



**Secure Cloud**

**Cloud Security Made Easy:  
Controls and Compliance for the Win**



# Goals for Cloud Security Discussion

**Describe  
Problem**

**Define  
Context**

**Develop  
Solution**

# The Definition of Cloud

## Essential Characteristics

- Broad network access
- Rapid elasticity
- Resource pooling
- On-demand self-service
- Measured service

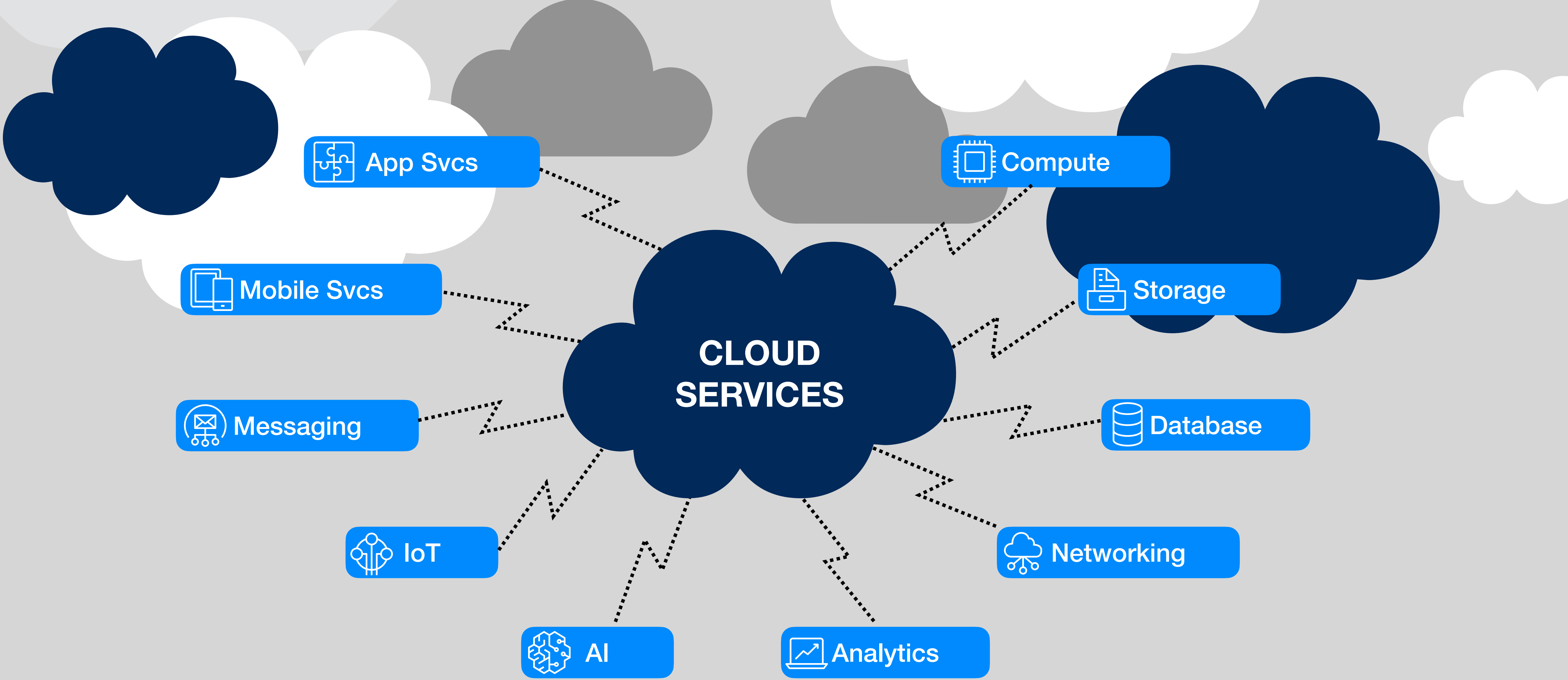
## Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

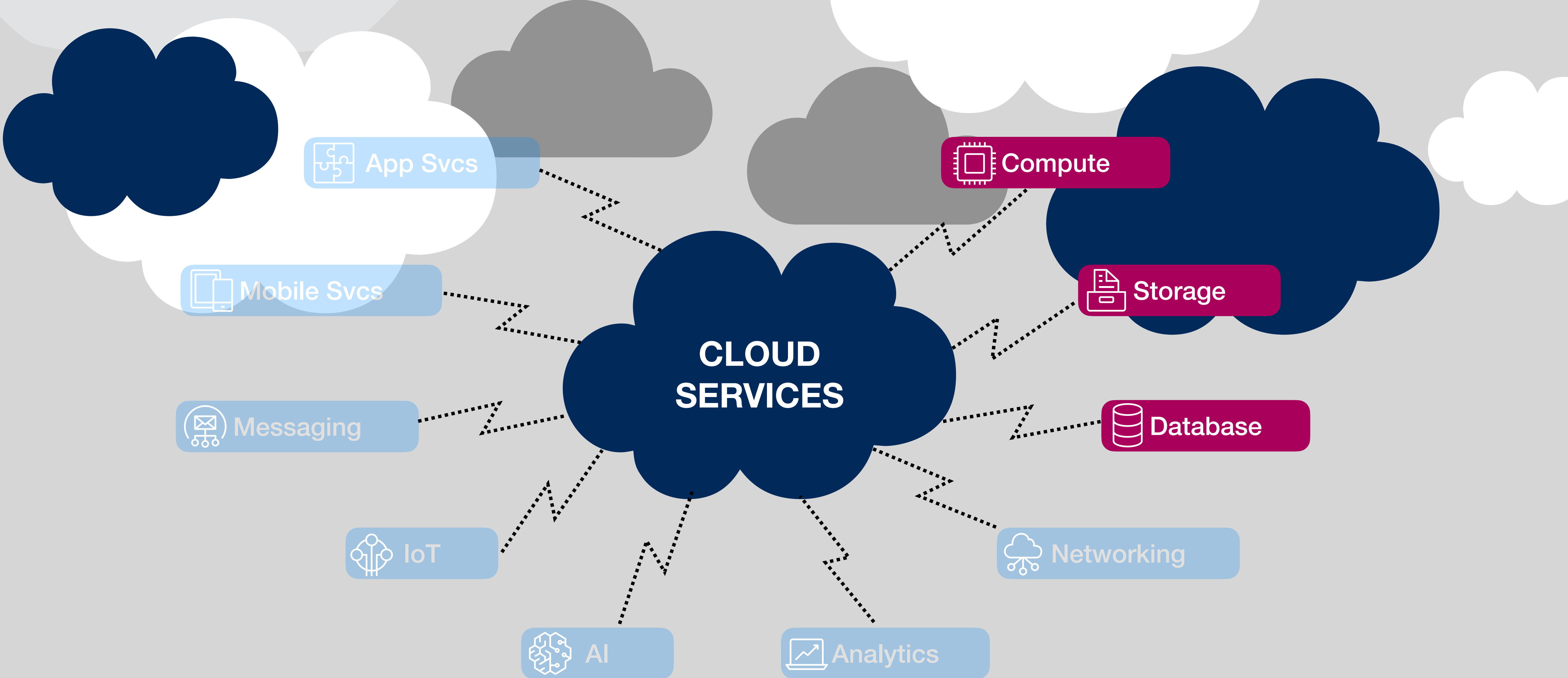
## Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)




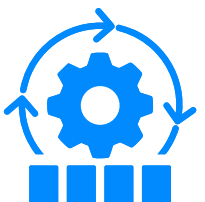
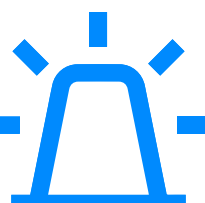
# What Developers Use in the Cloud



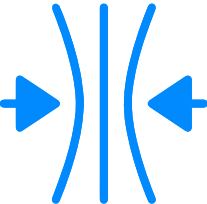
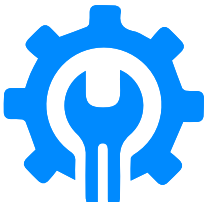



# What Security Understands in the Cloud



# Situational Awareness: Controls

| STANDARD  |                              |
|---|------------------------------|
|    | Identity & Access Management |
|    | Logging & Monitoring         |
|  | Infrastructure Security      |
|  | Data Protection              |
|  | Incident Response            |

| ENHANCED  |  |
|---|--|
|    | Secure CI/CD: DevSecOps                |
|    | Compliance Validation                  |
|  | Resilience                             |
|  | Configuration & Vulnerability Analysis |
|  | Security Big Data & Analytics          |

# Situational Awareness: Management

| ISO 27001 Control Section | Degree of Change in ISO 27017 |
|---------------------------|-------------------------------|
| Asset management          | MODERATE/LOW                  |
| Cryptography              | MODERATE                      |
| System Acquisition        | MODERATE                      |
| Incident management       | MODERATE                      |
| Operations security       | MODERATE/HIGH                 |
| Communication security    | MODERATE/HIGH                 |
| Supplier relationships    | MODERATE/HIGH                 |
| Compliance                | MODERATE/HIGH                 |
| Access control            | HIGH                          |

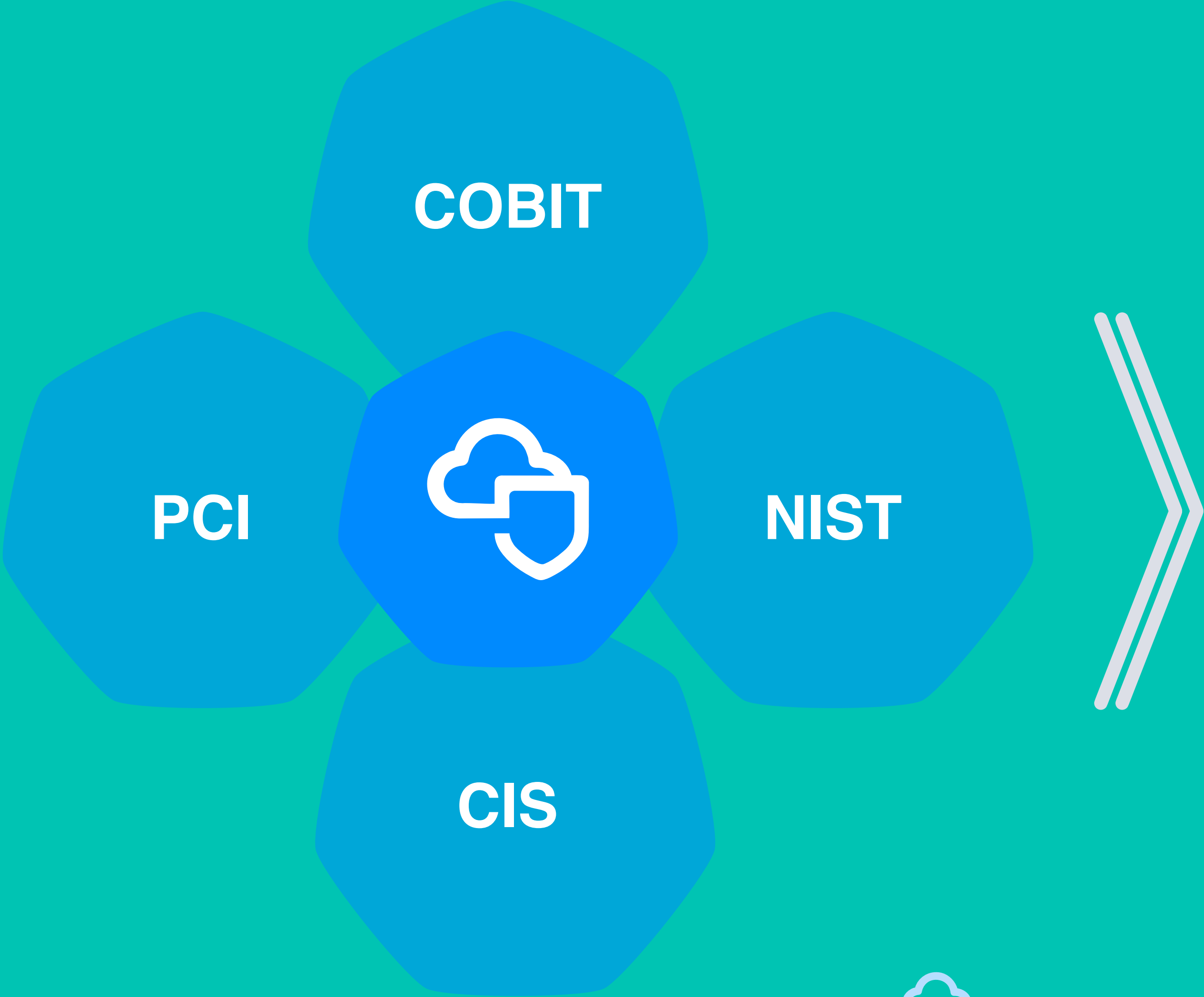
# Situational Awareness: Governance

## Cloud Challenges For Enterprise





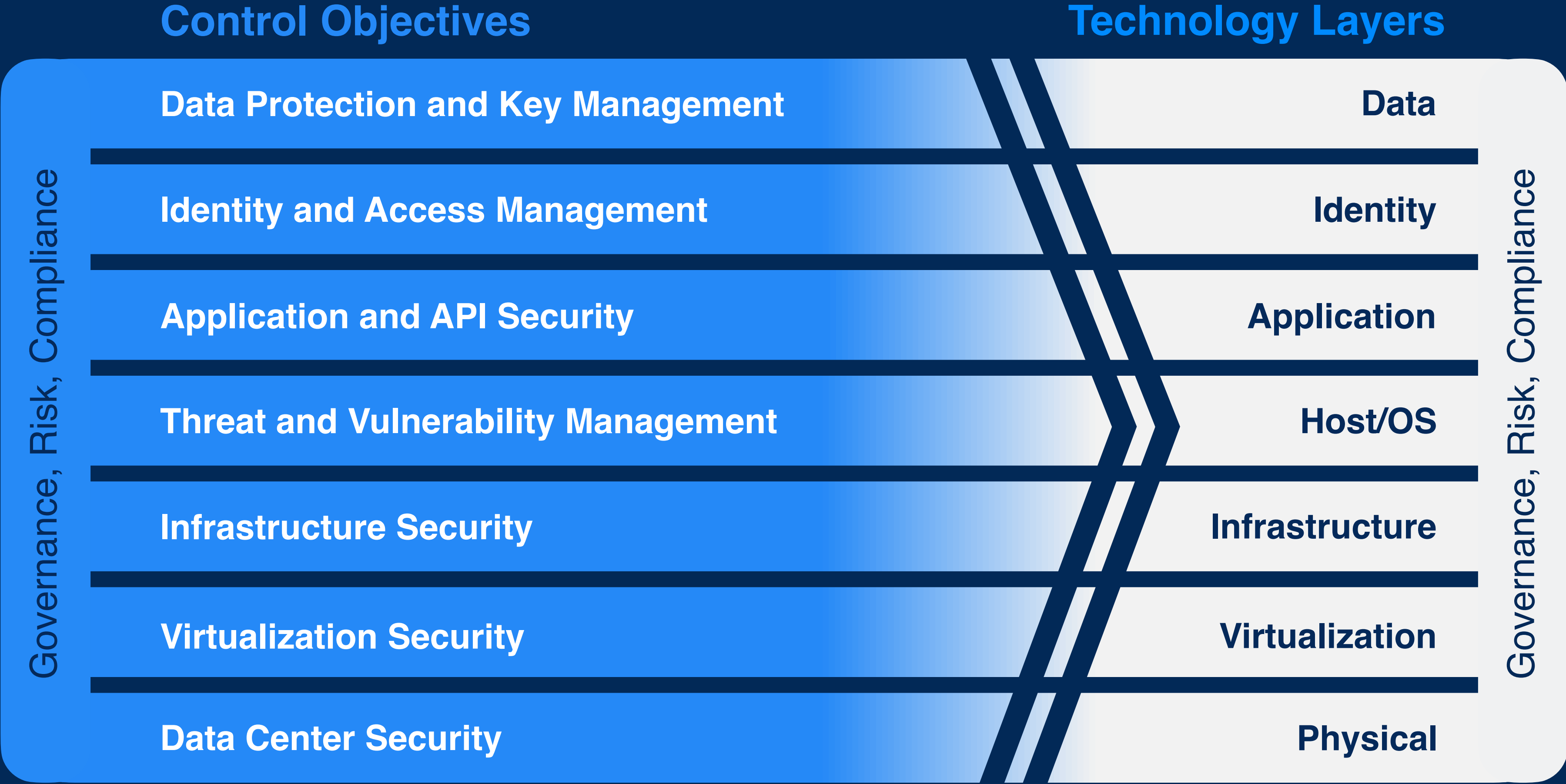
# Compliance to Cloud Control Objectives



## Control Objectives

- Governance, Risk, Compliance
- Data Protection and Key Management
- Identity and Access Management
- Application and API Security
- Threat and Vulnerability Management
- Infrastructure Security
- Virtualization Security
- Data Center Security















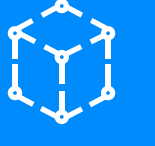







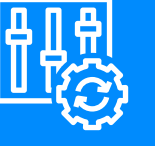


# Cloud Control Objectives to Technology Layers



# Technology Layers to Cloud Controls Matrix

## STANDARD


## ENHANCED


|                       |  |   |   |  |  |  |
|-----------------------|--|---|---|--|--|--|
| <b>GRC</b>            | <br>Organizations | <br>Security Hub | <br>Firewall Manager | <br>Control Tower | <br>Service Catalog |  |
| <b>DATA</b>           | <br>ACM           | <br>KMS          | <br>RDS              | <br>CloudHSM      | <br>Macie           |  |
| <b>IDENTITY</b>       | <br>IAM           |   |   |  |  |  |
| <b>APPLICATION</b>    | <br>API Gateway  | <br>WAF         | <br>CloudFront      | <br>AppMesh      | <br>Secrets Mgr    | <br>Shield     |
| <b>HOST/OS</b>        | <br>Auto Scale  | <br>ELB        |   |  |  |  |
| <b>INFRASTRUCTURE</b> | <br>VPC         | <br>CloudTrail | <br>CloudWatch     | <br>Config      | <br>GuardDuty     | <br>Detective |
| <b>VIRTUALIZATION</b> | HYPERVISOR   |   |   | PLATFORM   |  |  |
| <b>PHYSICAL</b>       | REGIONS  |   |   | AVAILABILITY ZONES   |  |  |


Managed by Customers





























Managed by AWS

# Shared Responsibility Matrix

 Customer Managed

 Shared Management

 Vendor Managed

|             | Data Center   | IaaS  | PaaS  | SaaS  |
|-------------|---|---|---|---|
| Data        |    |    |    |    |
| Identity    |    |    |    |    |
| Application |    |    |    |    |
| Host/OS     |   |   |   |   |
| Network     |  |  |  |  |
| Virtual     |  |  |  |  |
| Physical    |  |  |  |  |

# Security Architecture - Confidentiality: Protected



In-Transit



In-Use



At-Rest

# Security Architecture - Integrity: Automated



Code



Test

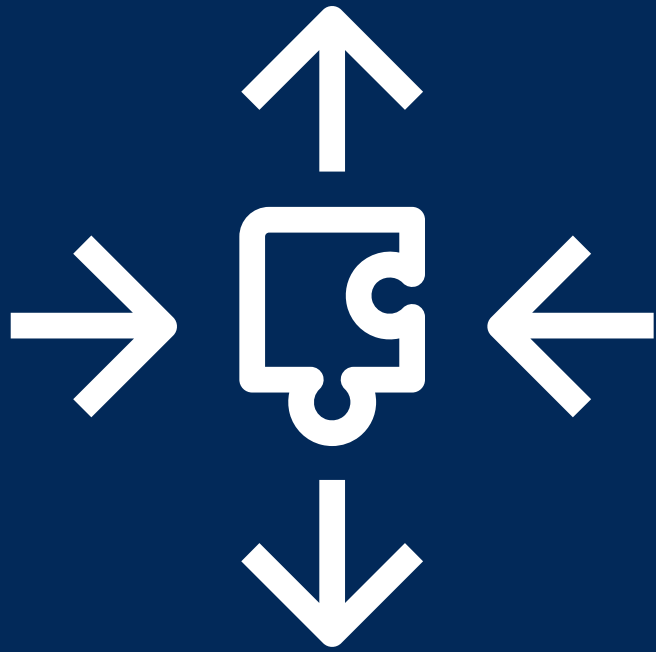


Release

# Security Architecture - Availability: Resilient



**Caching  
and  
Balancing**



**Auto-Scaling**



**Replication**

# Cloud Security Framework - Summary

## CONTROLS

- Standard
- Enhanced



**Technology:**  
Tactical



**CIS - CSC**  
Critical Security Controls

## MANAGEMENT

- Identity
- Protect
- Detect
- Respond
- Recover



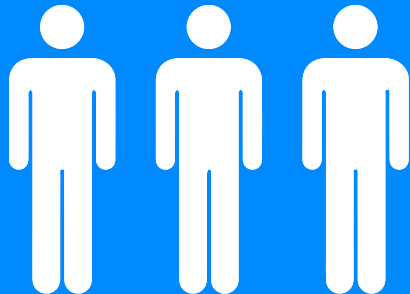
**Process:**  
Operational



**NIST - CSF**  
Cybersecurity Framework

## GOVERNANCE

- Plan
- Build
- Run
- Measure



**People:**  
Strategic



**ISACA - COBIT**  
Control Objectives for  
Information Technologies



# Next Steps for Cloud Security Framework

Cloud Controls Matrix

AWS, Azure, GCP Security Controls

Security Control Library

Security Controls mapped to Frameworks

Security Baselines

AI, Containers, Serverless