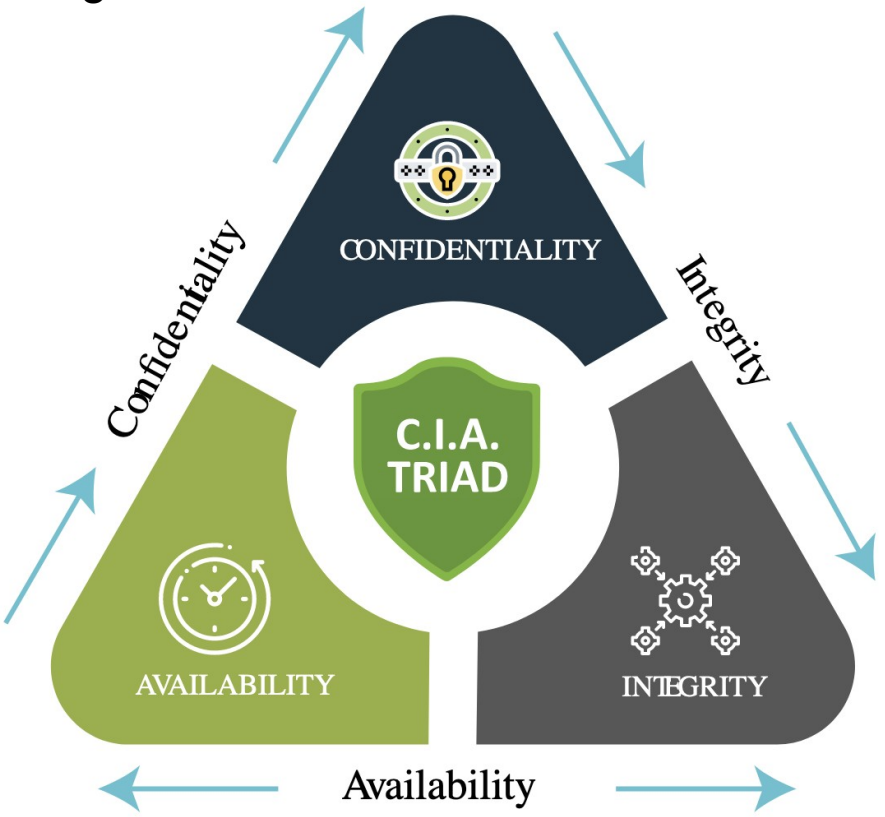
Cloud Data Risk Management

Protecting Data in Cloud Services

Data Protection

Data “CIA triad”

- protected from unwanted access
- locked from unwanted changes
- Present when needed



Data Risks In Cloud Services

- Vulnerabilities, data breaches
  - Misconfigurations, unpatched software
  - data exposure due to insecure APIs
  - insufficient encryption (data at rest)
  - Insecure transport mechanisms (data in flight)
  - credentials theft
- Data loss
  - provider outages or failures
  - Insider threats
- Compliance and Legal
  - Data residency and other compliance risks

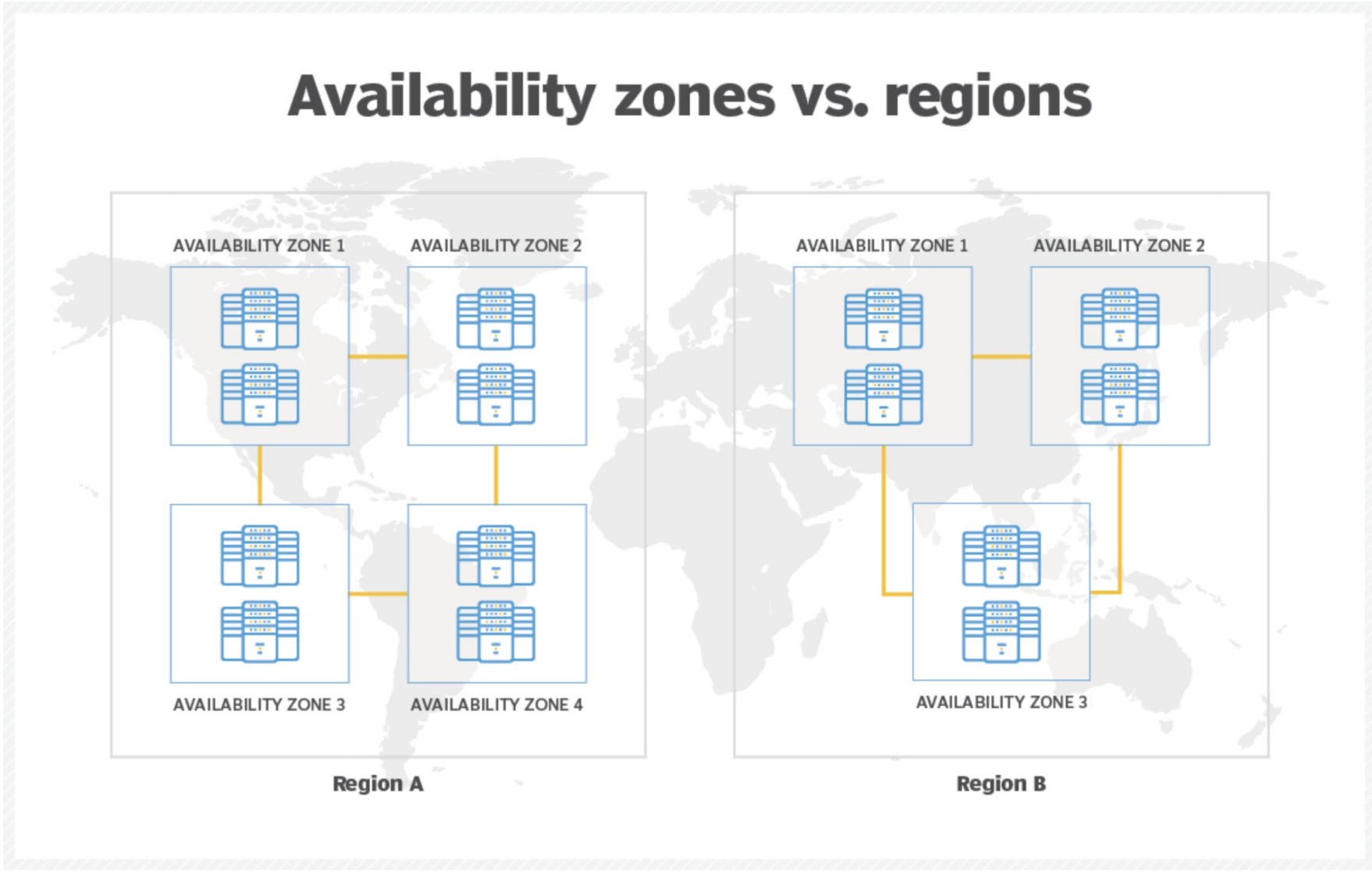
How to manage data risks in cloud services?

Protecting Data – Areas of concern

- Access and identity management
- Network
- Logging and monitoring
- Data
  - storage, backup and recovery
  - legal and regulatory requirements
  - access

Let's use AWS and its services as our "use case" for data risk management

AWS Regions and Availability Zones



Access and Identity Management

- centrally manage many accounts
- orchestrate controls (“guardrails”) across accounts
- single point of access four users (SSO)
- time-limited API credentials, MFA

<u>Services ecosystem</u>

- Organizations
- IAM Identity Center
- Control Tower

Network

- environment isolation (production, development, testing)
- protect the network perimeter
- detect and manage intrusion attempts
- test for unwanted external exposure of data

Services ecosystem

- VPC, Security Groups, ACLs
- WAF and Shield
- GuardDuty

Logging and Monitoring

- change management, log all change operations
- log access to sensitive data
- log all security-related events
- monitoring: you can’t manage what you don’t know

<u>Services ecosystem</u>

- CloudTrail, CloudWatch (logs, events, synthetics)
- Security Hub (centralized security monitoring)
- Personal Health Dashboard (relevant AWS service events)

Data Storage and Access

- encrypt data at rest and in flight
- protect data access
- high availability and fault tolerance

Services ecosystem

- Data storage
  - S3, Glacier
  - EC2 and EBS
  - RDS and Aurora
  - EFS
- Data protection and access
  - KMS
  - Secrets Manager

Data Backup and Recovery

- data versioning
- data replication local and remote
- data backup and recoverability

Services ecosystem

- EC2 Backup service
- EBS snapshots
- Secrets Manager (replication)
- RDS backup, replication, global databases
- S3 as backup (versioning and replication)
- EFS Backup