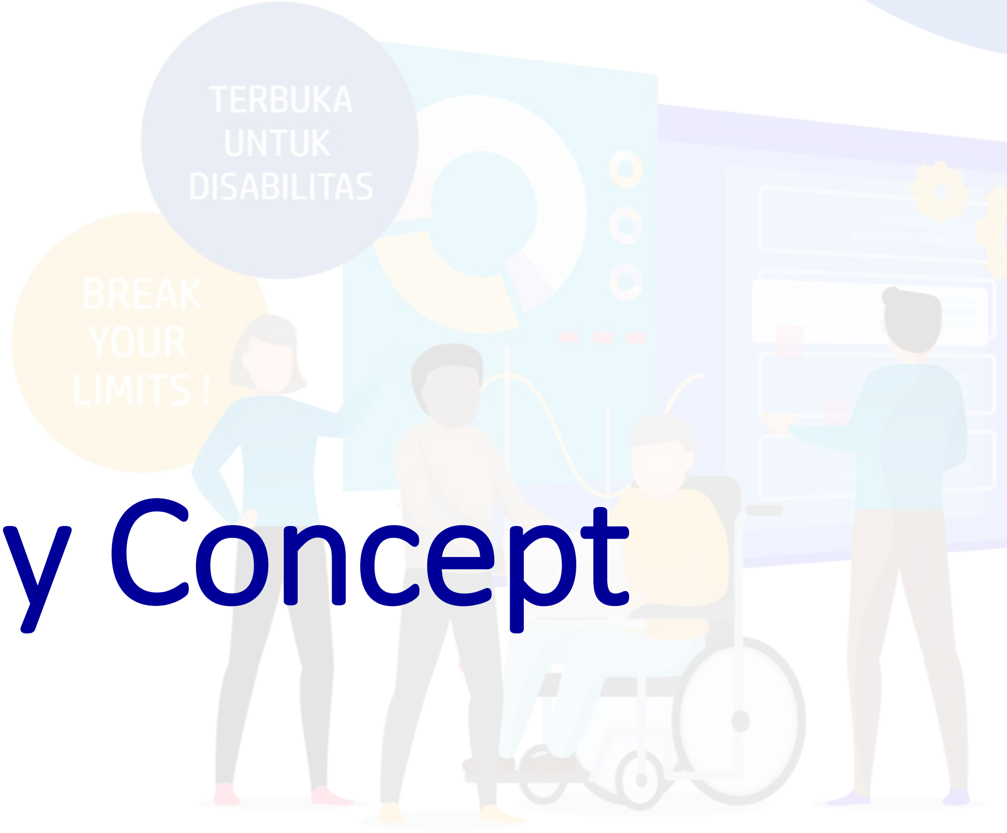
DIGITAL TALENT SCHOLARSHIP 2020

digitalent.kominfo.go.id

AWS Cloud Security

Agenda

- AWS Security Concept
- AWS Compliance
- Well Architected Framework : Security
- Study Case



AWS Security Concept

Security in Cloud

- Cloud Security at AWS is the highest priority
- Security in the cloud is much like security in your on-premises data centers—only without the costs of maintaining facilities and hardware.
- An advantage of the AWS Cloud is that it allows you to scale and innovate, while maintaining a secure environment and paying only for the services you use.
- The AWS Cloud enables a **shared responsibility model**. While AWS manages security **of** the cloud, you are responsible for security **in** the cloud.
- AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals

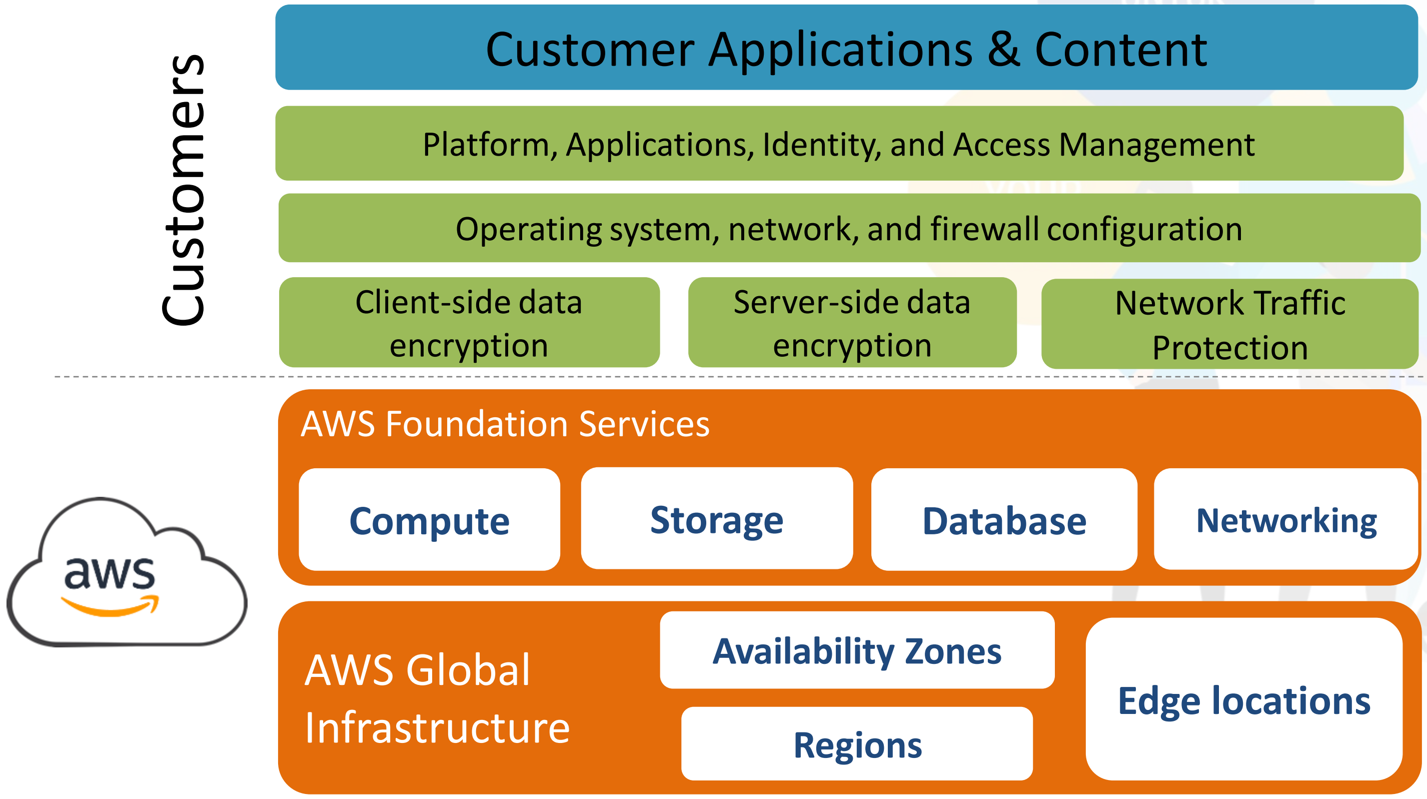
Benefit of AWS Security

- Keep your data safe
- Meet compliance requirements
- Save money
- Scale Quickly

Shared Responsibility Model

- Security and Compliance is a shared responsibility between AWS and the customer.
- Shared responsibility model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

AWS Shared Responsibility Model

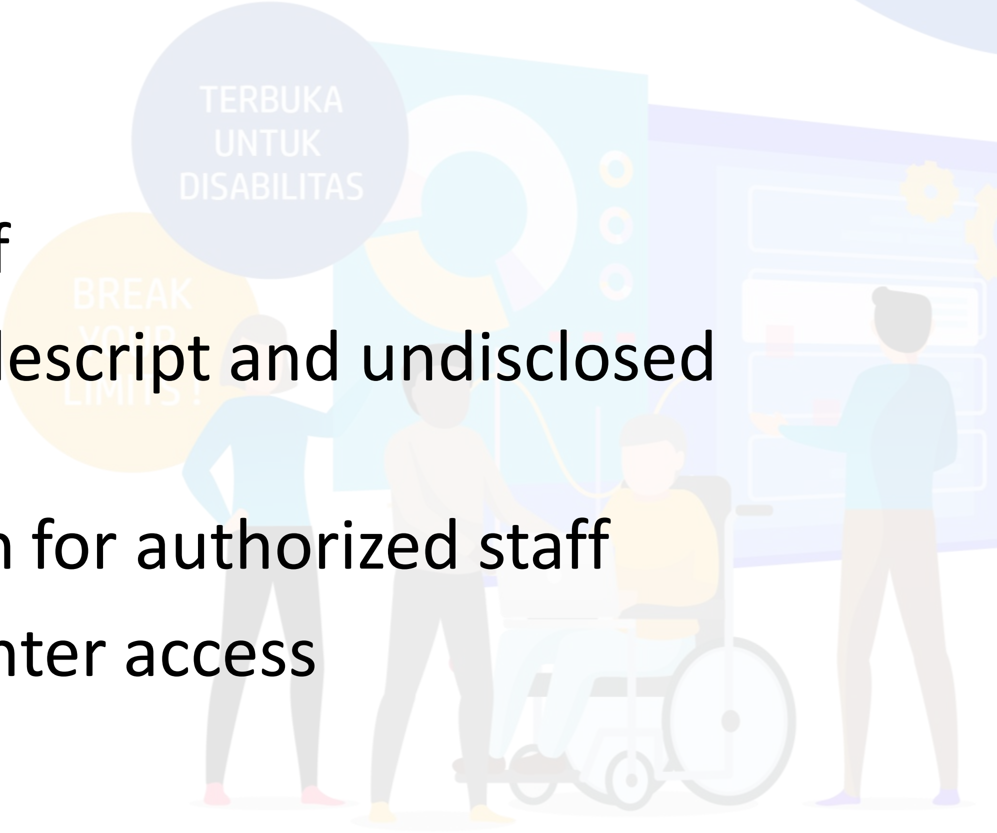

Customers
Customer Applications & Content
Platform, Applications, Identity, and Access Management
Operating system, network, and firewall configuration
Client-side data encryption
Server-side data encryption
Network Traffic Protection
aws
AWS Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Availability Zones
Regions
Edge locations

Customers are responsible for security **IN** the cloud

AWS is responsible for the security **OF** the cloud

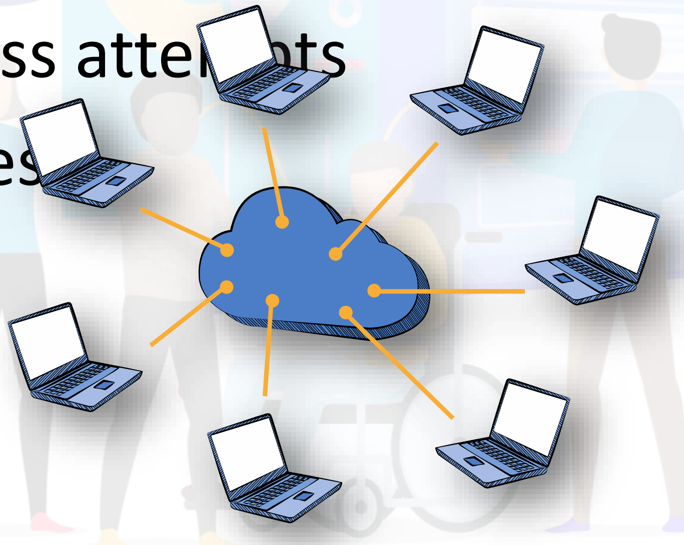
Physical Security

- 24/7 trained security staff
- AWS data centers in nondescript and undisclosed facilities
- Two-factor authentication for authorized staff
- Authorization for data center access



Hardware, Software, and Network

- Automated change-control process
- Bastion servers that record all access attempts
- Firewall and other boundary devices
- AWS monitoring tools



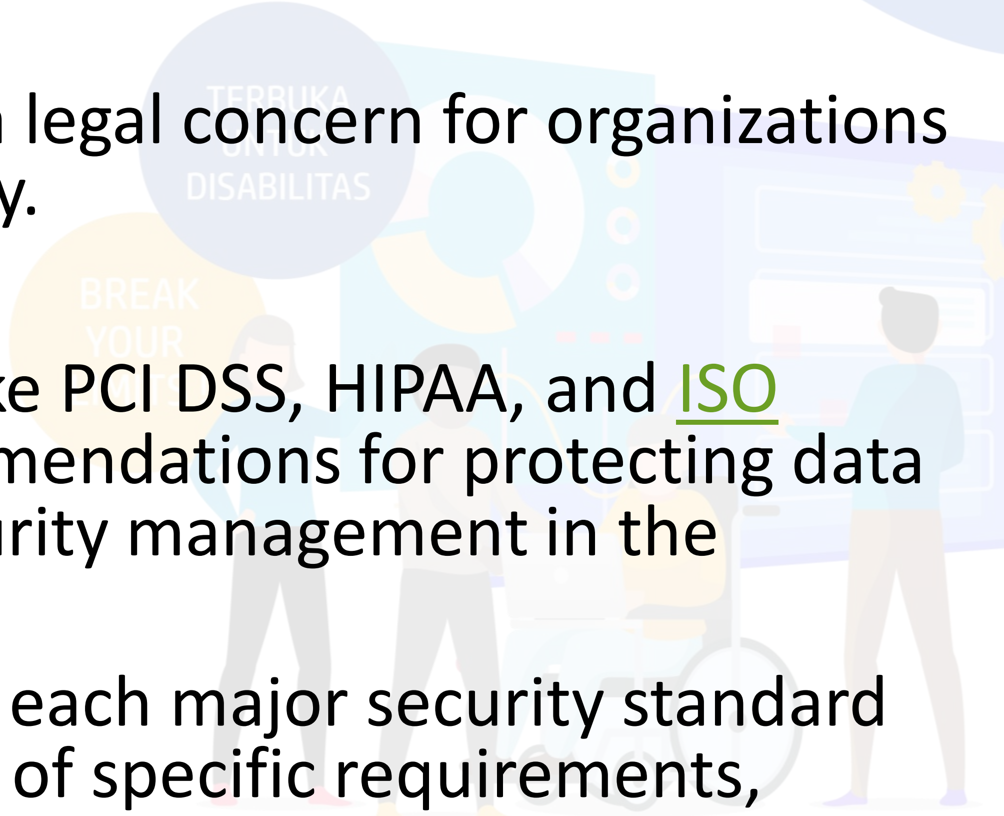
AWS Security Services Coverage

- Network and Infrastructure Security
- Host and Endpoint Security
- Data Protection and Encryption
- Compliance
- Logging, Monitoring, Threat Detection, and Analytics
- Identity and Access Control
- Vulnerability and Configuration Analysis
- Application Security

AWS Compliance

Security Compliance

- Security compliance is a legal concern for organizations in many industries today.
- Regulatory standards like PCI DSS, HIPAA, and ISO 27001 prescribe recommendations for protecting data and improving info security management in the enterprise.
- At the same time, since each major security standard involves an evolving set of specific requirements, achieving security compliance can be complicated and costly.

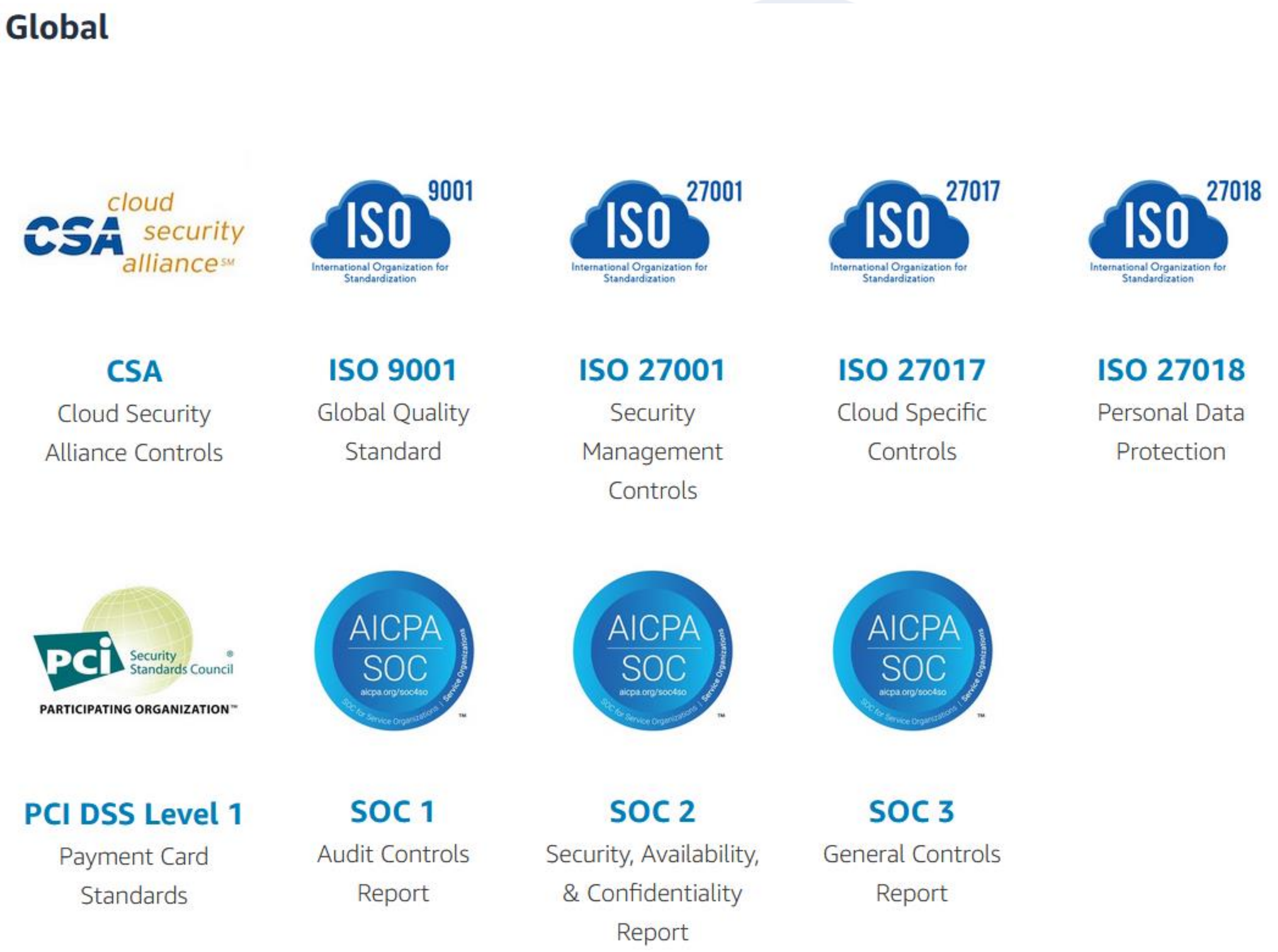


Security Compliance on AWS

- AWS comply to IT standards that are broken into 3 categories :
  - Certifications and Attestations
  - Laws, Regulations and Privacy
  - Alignments and Frameworks

- AWS Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance.

Security Compliance on AWS (Cont'd)



Global

CSA
Cloud Security Alliance Controls

ISO 9001
Global Quality Standard

ISO 27001
Security Management Controls

ISO 27017
Cloud Specific Controls

ISO 27018
Personal Data Protection

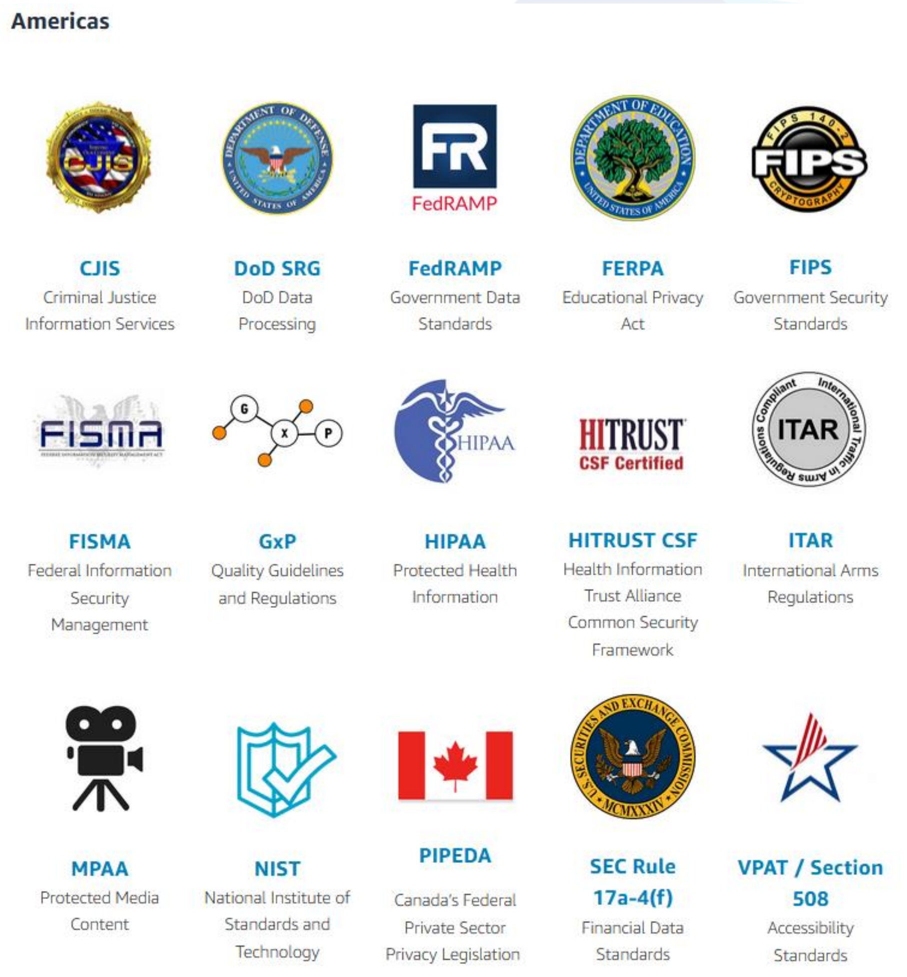
PCI DSS Level 1
Payment Card Standards

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

Security Compliance on AWS (Cont'd)



Americas

CJIS
Criminal Justice Information Services

DoD SRG
DoD Data Processing

FedRAMP
Government Data Standards

FERPA
Educational Privacy Act

FIPS
Government Security Standards

FISMA
Federal Information Security Management

GxP
Quality Guidelines and Regulations

HIPAA
Protected Health Information

HITRUST CSF
Health Information Trust Alliance Common Security Framework

ITAR
International Arms Regulations

MPAA
Protected Media Content

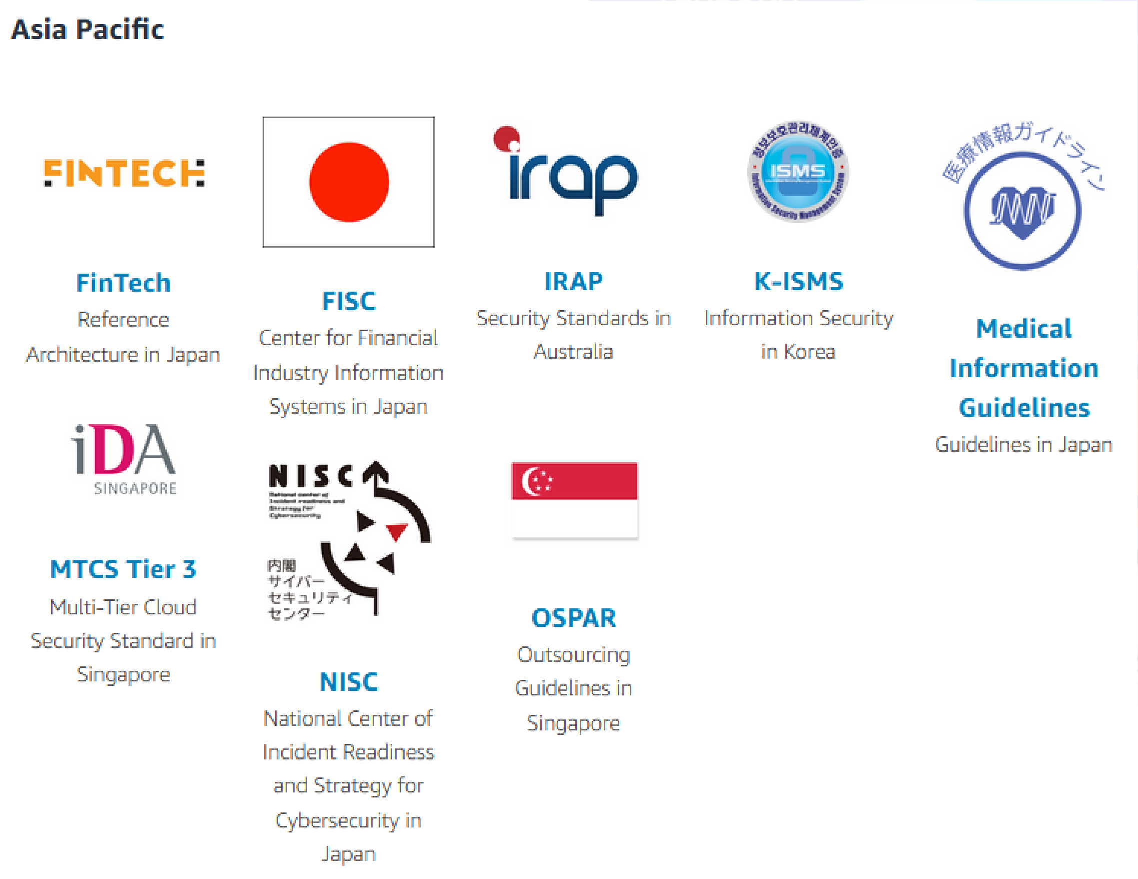
NIST
National Institute of Standards and Technology

PIPEDA
Canada's Federal Private Sector Privacy Legislation

SEC Rule 17a-4(f)
Financial Data Standards

VPAT / Section 508
Accessibility Standards

Security Compliance on AWS (Cont'd)



Asia Pacific

FinTech
Reference Architecture in Japan

FISC
Center for Financial Industry Information Systems in Japan

IRAP
Security Standards in Australia

K-ISMS
Information Security in Korea

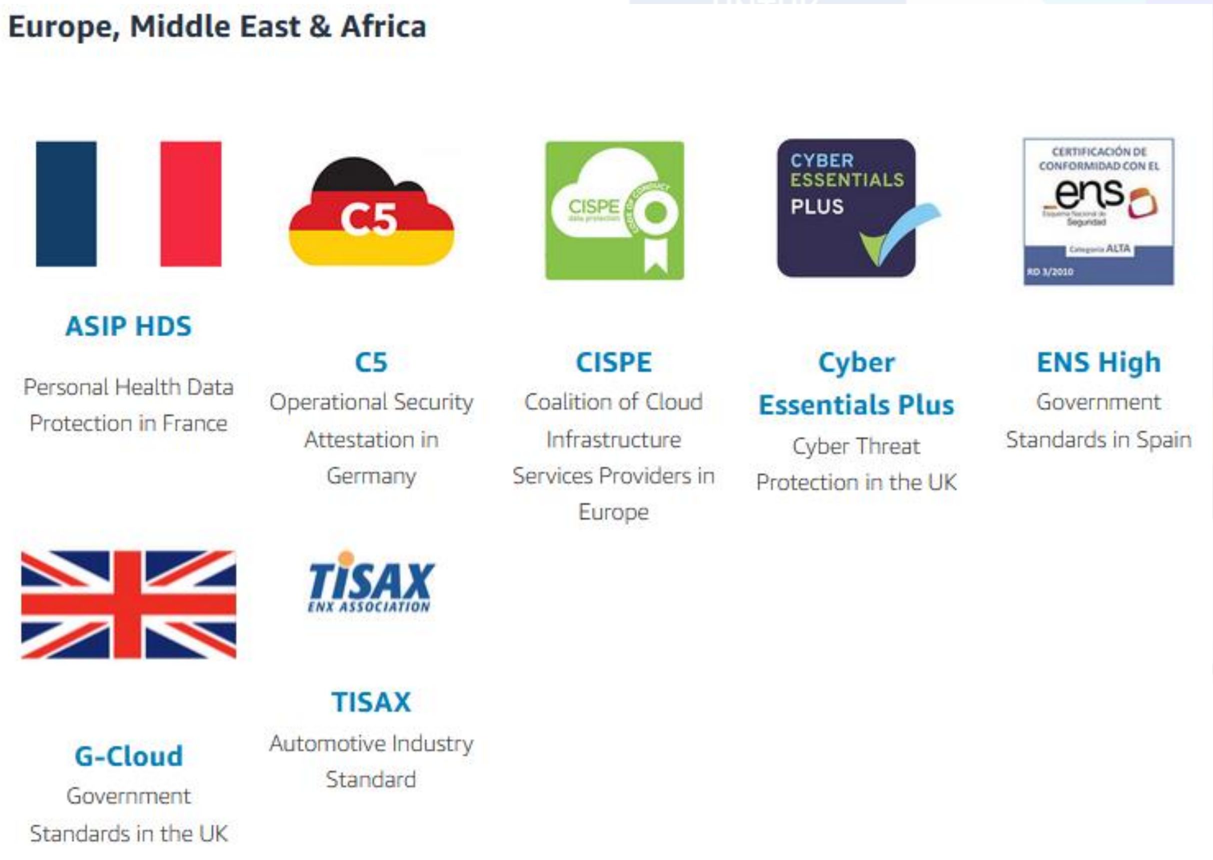
Medical Information Guidelines
Guidelines in Japan

MTCS Tier 3
Multi-Tier Cloud Security Standard in Singapore

NISC
National Center of Incident Readiness and Strategy for Cybersecurity in Japan

OSPAR
Outsourcing Guidelines in Singapore

Security Compliance on AWS (Cont’d)



Europe, Middle East & Africa

ASIP HDS
Personal Health Data Protection in France

C5
Operational Security Attestation in Germany

CISPE
Coalition of Cloud Infrastructure Services Providers in Europe

Cyber Essentials Plus
Cyber Threat Protection in the UK

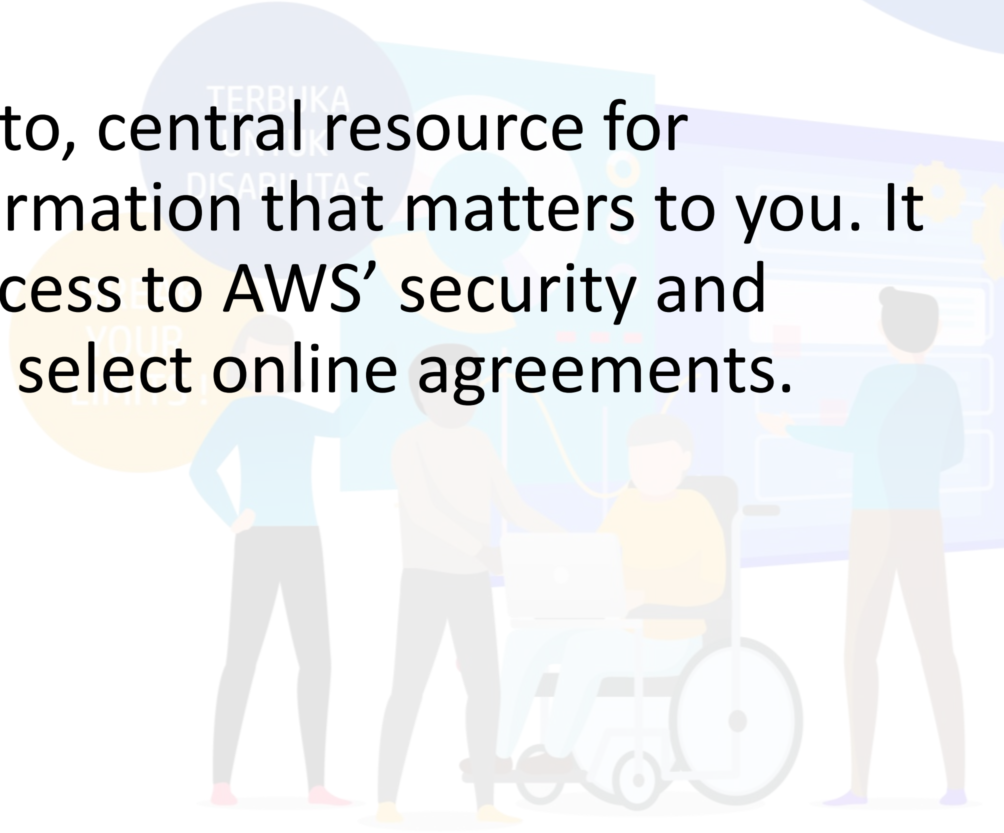
ENS High
Government Standards in Spain

G-Cloud
Government Standards in the UK

TISAX
Automotive Industry Standard

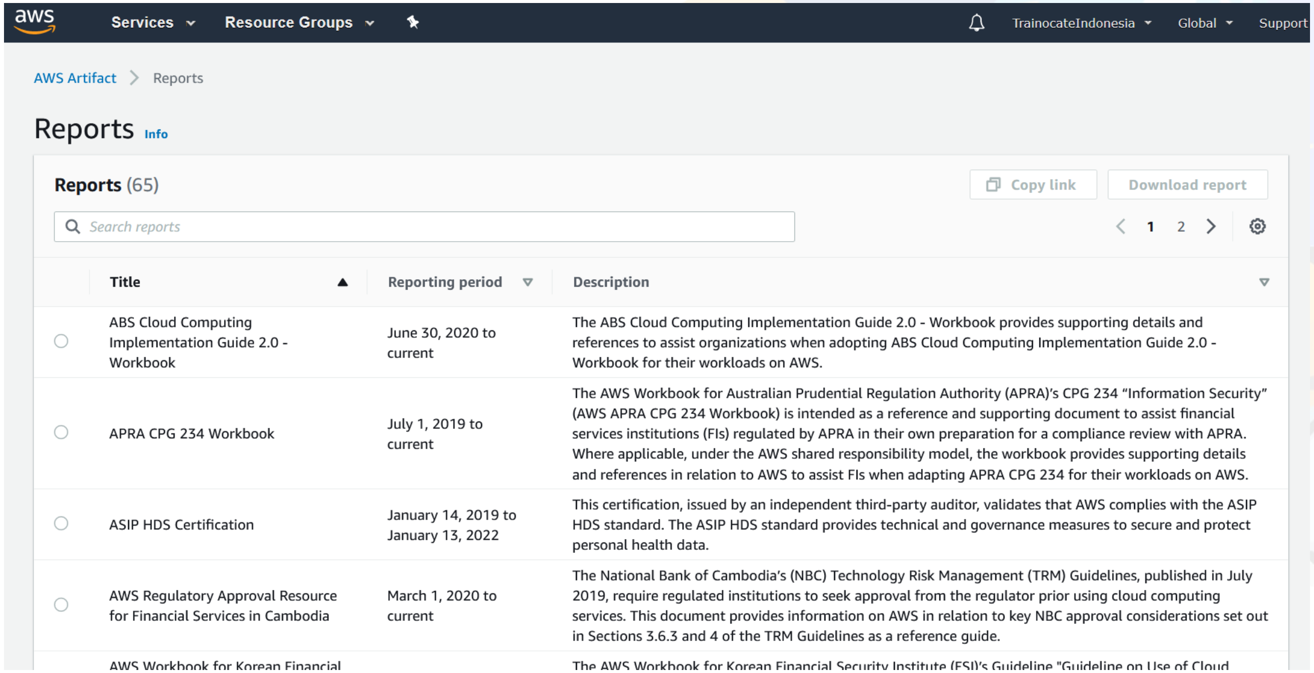
AWS Artifact

- 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.



AWS Artifact (Cont'd)

- AWS Artifact is accessed through web console



Reports

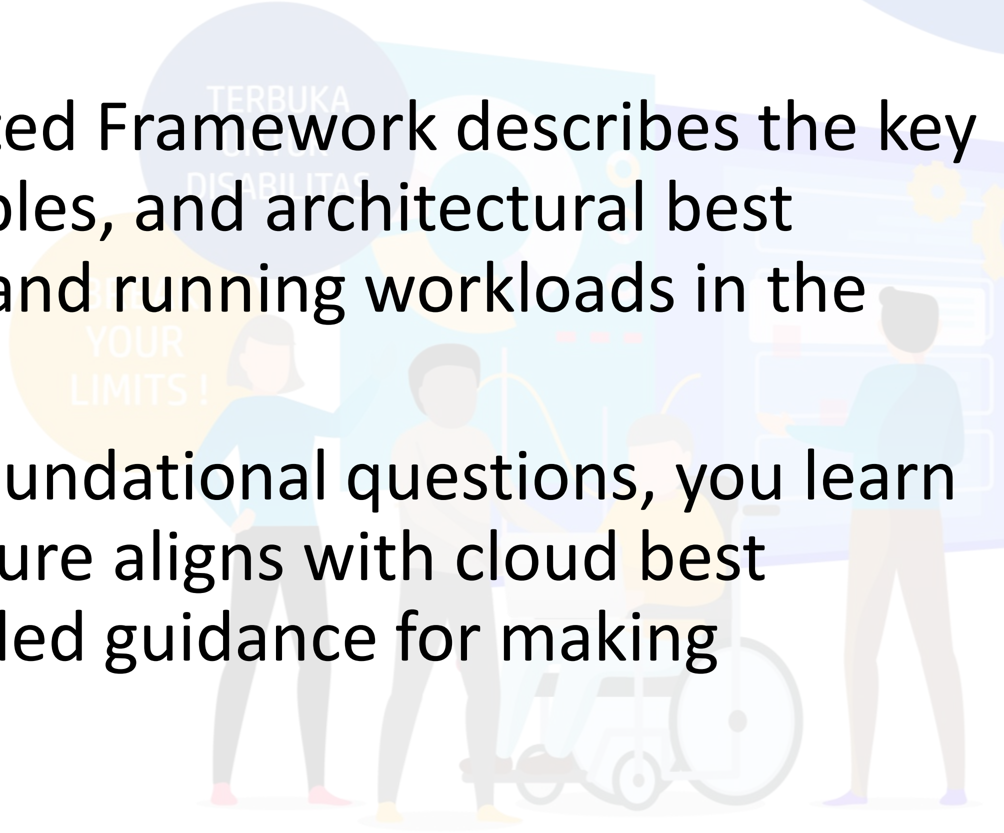
Reports (65)

	Title	Reporting period	Description
○	ABS Cloud Computing Implementation Guide 2.0 - Workbook	June 30, 2020 to current	The ABS Cloud Computing Implementation Guide 2.0 - Workbook provides supporting details and references to assist organizations when adopting ABS Cloud Computing Implementation Guide 2.0 - Workbook for their workloads on AWS.
○	APRA CPG 234 Workbook	July 1, 2019 to current	The AWS Workbook for Australian Prudential Regulation Authority (APRA)'s CPG 234 "Information Security" (AWS APRA CPG 234 Workbook) is intended as a reference and supporting document to assist financial services institutions (FIs) regulated by APRA in their own preparation for a compliance review with APRA. Where applicable, under the AWS shared responsibility model, the workbook provides supporting details and references in relation to AWS to assist FIs when adapting APRA CPG 234 for their workloads on AWS.
○	ASIP HDS Certification	January 14, 2019 to January 13, 2022	This certification, issued by an independent third-party auditor, validates that AWS complies with the ASIP HDS standard. The ASIP HDS standard provides technical and governance measures to secure and protect personal health data.
○	AWS Regulatory Approval Resource for Financial Services in Cambodia	March 1, 2020 to current	The National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines, published in July 2019, require regulated institutions to seek approval from the regulator prior using cloud computing services. This document provides information on AWS in relation to key NBC approval considerations set out in Sections 3.6.3 and 4 of the TRM Guidelines as a reference guide.
	AWS Workbook for Korean Financial		The AWS Workbook for Korean Financial Security Institute (FSI)'s Guideline "Guideline on Use of Cloud

Well-Architected Framework : Security

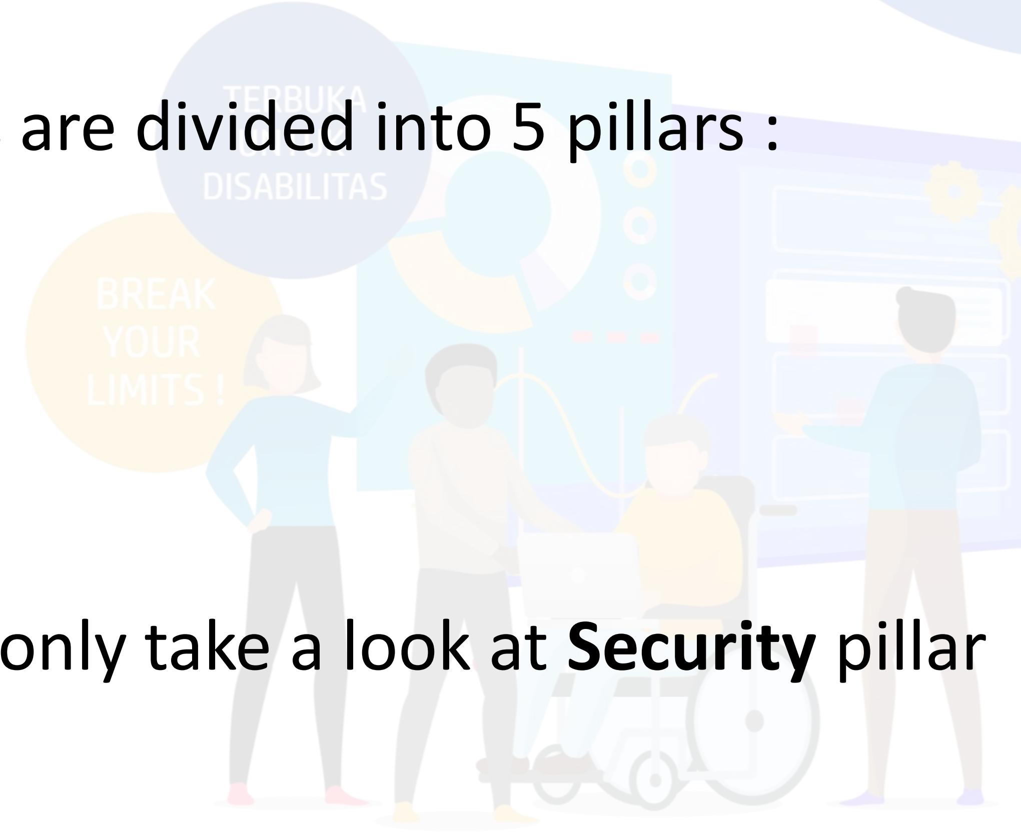
AWS Well-Architected Framework

- The AWS Well-Architected Framework describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.
- By answering a set of foundational questions, you learn how well your architecture aligns with cloud best practices and are provided guidance for making improvements.



AWS Well-Architected Framework (Cont’d)

- These design principles are divided into 5 pillars :
  - Operational Exellence
  - Security
  - Reliability
  - Performance Efficiency
  - Cost Optimization
- In this module, we will only take a look at **Security** pillar

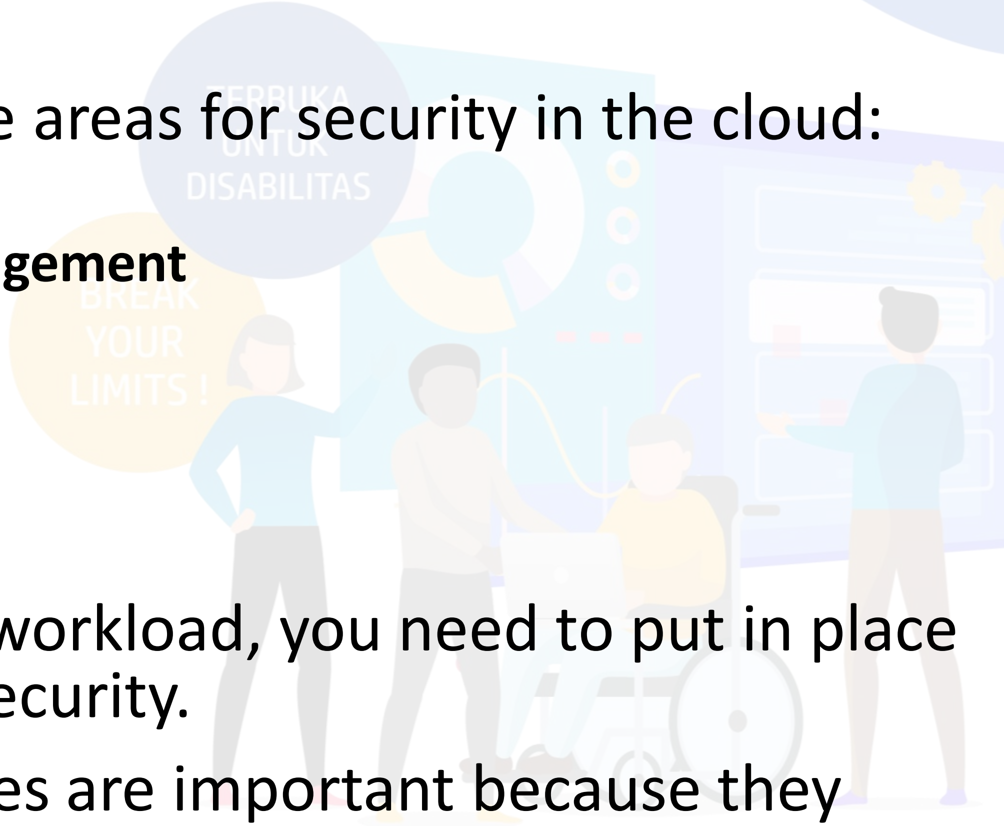


Security Pillar – Design Principles

- The Security pillar includes the security pillar encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.
- There are **7 design principles** for security in the cloud :
  - Implement a strong identity foundation
  - Enable 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

Security Pillar – Best Practices

- There are six best practice areas for security in the cloud:
  - **Security**
  - **Identity and Access Management**
  - **Detection**
  - **Infrastructure Protection**
  - **Data Protection**
  - **Incident Response**
- Before you architect any workload, you need to put in place practices that influence security.
- These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.



Security Pillar – Best Practices Example : IAM

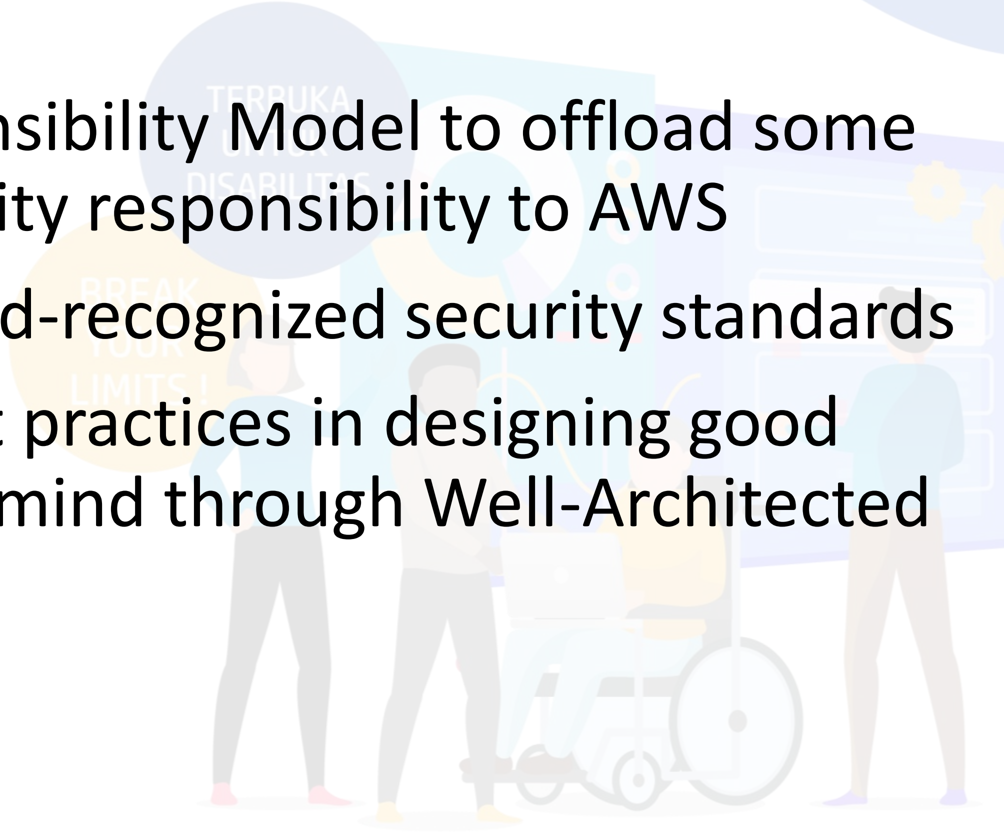
- Identity and access management are key parts of an information security program, ensuring that only authorized and authenticated users and components are able to access your resources, and only in a manner that you intend.
- In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user and programmatic access to AWS services and resources. You should apply granular policies, which assign permissions to a user, group, role, or resource.
- Credentials must not be shared between any user or system.
- User access should be granted using a least-privilege approach with best practices including password requirements and MFA enforced.

Study Case

Security Case Study : axialHealthcare

- axialHealthcare was founded in 2012 to combat risky opioid prescribing and use patterns. The company ingests prescription and claims data for analysis and refers cases for intervention by teams of licensed healthcare practitioners.
- In addition to the highly qualified team performing this work, axialHealthcare’s Clinical Consult Offerings offering depends on a **geographically distributed, HIPAA-compliant, virtual contact center powered by Amazon Connect**.
- This self-service, cloud-based contact center service is built on the same technology used by Amazon customer service associates around the world.

Key Point



- AWS has Shared Responsibility Model to offload some of the customer's security responsibility to AWS
- AWS comply many world-recognized security standards
- AWS provide set of best practices in designing good system with security in mind through Well-Architected Framework

Follow our social media!

digitalent.kominfo
digitalent.kominfo
DTS_kominfo
Digital Talent Scholarship 2020

Pusat Pengembangan Profesi dan Sertifikasi
Badan Penelitian dan Pengembangan SDM
Kementerian Komunikasi dan Informatika
Jl. Medan Merdeka Barat No. 9
(Gd. Belakang Lt. 4 - 5)
Jakarta Pusat, 10110

digitalent.kominfo.go.id

digitalent.kominfo.go.id