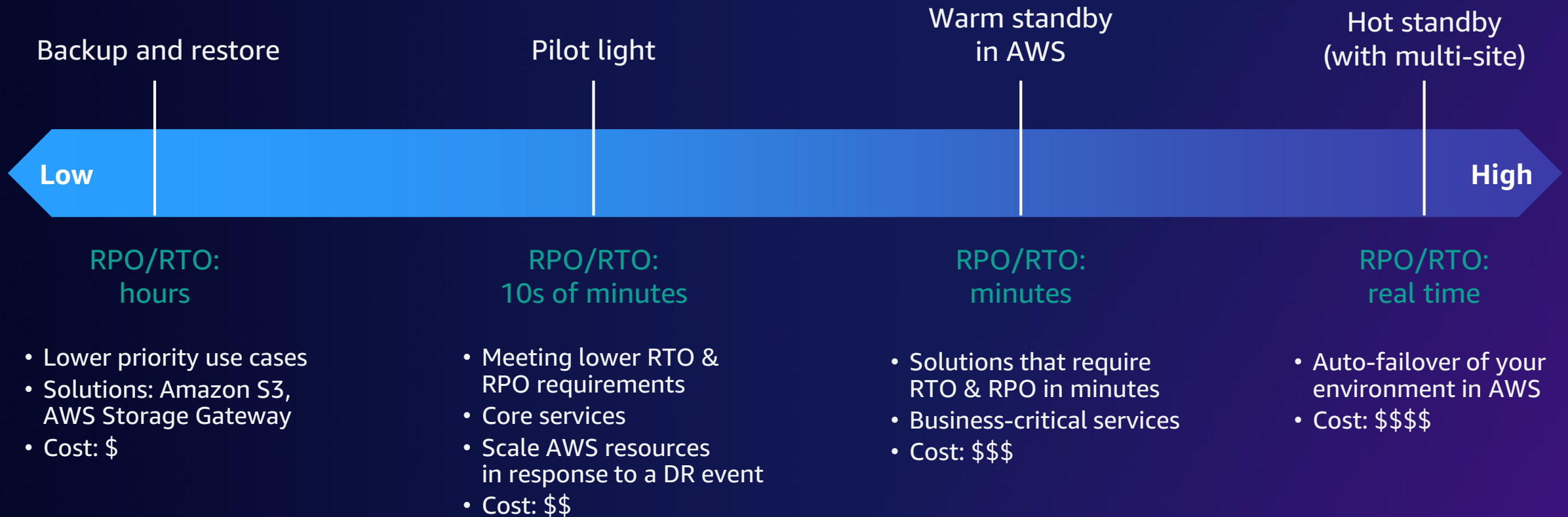


Highly unlikely scenarios






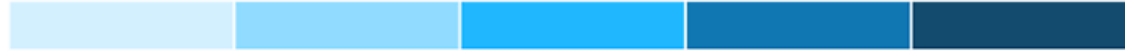
(e.g., all of internet failures, environmental disasters, supplier failures)



AWS DR strategies (factors: complexity & time)

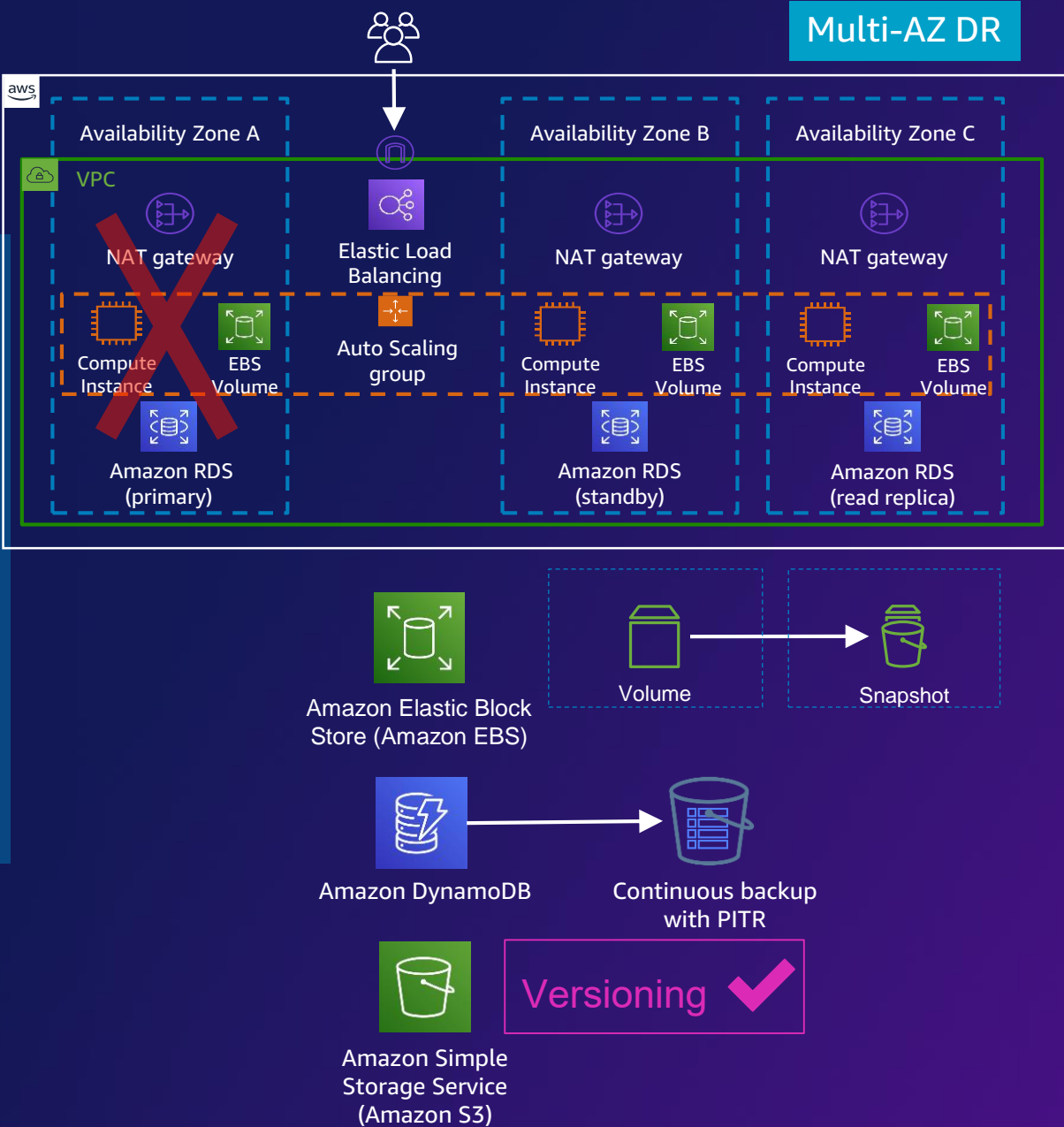
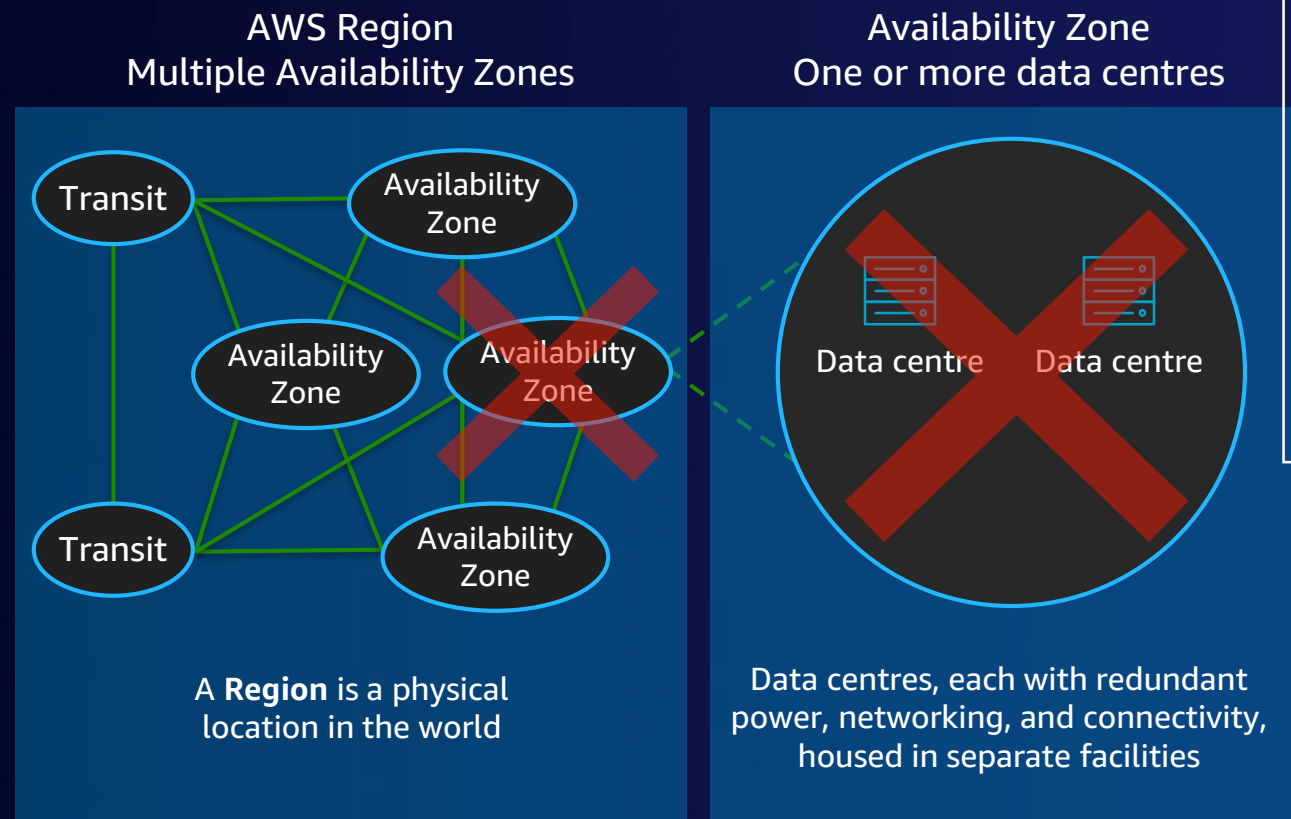


Resiliency patterns and trade-offs

		P1	P2	P3	P4	P5
		Multi-AZ Deployment	Static Stability in Region	Application Portfolio Distribution	Multi-AZ Deployment [Regional DR]	Multi-Region Active-Active Deployment
Design Complexity		Low	Medium	Medium	High	Very High
Cost to Implement		Low	High	Medium	High	High
Operational Effort		Low	Medium	Medium	Medium	Very High
Effort to Secure		Low	Medium	Medium	High	High
Environmental Impact		Low	Medium	Medium	High	High
						
		Lowest	Availability			Highest

Single Region

DISASTER EVENT SCOPE: AVAILABILITY ZONE



Develop & exercise your incident response plan

People

- ✓ Train security operations staff on AWS

Process

- ✓ Develop an incident response plan and strategy
- ✓ Run drills and automate simulations where possible

Technology

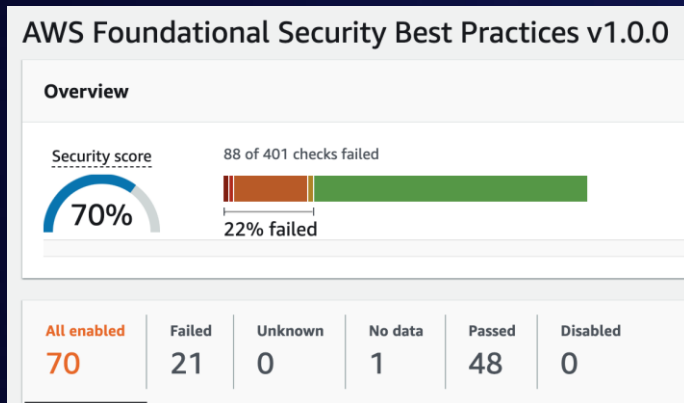
- ✓ Build AWS accounts for security operations and log archival
- ✓ Create read-only and break-glass roles for access to AWS accounts
- ✓ Set up security services like Amazon GuardDuty and AWS Security Hub to detect threats
- ✓ Use security services like Amazon Detective to help you investigate security findings

Perform self-assessments

AWS Well-Architected

Learn, measure, and build using architectural best practices

AWS Security Hub



 [awslabs](#) / [aws-security-assessment-solution](#)

These security assessments are from the open source projects "[Prowler](#)" and "[ScoutSuite](#)," which include custom modules that **check for ransomware-specific findings**

AWS Fault Injection Simulator

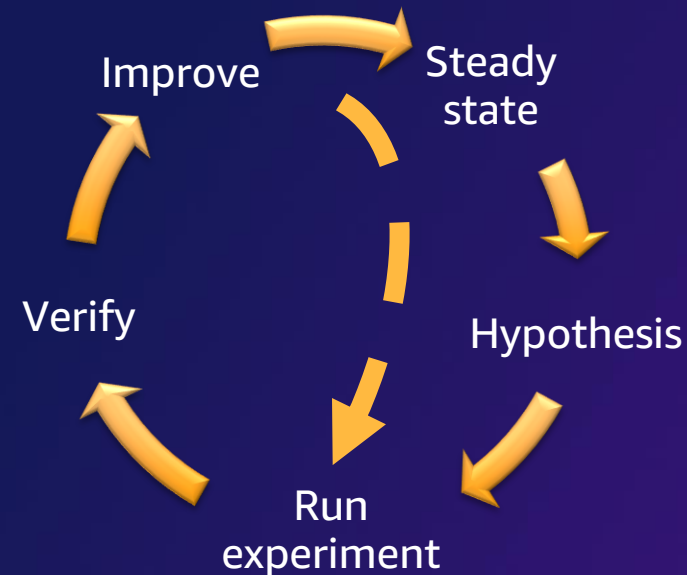
FULLY MANAGED CHAOS ENGINEERING SERVICE ON AWS



Improve application performance and resiliency

Safely run chaos experiments with fine-grained controls

Test complex, real-world failure scenarios



Key takeaways

- Availability and residency starts with the business
- State your requirements as objectives; avoid specifying solutions
- Understand, and explain, the optionality and impact of recovery choices
- Resiliency is not a pass/fail; it is something to work on continuously
- Make sure you have a plan
- TEST!

Additional resources



AWS resilience tools

HOW AWS HELPS YOU DESIGN RESILIENT WORKLOADS

AWS Resilience Hub

Protect



AWS Backup



AWS Elastic Disaster Recovery



CloudEndure Disaster Recovery



AWS Systems Manager

Protect data and applications

Define



AWS CloudFormation



AWS Service Catalog AppRegistry

Define resilience of applications

Test



AWS Fault Injection Simulator

Test to improve resilience

Monitor and Manage



Amazon DevOps Guru



AWS CloudTrail



Amazon CloudWatch



Amazon Route 53 Application Recovery Controller

Receive alerts and conduct readiness checks

Recover



AWS Backup



AWS Elastic Disaster Recovery



CloudEndure Disaster Recovery



AWS Systems Manager

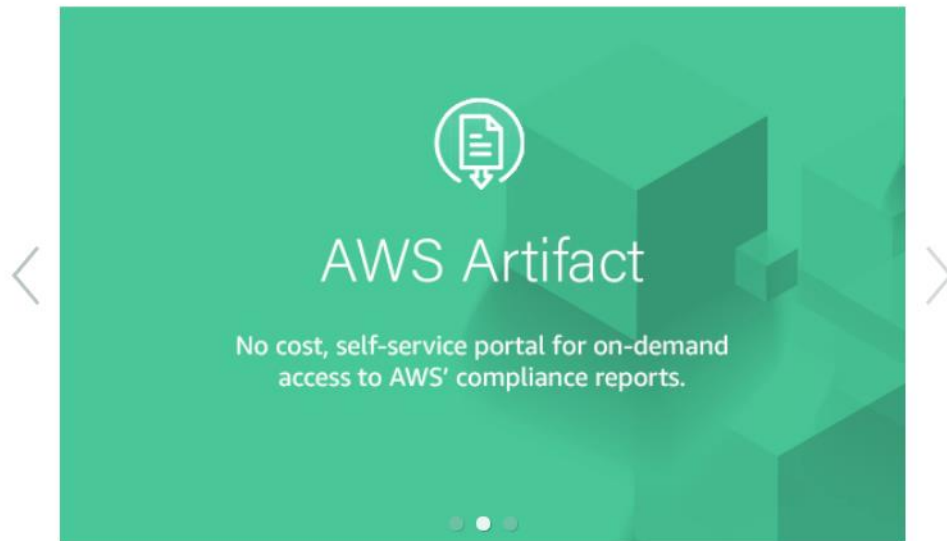
Restore data and applications

Available reports

AWS Compliance

Learn more about our compliance offerings and why we serve our customers best

Compliance Enablers



<https://aws.amazon.com/compliance/>

AWS Artifact

No cost, self-service portal for on-demand access to AWS' compliance reports.

Get Started with AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

You can access AWS Artifact directly from the [AWS Management Console](#) »

<https://aws.amazon.com/artifact/>

Security resources

Developer information, articles and tutorials, security products, and whitepapers

Learning

Security in the cloud is similar to security in your on-premises data centers — only without the costs of maintaining facilities and hardware. In the cloud, you don't have to manage physical servers or storage devices. Instead, you use software-based security tools to monitor and protect the flow of information into and out of your cloud resources. For this reason, cloud security is a **Shared Responsibility** between the customer and AWS, where customers are responsible for “security in the cloud” and AWS is responsible for “security of the cloud.”

The AWS cloud allows you to scale and innovate while maintaining a secure environment. As an AWS customer, you will benefit from data centers and network architecture designed to meet the requirements of the most security-sensitive organizations. AWS infrastructure is custom-built for the cloud and is monitored 24x7 to help protect the confidentiality, integrity, and availability of our customers' data.

Browse this page to learn more about key topics, areas of research, and training opportunities for cloud security on AWS.

Whitepapers, Technical Guides, and Reference Materials | Security Documentation | Provable Security: Research and Insights | Training | AWS Security Control Domains | International Content

<http://aws.amazon.com/security/security-resources/>

Security blog

Subscribe to the blog – it's a great way to stay up-to-date on AWS security and compliance

AWS Blog

Learn how to get started with AWS Network Firewall, available now for all your AWS virtual network security needs.

FEATURED STORY

Category or format:
[Clear all](#)

▼ Category

☐ Alexa

☐ Analytics

☐ Application Integration

☐ Architecture

☐ AR & VR

☐ AWS Cost Management

☐ AWS Marketplace

☐ AWS Partner Network

☐ Big Data

☐ Business Applications

☐ Compute

Bringing Agility to Financial Services with the Fujitsu Mainframe Modernization Solution

Yusuf Ali, Rob Evans, Eric Payeur, Serge Moro, Addy Dubhashi, 11/21/2020

Fujitsu offers a commercial and technical solution for mainframe modernization on AWS that makes application modernization possible and sensible.. Fujitsu's end-to-end approach helps financial services address their challenges in a cost-effective manner. This helps organizations realize the required future-proof scalability, agility, and extensibility of their core legacy systems. Fujitsu is an AWS Advanced Consulting Partner with the AWS Migration Competency.

Getting started with Amazon Kendra ServiceNow Online connector

David Shute, Juan Bustos, 11/21/2020

Amazon Kendra is a highly accurate and easy-to-use intelligent search service powered by machine learning (ML). To make it simple to search data across multiple content repositories, Amazon Kendra offers a number of native data source connectors to help get your documents easily ingested and indexed. This post describes how you can use the Amazon [...]

Amazon Augmented AI is now a HIPAA eligible service

Anuj Gupta, 11/20/2020

Amazon Augmented AI (Amazon A2I) is now a HIPAA eligible service. Amazon A2I makes it easy to build the workflows required for human review of machine learning (ML).

Learning levels:
▶ Choose a level

Industry
▶ Choose an industry

Product or solution:
▶ Analytics

▶ Artificial Intelligence

▶ Business Applications

▶ Compute

▶ Customer Enablement

▶ Customer Engagement

▶ Database

▶ Developer Tools

<http://blogs.aws.amazon.com/security/>

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learn in-demand AWS Cloud skills



AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand



Train now



AWS Certifications

Earn an industry-recognised credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits



Access **new** exam guides

Thank you!



Please complete the session survey in the mobile app

Android



iOS

