AWS Certified Cloud Practitioner Study Guide

First, let's start with some basic cloud computing concepts and terms that apply to all hyperscalers. Much of this section will be applicable and will appear on your AWS CCP exam.

Cloud Computing Concepts

Cloud Deployment Models

Public Cloud: Public cloud environments are provided by third-party cloud service providers and are accessible over the public internet. These services are available to anyone who wants to use or purchase them.

- Characteristics: Public clouds typically offer high scalability, reliability, and efficiency. They operate on a pay-as-you-go pricing model, which can be cost-effective for users.
- Examples: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Private Cloud: A private cloud is a cloud infrastructure operated solely for a single organization. It can be managed internally by the organization or by a third party and hosted either internally or externally.

- Characteristics: Private clouds offer greater control and security compared to public clouds, making them suitable for organizations with stringent regulatory or data privacy requirements.
- Use Cases: Often used by government agencies, financial institutions, and other organizations with sensitive data and high-security needs.

Hybrid Cloud: Hybrid clouds combine on-premises infrastructure (or a private cloud) with a public cloud, allowing data and applications to be shared between them.

- Characteristics: They provide flexibility and more deployment options, allowing businesses to optimize their existing infrastructure, security, and compliance.
- Use Cases: Ideal for businesses with dynamic workloads, large data processing requirements, or those with a need for a phased approach to cloud adoption.

Scalability: Scalability in cloud computing refers to the ability to increase or decrease IT resources as needed to meet changing demand.

- Importance: Scalability is essential in cloud computing for handling varying workloads efficiently. It ensures that the infrastructure can handle growth in users, data volume, or transaction volume without performance degradation.
- Types: There are mainly two types: vertical (scaling up or down by adding more power to existing machines) and horizontal (scaling out or in by adding more machines).

Elasticity: Elasticity is the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources automatically.

- Importance: It enables cloud systems to dynamically allocate resources to meet demand, ensuring cost-efficiency and maintaining performance.
- Comparison with Scalability: While scalability refers to the capability to handle growth, elasticity is about matching resources closely to current demand, often in real-time.

Cloud Services Models

Infrastructure as a Service (IaaS): Provides virtualized computing resources over the Internet. Example: Amazon Web Services (AWS), Microsoft Azure.

Platform as a Service (PaaS): Offers hardware and software tools over the internet, typically for application development. Example: Google App Engine.

Software as a Service (SaaS): Delivers software applications over the Internet, on a subscription basis. Example: Google Workspace, Salesforce.

Cloud Infrastructure

Hardware and software components for cloud computing, including servers, storage, networking, and virtualization.

Region: A geographical area where AWS data centers are located. Each region consists of multiple Availability Zones.

Availability Zone (AZ): Data centers within a region that are isolated from each other for fault tolerance.

Virtualization: Technology enabling multiple virtual machines on a single physical machine; foundational for cloud infrastructure.

Pay-As-You-Go Pricing: Flexible pricing model based on usage, characteristic of cloud services.

Identity Management: Identity and Access Management (IAM): A framework for managing digital identities and permissions, ensuring that the right individuals have access to the right resources at the right times for the right reasons.

Multi-Factor Authentication (MFA): A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Storage: Cloud Storage and Data Management: The practice of storing data in the cloud, where data is maintained, managed, backed up remotely, and made available to users over a network.

Object Storage: A storage architecture that manages data as objects, as opposed to other storage architectures like file systems (which manage data as a file hierarchy) and block storage (which manages data as blocks).

Block Storage: Storage architecture that manages data in blocks or volumes, typically used in storage area network (SAN) environments.

File Storage: A storage format that organizes and stores data as a hierarchy of files within directories.

Data Redundancy: The process of storing the same piece of data in multiple places to improve reliability and accessibility.

Data Lake: A large storage repository that holds a vast amount of raw data in its native format until it is needed.

Storage Classes/Tiers: Different categories of storage solutions based on access speed, cost, and frequency of use.

Data Archiving: The process of moving data that is no longer actively used to a separate storage device for long-term retention.

Snapshots: Point-in-time copies of data or a virtual machine's state, used for backup or restoration purposes.

SSD and HDD: Solid State Drives (SSD) and Hard Disk Drives (HDD) are types of storage devices; SSDs are faster and more durable but typically more expensive per GB than HDDs.

NAS (Network Attached Storage): A file-level storage architecture connected to a computer network providing data access to a group of clients.

Virtual Machines (VMs): Software emulations of physical computers, creating a virtual environment that behaves like a separate computer system.

Containers: Lightweight, executable packages that include everything needed to run a piece of software, including the code, runtime, system tools, libraries, and settings.

Serverless Computing: A cloud-computing execution model where the cloud provider runs the server and dynamically manages the allocation of machine resources.

CPU and GPU: Central Processing Unit (CPU) and Graphics Processing Unit (GPU) are the primary types of processors in a computer; CPUs are better for general-purpose tasks while GPUs are optimized for graphics rendering and parallel processing.

Provisioning: The process of setting up and configuring hardware and software resources in an IT environment.

Microservices Architecture: An approach to application development in which a large application is built as a suite of modular services.

Cloud Bursting: A configuration set up in cloud computing to handle peak loads by using public cloud resources when the private cloud's capacity is exceeded.

Quantum Computing in the Cloud: Providing access to quantum computing resources over the cloud, allowing users to perform quantum computing tasks without owning a quantum computer.

Machine Learning and AI in the Cloud: The use of cloud computing resources to facilitate machine learning and artificial intelligence processing and tasks.

Distributed Computing: A model in which components of a software system are shared among multiple computers to improve efficiency and performance.

Edge Computing: A distributed computing paradigm which brings computation and data storage closer to the sources of data, aiming to reduce latency and bandwidth use.

Fog Computing: An architecture that uses edge devices to carry out a substantial amount of computation, storage, and communication locally and routed over the internet backbone.

Virtual Networking

Software-Defined Networking (SDN): An approach to networking that uses software-based controllers or application programming interfaces (APIs) to direct traffic on the network and communicate with the underlying hardware infrastructure.

Virtual Private Network (VPN): A private network that extends across a public network, enabling users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Network Functions Virtualization (NFV): The concept of replacing traditional network hardware with software solutions that perform the same functions.

Subnet: A smaller network inside a large network, segmented for managing large networks more efficiently or for security or performance reasons.

VLAN (Virtual Local Area Network): A method of creating multiple distinct broadcast domains that are mutually isolated, on one physical network infrastructure.

Load Balancer: A device or software that distributes network or application traffic across multiple servers or network nodes to ensure efficiency and reliability of resource use.

IP Addressing: The method of assigning a numeric label to each device connected to a computer network that uses the Internet Protocol for communication.

DNS (Domain Name System): The hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network, translating more readily memorized domain names to numerical IP addresses.

Gateway: A network node that serves as an access point to another network, often used to connect a local network to the internet.

Monitoring

Performance Monitoring: The process of monitoring and managing the performance of a computer, network, application, or other IT resources.

Cloud Audit: The process of reviewing and evaluating a cloud service provider's infrastructure, policies, and operations for compliance, security, and risk management.

Usage Reporting: The process of documenting and analyzing how cloud resources are being used, often for the purpose of improving efficiency, planning capacity, and managing costs.

Security

Encryption: The method of converting information or data into a code, especially to prevent unauthorized access.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Cryptographic protocols designed to provide communications security over a computer network.

Penetration Testing: A method of evaluating the security of a computer system or network by simulating an attack from a malicious source.

Compliance Standards: Set of guidelines and regulations that an organization must follow, often related to security and privacy (e.g., GDPR, HIPAA, SOC 2).

DDoS Attack (Distributed Denial of Service): A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Firewall: A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

Security and Compliance: The state of being in accordance with established security policies and regulations.

Security Audit: A systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.

Data Privacy: The handling and processing of data in a manner that maintains its confidentiality and privacy.

Blockchain in Cloud Computing: The use of blockchain technology within cloud computing for enhanced security, transparency, and traceability.

Cost Optimization

Pay-As-You-Go Pricing: A cost model for cloud services where you pay only for the resources you consume.

Cost Optimization: The process of reducing overall costs while maximizing the efficiency and effectiveness of cloud resources.

Resource Utilization: A measure of how effectively an organization is using its available resources.

Billing and Metering: The process of measuring and charging users for the consumption of cloud resources.

Cloud Budgeting: The practice of allocating and managing financial resources for cloud computing.

Cost Management and Analysis: The process of tracking, analyzing, and optimizing the costs associated with cloud computing.

Capacity Planning: The process of determining the necessary resources to meet future workload demands.

Service Level Agreements (SLAs): Formal agreements between service providers and users that specify the level of service expected, often including performance metrics and uptime guarantees.

Total Cost of Ownership (TCO): An estimation of the expenses associated with purchasing, deploying, using, and retiring a product or piece of equipment.

Cloud Cost Allocation: The process of attributing cloud costs to specific departments, projects, or users within an organization.

Usage Reporting: The detailed documentation and analysis of how and where cloud resources are being consumed.

Now, let's move on to the AWS-specific portion.

- Amazon EC2 (Elastic Compute Cloud): Provides scalable computing capacity in the cloud. It allows users to run and manage server instances.
- Amazon S3 (Simple Storage Service): Offers scalable object storage for data backup, archival, and analytics.
- Amazon RDS (Relational Database Service): Simplifies setup, operation, and scaling of a relational database. Supports MySQL, PostgreSQL, Oracle, SQL Server, and more.
- AWS Lambda: Lets you run code without provisioning or managing servers. You pay only for the compute time you consume.
- Amazon VPC (Virtual Private Cloud): Offers a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.
- Amazon S3 Glacier: A secure, durable, and low-cost storage service for data archiving and long-term backup.
- Amazon DynamoDB: A fast and flexible NoSQL database service for any scale.
- Amazon CloudFront: A fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally.
- AWS IAM (Identity and Access Management): Enables you to manage access to AWS services and resources securely.
- Amazon Route 53: A scalable and highly available Domain Name System (DNS) web service.
- Amazon SQS (Simple Queue Service): Offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components.
- Amazon SNS (Simple Notification Service): A flexible, fully managed pub/sub messaging and mobile notifications service for coordinating the delivery of messages to subscribing endpoints and clients.

- Amazon Elastic Beanstalk: An easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.
- AWS CloudFormation: Gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.
- Amazon Redshift: A fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake.
- Amazon ElastiCache: A web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud.
- Amazon EKS (Elastic Kubernetes Service): A managed service that makes it easy to run Kubernetes on AWS without needing to install and operate your own Kubernetes clusters.
- Amazon Sagemaker: A fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning models quickly.
- AWS CodeDeploy: A service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises.
- AWS Direct Connect: Makes it easy to establish a dedicated network connection from your premises to AWS.
- AWS Fargate: A serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).
- Amazon Kinesis: A platform for streaming data on AWS, offering powerful services to make it easy to load and analyze streaming data, and also providing the ability for you to build custom streaming data applications for specialized needs.
- AWS WAF (Web Application Firewall): Helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.
- AWS Step Functions: Lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly.
- Amazon EMR (Elastic MapReduce): A cloud-native big data platform, allowing processing of vast amounts of data quickly and cost-effectively across resizable clusters of Amazon EC2 instances.
- AWS Glue: A fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.
- Amazon Aurora: A MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases.
- AWS CloudTrail: A service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.
- Amazon Lightsail: Designed to be the easiest way to launch and manage a virtual private server with AWS. It offers everything needed to get a project or website off the ground quickly.
- Amazon Lex: A service for building conversational interfaces into any application using voice and text.

- AWS Shield: A managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.
- Amazon Polly: A service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products.
- Amazon CloudFront: A fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.
- AWS X-Ray: Helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture.
- Amazon Chime: A communication service that lets you meet, chat, and place business calls inside and outside your organization, all using a single application.
- AWS AppSync: An enterprise-level, fully managed GraphQL service with real-time data synchronization and offline programming features.
- AWS Transfer for SFTP: A fully managed service which enables the transfer of files directly into and out of Amazon S3 using the Secure File Transfer Protocol (SFTP).
- Amazon QuickSight: A fast, cloud-powered business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get business insights from your data.
- AWS Backup: A fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services.
- Amazon WorkSpaces: A managed, secure Desktop-as-a-Service (DaaS) solution which helps you provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users.
- Amazon Connect: A cloud-based contact center service that makes it easy for any business to deliver better customer service at lower cost.
- AWS Chef Automate: An automation platform that provides a full suite of enterprise capabilities for workflow, node visibility, and compliance. It is essentially a managed service version of the Chef Automate platform.
    - Features:
    - Automated Configuration Management: It automates the configuration of cloud and on-premises infrastructure using code, allowing for consistency and compliance of configurations.
    - Workflow Automation: Chef Automate includes a pipeline for continuous deployment, managing changes through environments like testing, staging, and production.
    - Compliance and Security: It offers tools for defining compliance as code and automatically validating infrastructure against compliance policies.
    - Visibility and Reporting: Provides dashboards and reports for infrastructure visibility, compliance, and the status of continuous delivery processes.
    - Use Cases: Ideal for organizations looking to automate infrastructure and application management, enforce compliance, and streamline deployment processes.

- AWS OpsWorks: A configuration management service that uses Chef and Puppet, two popular automation platforms. It allows you to manage and configure both your on-premises servers and AWS instances.
    - Features:
    - Automated Configurations: OpsWorks automates various aspects of server configurations, including software installations, database setups, and server scaling.
    - Integration with AWS Services: It integrates seamlessly with other AWS services, enabling easier management of AWS resources.
    - Support for Chef and Puppet: OpsWorks supports Chef Automate and Puppet Enterprise, allowing you to use existing recipes and configurations.
    - OpsWorks Stacks: A service that provides a simple and flexible way to manage stacks and applications. It uses Chef, automates tasks like software configurations, and integrates with AWS services for efficient resource management.
- AWS CloudFormation is an automated provisioning tool from Amazon Web Services that enables the modeling, provisioning, and management of AWS resources using template files. These templates, written in JSON or YAML, describe the AWS resources and their configurations. CloudFormation creates “stacks” from these templates, allowing for easy creation, update, and deletion of resource collections as single units.
- AWS Cost Explorer: Allows you to view and analyze your AWS costs and usage. You can identify trends, pinpoint cost drivers, and detect anomalies.
- AWS Budgets: Enables you to set custom budgets to track your cost and usage from the simplest to the most complex use cases. You receive alerts when your budget thresholds are breached.
- AWS Price List API: Offers programmatic access to pricing information for all AWS services, enabling detailed cost analysis and budgeting.
- AWS Cost and Usage Report: Delivers the most comprehensive set of AWS cost and usage data available, enabling detailed analysis.
- AWS Trusted Advisor: Provides insights into your AWS environment, including ways to reduce cost, increase performance, and improve security.
- AWS Savings Plans: Offers significant savings over on-demand pricing, in exchange for a commitment to a consistent amount of usage (measured in $/hour) for a 1 or 3 year period.
- AWS Reserved Instances: Provides a significant discount compared to on-demand pricing in exchange for committing to a specific instance type in a region for a term of one or three years.
- AWS Migration Hub: Provides a central location to track the progress of application migrations across multiple AWS and partner solutions. It offers a comprehensive view of your migration status and helps in planning and tracking.
- AWS Application Discovery Service: Helps enterprise customers plan migration projects by gathering information about their on-premises data centers.
- AWS Database Migration Service (DMS): Allows easy migration of relational databases, data warehouses, NoSQL databases, and other types of data stores to AWS.

- AWS Server Migration Service (SMS): An agentless service for migrating thousands of on-premises workloads to AWS.
- AWS Snow Family: For large-scale data migrations, including Snowball and Snowmobile, these tools facilitate moving huge volumes of data into AWS, bypassing the internet.
- AWS DataSync: Used for online data transfer, this helps in moving large amounts of data quickly and securely between on-premises and AWS storage services.
- AWS Cloud Adoption Framework (CAF): Offers guidance and best practices to help organizations understand how to develop and implement efficient and effective plans for their cloud adoption journey.
- AWS Well-Architected Tool: Helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications.

Important Services To Review:

1. EC2 - Virtual servers
2. S3 - Object storage
3. IAM - Access control
4. RDS - Managed databases
5. Lambda - Serverless computing
6. VPC - Virtual network
7. Route 53 - DNS service
8. SNS - Notification service
9. SQS - Message queue service
10. Elastic Beanstalk - Application deployment

Pricing Models:

1. On-Demand: Pay for compute capacity by the hour or by the second.
2. Reserved: Reserved capacity for 1 or 3 years, offering significant cost savings.
3. Spot: Bid for unused EC2 capacity at potentially lower costs.
4. Savings Plans: Commit to a consistent amount of usage for a 1 or 3 year term.

Security Best Practices:

1. Use IAM roles for granting permissions.
2. Enable MFA (Multi-Factor Authentication) for account security.
3. Regularly rotate access keys and passwords.
4. Use security groups and network ACLs for network access control.
5. Encrypt sensitive data in transit and at rest.
6. Regularly backup data and test your disaster recovery plan.

AWS Shared Responsibility Mode

The AWS Shared Responsibility Model is a guideline that defines the responsibilities of AWS and its customers in maintaining the security and compliance of the cloud environment. Here's a brief outline:

1. AWS Responsibilities:

- Infrastructure Security: AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This includes hardware, software, networking, and facilities.
- Managed Services Security: For managed services like Amazon RDS, DynamoDB, etc., AWS handles basic security tasks like patching database or operating system software.
- Compliance Validation: AWS ensures compliance with various certifications and regulations for their data centers and services.

2. Customer Responsibilities:

- Data Security: Customers are responsible for protecting their data, which includes encryption, access control, and secure transmission.
- Identity and Access Management: Customers must manage and secure account credentials and set permissions to control access to AWS resources.
- Operating System and Network Configuration: For IaaS offerings like Amazon EC2, customers are responsible for managing the guest OS (including updates and security patches), firewall configuration, and network routing rules.

- Client-Side Data Encryption and Data Integrity Authentication: Customers are responsible for encrypting data in transit and ensuring appropriate measures for data integrity.

- Application Security: Customers should ensure their applications are secure against threats by implementing measures like regular security testing and application-layer firewalls.

3. Shared Controls:

- These are the controls that apply to both the infrastructure layer and customer layers. They include patch management, configuration management, and awareness & training.

In summary, AWS manages the security of the cloud (infrastructure and managed services), while customers are responsible for security in the cloud (data, applications, and operating systems). This model allows customers to tailor their cloud environments according to their specific security needs.

AWS Well-Architected and the Six Pillars

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

Operational Excellence Pillar: The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

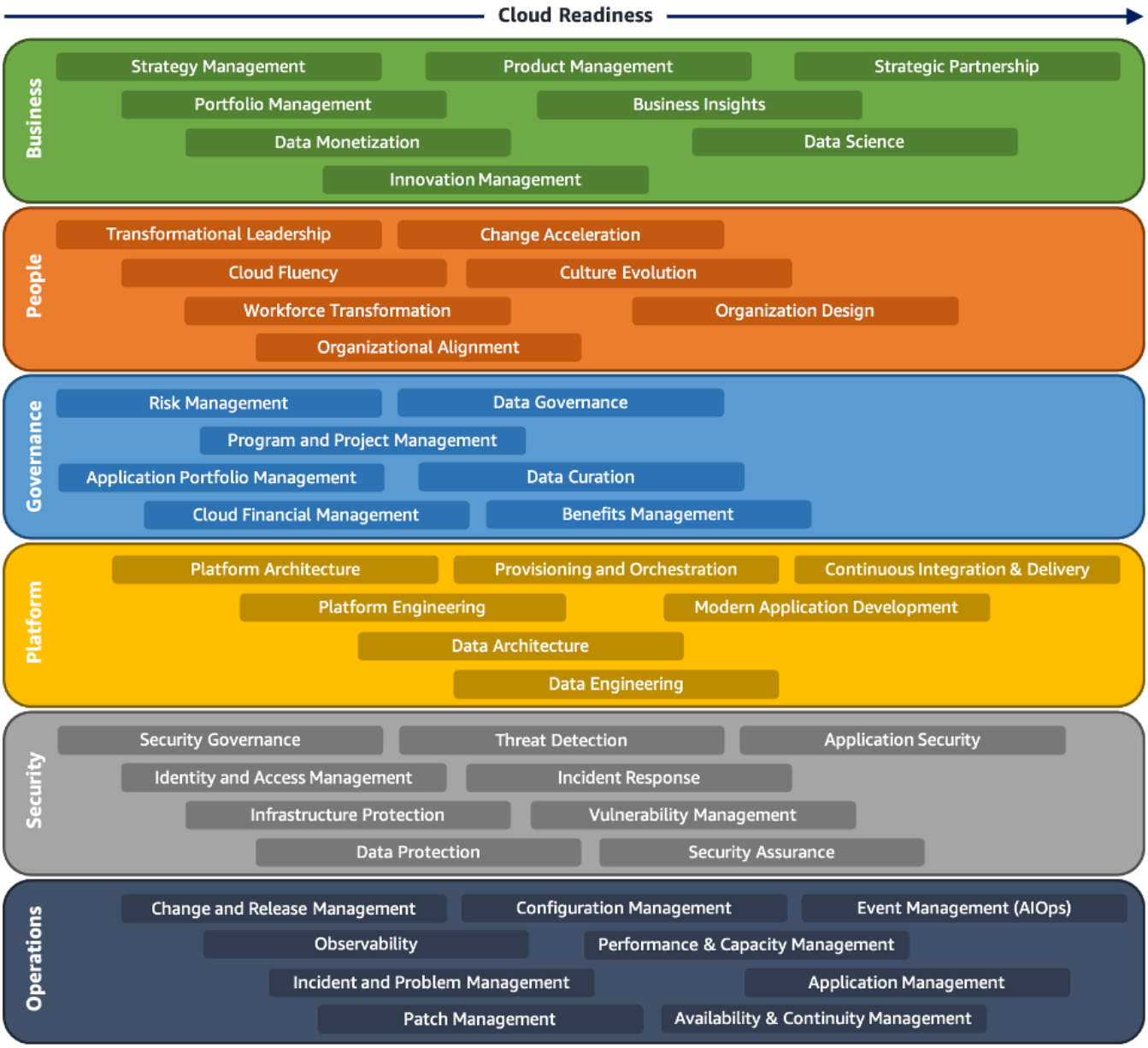
Security Pillar: The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

Reliability Pillar: The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.

Performance Efficiency Pillar: The performance efficiency pillar focuses on the structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

Cost Optimization Pillar: The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.

Sustainability Pillar: The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.



Cloud Adoption Framework

The AWS Cloud Adoption Framework (AWS CAF) is a guideline and framework provided by Amazon Web Services (AWS) to help organizations develop and execute an effective cloud adoption strategy. It is structured to help businesses understand the aspects of cloud adoption, organize their cloud journey, and utilize AWS services efficiently. The framework is divided into several key areas, typically including:

Business Perspective: This focuses on ensuring that IT aligns with business objectives and adds value. It involves identifying stakeholders, defining business outcomes, and establishing governance models. Business perspective helps ensure that your cloud investments accelerate your digital transformation ambitions and business outcomes. Common stakeholders include chief executive officer (CEO), chief financial officer (CFO), chief operations officer (COO), chief information officer (CIO), and chief technology officer (CTO).

People Perspective: Addresses the human element, including skills and organizational changes necessary for cloud adoption. It involves training, staffing, and new roles creation. People perspective serves as a bridge between technology and business, accelerating the cloud journey to help organizations more rapidly evolve to a culture of continuous growth, learning, and where change becomes business-as-normal, with focus on culture, organizational structure, leadership, and workforce. Common stakeholders include CIO, COO, CTO, cloud director, and cross-functional and enterprise-wide leaders.

Governance Perspective: Involves managing and measuring cloud investments to align with business outcomes. It includes risk management, resource allocation, and compliance controls. Governance perspective helps you orchestrate your cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks. Common stakeholders include chief transformation officer, CIO, CTO, CFO, chief data officer (CDO), and chief risk officer (CRO).

Platform Perspective: This is about the technical aspects of the cloud environment, including the architecture, operations, and optimization of cloud resources. Platform perspective helps you build an enterprise-grade, scalable, hybrid cloud platform, modernize existing workloads, and implement new cloud-native solutions. Common stakeholders include CTO, technology leaders, architects, and engineers.

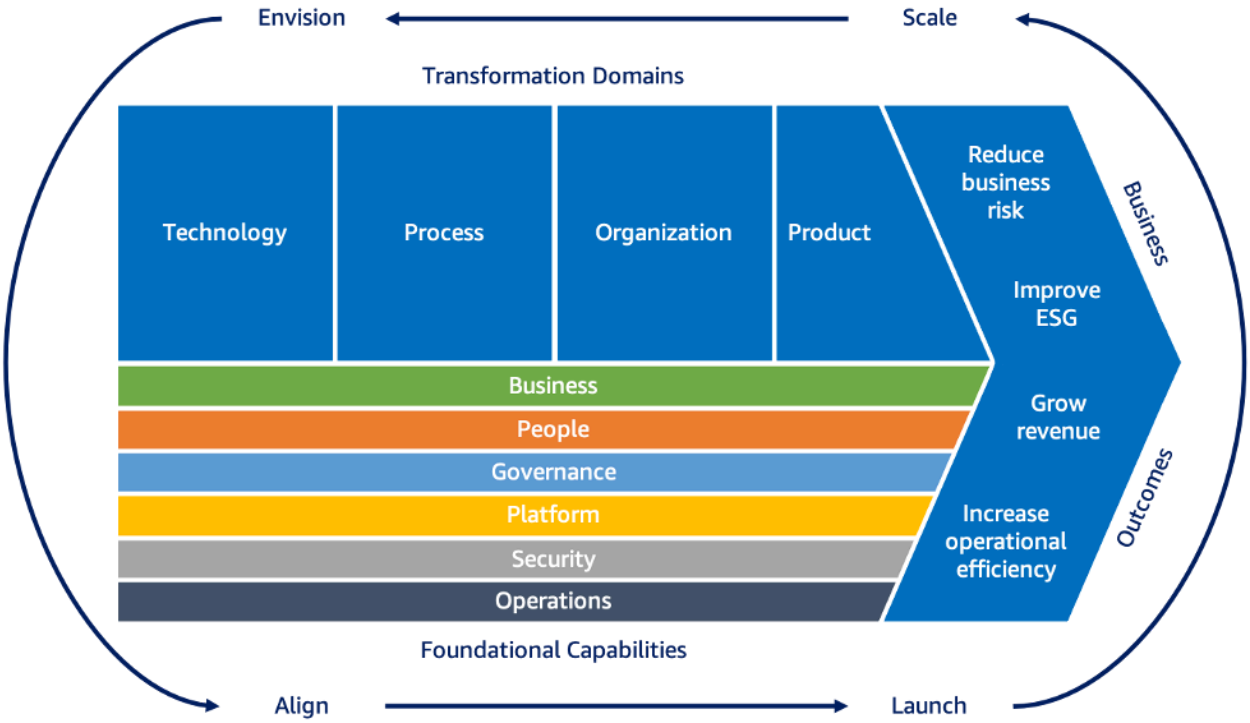
Security Perspective: Focuses on the protection of information, systems, and assets while delivering business value through risk assessments and mitigation strategies. Security perspective helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads. Common stakeholders include chief information security officer (CISO), chief compliance officer (CCO), internal audit leaders, and security architects and engineers.

Operations Perspective: Ensures operational excellence in the cloud. It includes processes like monitoring, incident response, and continuous improvement. Operations perspective helps ensure that your cloud services are delivered at a level that meets the needs of your business. Common stakeholders include infrastructure and operations leaders, site reliability engineers, and information technology service managers.

The AWS CAF helps organizations in their transition to the cloud by providing a structured approach, identifying gaps in skills and processes, and guiding the development of an effective cloud strategy. It’s particularly useful for large-scale cloud adoption, as it covers a broad range of areas that need to be considered for a successful transition.

The AWS Cloud Adoption Framework (AWS CAF) leverages AWS experience and best practices to help you digitally transform and accelerate your business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations.

These capabilities provide best-practice guidance that helps you improve your cloud readiness. AWS CAF groups its capabilities in six perspectives: Business, People, Governance, Platform, Security, and Operations. Each perspective comprises a set of capabilities that functionally related stakeholders own or manage in the cloud transformation journey.



From there it identifies four transformation domains (Technology, Process, Organization, and Product) that must participate in a successful digital transformation.

- Envision phase focuses on demonstrating how cloud will help accelerate your business outcomes. It does so by identifying and prioritizing transformation opportunities across each of the four transformation domains in line with your strategic business objectives. Associating your transformation initiatives with key stakeholders (senior individuals capable of influencing and driving change) and measurable business outcomes will help you demonstrate value as you progress through your transformation journey.
- Align phase focuses on identifying capability gaps across the six AWS CAF perspectives, identifying cross-organizational dependencies, and surfacing stakeholder concerns and challenges. Doing so will help you create strategies for improving your cloud readiness, ensure stakeholder alignment, and facilitate relevant organizational change management activities.

- Launch phase focuses on delivering pilot initiatives in production and on demonstrating incremental business value. Pilots should be highly impactful and if/when successful they will help influence future direction. Learning from pilots will help you adjust your approach before scaling to full production.
- Scale phase focuses on expanding production pilots and business value to desired scale and ensuring that the business benefits associated with your cloud investments are realized and sustained.