Cloud architectural patterns:

Platform and application best practices

Vinod Kisanagaram

Solutions Architect
Amazon Web Services
vinodaws@amazon.com

aws Learning Days
State, Local, and Education

Cloud Foundations

10:15am – 11:15am

200 level

Cloud architectural patterns:

Master Cloud Architecture: Build Secure, Scalable Solutions with AWS Best Practices and Enterprise-Grade Design Strategies.

11:30am – 12:30pm

200 level

Cultural Transformation Through FinOps:

Go Beyond Cost Management: FinOps unites teams to optimize cloud costs while driving efficient growth

1:30pm – 3:00pm

200 level

Cloud Lab Potpourri

Hands-On Cloud Adventure: Customize Your AWS Learning with Interactive Technical Workshops and Personalized Lab Experiences.

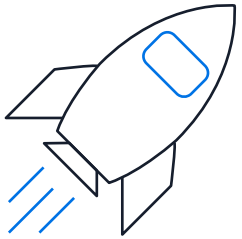
3:15pm – 4:15pm

300 level

Designing modern applications in AWS

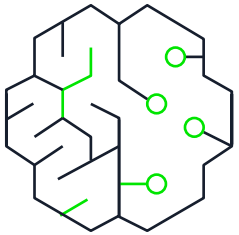
Unlock Serverless Potential: Reduce Costs, Boost Scalability, and Enhance Security with Cloud-Native Architectures.

Why Cloud Architecture Matters



Build and deploy faster

Lower or mitigate risks



Make informed decisions

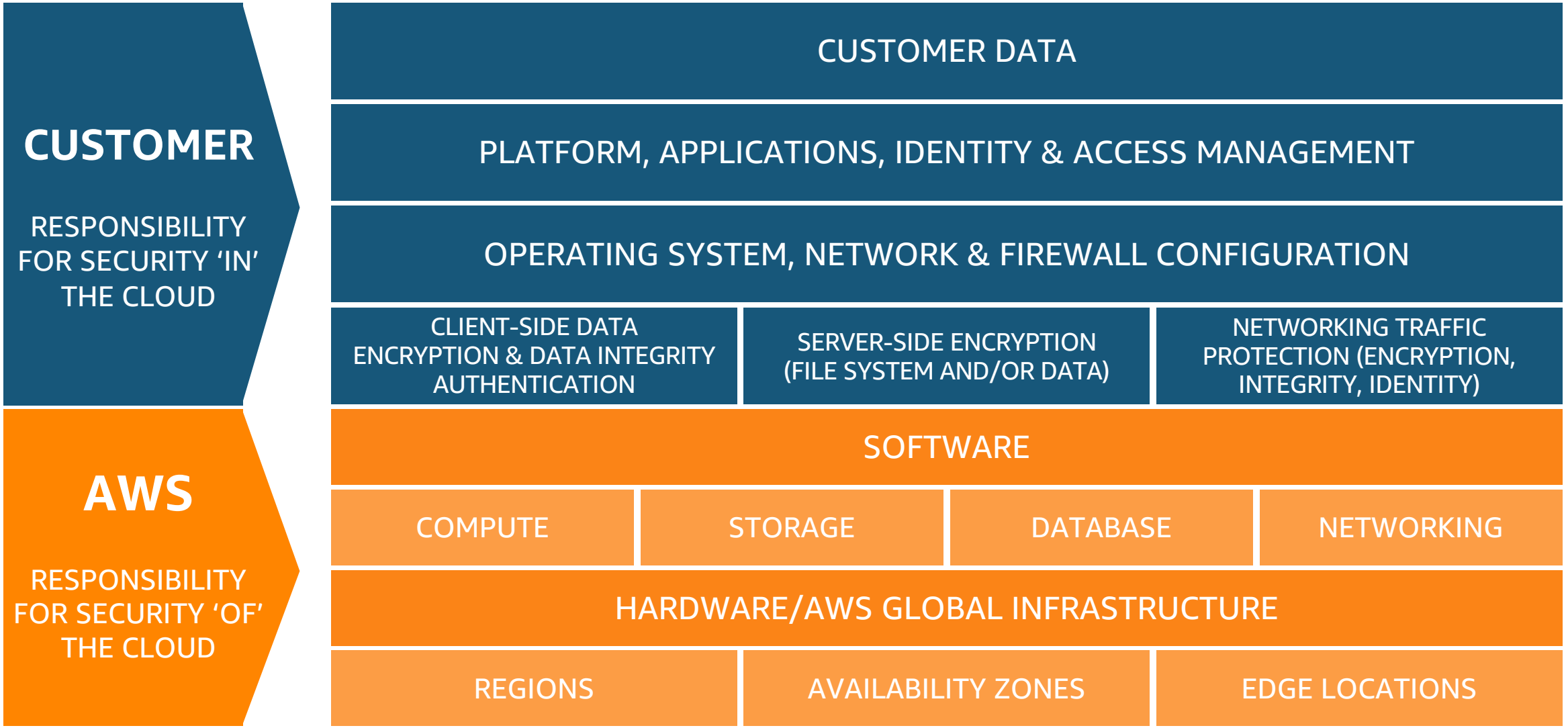
Also -

“Everything fails, all the time.”

Werner Vogels

CTO, Amazon.com

AWS Shared Responsibility Model



The Situation

Meet Bob – Our new Junior developer, and taco enthusiast.

Bob just joined the team three months ago, fresh out of college. When he's not dreaming about finding the perfect taco truck, he's eager to prove himself as a developer. His manager just gave him his first solo project: **deploying a website** for a **major government service** that's expected to go viral once citizens discover how much time it will save them.

The conversation went something like this:
Manager: "Bob, can you get this website **up in AWS** for the client?"
Bob (confidently): "No problem! I've built WordPress sites on my laptop before!"

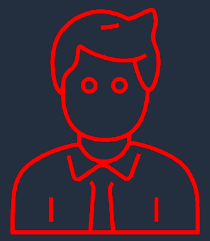
Bob gets to work and implements the application.
Proudly told his manager "It's live!" while heading out for his celebratory taco lunch

A is for “Alice” and B is for “Bob”

Alice follows best practices

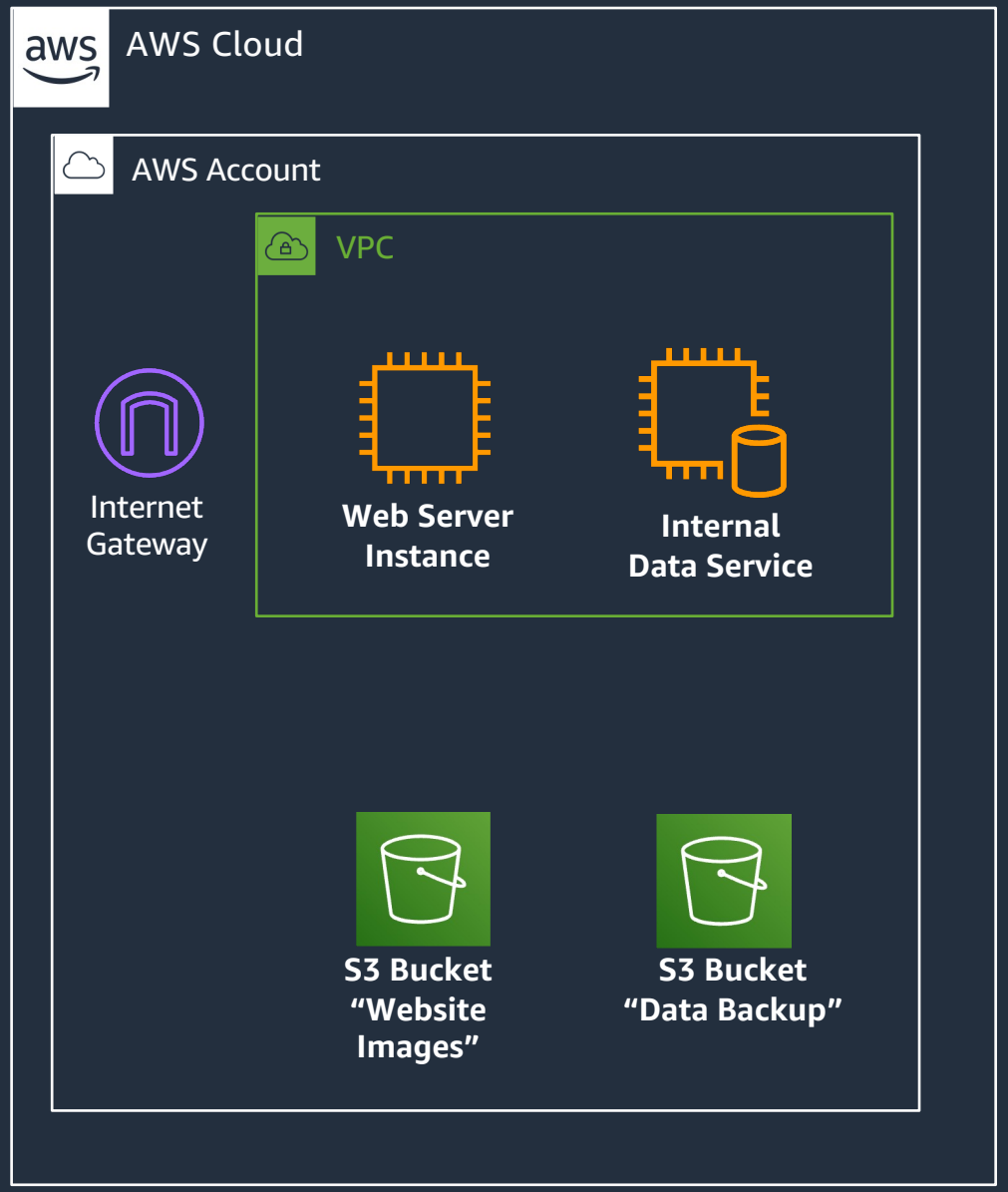
Bob does NOT follow best practices

Bob's Bad Day

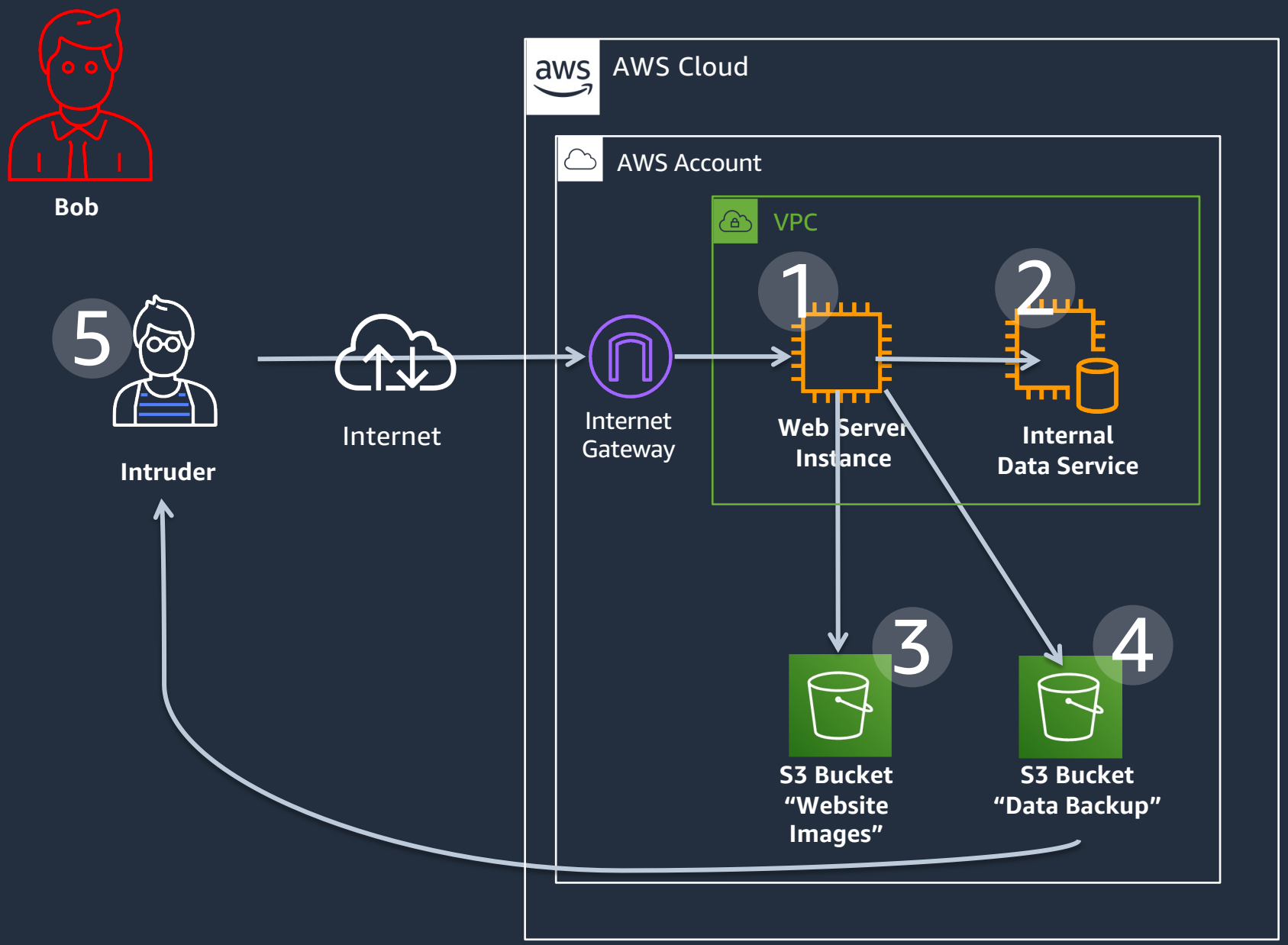


Bob

Internet

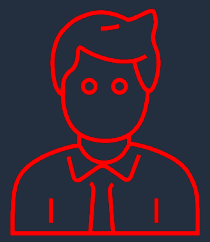


Bob's Bad Day



1. Access the vulnerable web application
2. Pivot to the data service
3. Delete the website image files
4. Change permissions to the data backup
5. Download the data backup

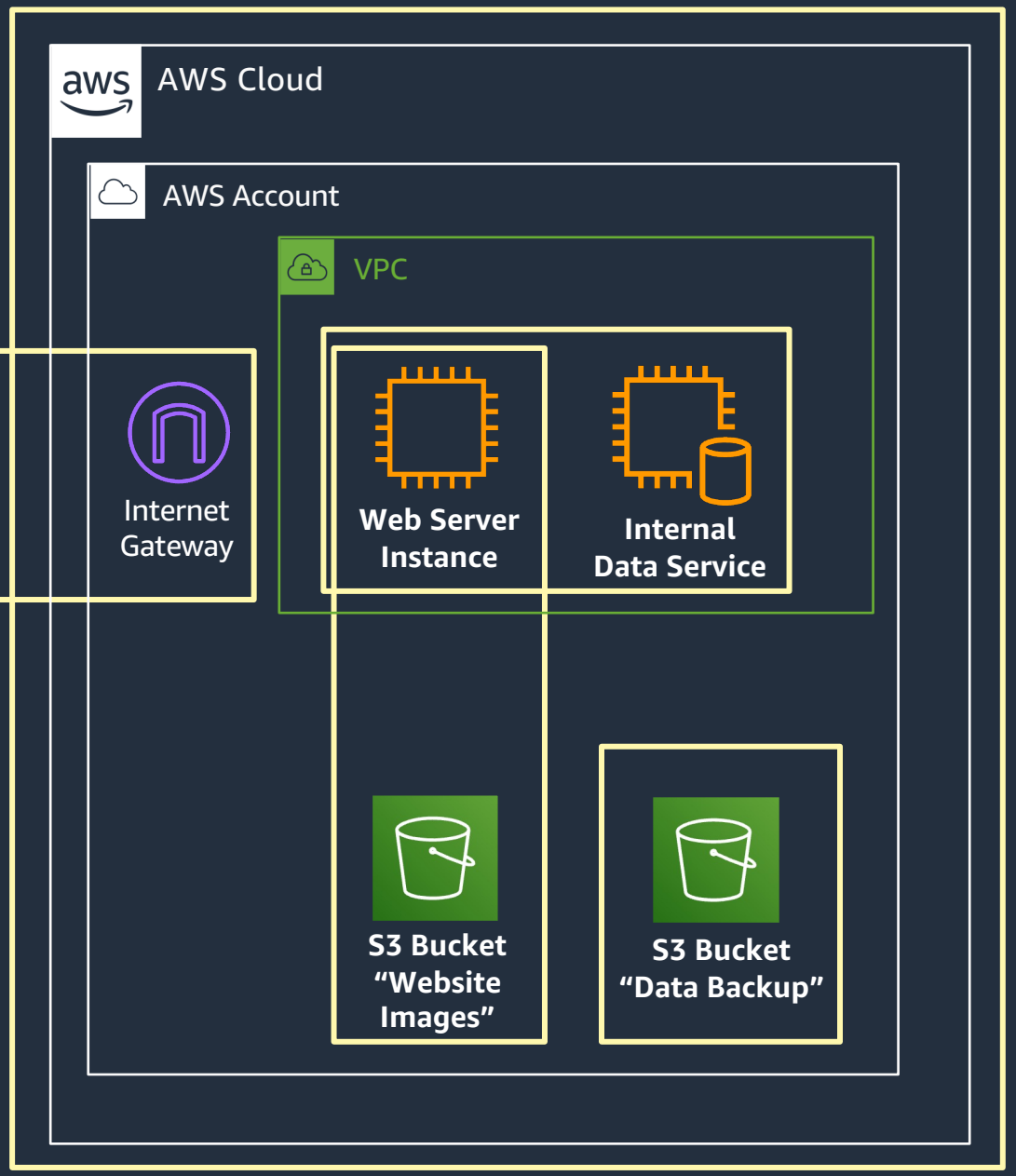
Bob's Bad Day



Bob

Alice

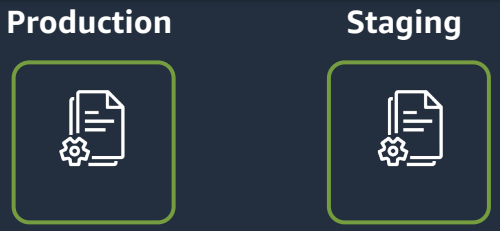
… now let's help Alice have a great day!



1. No web application protection
2. No segmentation
3. One account
4. All permissions granted
5. Sensitive data not encrypted
6. No logging, monitoring, alerting

Better Practices: Identity and access management

1) Use **multiple AWS accounts** to reduce scope of impact



AWS accounts provide administrative isolation between workloads across different lines of business, regions, stages of production and classes of data.

5	0
CIS Foundation Benchmark	CIS Web-Tier Benchmark

2) Use **limited roles** and grant **temporary security credentials**

IAM roles and temporary security credentials mean you don't always have to manage long-term credentials and IAM users for each entity that requires access to a resource.

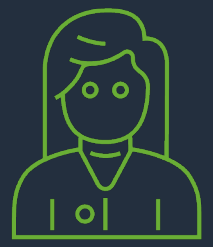
13	8
CIS Foundation Benchmark	CIS Web-Tier Benchmark

3) **Federate** to an existing identity service

Control access to AWS resources, and manage the authentication and authorization process without needing to recreate all your corporate users as IAM users.

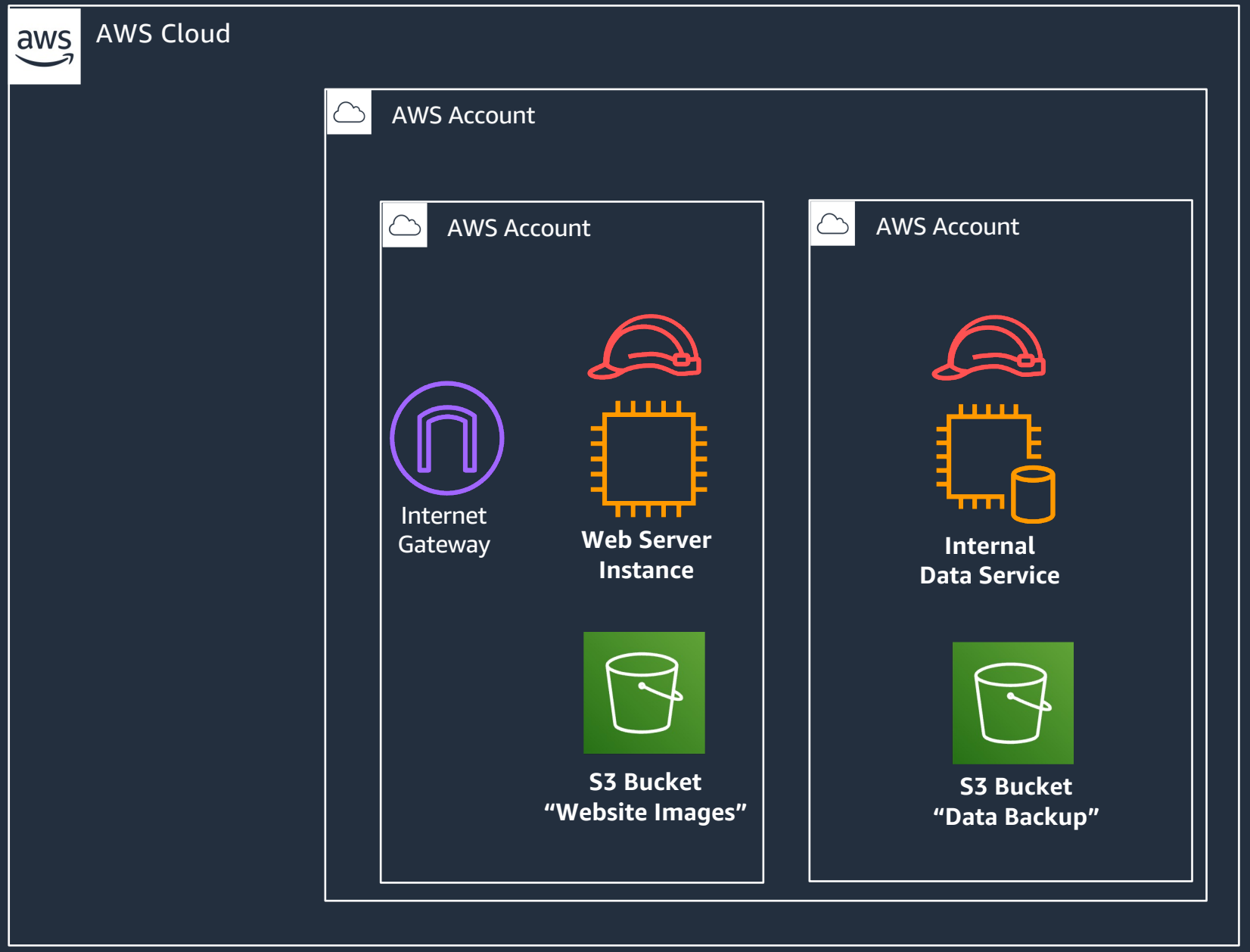
0	0
CIS Foundation Benchmark	CIS Web-Tier Benchmark

Identity and Access Management



Alice

Internet



AWS IAM Identity Center

MFA token

1

IAM

Secrets Manager

Better Practices: logging and monitoring

4) **Turn on logging** in all accounts, for all services, in all regions

AWS CloudTrail

Amazon GuardDuty

The AWS API history in CloudTrail enables security analysis, resource change tracking, and compliance auditing. GuardDuty provides managed threat intelligence and findings.

8 CIS Foundation Benchmark

6 CIS Web-Tier Benchmark

5) Use the AWS platform's built-in **monitoring and alerting** features

AWS Security Hub

AWS Config

Monitoring a broad range of sources will ensure that unexpected occurrences are detected. Establish alarms and notifications for anomalous or sensitive account activity.

15 CIS Foundation Benchmark

3 CIS Web-Tier Benchmark

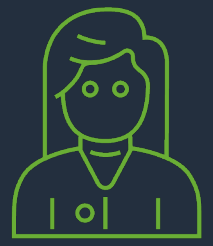
6) Use a separate AWS account to fetch and **store copies of all logs**

Configuring a security account to copy logs to a separate bucket ensures access to information which can be useful in security incident response workflows.

2 CIS Foundation Benchmark

3 CIS Web-Tier Benchmark

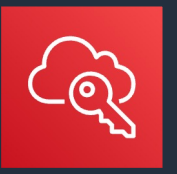
Logging and Monitoring



Alice

Internet

1



AWS IAM Identity Center

MFA token

IAM

Secrets Manager

Better Practices: Infrastructure security

7) Create a **threat prevention layer** using AWS edge services

Use the hundreds of worldwide points of presence in the AWS edge network to provide scalability, protect from denial-of-service attacks, and protect from web application attacks.

0	5
CIS Foundation Benchmark	CIS Web-Tier Benchmark

8) Create **network zones** with Virtual Private Clouds (VPCs) and security groups

Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.

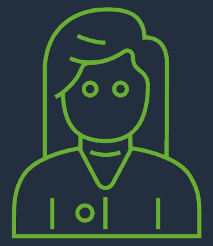
5	30
CIS Foundation Benchmark	CIS Web-Tier Benchmark

9) Manage vulnerabilities through **patching and scanning**

Test virtual machine images and snapshots for operating system and application vulnerabilities throughout the build pipeline, and into the operational environment.

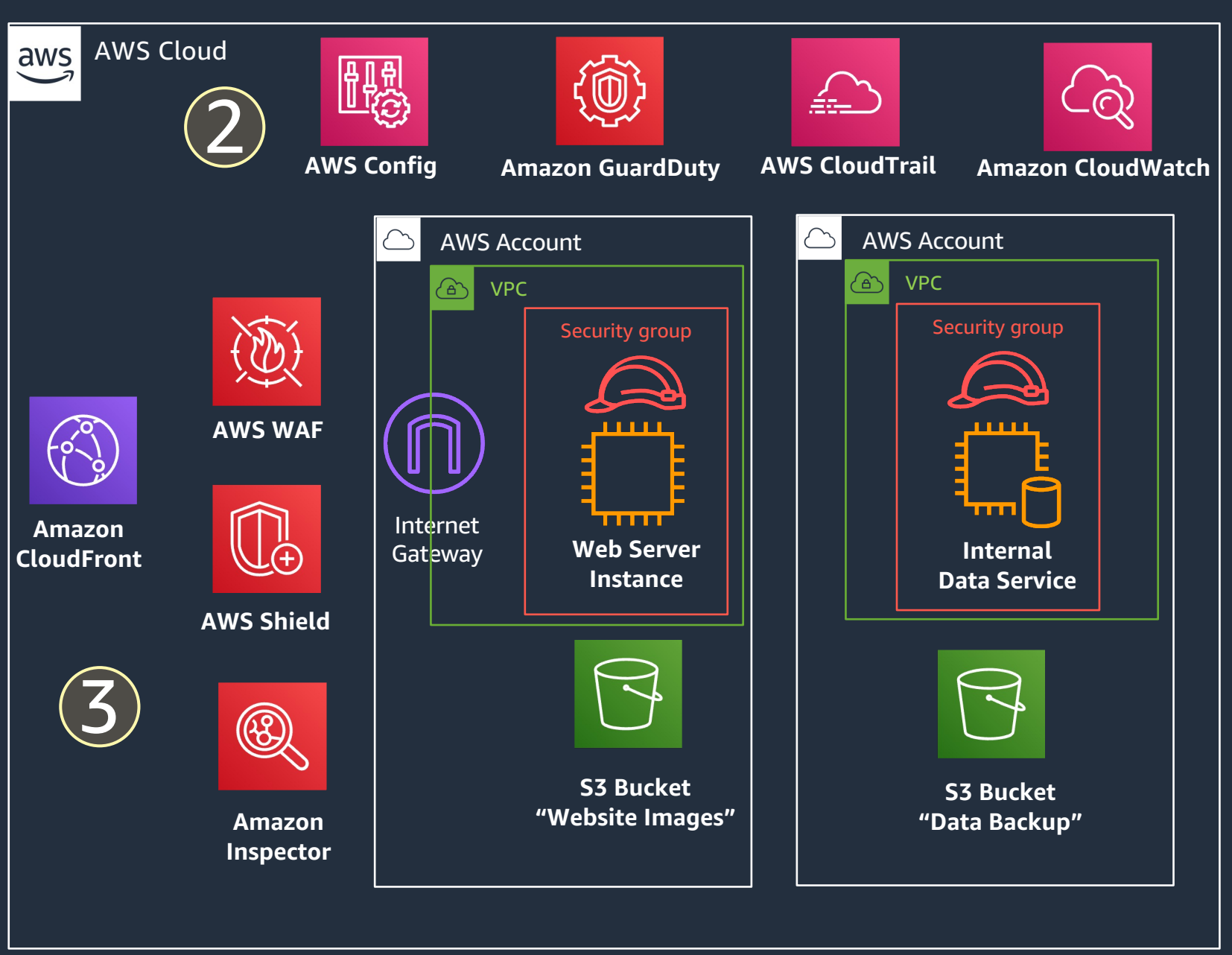
0	1
CIS Foundation Benchmark	CIS Web-Tier Benchmark

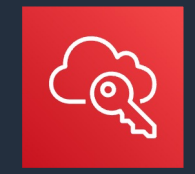
Infrastructure Security



Alice

Internet





AWS IAM Identity Center

MFA token

1

IAM

Secrets Manager

Better Practices: Data protection

10) Use **server-side encryption** with provider managed keys

AWS KMS

Data Encryption Key

AWS Key Management Service (KMS) is seamlessly integrated with multiple AWS services. You can use a default master key or select a custom master key, both managed by AWS.

1 CIS Foundation Benchmark

1 CIS Web-Tier Benchmark

11) Encrypt **data in transit** (with no exceptions)

Amazon CloudFront

Certificate Manager

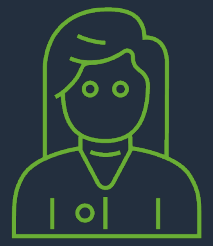
SSL / TLS / HTTPS

Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.

0 CIS Foundation Benchmark

9 CIS Web-Tier Benchmark

Data Protection


Alice

Internet

AWS Cloud

AWS Config

Amazon GuardDuty

AWS CloudTrail

Amazon CloudWatch

AWS Account

VPC

Security group

Internet Gateway

Web Server Instance

AWS Account

VPC

Security group

Internal Data Service

Amazon CloudFront

AWS WAF

AWS Shield

ACM

4

Amazon Inspector

AWS KMS

S3 Bucket "Website Images"

S3 Bucket "Data Backup"

AWS IAM Identity Center

MFA

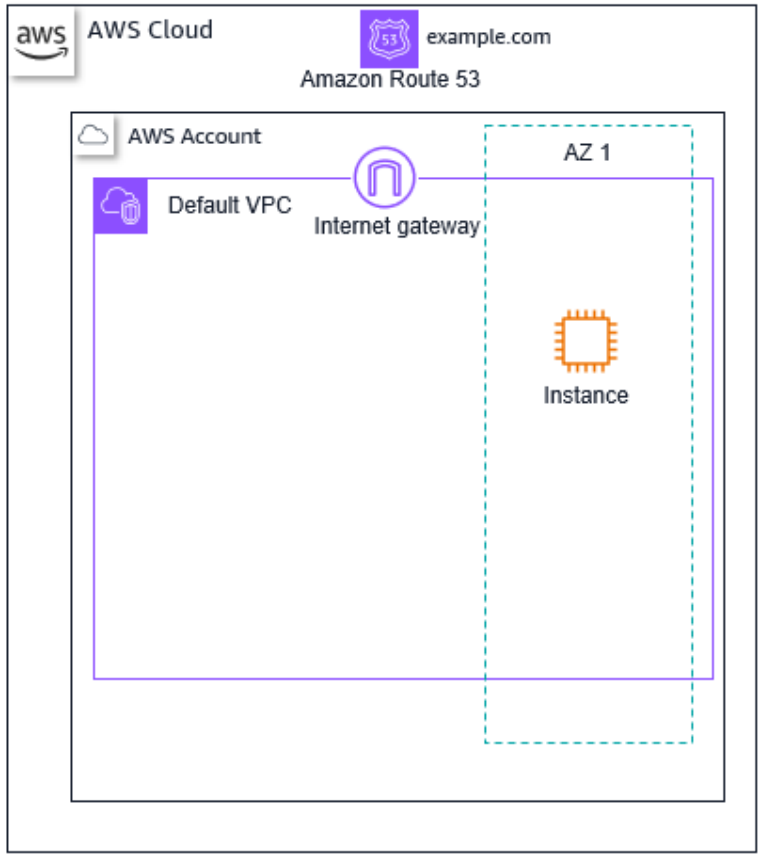
MFA token

IAM

Secrets Manager

Pillars of the AWS well-architected framework

Bob’s Bad Day



Security

Reliability

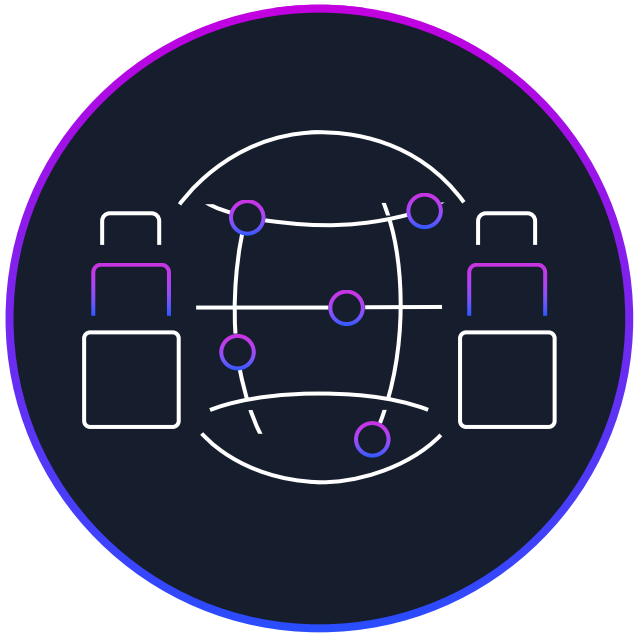
Operational Excellence

Performance Efficiency / Cost Optimization

Security – Top design principles

- Implement a strong identity foundation
- Maintain traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Reliability – Top design principles



- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Manage change through automation

Operational Excellence

- Perform operations as code
- Make frequent, small, reversible changes
- Refine operation procedures frequently
- Anticipate failure
- Learn from all operational failures
- Use managed services

Performance Efficiency & Cost Optimization

- Scale based on need
- Go global in minutes
- Use serverless architectures
- Monitor usage and optimize for cost

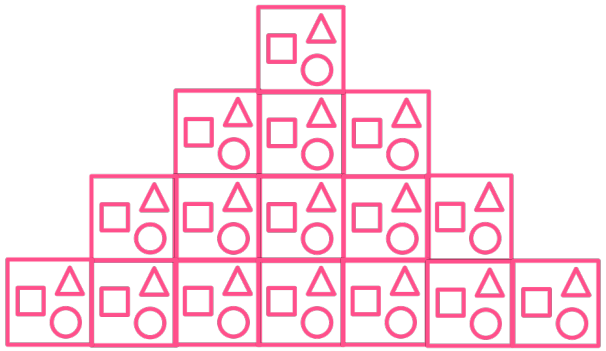
…but how do you scale this?

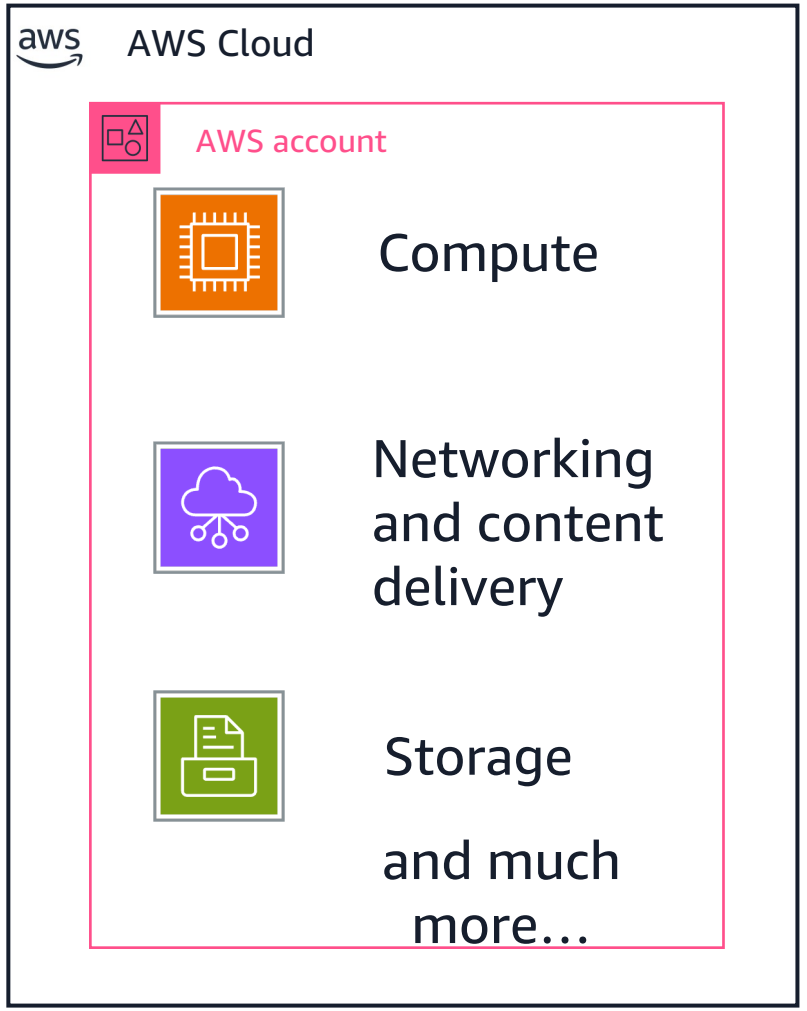
Use accounts as building blocks

Account limits
Quotas

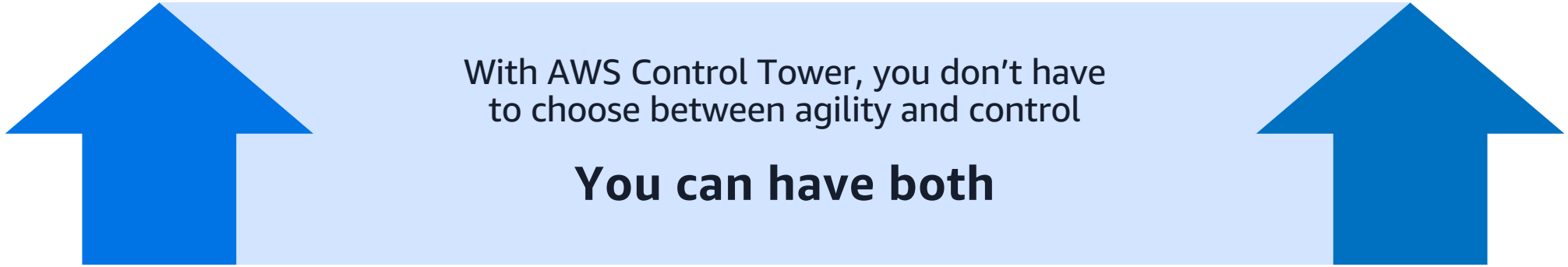
Security
Natural boundaries, isolation

Compliance/ business processes
Billing, custom requirements





Business agility and governance control



Governance

Security

Compliance

Operations

Spend management

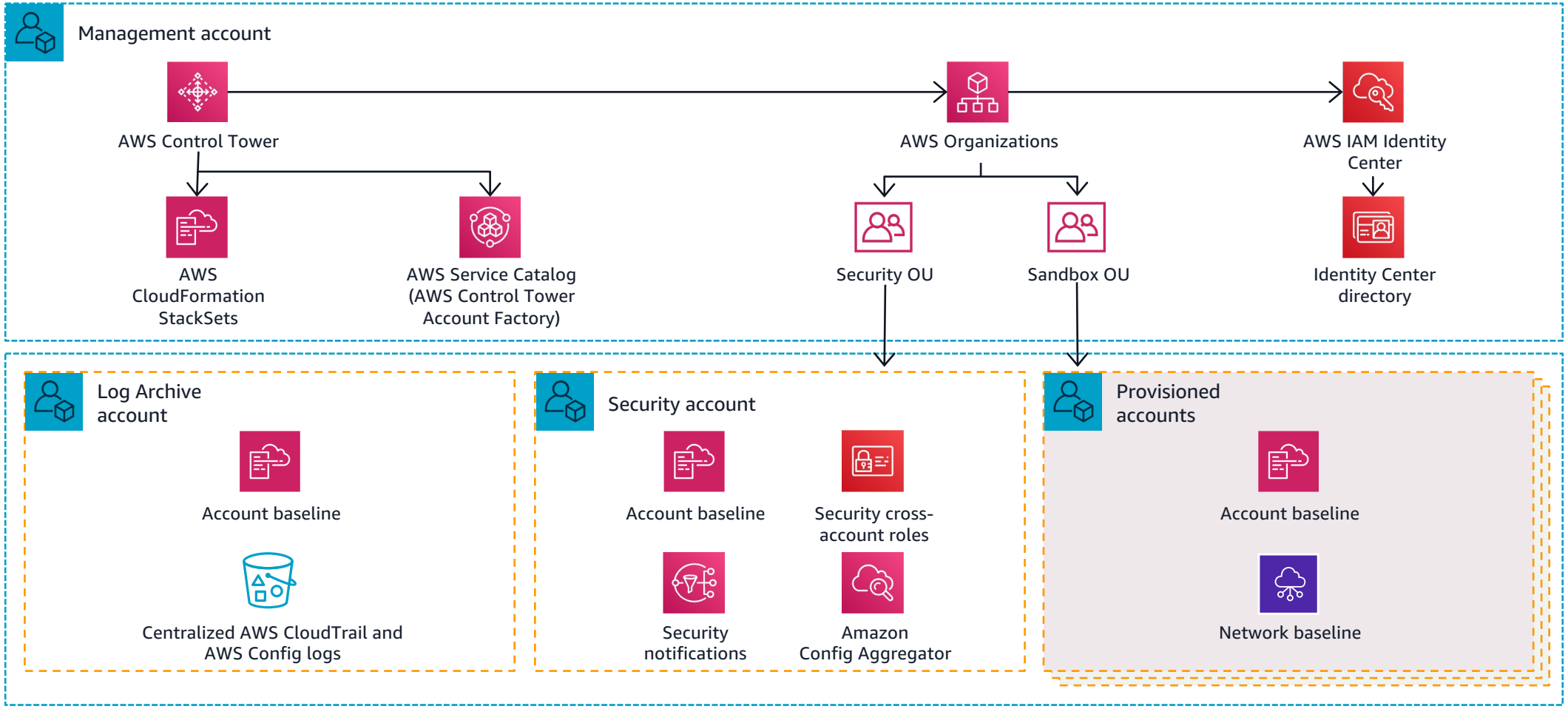
Agility

Self-service access

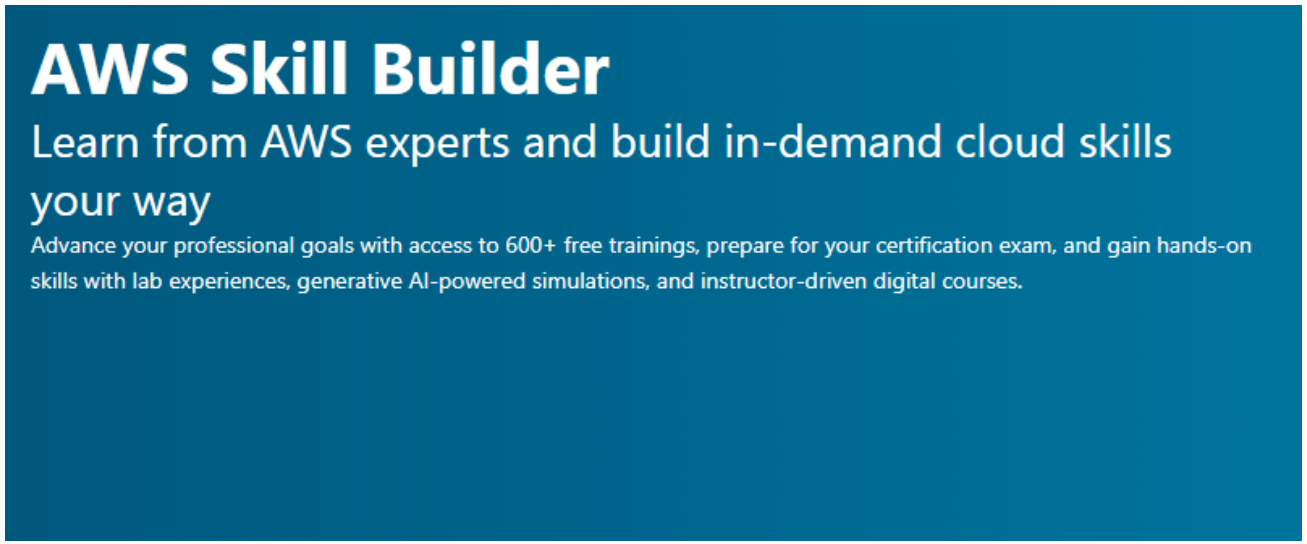
Experiment fast

Respond quickly to change

Landing zone foundation of AWS Control Tower



Want to learn more about Well Architected Foundations?



Thank you!

Vinod Kisanagaram

Solutions Architect
AWS
vinodaws@amazon.com

Please complete the survey for this session

Cloud architectural patterns: Platform and application best practices

aws Learning Days
State, Local, and Education