Domain 1: Cloud Concepts

1.1 Define the Benefits of the AWS Cloud

- AWS Cloud provides cost savings through economies of scale by converting fixed data center costs into manageable, variable expenses with the pay-as-you-go model. This eliminates the need for upfront capital investments in hardware.
- The global infrastructure ensures low latency, high availability, and fault tolerance via a vast network of regions and edge locations. Features like multi-region redundancy and distributed systems improve disaster recovery capabilities.
- AWS's elasticity allows for automatic scaling of resources based on demand, enabling businesses to adjust quickly to changing workloads without overprovisioning. Agility is enhanced through rapid deployment and resource provisioning.
- High availability is achieved with services like **Elastic Load Balancing** and **Auto Scaling**, which distribute traffic and maintain system performance during peak times.

1.2 Identify Design Principles of the AWS Cloud

- The AWS Well-Architected Framework provides six key pillars:
    - **Operational Excellence**: Focuses on automation tools like **AWS CloudFormation** to enable efficient provisioning and configuration of resources while monitoring with tools such as **Amazon CloudWatch**.
    - **Security**: Includes features like encryption (in transit and at rest), Identity and Access Management (IAM) for controlling access, and services like **AWS Shield** for DDoS protection.
    - **Reliability**
        - 3 Best Practices
            - Foundations
            - Change Management
            - Failure Management
        - CloudWatch, CloudTrail, and Config
    - **Performance Efficiency**: Offers scalable resources and computing options tailored to workloads, such as compute-optimized EC2 instances and serverless computing with AWS Lambda.
    - **Cost Optimization**: Supports resource efficiency through rightsizing, choosing the right pricing models (e.g., Reserved Instances), and leveraging lifecycle policies for storage
    - **Sustainability**: Aligns with environmental goals by providing energy-efficient infrastructure and shared resources.

1.3 Migration to the AWS Cloud

- AWS Cloud Adoption Framework (AWS CAF) assists organizations in planning and executing migrations with **six perspectives: business, people, governance, platform, security, and operations**. This reduces business risks and increases operational efficiency.
    - The CAF consists of 4 main steps
        1. Envision
            a. How will the cloud help accelerate business outcomes
        2. Align
            a. Identify gaps across the 6 main CAF perspectives
        3. Launch
            a. Deliver pilot initiatives in production and demonstrate incremental business value.
        4. Scale
            a. Focuses on expanding production pilots and business value to the desired scale and ensuring that the business benefits from associated cloud investments
- Migration tools like **AWS Snowball** allow for the physical transfer of data for large-scale migrations, while **Database Replication** ensures minimal downtime during database migrations.
    - Use **AWS Snowball** to transfer large (up to 80TB) quantities of data from AWS Cloud to a remote location with limited bandwidth
    - Use Snowmobile to transfer petabyte size quantities of data to AWS
    - Use Snowball Edge to transfer up to 100TB of data to Edge Locations
- AWS offers extensive support through migration playbooks, documentation, and customer success teams to streamline the process.
- Real-world strategies include rehosting (lift-and-shift), platforming (minimal changes), and rearchitecting (modernizing applications for the cloud).

1.4 Understand Concepts of Cloud Economics

- Transitioning to AWS helps convert fixed costs (e.g., maintaining on-premises data centers) into variable costs, allowing businesses to scale expenses based on actual usage. This model is especially beneficial for startups and businesses with fluctuating workloads.
- Rightsizing ensures the efficient use of resources by scaling up or down to match workload requirements, reducing overprovisioning and waste.
- AWS automation services, such as **CloudFormation** for infrastructure provisioning
- **AWS Systems Manager** for operational tasks, lower administrative overhead.
    - Allows for users to get operation insights into their resources to quickly identify any issues that might impact applications using those resources

- AWS provides cost analysis and budgeting tools like **AWS Cost Explorer**, **AWS Budgets**, and the **AWS Pricing Calculator** to optimize spending and forecast costs accurately.
- **Scaling Up vs Out**
    - Up relates to more computing power, whereas out means more resources
    - Scale-out to increase **fault tolerance**

Domain 2: Security and Compliance

2.1 Understand the AWS Shared Responsibility Model

- The AWS Shared Responsibility Model defines clear security responsibilities:
    - **AWS Responsibilities ("Security of the Cloud")**: AWS manages the infrastructure, including hardware, software, networking, and facilities.
    - **Customer Responsibilities ("Security in the Cloud")**: Customers are responsible for securing their data, configuring access permissions, and managing IAM policies.
    - Responsibilities vary by service type: For example, in **Amazon RDS**, AWS handles the database infrastructure, while customers secure data and manage access policies; in **AWS Lambda**, customers only focus on code security and IAM settings.
- Emphasizes protecting the root user account with multi-factor authentication (MFA) and adhering to the principle of least privilege.

2.2 Understand AWS Cloud Security, Governance, and Compliance

- AWS provides robust compliance options with certifications like PCI DSS, HIPAA, and GDPR. Compliance information can be accessed via **AWS Artifact**.
- Security tools and services include:
    - **AWS Security Hub** and **Amazon GuardDuty** for threat detection and management.
    - **AWS Shield** for DDoS protection and **AWS WAF** for web application security.
        - Automatically on for all web apps hosted on AWS
    - **Amazon Inspector** for automated vulnerability scanning and deviation from best practices
- Governance tools like
    - **AWS Config**
        - Enables assessment and audit of the configurations of AWS Resources.
        - Continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations
    - **AWS CloudTrail**

        - Enables GRC on AWS accounts
        - Continuously log, monitor nad retain account activity related to actions
        - The logs are automatically encrypted and stored in an S3 Bucket
    - **AWS CloudWatch**
        - Monitoring and Observability service
        - Provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health
        - CloudWatch Billing Alarms
            - Can be used to monitor and calculate estimated charges
            - Sends an alarm when the cost exceeds a certain threshold
- Encryption is a cornerstone of cloud security:
    - **Encryption in transit** using SSL/TLS and **encryption at rest** via services like **AWS Key Management Service (KMS)**.
        - **AWS KMS**
            - Makes it easy to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications
        - **Customer Managed Key (CMK)**
            - A company wants to have control over creating and using its own keys for encryption on AWS services.
    - Managed services like **Amazon S3** and **RDS** offer built-in encryption capabilities.

2.3 Identify AWS Access Management Capabilities

- Identity and Access Management (IAM) allows users to define and enforce granular access permissions:
    - Use IAM roles, groups, and managed policies to minimize direct reliance on the root account.
        - Use JSON files to store policies, which must include a Effect and Action
    - IAM best practices include enforcing MFA, creating custom policies, and using **AWS Secrets Manager** for managing access credentials securely.
    - Use **Credentials Report** to generate a list of all users in an account and the status of various aspects like passwords, access keys, and MFA devices
    - Multi-factor authentication (MFA) ensures an added layer of security, especially for sensitive accounts.
- **AWS IAM Identity Center (AWS SSO)** simplifies centralized access management across multiple AWS accounts and third-party applications.
- Access management extends to cross-account roles, federated identity solutions, and AWS services that support external identity providers.

- AWS Security Token Service (AWS STS)
    - Create and provide trusted users with temporary security credentials that control access to your AWS resources

2.4 Identify Components and Resources for Security

- Security services:
    - **Security Groups**: Operate as virtual firewalls at the instance level.
        - Can only have **allow** rules
        - Stateful, meaning it automatically allows the return traffic
    - **Network ACLs**: Provide an additional layer of security at the subnet level.
        - Contains a numbered lift of rules and evaluates these rules in increasing order while dividing whether to allow the traffic
        - Stateless, meaning return traffic must be explicitly allowed
    - **AWS Trusted Advisor**: Offers security recommendations, such as checking for open ports or inactive IAM keys.
    - **AWS WAF:** Protects HTTP HTTPS traffic at the Application Layer 7
- Documentation and resources:
    - AWS maintains an extensive **Knowledge Center**, **Security Center**, and **Security Blog** for updated best practices.
- Third-party integrations:
    - The AWS Marketplace offers tools for advanced security needs, including third-party firewalls and SIEM solutions.
    - Allows for software vendors to sell SaaS products running on AWS Cloud
    - Allows sellers to sell software that has been bundled with AMIs

Domain 3: Cloud Technology and Services

3.1 Define Methods of Deploying and Operating in the AWS Cloud

- **Deployment Options**:
    - Use the **AWS Management Console** for an intuitive web interface.
    - Access AWS programmatically via **AWS CLI**, **SDKs**, or APIs.
        - **AWS SDK**
            - Takes the complexity out of coding by providing language specific APIs for AWS Services
        - **AWS Access Keys**
            - long-term credentials for an **IAM User** or the AWS account root user.
            - **Consists of a Access Key ID and a Secret Access Key**
    - Implement **Infrastructure as Code (IaC)** using tools like **AWS CloudFormation** or **Terraform** for automated provisioning.

        - **Cloud Formation**
            - Allows you to use a programming language or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts
    - **Elasic Beanstalk**
        - Easy to use service for deploying and scaling web applications and services developed with various programming languages
        - Upload your code, and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto-scaling to application health monitoring
- **Operational Models**:
    - **One-time operations**: Suitable for manual, infrequent tasks.
    - **Repeatable processes**: Ideal for scalable operations using automation tools.
- **Deployment Types**:
    - **Cloud-only**: Fully hosted on AWS.
    - **Hybrid**: Combines on-premises and cloud resources.
    - **On-premises**: Using AWS services like **Outposts** for local infrastructure management.
- **Connectivity Options**:
    - **AWS Direct Connect**: Provides a private connection to AWS resources.
        - Allows for a company's on premises environment to connect to a VPC without using the public internet
    - **AWS VPN**: Enables secure connectivity over the internet.
    - **AWS Site-to-Site VPN**
        - Creates a secure connection between your data center or branch office and your AWS Cloud Resources over the public internet
    - **Internet Gateway**
        - Horizontally scaled, redundant, and highly available VPC Component that allows communication between your VPC and the internet
        - NOT used to connect on prem to AWS Cloud
    - **Network Address Translation (NAT)**
        - Managed by AWS
    - **AWS Transit Gateway**
        - Connect VPCs and on premises networks through a central hub
        - Use in combination with AWS Direct Connect for the most efficient solution to connecting on-prem with multiple VPCs
    - VPC Peering Connection
        - Connect two VPCs together

3.2 Define the AWS Global Infrastructure

- **Core Components**:
    - **Regions**: Fully isolated locations hosting AWS resources.
    - **Availability Zones (AZs)**: Independently powered and networked facilities within a Region, designed to avoid single points of failure.
        - At least 3 AZs per Region
        - At least 1 discrete datacenter per AZ
    - **Edge Locations**: Distributed network endpoints for caching content and reducing latency using **Amazon CloudFront**.
    - Specialized zones:
        - **AWS Local Zones**: Extend AWS infrastructure to locations closer to end-users.
        - **AWS Wavelength Zones**: Tailored for ultra-low latency applications.
- **Key Benefits**:
    - High availability and fault tolerance using multiple AZs.
    - Disaster recovery and business continuity via multi-region deployments.

3.3 Identify AWS Compute Services

- **Compute Options**:
    - **Amazon EC2**: Offers configurable virtual machines (e.g., compute-optimized, storage-optimized).
        - The easiest way to access resizable compute capacity in the cloud with support for per-second billing and access to the underlying OS.
        - Must be launched by an **Amazon Machine Image (AMI),** which includes:
            - EBS snapshots
            - Instance Store backed AMIA
            - A template for the root volume (OS, App Server, and applications)
    - **Serverless**:
        - **AWS Lambda** eliminates the need to manage servers for code execution.
            - Charged based on the execution time and number of requests
    - **Containers**: Managed options like **Amazon ECS**, **EKS**, and **AWS Fargate** for container orchestration.
        - ECS
            - A highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster
        - EKS
        - Fargate
            - A serverless compute engineer for containers
            - Moves the need to provision and manage servers, and instead
        - Elastic Container Registry (ECR)

            - Used to store, manage, and deploy Docker container images
    - **Elasticity**: Auto Scaling ensures applications adapt to workload changes automatically.
        - **AWS Auto Scaling**
            - Monitor applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost
            - Can automatically remove unhealthy instances
            - Can automatically register new instances to the load balancer
            - Great against DDOS attacks, but cannot deploy AWS Shield automatically
- **Load Balancing**:
    - **Elastic Load Balancer (ELB)** distributes traffic across multiple EC2 instances to enhance availability.

3.4 Identify AWS Database Services

- **Relational Databases**:
    - Managed options like **Amazon RDS** and **Aurora** offer scalability and reliability.
    - **Amazon Aurora**
        - MySQL and PostgreSQL-compatible relational database
- **NoSQL Databases**:
    - **Amazon DynamoDB**
        - fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale.
        - schemaless
        - built-in security, continuous backups, automated multi-region replication, in-memory caching, and data export tools.
        - offers active-active cross-region support that is needed for the company.
        - Use Global Tables for replication across distributed systems
        - Use DynamoDB Accelerator for faster read speeds
- **Other Database Types**:
    - In-memory databases: **Amazon ElastiCache** for low-latency data.
        - **ElastiCache**
            - Allows you to seamlessly set up, run, and scale popular open-Source compatible in-memory data stores in the cloud
            - Blazing fast and low latency
            - Can take the load off of EC2 instances that are intensely reading data from databases
    - Graph databases: **Amazon Neptune** for relationships and network models.
- **Migration Tools**:

    - **AWS Database Migration Service (DMS)** supports seamless migrations to AWS databases.
    - **Migration Evaluator** is a complimentary service to create data-driven business cases for AWS Cloud planning and migration
- **Amazon Redshift**
    - A fully managed data warehare product designed for large scale dataset storage and analysis
    - Allows you to run complex analytic queries against terabytes to petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance storage, and massively parallel query execution.
- **Amazon EMR**
    - Industry-leading cloud big data platform for processing vast amounts of data using OS tools
- **Amazon Kinesis**
    - a real-time data streaming service that allows you to continuously capture, process, and analyze large amounts of data from sources like applications, IoT devices, and logs.

3.5 Identify AWS Network Services

- **Networking Components**:
    - **Amazon VPC**: Provides an isolated network environment.
    - **Subnets and Gateways**: Control network segmentation and connectivity.
- **Security Features**:
    - **Security Groups** and **Network ACLs** for fine-grained access control.
- **DNS Services**:
    - **Amazon Route 53** enables domain registration and DNS management.
        - Web Apps using R53 can be protected with AWS Shield
        - **Weighted**
            - Allows multiple resources to be accessed from 1 domain name
        - **Simple**
            - Use for a single resource with a given function
        - **Geolocation**
            - Use to route traffic based on location of user
        - **Geoproximity**
            - Use to route traffic based on the location of resources
        - **Latency**
            - Use when you have multiple resources in different regions and want to route traffic to the destination with least latency
        - **Failover**
            - Active-passive configuration

                - Allows you to route traffic to another resource when the first in unhealthy
- **Edge Services**:
    - **Amazon CloudFront**: A content delivery network for caching and reducing latency.
    - **AWS Global Accelerator**: Improves application availability and performance globally.
        - Web applications running on Global Accelerator can be protected from DDoS attacked with AWS Shield
        - Provides static IP addresses that act as fixed entry points to applications
        - Good fit for non-HTTP use cases

3.6 Identify AWS Storage Services

- **Object Storage**:
    - **Amazon S3**: Ideal for scalable object storage with multiple storage classes (e.g., S3 Standard, S3 Glacier for archival).
        - Standard
            - High durability, availability, and performance object storage for frequently accessed data
        - Intelligent-Tiering
            - Optimizes costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead
        - Infrequent Access (IA)
            - Charged per access
        - Glacier
            - Supports long term retention and preservation for data that may be accessed once to twice a year
            - Great for healthcare, finance, and public sectors, where data retention policies are long
            - Charged per access
    - **S3 Lifecycle**
        - Use this to ensure cost-effective storage throughout their lifecycle
        - Two Actions
            - Transition Actions
                - When to move
            - Expiration Actions
                - When to delete
    - **S3 Replication**

        - Use this to copy data between multiple test accounts while retaining object metadata
- **Block Storage**:
    - **Amazon EBS**: Designed for high-perfor*f*mance storage attached to EC2 instances.
        - EBS volume can be attached to a single instance in the same Availability Zone (AZ) whereas EFS file system can be mounted on instances across multiple Availability Zones (AZ)
- **File Storage**:
    - **Amazon EFS**: Provides elastic file storage for shared file access.
        - Stores files across AZs, Regions, and VPCs
    - **Amazon FSx**: Optimized for Windows File Server and Lustre workloads.
- **Backup Solutions**:
    - **AWS Backup** centralizes and automates backup tasks across AWS services.
- **Lifecycle Policies**:
    - Automates data transfer to cost-effective storage tiers based on access patterns.
- **Instance Store**
    - Temporary Block Level Storage for an instance. They are attached physically to the host computer and cannot be accessed by multiple instances.
- **AWS Storage Gateway**
    - Hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud
    - Gateway Types
        - Tape
        - File
        - Volume

3.7 Identify AWS Artificial Intelligence and Machine Learning (AI/ML) Services

- **AI/ML Services**:
    - **Amazon SageMaker**: End-to-end service for building, training, and deploying ML models.
    - **Amazon Rekognition**: Image and video analysis.
        - Identify object in a photo
    - **Amazon Lex**: Conversational AI for chatbots.
- **Analytics Services**:
    - **Amazon Athena**: SQL queries on data stored in S3.
    - **AWS Glue**: fully managed data integration and ETL service
    - **Amazon QuickSight**: Business intelligence and visualization.
- **Security Services**
    - **Amazon Macie**

        - A fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in AWS

3.8 Identify Services from Other In-Scope AWS Service Categories

- **Application Integration**:
    - **Amazon EventBridge**, **SNS**, and **SQS** for decoupled architectures.
    - **Amazon SQS (Simple Queue Service)**
        - fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.
    - **Amazon SNS (Simple Notification Service)**
        - highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications
        - Pair with other services to get alerts
            - CloudWatch
                - Whenever someone logs in
            -
    - **Amazon MQ**
        - Managed message broker service for Apache ActiveMQ and RabbitMQ that makes it easy to set up and operate message brokers on AWS
        - Use this for an easy move to the cloud, but new applications should use SNS and SQS
    - **Amazon EventBridge**
        - A Service that provides real-time access to changes in data in AWS Services without writing code
- **Business Applications**:
    - **Amazon Connect**: Cloud-based contact center.
- **End-User Computing**:
    - Services like **Amazon WorkSpaces** for virtual desktops.
- **Developer Tools**:
    - CI/CD pipelines with **CodeCommit**, **CodePipeline**, and **CodeBuild**.
- **IoT**:
    - **AWS IoT Core** manages device connectivity and messaging.
- **Speech;**
    - **Translate**
        - Uses neural machine translation via deep learning models to deliver more accurate and more natural sounding translations
    - **Polly**
        - Text to Speech

    - **Transcribe**
        - Converts speech to test for downstream analysis
- **Others**
    - **Xray (AWS X-Ray)**
        - Analyze and debug serverless and distributed applications such as those built using a microservices architecture
    - **PinPoint**
        - Allows marketers and developers to deliver customer centric engagement experience by capturing customer usage data to draw real-time insights
    - **Amazon OpenSearch Service**
        - Makes it easy to perform interactive log analytics, real-time application monitoring, website search, and more
    - **AWS Lightsail**
        - a simplified cloud platform offering pre-configured, cost-effective virtual private servers, storage, and networking for developers to quickly deploy applications, websites, and small workloads without managing complex infrastructure.
    - **AWS Fault Injection Simulator**
        - A fully managed service for running fault injection experiments on AWS
    - **AWS Kendra**
        - An intelligent search service powered by machine learning
        - Can search across multiple locations and location repositories
    - **AWS Code**
        - **AWS CodeDeploy**
            - Automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises
        - **AWS CodeCommit**
            - A fully managed source control service that hosts secure Git-Based repositories
            - Makes it easy for the team to collaborate on code in a secure and highly scalable ecosystem
        - **AWS CodePipeline**
            - Continuous delivery service that enables you to model, visualize, and automate the steps required to release your software
    - **Device Farm**
        - Allows for application testing on many desktops and mobile devices
    - AWS Batch
        - Enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.
    - AWS OpsWorks

        - AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.
    - AWS CodeGuru
        - Amazon CodeGuru is a developer tool that provides intelligent recommendations to improve code quality and identify an application's most expensive lines of code.

Domain 4: Billing, Pricing, and Support

4.1 Compare AWS Pricing Models

- **Compute Purchasing Options**:
    - **On-Demand Instances**: Pay for compute capacity by the second with no upfront commitment.
    - **Reserved Instances (RI)**: Commit to one- or three-year terms for significant savings.
        - **Services that support RI**
            - Amazon EC2
            - Amazon DynamoDB
            - Amazon RDS
        - Up to a 72% Discount
    - **Savings Plans**: Flexible pricing model for consistent savings across EC2, Lambda, and Fargate usage.
    - **Spot Instances**: Utilize unused EC2 capacity at **up to 90% savings** for fault-tolerant workloads.
    - **Dedicated Hosts**: Physical servers for meeting specific compliance and licensing requirements.
- **Storage Pricing**:
    - Amazon S3 offers multiple pricing tiers based on frequency of access and retrieval time, such as **S3 Standard**, **S3 Intelligent-Tiering**, and **S3 Glacier**.
    - Costs are also incurred for data transfers between regions or to the internet
    - **Inbound data transfer are not charged, only outbound**
- **Data Transfer Charges**:
    - **Inbound traffic** is free; **outbound traffic** incurs costs based on the amount of data transferred and destination
- **Concierge Support Team**
    - Intern AWS Billing and Account experts that specialize in working with enterprise accounts

4.2 Understand Resources for Billing, Budget, and Cost Management

- **Cost Management Tools**:

    - **AWS Cost Explorer**: Visualizes cost and usage trends over time.
    - **AWS Budgets**: Sets custom alerts for cost and usage thresholds.
        - Usage - how much you want to spend on a service
        - Cost - how much you want to use one or more services
        - Reservation - track usage of reserved instances
    - **AWS Pricing Calculator**: Estimates monthly costs for AWS services based on expected usage.
    - **AWS Billing Conductor**: Manages and allocates costs across business units or linked accounts.
- **Billing and Cost Optimization**:
    - **AWS Organizations**
        - Consolidate billing, compliance, access control and resource sharing across multiple accounts.
            - Allows for multiple users to share Reserved Instanced (RIs)
        - Automate account creation, create croups of accounts, and apply policies for these groups
        - An account must be able to stand alone before it can be removed from org
    - Use **cost allocation tags** to categorize and track resource costs effectively.
        - Consists of a key and ONLY ONE value for each key
        - Types
            - AWS Generated Tag
            - User Defined Tag
    - The **AWS Cost and Usage Report** provides detailed insights into spending patterns.
    - **Computer Optimizer**
        - Recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics

4.3 Identify AWS Technical Resources and Support Options

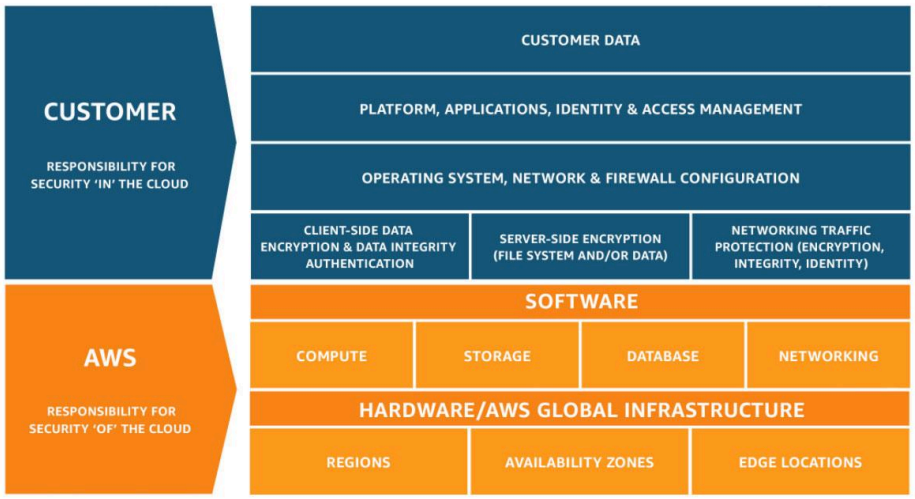
- **AWS Support Plans**:
    - **Basic**: Free tier with access to documentation, whitepapers, and AWS re:Post.
    - **Developer**: Provides business hours access to support engineers and general guidance for production workloads.
    - **Business**: 24/7 access to support engineers, Trusted Advisor checks, assistance with 3rd party platforms, and best practice recommendations.
    - **Enterprise**: Tailored support with Technical Account Managers (TAMs), proactive guidance, and a response time of <15 minutes for critical issues.
    - **Enterprise On Ramp Support**

        - Use this is you have business critical workloads in AWS and want 24x7 access to technical support and need expert guidance
- **Technical Resources**:
    - **AWS Documentation and Whitepapers**: Official AWS guides for service details and architecture best practices.
    - **AWS re:Post and Knowledge Center**: Community-driven Q&A and troubleshooting guides.
    - **AWS Trust and Safety Team**: Helps report abuse and security incidents.
- **Monitoring and Optimization Tools**:
    - **AWS Trusted Advisor**: Checks security, performance, and cost optimization best practices.
        - Cost Optimization
            - Helps identify underutilized and unattached EBS Elastic Volumes
        - Performance
        - Security
        - Fault Tolerance
        - Service Limits
    - **AWS Health Dashboard**: Provides alerts and updates on the status of AWS services impacting customer environments.
    - **AWS Professional Services** and **Solutions Architects**: Assist with architecture design, migrations, and workload optimization.
        - **Professional Services**
            - Global team of experts that can help with desired business outcomes in AWS
- **AWS Partner Network (APN)**:
    - Includes independent software vendors (ISVs) and system integrators for specialized solutions.
    - Benefits include training, certifications, and partner events for organizations leveraging AWS services.
    - **APN Consulting Partner**
        - Professional services firms that help customers design, architect, build, migrate and manage their workloads and applications on AWS
    - **APN Technology Partner**
        - Provide hardware, connectivity, or software solutions that are hosted on AWS Cloud

Extra: My Own Questions

- What is the difference between AWS S3, EBS, and EFS?

    - **Amazon S3**: **Object storage** for unstructured data (images, videos, backups, archives). Accessible globally via HTTP/HTTPS. Best for static content, data lakes, and long-term storage. Highly durable (11 9s) and scalable.
    - **Amazon EBS**: **Block storage** for a single **EC2 instance**. Provides low-latency, high-performance volumes. Ideal for databases, operating systems, and applications requiring consistent IOPS.
    - **Amazon EFS**: **File storage** for shared access across multiple EC2 instances. Scalable and multi-AZ. Best for workloads like web servers, media processing, and containerized applications.
- How often do Linux Based On Demand EC2 instances get charged
    - Every 60 seconds



    - Confusing ones below:
        - Part of AWS Responsibility
            - Edge Location Management
                - Manage and secure the physical and network infrastructure of its globally distributed edge locations
        - Part of Customer Responsibility
            - Both Server-Side and Client-Side Encryption
- What is the difference between a Dedicated Host and Dedicated Instance?
    - You use dedicated hosts wben you need to use software licenses
- What is the difference between AWS CloudTrail and CloudWatch
    - **Amazon CloudWatch** monitors and logs the **performance and health** of AWS resources and applications, while **AWS CloudTrail** tracks and records **API activity and user actions** for auditing and compliance.
    - **CloudWatch Logs** monitors, stores, and allows access to log files from EC2 instances, CloudTrail, Route 53, and other sources such as on premises servers
- Who are the main stakeholders in the AWS CAF
    - Chief Technology Officer (CTO), technology leaders, architects, and engineers.

- What is the difference between a VPC and an AZ?
    - A VPC spans ALL AZs in a Region whereas a subnet spans only one AZ in a Region.
- Why use a Local Zone over a Edge Location for consistent service for users?
    - A Local Zone puts the storage and compute services closer to end users, whereas AWS Edge Locations only cache copies of the data for local access
- What is the difference between an NACL and a Security Group
    - Network ACLs are for the subnet level, whereas security groups are instance-specific, with up to 5 per instance.
- What is the difference between Amazon EC2 Instance Connect and AWS Systems Manager Session Manager?
    - Instance Connect is for connecting securely into Linux instances and uses Port 22. Session Manager is for connection securely into all instances without opening ports.
- What are 3 options in AWS to manage all services?
    - AWS Management Console
    - AWS CLI
    - AWS SDK
- What are the AWS Services that are global in nature?
    - IAM, CloudFront, Route 53, WAF
- Which of the following solutions can you use to connect your on-premises network with AWS Cloud?
    - AWS VPN
    - AWS Direct Connect
- What services have encryption enabled by default?
    - By Default - S3, Storage Gateway
    - Not By Default - Redshift, EBS, EFS
- What S3 service can we use to avoid accidental deletion
    - S3 Versioning
- What would you need to do to get 2 separate invoices for dev and prod environments?
    - 2 separate AWS accounts for dev and prod
- What is the difference between Direct Connect and Transit Gateway?
    - DC is for direct connections
    - TG is for a connection through a central hub
- A company is looking for a guided path to help deploy, configure, and secure its new workloads while ensuring that it is ready for on-going operations in the cloud. Which of the following AWS services/tools can be leveraged for this use case?
    - Cloud Foundations
- Where is CloudWatch billing metric data stored region-wise?
    - US East 1

- How are on demand EC2 instances charged?
    - By the Second
- When would you use different accounts?
    - When you want a dev, test, and prod environment, each with its own billing
- When would you use S3 One Zone over standard?
    - Mainly for long term backups bc there is a 20% discount
- Whats the difference between IAM Policy and IAM Access Advisor
    - Former is for creation, and the latter is for detailed analysis and review of individual user permissions to resources
-