



Certified Cloud Security Engineer v1

COURSEWARE

Certified Cloud Security Engineer

Version 1

EC-Council

Copyright © 2021 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at legal@eccouncil.org. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at legal@eccouncil.org. If you have any issues, please contact us at support@eccouncil.org.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Foreword

Organizations are migrating to the cloud to provide 24 × 7 access to company records, files, and data to their employees. Cloud provides an organization with various benefits, including productivity and cost effectiveness. With the majority of organizations migrating to cloud services, the security risks associated with it are also increasing. In addition to traditional security challenges, cloud encounters its own security challenges. Thus, ensuring cloud security has become a major concern for organizations. Moreover, owing to the lack of skills in the field of cybersecurity, organizations strive to find people with specific skills related to cloud security. Therefore, there is a huge demand for professionals who are certified in the best practices of cloud security. Cloud security professionals with proper skill sets and responsibilities can mitigate the security issues related to the cloud infrastructure to a great extent.

Cloud adopts various approaches with respect to security. The traditional security measures do not change with the adoption of cloud, but the focus does. The implementation of cloud does not change the security protocols required in traditional networks (on-premises); instead, it changes the security focus of cloud consumers. The shared responsibility model provided by a cloud service provider plays a vital role in planning, configuring, implementing, and maintaining cloud security. It is important to understand and analyze the shared responsibility model along with the utilization of various services and tools provided by the service provider to ensure security in the cloud infrastructure and data.

This course includes both vendor neutral and vendor specific cloud security concepts. Vendor neutral concepts include universally applicable general cloud security best practices, technology, frameworks, and principles that help individuals to strengthen their fundamentals. Vendor specific concepts help individuals to gain the practical skills required when they actually start working with a specific cloud platform. Thus, this course helps individuals in strengthening their fundamental cloud security knowledge and gain practical knowledge of security practices, tools, and techniques used to configure widely used public cloud providers such as AWS, AZURE, and GCP. It helps professionals to develop and enhance their knowledge and skills in planning, configuring, implementing, and maintaining a secure cloud environment for their organizations, and validates their knowledge, skills, and abilities in protecting, detecting, and responding to threats in the cloud network infrastructure.

The course covers all major domains in such a manner that the reader will be able to appreciate the way network security mechanisms have evolved over time; as well as gain insight into the fundamental workings relevant to each domain. It is a blend of academic and practical wisdom, supplemented with tools that the reader can readily access and obtain a hands-on experience.

Finally, this is not the end. This courseware is to be considered as a 'work-in-progress', as it is updated by adding value to it over time. You may find some aspects detailed, while others may be in brief. The yardstick that is used in this respect is simple- "does the content explain the point at hand?" It would be great to hear the views of the reader with respect to viewpoints and suggestions. You can send your feedback so that this courseware can be a more useful one.

Please visit <https://www.eccouncil.org> for more information.

Notice: Third-Party Connected Apps and Paid Services

Introduction

The guiding principle of EC-Council Education Content and Labs is simple, we want to provide a safe environment to learn, practice, and assess Cyber Security Skills that directly translate to Job-ready skills. We believe in providing our students, educator partners, and professionals with real software and live experiences that behave like those in the "real world" because they are the actual tools and services used in the field, not simulations.

Third-Party and Internet Connected Resources

To provide the most realistic learning experience, EC-Council may employ connections to live networks and services through its labs and lab platforms. While many software and service providers provide education use licenses, trials, or are Open Source, some require a live account with setup requirements and agreements you must review and consent to in order to participate in and/or complete the exercises in our Labs.

Subscription Fees and/or License Fees

EC-Council will never ask you for payment details or sensitive information during our course of learning, however, some of our Live Labs connect to third-party services such as Amazon AWS, Google Cloud Platform, Microsoft Azure, etc. While many of these service providers allow you to sign up for free-tier usage, Education Accounts, or provide promotional credits for trials, many do ask for your credit card during sign-up and may bill for the use of their services, during and even after you have completed your course of study with EC-Council. Be aware, signing up for third-party services may incur expenses related to the use of their services. Our labs can be completed without any additional charges unless explicitly marked, but you are ultimately responsible for any services you may intentionally or unintentionally sign up for when connected to those platforms.

CCSE, AWS, Azure, and GCP

CCSE provides labs that utilize three major cloud platforms, AWS, Azure, and GCP. In order to provide a thorough hands-on experience, you must create accounts with each cloud platform. While account creation typically requires a credit card, you do have options to bypass this; ask your school or training center if they are an education partner with these cloud players and complete your sign up with an education account, or you can apply directly for a student account with each platform. If you choose to set up a live account with a credit card, be sure to check with each platform how to identify what services are being created that may incur charges. We do provide guides in our programs to check that all services created have been removed, and we do notify you if a lab activity may incur charges if done incorrectly or not terminated, but be aware, you are connecting to live third party services that charge for the use of their platforms if you exceed free tier usage guidelines.

Alternatives

If you are unable to secure an Education/Student account and are not comfortable creating a live account in these platforms, EC-Council provides comprehensive Lab Guides that include complete instruction sets with screenshots (images) of each step. EC-Council also provides video-based walk-through of each lab for you to follow along without actually creating an account. Though you won't be creating an account or performing the live configurations with this method, you will still receive adequate exposure to the platforms, configuration steps, techniques, and knowledge elements required for you to prepare for certification or grasp the knowledge conveyed in the program.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User



The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Cyber Security: Certified Cybersecurity Technician



The Certified Cybersecurity Technician (CCT) program covers the fundamental concepts of cybersecurity. It equips students with the skills required to identify the increasing network security threats that reflect on the organization's security posture and implement general security controls to protect the underlying IT infrastructure from unauthorized access, alteration, destruction, or disclosure.

This program gives a holistic overview of the key components of cybersecurity. The course is designed for those interested in learning the various fundamentals of cybersecurity and aspire to pursue a career in cybersecurity.

Network Defense: Certified Network Defender



Students enrolled in the Certified Network Defender course, will gain a detailed understanding and hands on ability to function in real life situations involving network defense. They will gain the technical depth required to actively design a secure network in your organization. This course gives you the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that you understand how networks operate, understand what software is automating and how to analyze the subject material.

You will learn how to protect, detect, respond and predict the network attacks. You will learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration. You will then learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans. These skills will help you foster resiliency and continuity of operations during attacks.

Ethical Hacking: Certified Ethical Hacker



The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment, This course was designed to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, “To beat a hacker, you need to think like a hacker”.

This program will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver’s seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the Five Phases of Ethical Hacking and thought how you can approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Penetration Testing: Certified Penetration Testing Professional



CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council's CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council's credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

Computer Forensics: Computer Hacking Forensic Investigator



Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Incident Handling: EC-Council Certified Incident Handler



EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program

that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer



The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer



The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities

involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst



Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst



The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

CCSE Exam Information

CCSE Exam Details	
Exam Title	Certified Cloud Security Engineer (CCSE)
Exam Code	312-40
Availability	EC-Council Exam Portal (please visit https://www.eccexam.com) VUE (please visit https://home.pearsonvue.com/eccouncil)
Duration	4 Hours
Questions	125
Passing Score	Please refer https://cert.eccouncil.org/faq.html

Please visit <https://cert.eccouncil.org> for more information.

hide01.ir

Table of Contents

Module 01: Introduction to Cloud Security	1
Cloud computing fundamentals	4
Cloud security objectives	19
Cloud security insights	25
CSPs Evaluation for security before consuming a cloud service	39
Shared responsibility model in Amazon Cloud (AWS)	44
Shared responsibility model in Microsoft Azure Cloud	54
Shared responsibility model in Google Cloud Platform (GCP)	59
Module 02: Platform and Infrastructure Security in Cloud	65
Cloud platform and infrastructure	68
Risks and threats associated with cloud platform and infrastructure	89
Secure key components of cloud platform and infrastructure	98
Secure data center design in the cloud	140
Cloud platform and infrastructure security in AWS	152
Cloud platform and infrastructure security in GCP	208
Cloud platform and infrastructure security in Microsoft Azure	247
Module 03: Application Security in Cloud	317
Cloud application security	320
Cloud application security risks	333
Secure Software Development Lifecycle (SSDLC) of Cloud Applications	339
DevOps and continuous integration/continuous deployment (CI/CD)	356
Cloud application security controls	371
Application security in AWS	417
Application security in Azure	500
Application security in GCP	568

Module 04: Data Security in Cloud	671
Cloud data security	675
Cloud data storage fundamentals	683
Cloud storage architecture and life cycle phases	728
Evaluation of the risks, attacks, and issues in cloud data storage	739
Cloud data security strategies and technologies	746
Data security in AWS	816
Data security in GCP	920
Data security in Microsoft Azure	959
Module 05: Security Operations in Cloud	1099
Cloud security operations	1103
Elements in cloud data center physical/logical Operations	1110
Physical and logical infrastructures for cloud Environments	1121
Managing Cloud Security Operations	1134
Security operations in Microsoft Azure	1296
Security operations in AWS	1392
Security operations in GCP	1447
Module 06: Penetration Testing in Cloud	1475
Cloud penetration testing	1478
Generic cloud penetration testing steps	1483
AWS-specific penetration testing steps	1510
Azure-specific penetration testing steps	1532
GCP-specific penetration testing steps	1553

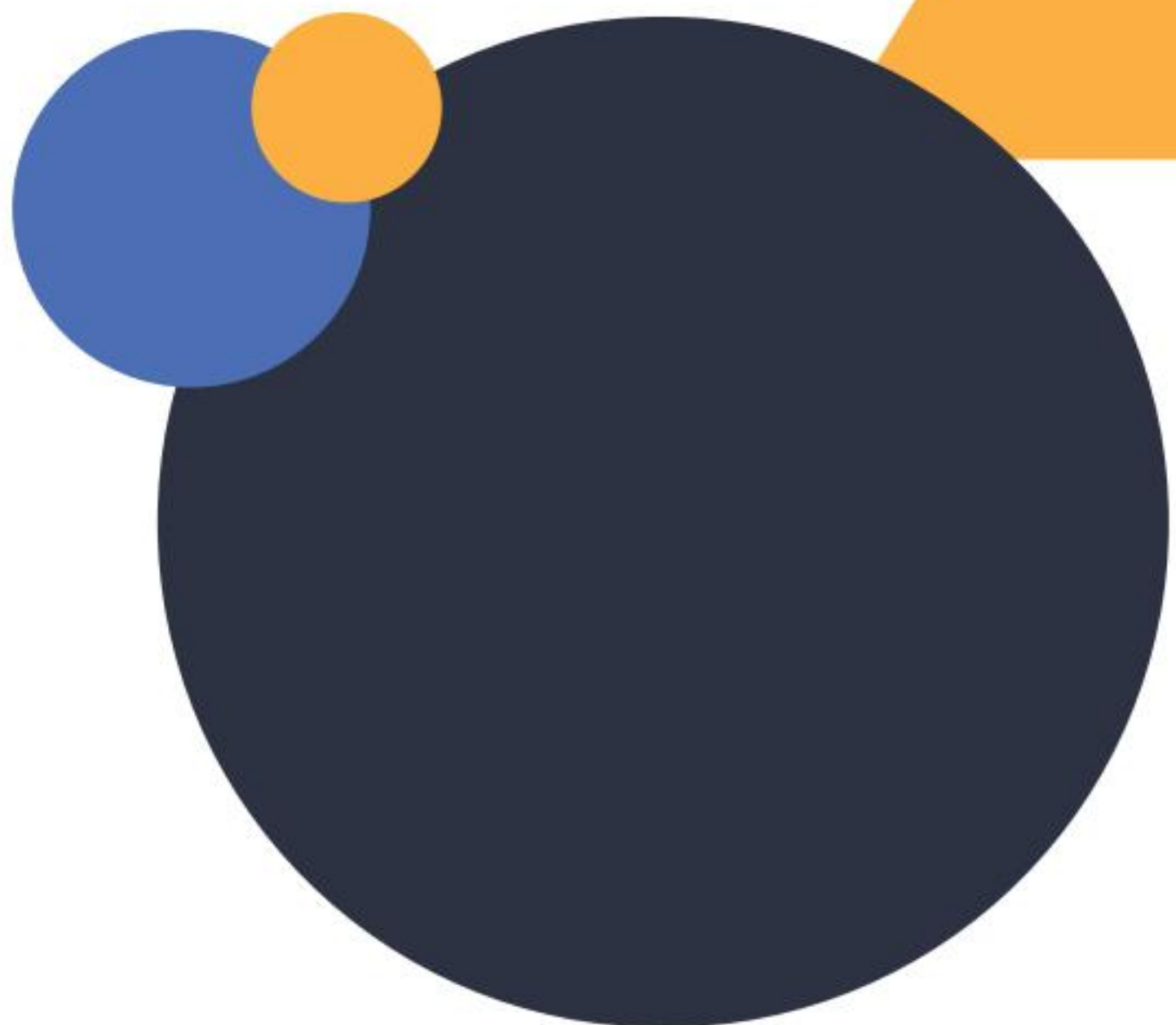
Module 07: Incident Response in Cloud	1561
Cloud incident response	1564
Cloud incident response lifecycle	1570
Security incident response in AWS	1624
Security incident response in Microsoft Azure	1666
Security incident response in GCP	1718
Module 08: Forensic Investigation in Cloud	1799
Cloud forensics	1802
Security incidents investigation in AWS	1821
Security incidents investigation in Microsoft Azure	1846
Security incidents investigate in Google GCP	1871
Module 09: Business Continuity and Disaster Recovery in Cloud	1893
Cloud disaster recovery and business continuity	1897
Disaster recovery and business continuity design	1961
Recovery and resilience implementation in AWS	1999
Business continuity and disaster recovery in Microsoft Azure	2049
Disaster recovery configurations in Azure	2091
BC/DR in Azure	2097
BC/DR in GCP	2181
Module 10: Governance, Risk Management, and Compliance in Cloud	2253
Cloud governance	2256
Cloud risk management	2327
Cloud compliance	2373
GRC in AWS	2431
GRC in Azure	2459
GRC in GCP	2504

Module: 11 Standards, Policies, and Legal Issues in Cloud	2527
Laws impacting cloud computing	2530
Cloud computing standards	2546
Cloud audit planning and reporting	2626
Standards, policies, and auditing in Azure	2665
Standards, policies, and auditing in AWS	2676
Standards, policies, and auditing in GCP	2697
Glossary	2709
References	2723

hide01.ir

EC-Council

C|CSETM
Certified Cloud Security Engineer



Introduction to Cloud Security

Module 01

This page is intentionally left blank.

LEARNING OBJECTIVES

The learning objectives of this module are:

- LO#01: Understand the cloud computing fundamentals
- LO#02: Understand cloud security objectives and issues
- LO#03: Understand cloud security insights
- LO#04: Evaluate CSPs for security before consuming a cloud service
- LO#05: Discuss security in Amazon Cloud (AWS)
- LO#06: Discuss security in Microsoft Azure Cloud
- LO#07: Discuss security in Google Cloud Platform (GCP)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Learning Objectives

This module explains the various aspects of enterprise cloud security that is important for an organization to securely store or process data on cloud. This module includes various elements of cloud security, such as user identity and access management (IAM), encryption and key management, application-level security, data storage security, monitoring, logging, and compliance to secure sensitive data on cloud. The learning objectives of this module are:

- Cloud computing fundamentals
- Cloud security objectives and issues
- Cloud security insights
- Evaluate the Cloud Service Providers (CSPs) for security before consuming a cloud service
- Security in Amazon cloud (AWS)
- Security in Microsoft Azure cloud
- Security in the Google Cloud Platform (GCP)




LO#01: Understand the Cloud Computing Fundamentals

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#01: Cloud Computing Fundamentals

This section introduces cloud computing along with its various elements such as types of cloud computing services, separation of responsibilities, cloud deployment models, and the NIST reference architecture.

Cloud Computing



Cloud computing is an on-demand delivery of **IT capabilities** where the IT infrastructure and applications are provided to **subscribers** as a metered service over a network

Characteristics of Cloud Computing

On-demand self service	Broad network access
Distributed storage	Resource pooling
Rapid elasticity	Measured service
Automated management	Virtualization technology

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing

Cloud computing is an on-demand delivery of IT capabilities in which an IT infrastructure and applications are provided to subscribers as metered services over a network. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce.

Characteristics of Cloud Computing

The characteristics of cloud computing that attract many businesses to adopt the cloud technology are discussed below.

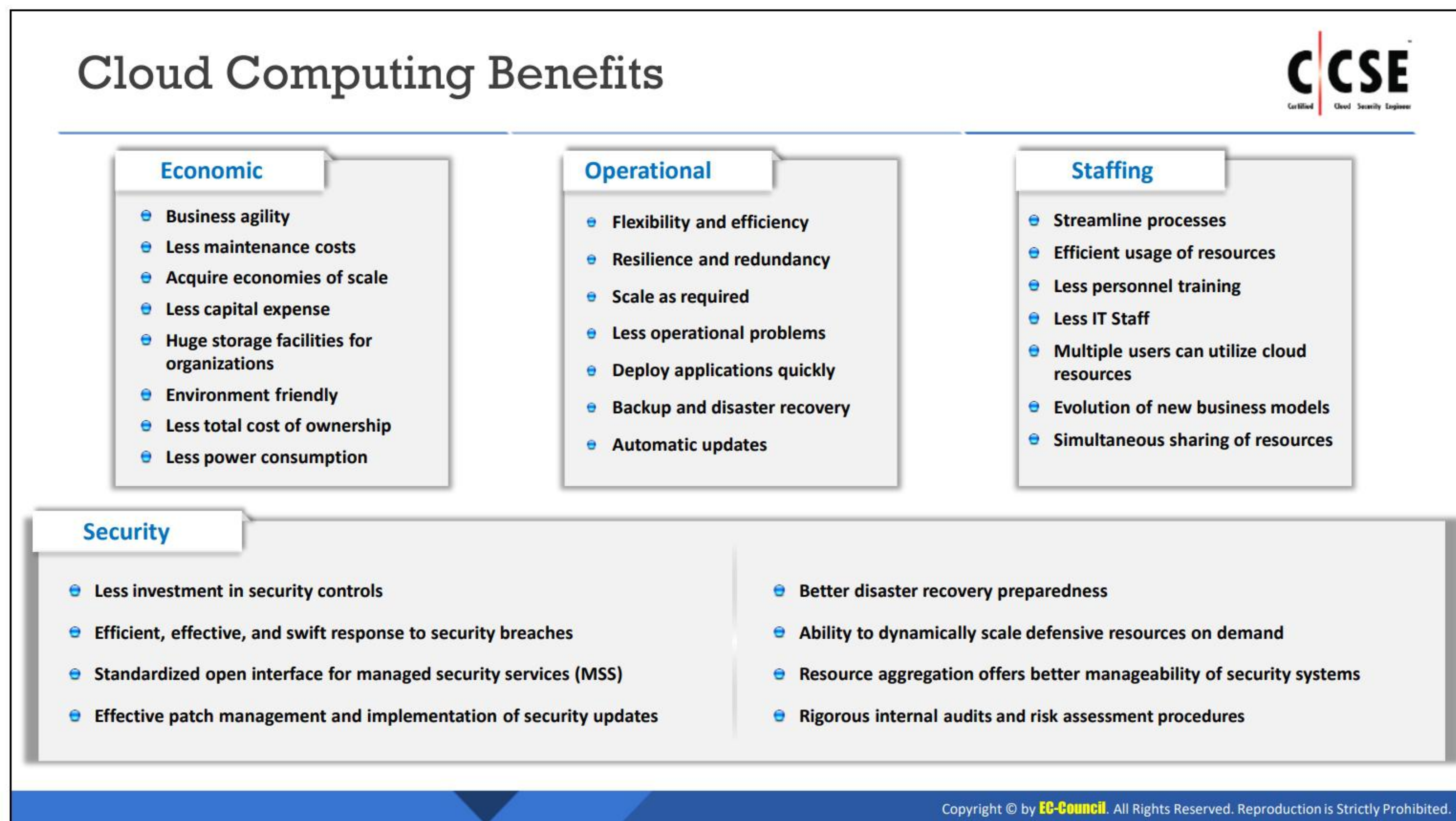
- **On-demand self-service:** A type of service rendered by cloud service providers that provides on-demand cloud resources such as computing power, storage, and network, without the need for human interaction with service providers.
- **Distributed storage:** Distributed storage in cloud offers better scalability, availability, and reliability of data. However, it can potentially involve security and compliance concerns.
- **Rapid elasticity:** The cloud offers instant provisioning of capabilities to rapidly scale up or down according to demand. The resources available for provisioning to the consumers seem to be unlimited that can be purchased invariably in the desired quantity.
- **Automated management:** By minimizing user involvement, cloud automation speeds up the processes, reduces labor costs, and reduces the possibility of human error.
- **Broad network access:** Cloud resources are available over the network and can be accessed through standard procedures via a wide variety of platforms, including laptops, mobile phones, and PDAs.

- **Resource pooling:** The cloud service provider pools all the resources together to serve multiple customers in a multi-tenant environment, wherein the physical and virtual resources are dynamically assigned and reassigned on demand by the consumers.
- **Measured service:** Cloud systems employ the “pay-per-use” metering method. Subscribers pay for the cloud services via monthly subscriptions or according to the usage of resources such as the storage levels, processing power, and bandwidth. Cloud service providers monitor, control, report, and charge the customers according to the resources consumed with complete transparency.
- **Virtualization technology:** It enables the rapid scaling of resources in such a way that could not be achieved by non-virtualized environments.

Limitations of Cloud Computing

- Organizations have limited control and flexibility
- Prone to outage and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Dependence on network connections

hide01.ir



Cloud Computing Benefits

Cloud computing offers economic, operational, staffing, and security benefits.

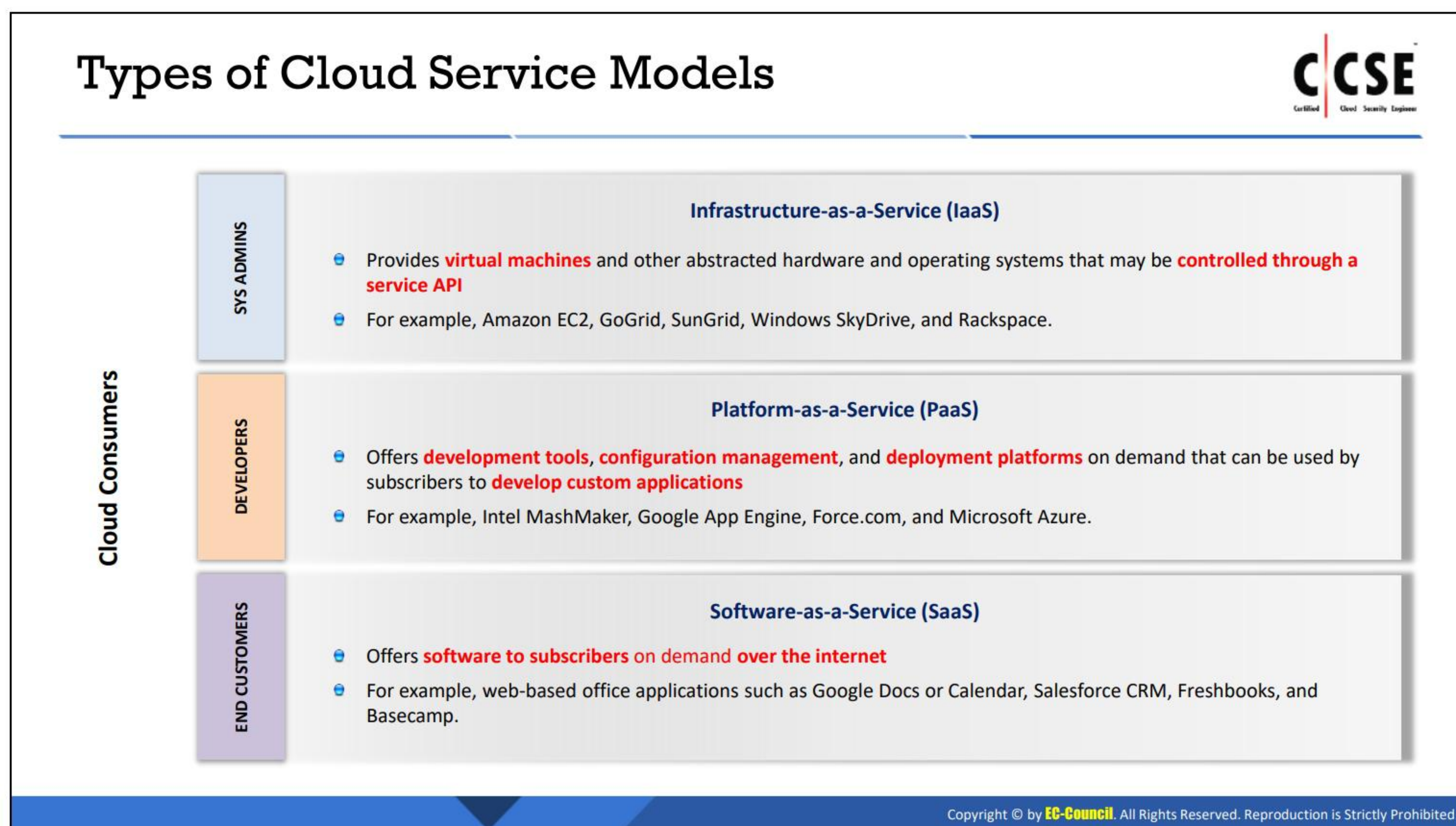
■ Economic

- Business agility
- Less maintenance costs
- Acquire economies of scale
- Less capital expenditure
- Huge storage facilities for organizations
- Environment friendly
- Less total cost of ownership
- Less power consumption

■ Operational

- Flexibility and efficiency
- Resilience and redundancy
- Scale as required
- Less operational problems
- Deploy applications quickly
- Backup and disaster recovery

- Automatic updates
- **Staffing**
 - Streamline processes
 - Efficient usage of resources
 - Less personnel training
 - Less IT Staff
 - Multiple users can utilize cloud resources
 - Evolution of new business models
 - Simultaneous sharing of resources
- **Security**
 - Less investment in security controls
 - Efficient, effective, and swift response to security breaches
 - Standardized open interface for managed security services (MSS)
 - Effective patch management and implementation of security updates
 - Better disaster recovery preparedness
 - Ability to dynamically scale defensive resources on demand
 - Resource aggregation offers better management of security systems
 - Rigorous internal audits and risk assessment procedures



Types of Cloud Service Models

Cloud services can be broadly divided into three categories.

■ Infrastructure-as-a-Service (IaaS)

This cloud computing service enables subscribers to use on demand fundamental IT resources such as the computing power, virtualization, data storage, and network. This service provides virtual machines and other abstracted hardware and operating systems (OSes) that may be controlled through a service API. Because cloud service providers are responsible for managing the underlying cloud-computing infrastructure, subscribers can avoid the human capital and hardware costs, among others (for example, Amazon Elastic Compute Cloud (EC2), GoGrid, SunGrid, Windows SkyDrive, and Rackspace).

Advantages:

- Dynamic infrastructure scaling
- Guaranteed uptime
- Automation of administrative tasks
- Elastic load balancing (ELB)
- Policy-based services
- Global accessibility

Disadvantages:

- Software security is at high risk (third-party providers are more prone to attacks)
- Performance issues and slow connection speeds

■ Platform-as-a-Service (PaaS)

This type of cloud computing service offers a platform for the development of applications and services. Subscribers need not buy and manage the software and infrastructure underneath, but have authority over the deployed applications and probably the application hosting environment configurations. This service offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications (such as Intel Mash Maker, Google App Engine, Force.com, and Microsoft Azure). The advantages of writing applications in the PaaS environment include dynamic scalability, automated backups, and other platform services without requiring explicit codes.

Advantages:

- Simplified deployment
- Prebuilt business functionality
- Lower risk
- Instant community
- Pay-per-use model
- Scalability

Disadvantages:

- Vendor lock-in
- Data privacy
- Integration with other system applications

■ **Software-as-a-Service (SaaS)**

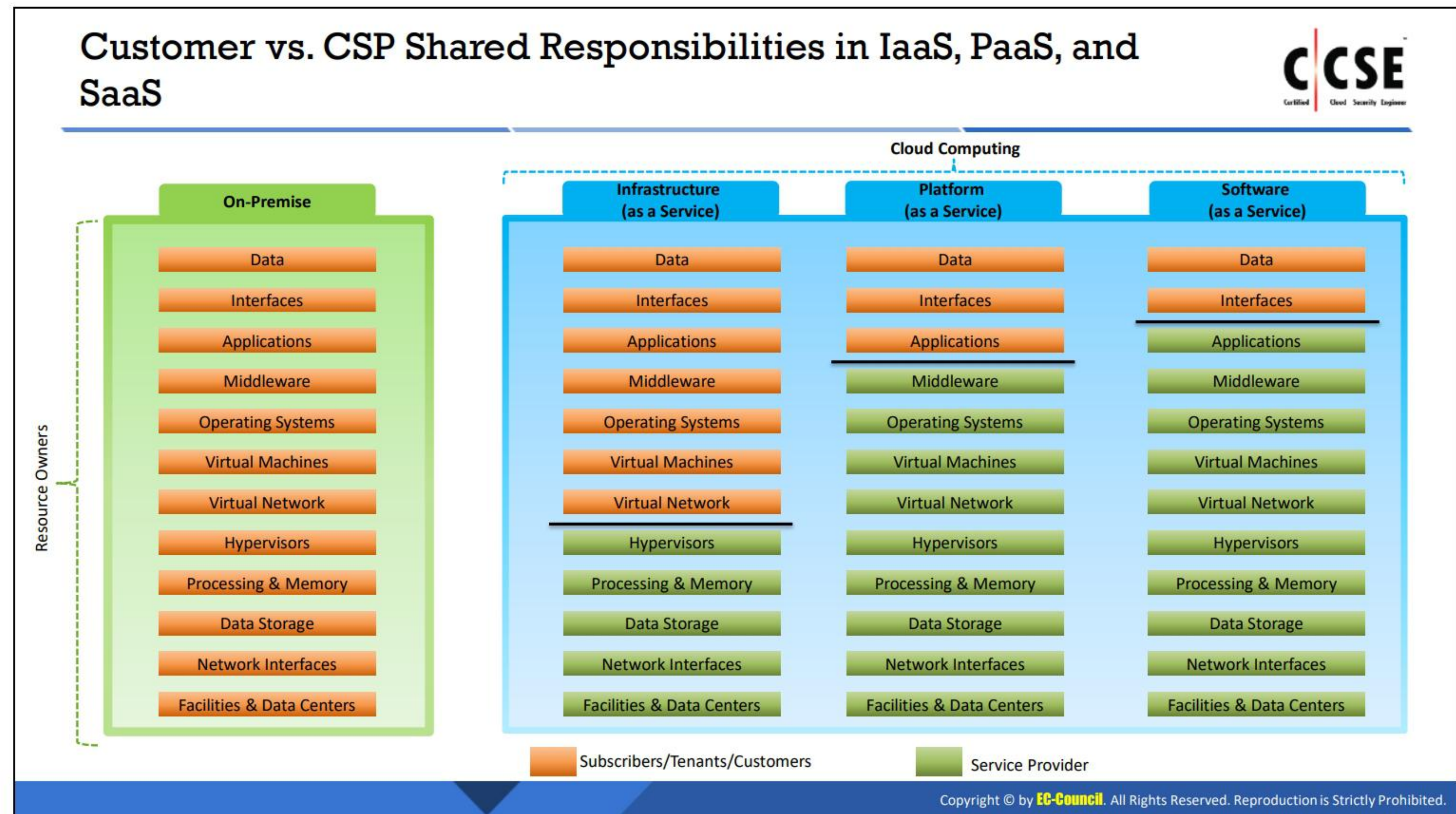
This cloud computing service offers application software to subscribers on demand over the internet. The providers charge for this service on a pay-per-use basis via subscription, advertising, or sharing among multiple users (for example, web-based office applications such as Google Docs or Calendar, Salesforce CRM, FreshBooks, and Basecamp).

Advantages:

- Low cost
- Easy administration
- Global accessibility
- Compatible (no specialized hardware or software is required)

Disadvantages:

- Security and latency issues
- Total dependency on the internet
- Switching between SaaS vendors is difficult




Customer vs. CSP Shared Responsibilities in IaaS, PaaS, and SaaS

In cloud computing, it is important to ensure the separation of responsibilities of the subscribers and service providers. The separation of duties prevents conflicts of interest, illegal acts, fraud, abuse, and errors, and it helps in identifying security control failures, including information theft, security breaches, and invasion of security controls. It also helps in restricting the amount of influence held by an individual and ensures that there are no conflicting responsibilities.

It is essential to know the limitations of each cloud service delivery model when accessing specific clouds and their models.

Cloud Deployment Models



Cloud deployment model selection is based on the **enterprise requirements**

Types of Cloud Deployment Models

- Public Cloud:** Services are rendered over a public network
- Private Cloud:** Cloud infrastructure operated exclusively for a single organization
- Community Cloud:** Shared infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.)
- Hybrid Cloud:** Composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Deployment Models

Cloud deployment model selection is based on the enterprise requirements. The cloud services can be deployed in different ways according to the following factors:

- Where cloud computing services are hosted
- Security requirements
- Sharing cloud services
- Ability to manage some or all cloud services
- Customization capabilities

The four standard cloud deployment models are:

- **Public Cloud**

In this model, the provider offers services such as applications, servers, and data storage to the public over the internet. In this model, the cloud provider is liable for the creation and constant maintenance of the public cloud and its IT resources. Public cloud services may be free or based on a pay-per-usage model (e.g., Amazon EC2, IBM's Blue Cloud, Google App Engine, Windows Azure Services Platform).

- **Advantages:**

- Simplicity and efficiency
 - Low cost
 - Reduced time (when a server crashes, the cloud must be restarted or reconfigured)

- No maintenance (public cloud service is hosted off-site)
- No contracts (no long-term commitments)
- **Disadvantages:**
 - Security is not guaranteed
 - Lack of control (third-party providers are in charge)
 - Slow speed (relies on internet connections, data transfer rate is limited)
- **Private Cloud**

A private cloud, also known as an internal or corporate cloud, is a cloud infrastructure that is exclusively operated by an organization. An organization can implement a private cloud within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data.

 - **Advantages:**
 - Enhance security (services are dedicated to a single organization)
 - More control over resources (organization is in charge)
 - Greater performance (deployed within the firewall; therefore, the data transfer rates are high)
 - Customizable hardware, network, and storage performances (because organizations own private clouds)
 - Sarbanes Oxley, PCI DSS, and HIPAA compliance data are significantly easier to acquire
 - **Disadvantages:**
 - Expensive
 - On-site maintenance
- **Community Cloud**

It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns such as security, regulatory compliance, performance requirements, and jurisdiction. A community cloud can be either on-premise or off-premise; it is either governed by the participated organizations or a third-party managed service provider.

 - **Advantages:**
 - Less expensive compared to private cloud
 - Flexibility to meet the community needs
 - Compliance with legal regulations
 - High scalability

- Organizations can share a pool of resources from anywhere via the internet
- **Disadvantages:**
 - Competition between consumers in usage of resources
 - No accurate prediction of required resources
 - Who is the legal entity in case of liability?
 - Moderate security (other tenants may be able to access data)
 - Trust and security concerns between tenants
- **Hybrid Cloud**

It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities, but bound together to offer the benefits of multiple deployment models. In this model, the organization provides and manages some resources in-house, while other resources are offered externally.

Example: An organization performs its critical activities on a private cloud (such as operational customer data) and non-critical activities on a public cloud.

 - **Advantages:**
 - More scalable (contains both public and private clouds)
 - Offers secure and scalable public resources
 - High level of security (comprises private cloud)
 - Allows to reduce and manage the cost according to the requirement
 - **Disadvantages:**
 - Communication at the network level may be conflicted as it uses both public and private clouds
 - Challenging data compliance
 - Organization has to rely on the internal IT infrastructure for support to handle any outage (maintain redundancy across data centers to overcome)
 - Complex service-level agreements (SLAs)



The combination of service and deployment models categorize the delivery of cloud services.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

hide01.ir

NIST Cloud Deployment Reference Architecture



The NIST cloud computing reference architecture defines **five** major actors:

Cloud Consumer

A person or organization that uses **cloud computing services**

Cloud Provider

A person or organization providing services to interested parties

Cloud Carrier

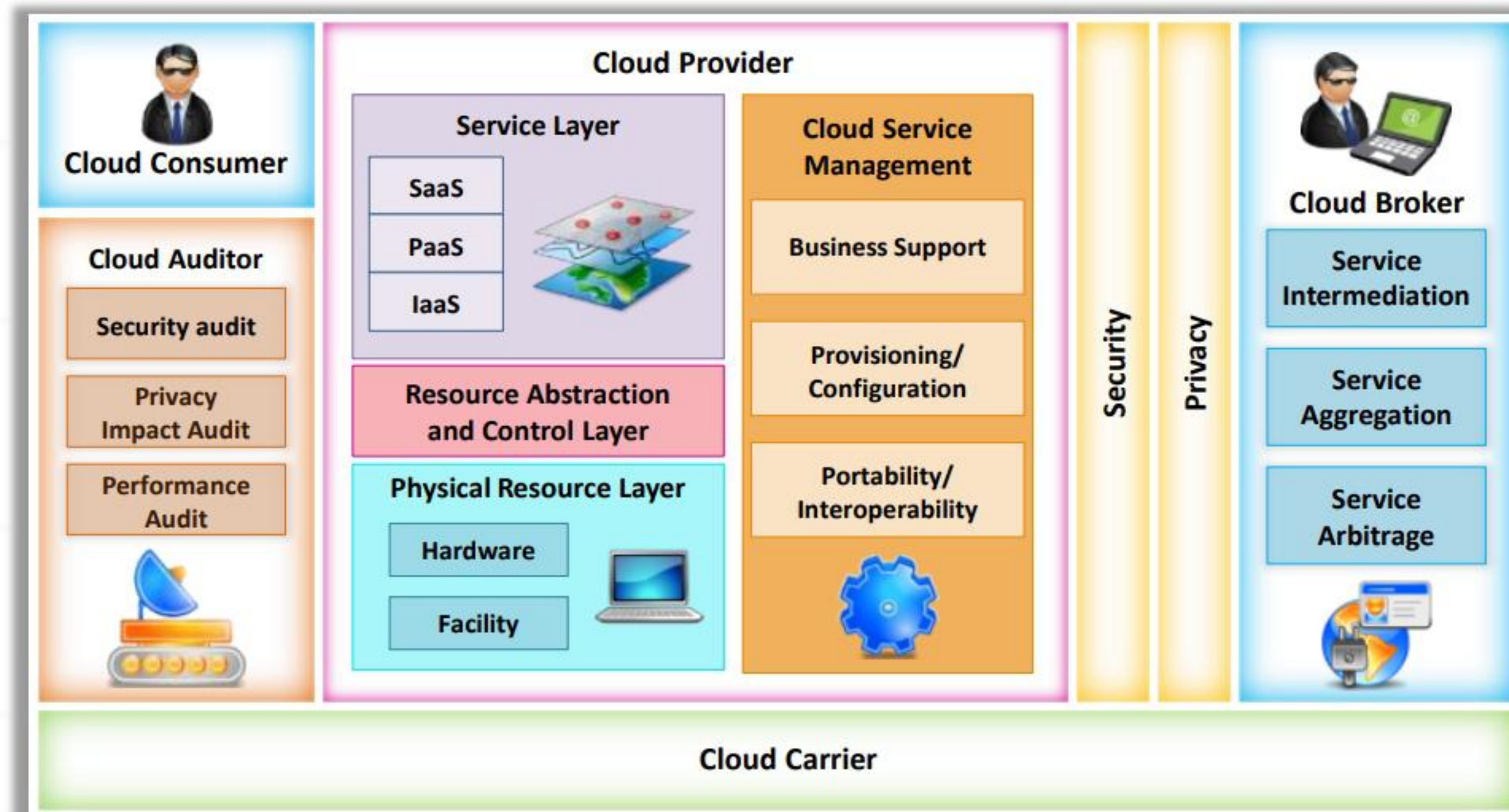
An intermediary for **providing connectivity** and **transport services** between cloud consumers and providers

Cloud Auditor

A party for making **independent assessments** of the **cloud service controls** and providing an opinion

Cloud Broker

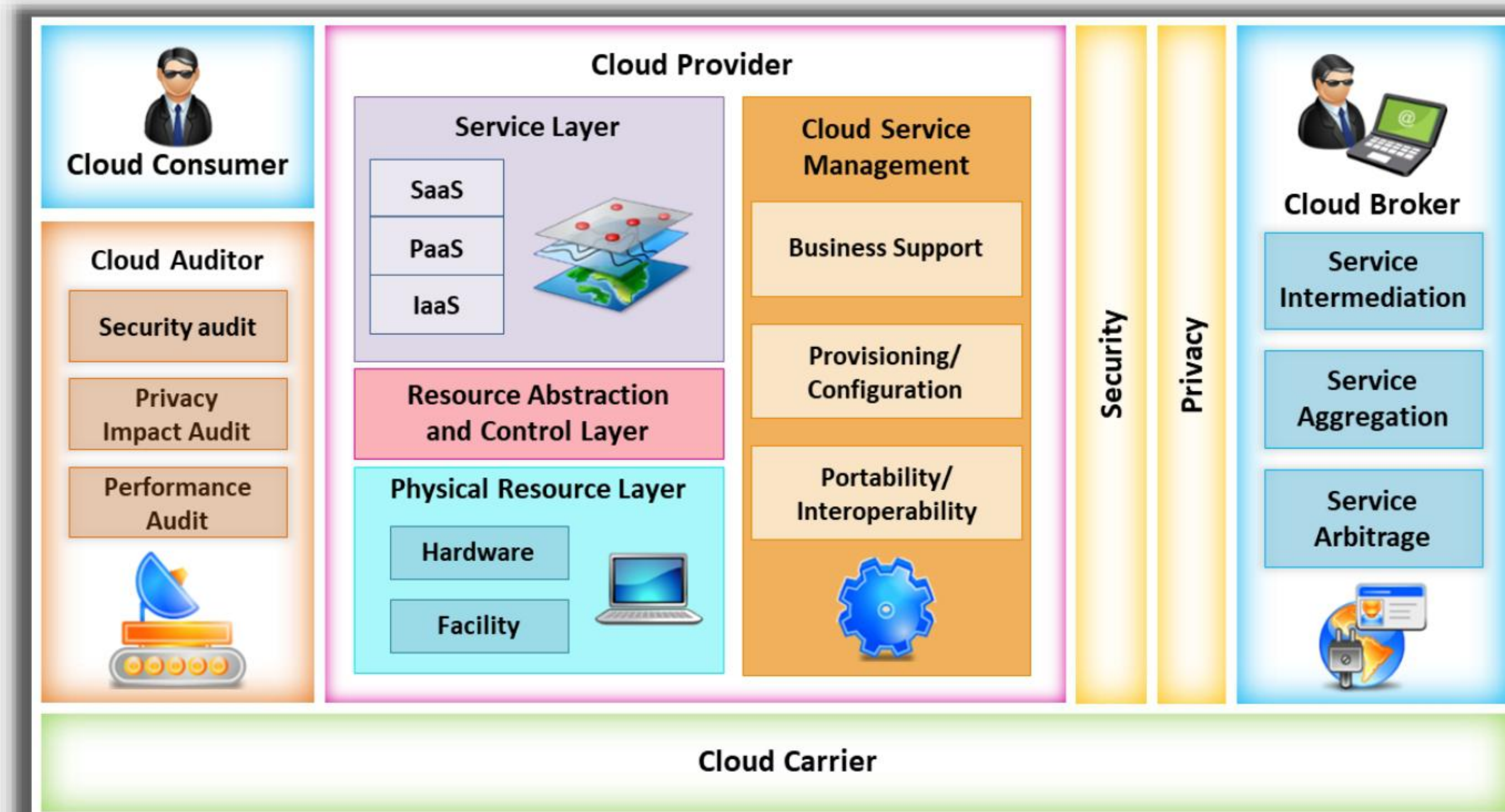
An entity to **manage cloud services** considering the use, performance, and delivery; additionally, a cloud broker maintains the relationship between cloud providers and consumers



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NIST Cloud Deployment Reference Architecture

An overview of the NIST cloud computing reference architecture, displaying the primary actors, their activities, and functions in cloud computing, is presented below. The diagram illustrates a generic high-level architecture to better understand the applications, requirements, characteristics, and standards of cloud computing.



Module 1.2: FIGURE: Separation of Cloud Responsibilities Specific to Service Delivery Models

The five significant actors are:

- **Cloud consumer**

A cloud consumer is a person or an organization that maintains a business relationship with the cloud service providers and uses cloud computing services. The cloud consumer browses the service catalog requests of the CSP for the desired services, sets up service contracts with the CSP (either directly or via a cloud broker), and uses the service. The CSP bills the consumer based on the services provided. The CSP should fulfill an SLA in which the cloud consumer specifies the technical performance requirements such as the quality of service, security, and remedies for performance failure. The CSP may also define the limitations and obligations, if any, that a cloud consumer must accept.

Services available to a cloud consumer in the **PaaS, IaaS, and SaaS** models are as follows.

- **PaaS** – database, business intelligence, application deployment, development and testing, and integration
- **IaaS** – storage, service management, content delivery network (CDN), platform hosting, backup and recovery, and computing
- **SaaS** – human resources, enterprise resource planning (ERP), sales, customer relationship management (CRM), collaboration, document management, email and office productivity, content management, financials, and social networks

- **Cloud Provider**

A cloud provider is a person or an organization that acquires and manages the computing infrastructure intended for providing services (directly or via a cloud broker) to the interested parties via network access.

- **Cloud Carrier**

A cloud carrier acts as an intermediary that provides connectivity and transport services between the CSPs and cloud consumers. The cloud carrier provides access to consumers via networks, telecommunication, and other access devices.

- **Cloud Auditor**

A cloud auditor is a party that independently examines the cloud service controls to express a corresponding opinion. Audits verify the adherence to standards by reviewing the objective evidence. A cloud auditor can evaluate the services provided by a cloud provider regarding security controls (management, operational, and technical safeguards intended to protect the confidentiality, integrity, and availability of the system and its information), privacy impact (compliance with applicable privacy laws and regulations governing the privacy of an individual), and performance.

- **Cloud Broker**

The integration of cloud services has become significantly complicated to be managed by the cloud consumers. Thus, a cloud consumer may request cloud services from a cloud broker instead of directly contacting a CSP. A cloud broker is an entity that manages cloud

services regarding the usage, performance, and delivery, and maintains the relationship between the CSPs and cloud consumers.

Cloud brokers provide services in three categories:

- **Service Intermediation**

Improves a given function by a specific capability and provides value-added services to cloud consumers.

- **Service Aggregation**

Combines and integrates multiple services into one or more new services.

- **Service Arbitrage**

Similar to service aggregation, but here, the services being aggregated are not fixed (cloud broker has the flexibility to choose services from multiple agencies).

hide01.ir

LO#02: Understand Cloud Security Objectives and Issues

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

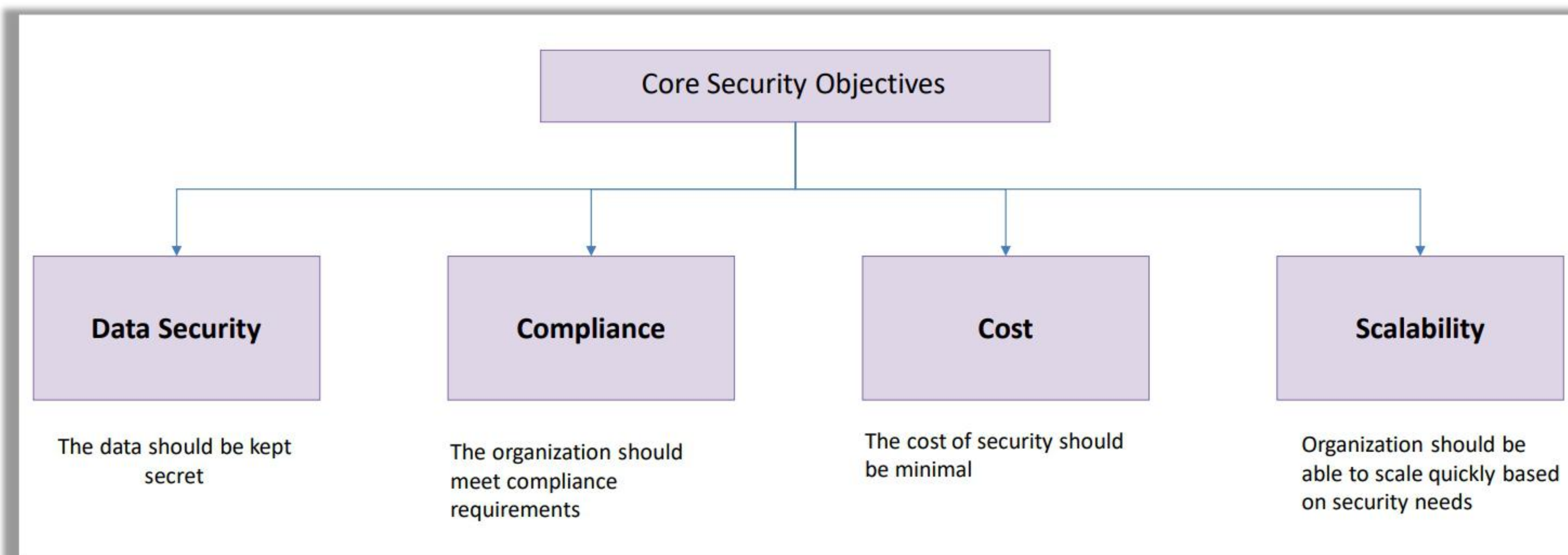
This section describes the core objective of cloud security and security issues and concerns related to cloud security.

hide01.ir

Core Security Objectives



Core security objectives of an organization should be following when migrating their workloads to cloud platform.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Core Security Objectives

As organizations are migrating their data to the cloud, they should follow strong security measures to ensure the security of the data. The core security objectives of an organization while migrating its workloads to the cloud environment should be the following.

- **Data Security**

While moving the workloads to the cloud, ensure that the data is kept secure. This includes ensuring encryption of data (both data at rest and data in transit) to maintain the secrecy of data.

- **Compliance**

The organization should understand the compliance requirements of data storage. Organizations should classify the data based on the compliance requirements like SOX, GDPR, HIPAA while migrating to the cloud.

- **Cost**

An advantage of migrating the data to the cloud is minimal costs. The cost of security is one of the essential factors while migrating the data to the cloud.

- **Scalability**

The organization should be able to scale quickly based on security needs. Scalability improves the disaster recovery and business continuity needs of the organization.

Cloud Security Concerns



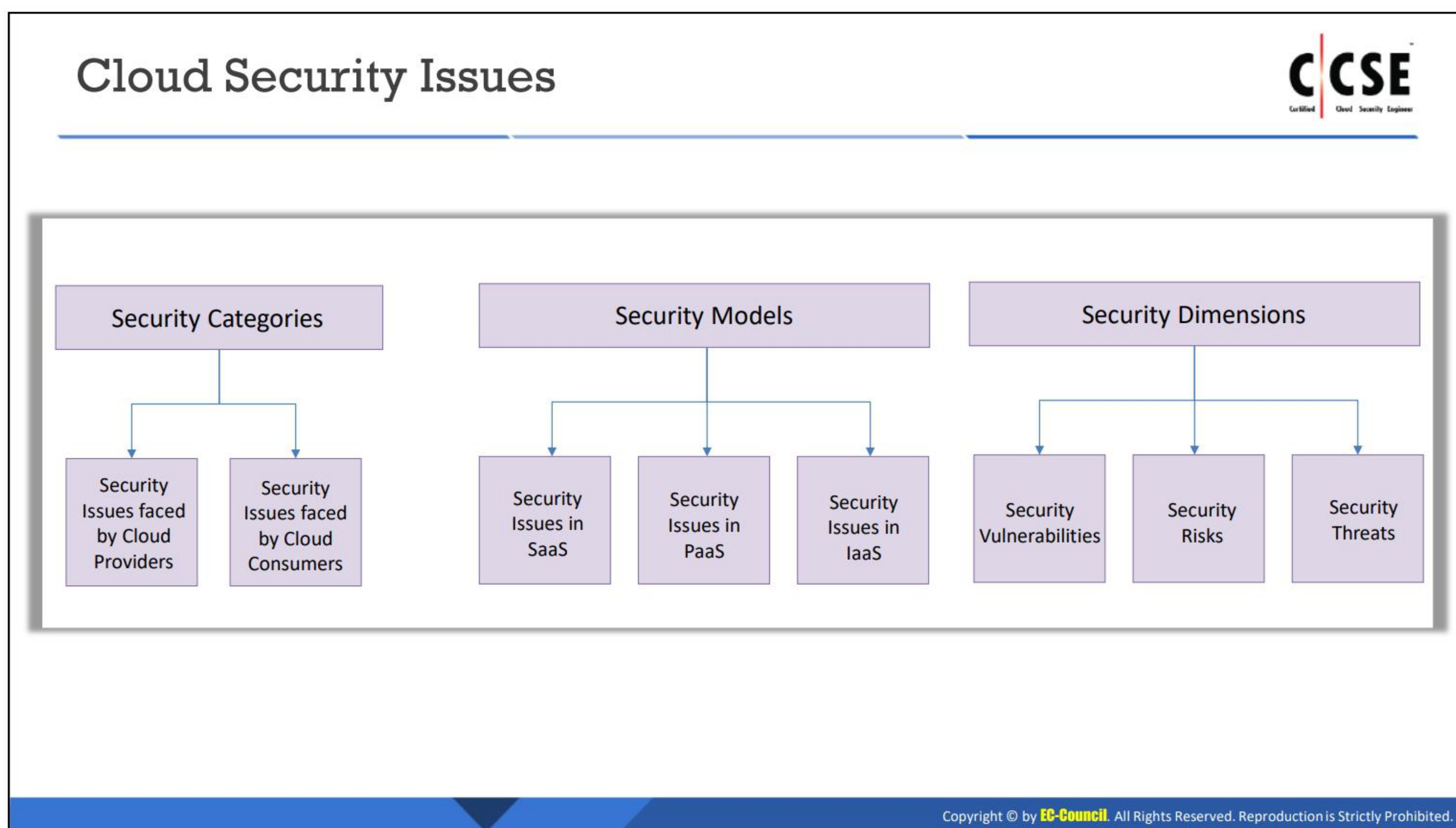
- Security of the cloud is designed and implemented with the help of certain security **controls** and **compliance**
- There is **not much difference** in security controls and compliance used in cloud and those used in a typical IT environment
- However, cloud service faces certain **other risks**, in addition to traditional IT security risks
- **Data security** is the **major concern** regarding the cloud, as the organization's critical data can be dispersed geographically without the organization having control of it
- Risks arise according to **models employed**, operation models, and the technology used to enable the cloud service

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Concerns

Cloud security is designed and implemented with the help of specific security controls and compliance. There is not much difference between the security controls implemented in the cloud and the traditional IT environment. The compliance requirements in traditional environments should also be followed in cloud environments. As a cloud environment follows a shared responsibility model, it is the responsibility of the user and also the cloud service provider to ensure security and compliance requirements.

However, cloud data storage possesses some other security concerns when compared with traditional IT environments. A significant concern with cloud environments is the security of critical data. The data stored in the cloud is dispersed geographically into different locations. The cloud service provider provides the physical security of the data, whereas the organization can implement only the logical security measures to protect their data based on the shared responsibility model. Also, there are risks due to the models employed, operation models, and the technology used to enable the cloud service.



Cloud Security Issues

As cloud services follow a shared responsibility model, it is the responsibility of the cloud service provider to ensure the security of the cloud environment and the responsibility of the consumer to ensure the security in the cloud. Following are the security issues in cloud-based on three aspects.

■ Security Categories

- **Security Issues faced by Cloud Providers:** The primary security issue the cloud service providers encounter is securing the physical hardware. The servers should be protected from outsider threats, natural calamities, etc., to ensure the continuity of services.
- **Security Issues faced by Cloud Consumers:** Cloud consumers have data security concerns as the data is stored in geographically dispersed locations. Other concerns include data integrity and the compliance requirements of the organization.

■ Security Models

- **Security Issues in SaaS:** SaaS model is vulnerable to different security issues such as identity theft, data security, data access risks, etc.
- **Security Issues in PaaS:** PaaS model is vulnerable to attacks like phishing, brute force, etc.
- **Security Issues in IaaS:** IaaS model is vulnerable to compliance issues and data loss.

■ Security Dimensions

- **Security Vulnerabilities:** Cloud security vulnerabilities arise due to misconfigured cloud services, improper access management, etc.
- **Security Risks:** The cloud security risks include identity theft, malware attacks, compliance violations, etc.
- **Security Threats:** Cloud security threats include data loss, DDOS attacks, etc.

Core Cloud Security Risks, Threats, Vulnerabilities



■ Risk profile is not known	■ Unauthorized access due to misuse of credentials
■ Account or service hijacking	■ Improper access control mechanism with enterprises
■ Data loss or leakage	■ Lack of Multifactor Authentication (MFA) mechanism
■ Vulnerabilities in shared technology	■ Increased Denial of Service (DoS) attacks
■ Malignant insiders	■ Hijacking the entire Network traffic
■ Insecure application programming interfaces	■ Improper use of cloud computing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Core Cloud Security Risks, Threats, Vulnerabilities

- **Risk profile is not known**

An organization's risk profile determines the risks the organization can encounter and the steps to address these risks. If the risk profile is unknown, the organization cannot take the necessary measures to protect its assets.

- **Account or service hijacking**

Account hijacking in cloud computing occurs when a hacker takes over the accounts of the legitimate user and collects confidential data or tampers it.

- **Data loss or leakage**

Data loss or leakage occurs due to improper data encryption at rest and in transit and misconfigurations.

- **Vulnerabilities in shared technology**

As cloud computing uses shared servers, they are prone to different vulnerabilities like DDOS attacks and unavailability of services.

- **Malignant insiders**

Malignant insiders like disgruntled employees or former employees who access confidential information might use it for unauthorized activities.

- **Insecure application programming interfaces**

If the API keys get exposed, they can be used by a malicious attacker to launch a DOS attack.

- **Unauthorized access due to misuse of credentials**

If the user credentials get stolen due to misconfigurations in the cloud environment, they can be used by the attackers to gain unauthorized access and compromise the data and other services.

- **Improper access control mechanism with enterprises**

Improper access control mechanisms will cause unauthorized access to the services

- **Lack of Multifactor Authentication (MFA) mechanism**

Multifactor Authentication(MFA) is added as an extra layer of security to enforce a secure authentication. Lack of MFA will cause unauthorized access to the cloud environment

- **Increased Denial of Service (DOS) attacks**

DOS attacks prevent cloud computing services from delivering the services for a while.

- **Hijacking the entire Network traffic**

The attacker can take control over the network and performs malicious activities like eavesdropping attacks in the cloud environment.

- **Improper use of cloud computing**

The improper use of the cloud computing environment, like improper access control mechanisms, encryption of data, will cause security issues.

hide01.1



LO#03: Understanding Cloud Security Insights

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#03: Understand Cloud Security Insights

The objective of this section is to explain the shared responsibility of security in different cloud service models (IaaS, PaaS, and SaaS). This section explains the enterprise roles in securing the various elements of cloud such as user security and monitoring (e.g., IAM, encryption and key management, application-level security, data storage security, and monitoring), logging, and compliance.



Traditional security measures do not change with the adoption of cloud, but the focus does. The implementation of cloud does not change the security protocols required in traditional networks (on premise); instead, it changes the security focus of the cloud consumers.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

hide01.ir

Cloud Security Vs Traditional IT Security



Cloud Security	Traditional IT Security
Quickly scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Low upfront infrastructure	High upfront cost
Usage-based cost	Higher cost
Third-party data centers	In-house data centers
Reduced time to market	Longer time to market

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security VS Traditional IT Security

The following are the advantages of cloud security over traditional on-premise IT security.

Cloud Security	Traditional IT Security
Quickly scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Low upfront infrastructure	High upfront cost
Usage-based cost	Higher cost
Third-party data centers	In-house data centers
Reduced time to market	Longer time to market

Module 1.1 Figure: Cloud Security Vs Traditional IT security

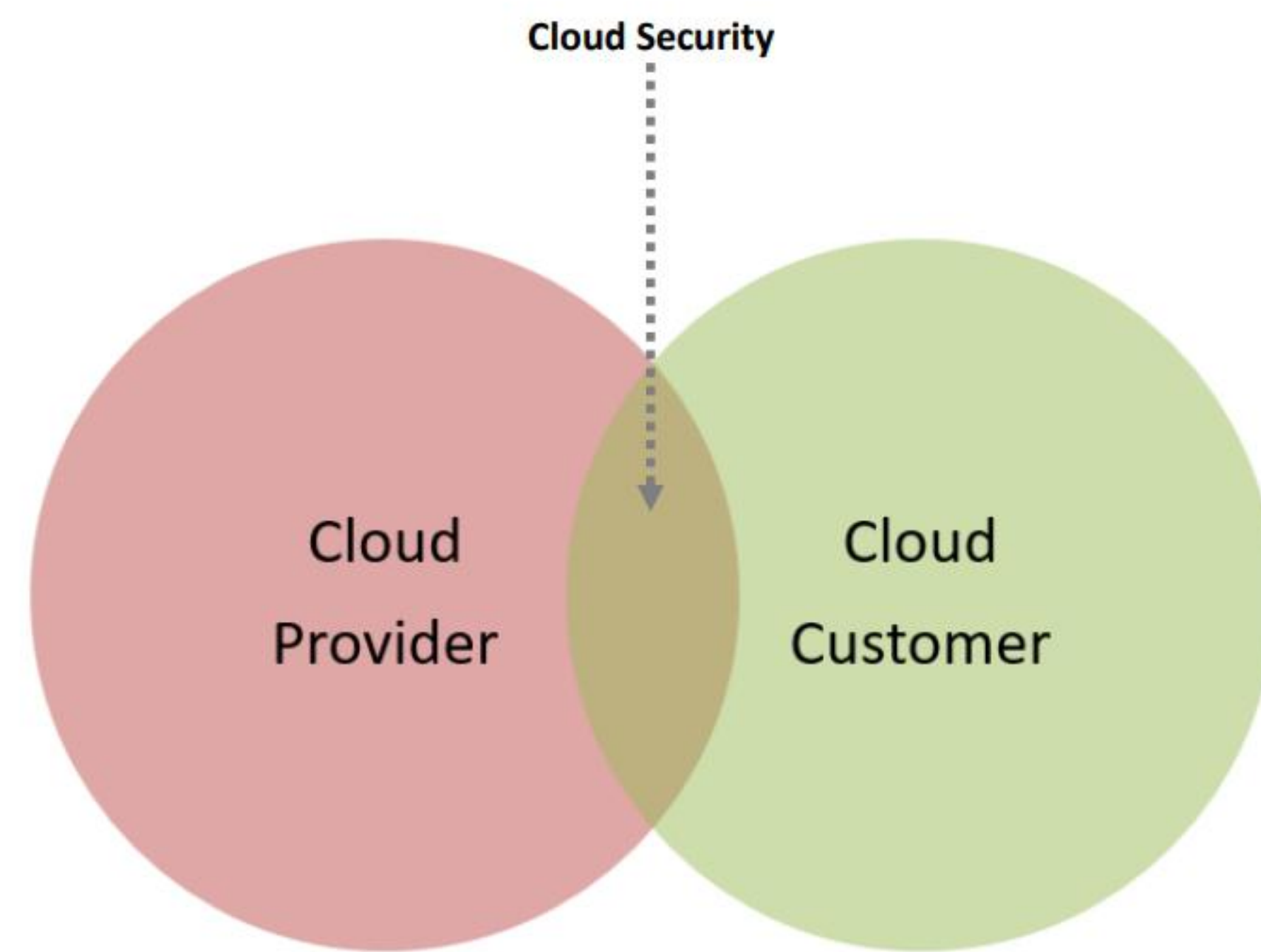
Cloud Security: Shared Responsibility



Cloud security and compliance are the **shared responsibility** of the cloud provider and consumer

According to the selected cloud module, security responsibilities are divided based on the **shared responsibility model**

If the **consumers do not secure their functions**, the entire cloud security model will **fail**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security: Shared Responsibility (Cont'd)



Shared Responsibility Model for Security in the Cloud				
Responsibility	On-Premises (for reference)	IaaS (Infrastructure-as-a-service)	PaaS (Platform-as-a-service)	SaaS (Software-as-a-service)
User Access				
Data				
Applications				
Operating System				
Network Traffic				
Hypervisor				
Infrastructure				
Physical				

Customer Responsibility Cloud Provider Responsibility

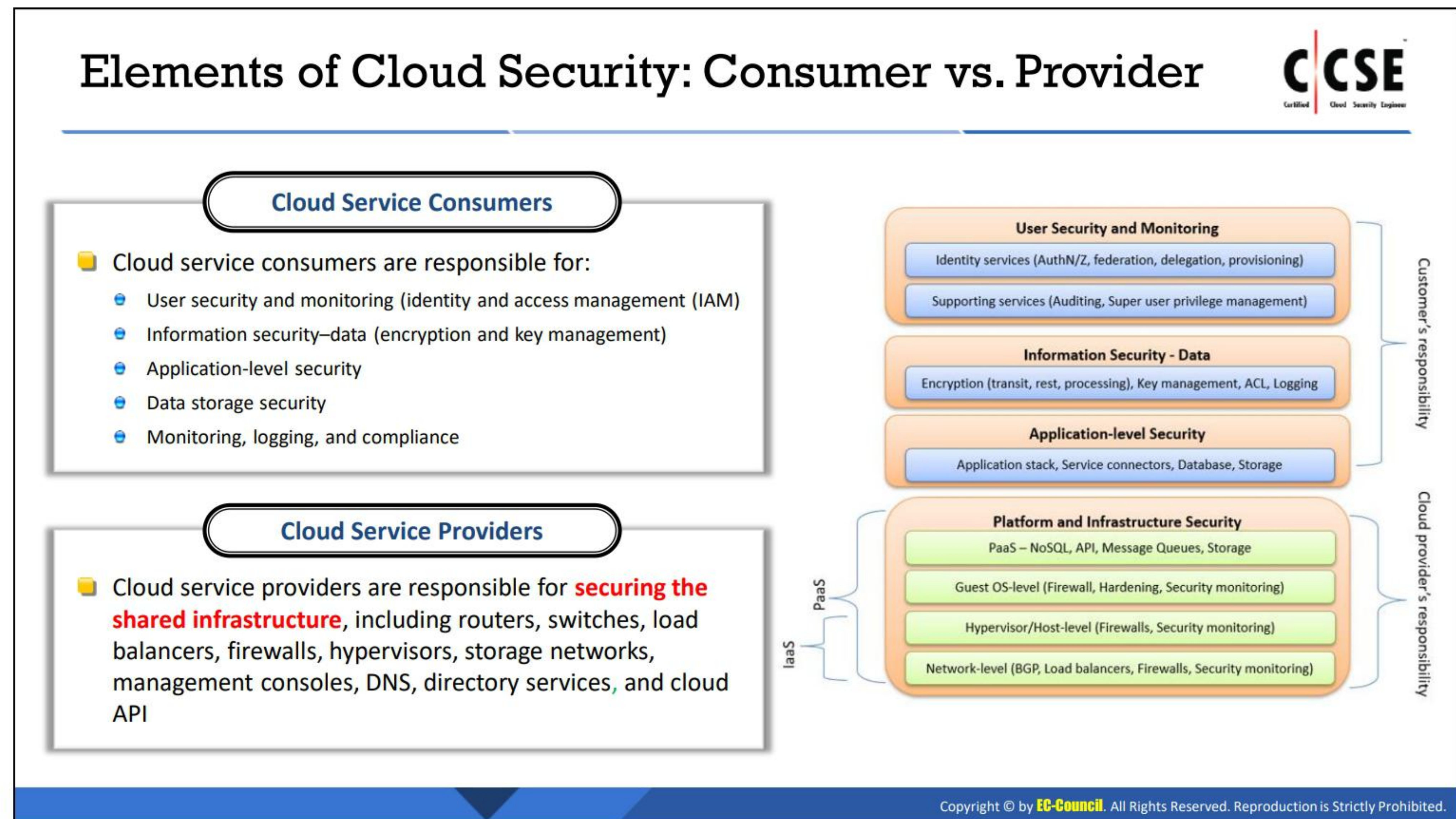
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security: Shared Responsibility

Security is a shared responsibility in cloud systems, wherein the cloud consumers and cloud service providers have varying levels of control over the available computing resources. Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources and the entire life cycle of systems, cloud service providers and consumers work together to design, build, deploy, and operate cloud-based

systems. Therefore, both parties share responsibilities to maintain adequate security in these systems. Different cloud service models (IaaS, PaaS, and SaaS) imply varying levels of controls between the cloud service providers and cloud consumers.

hide01.ir



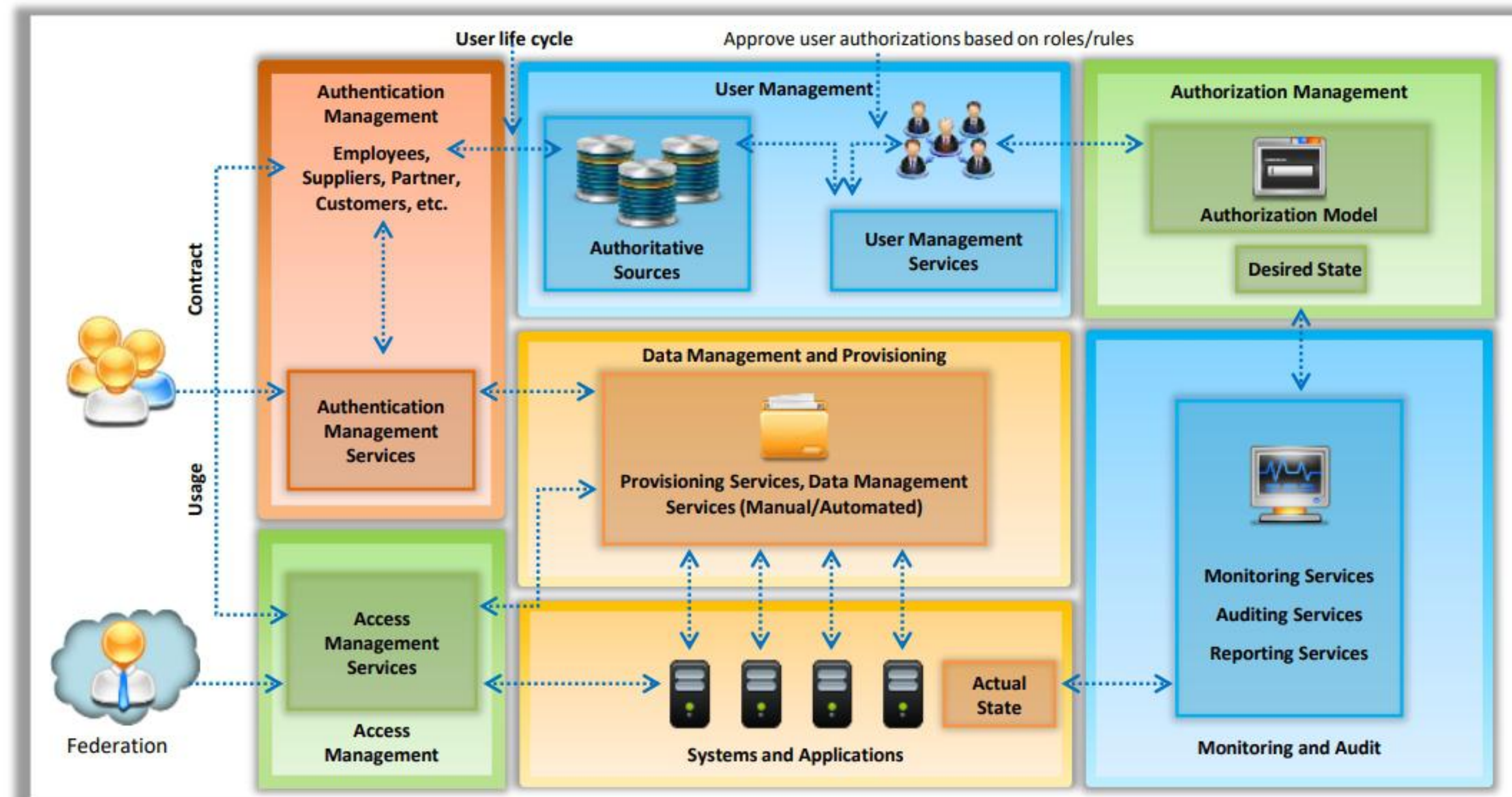
Elements of Cloud Security: Consumer vs. Provider

In the cloud security shared responsibility module, cloud service consumers focus on implementing security controls such as user identity and Access Management (IAM), encryption and key management, application-level security, data storage security, monitoring, logging, and compliance. Meanwhile, the cloud service providers focus on ensuring a secured infrastructure, including routers, switches, load balancers, and firewalls.

Identity and Access Management (IAM)



- IAM is the management of the **digital identities of users** and their **rights** to access cloud resources
- It includes creating, managing, and removing digital identities, as well as the authorization of users



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identity and Access Management (IAM)

Identity and Access Management (IAM) offers role-based access control to the customers or employees of an organization for accessing critical information within the enterprise. It comprises business processes, policies, and technologies that enable the surveillance of electronic or digital identities. IAM products provide tools and technologies to the system administrators for regulating user access (creating, managing, and removing access) to systems or networks based on the roles of individual users within the enterprise. Organizations generally prefer all-in-one authentication that can be extended to Identity Federation. Because Identity Federation includes IAM with single sign-on (SSO) and a centralized AD account for secure management. Additionally, IAM enables multi-factor authentication (MFA) for the root user and its associated user accounts. MFA is used to control the access to cloud service APIs. However, the best option is selecting either a virtual MFA or hardware device.

Data Storage Security



■ In a cloud, data are stored on internet-connected servers in **data centers** and it is the responsibility of data centers to secure the data

■ However, customers should protect their data to ensure comprehensive data security

Data Storage Security Techniques

- **Local data encryption:** Ensuring confidentiality of sensitive data in the cloud
- **Key management:** Generating, using, protecting, storing, backing up, and deleting encryption keys. Key management in cloud ensures strict key security owing to the increased possibility of key exposure
- **Strong password management:** Using strong passwords and changing them at regular intervals
- **Periodic security assessment of data security controls :** Continuously monitoring and reviewing the implemented data security controls
- **Cloud data backup:** Taking local backups of the cloud data prevents possible data loss in the organization


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Storage Security

Given below is a list of data security measures for a business to ensure data security in the cloud.

- Generally, IT organizations depend on data considerably. Loss of data may imply financial loss as well as legal actions. Therefore, it is essential for an organization to locally backup the data to prevent possible data loss.
- Compromising with the storage of sensitive information (patents and copyrights) on clouds may create problems for the organizations. Therefore, the organizations should avoid saving sensitive information on the cloud.
- Using local encryption before uploading data to the cloud can protect data from threats. It is better to select a service provider that can provide prerequisite data encryption or a primary encryption service to provide extra security to the consumers who already have an encrypted cloud service.
- Key management involves generating, using, protecting, storing, backing up, and deleting the encryption keys.
- Strengthen passwords and change them at regular intervals to improve data security on the cloud. A two-step verification process and updated patches prevent hackers from attacking the systems easily.
- In addition to encrypting data and applying passwords to secure data on the cloud, securing the cloud with security measures such as antivirus programs, admin privileges, and local encryption offered by cloud services can further secure the data.
- It is essential to test the cloud data security to determine its performance. This step can help in finding security loopholes. Ensuring data security on the cloud required constant action.

Network Security



■ Main challenge in cloud network security includes the **lack of network visibility** in monitoring and managing suspicious activities by the consumer

■ Cloud network security requires the following **additional security features** in comparison to the traditional network security features

- Encrypt data-in-transit
- Provide multi-factor authentication
- Install firewalls
- Enable data loss prevention

■ Methods to secure a cloud network

- Using DMZs
- Isolating resources with subnets, firewalls, and routing tables
- Securing DNS configurations
- Limiting inbound/outbound traffic
- Securing accidental exposures
- Intrusion detection and prevention systems
- Implementing layers of firewall

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Security


As a part of cloud services, the cloud service providers ensure network level protection by implementing certain network security controls. For example, Network Access Control List (NACL) is implemented in the AWS cloud, while Endpoint and NSG are implemented in the Azure cloud.

The cloud consumers are recommended to use additional network security levels for network layer protection via firewall and web application firewalls (WAF). The use of firewalls guarantees isolation between multiple zones.

The following principles should be considered for network security in cloud computing to enable a network security architecture in an organization to satisfy the technology and security principles established by the providers.

- Network control for traffic flow
- End-to-end transport level encryption
- Using standard secure encapsulation protocols such as IPSEC, SSH, and SSL during deployment

Monitoring



- Monitoring is required to manage **cloud-based services, applications, and infrastructure**
- Activity monitoring should observe the following **activities** to monitor unauthorized data access:

- 1 Data replication
- 2 Data file name changes
- 3 Data file classification changes
- 4 Data ownership changes

Data Monitoring should:

- Define thresholds and rules for normal activity
- Alert the data owner if data activity exceeds the defined thresholds

Cloud Monitoring Plan should:

- Identify metrics and events
- Use one platform to report all data
- Monitor cloud service usage and fees
- Monitor user experience
- Trigger rules with data
- Separate and centralize data

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Monitoring

Cloud monitoring is required to manage cloud-based services, applications, and infrastructure. Effective cloud monitoring helps an organization to protect a cloud environment from potential threats, store and transfer data in the cloud easily and safeguard the personal data of customers.

Activity monitoring should observe the following activities to monitor unauthorized data access:

- **Data replication:** It plays a key role in data management by migrating databases online and synchronizing the data in real time. Migration monitoring should be performed during data replication.
- **Data file name changes:** Data handling activities such as data file name changes should be monitored. The file change attributes should be utilized for monitoring changes in the file system.
- **File classification changes:** Activity monitoring through file classification changes helps in determining any changes in the cloud data files.
- **Data ownership changes:** Data activity monitoring via data ownership changes should be closely monitored to prevent unauthorized access and security breach.

Data monitoring should define thresholds and rules for normal activities, which can help in detecting unusual activities and send alerts to data owners if any breach is observed in the defined threshold.


Cloud monitoring plan: The essential aspects of the cloud monitoring plan are as follows:

- **Identify metrics and events:** Identify key metrics and events that can potentially affect the business of an organization and monitor it.

- **Use one platform to report all data:** Organizations should have services that report data from various sources on a single platform to ensure a complete perspective of the performance.
- **Monitor cloud service usage and fees:** Implement robust monitoring solutions to track the activities of an organization on the cloud and the relevant cost.
- **Monitor user experience:** An organization should implement metrics such as the response time and frequency to monitor user experience.
- **Trigger rules with data:** If the cloud-based activities increased or decreased with respect to a specific threshold, then add or remove servers for maintaining efficiency and performance.
- **Separate and centralize data:** The monitoring of data should be centralized and separated from the monitoring of applications and services.
- **Try failure:** An organization should evaluate its alert system by testing its tools to determine the potential outcome during outage or data breach.

hide01.ir

Logging



Security logs are used for threat detection, data analysis, and compliance audits to enhance cloud security

Efficient Security Log Management for Cloud includes:

- **Aggregating all logs:** Capture maximum data and transfer them to log analytics or the security information and event management (SIEM) system to provide organizations with a database of valuable information to access and analyze on demand
- **Capturing appropriate data:** Ensure to log the required information by asking the following questions
 - Who is accessing the network?
 - What assets are they accessing?
 - From where are they accessing the asset?
 - When are they doing this?
 - Are there established permissions to allow their activity?
- **Controlling log collection and distribution frequency:** The frequency of log collection and distribution impacts the server resource utilization; hence, it should be configured and controlled to ensure that the application performance is not disturbed
- **Ensuring system scalability:** Ensure that the log analytics and management capabilities are scaled according to the log data stored

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Logging

Security logs provide a record of the activities in the IT environment of an organization. They are used for threat detection, data analysis, and compliance audits to enhance cloud security.

After the accelerated adoption of cloud platforms, instead of using a few servers, companies now maintain thousands of servers that play a smaller role within the application infrastructure stack. This complicates the aggregation of data silos.

To ensure efficient and secure log management in the cloud, organizations should follow the following practices.

Aggregate All Logs

Organization should capture the maximum data and transfer them to log analytics or a security information and event management (SIEM) system. This enables organizations to have a database of valuable information to access and analyze on demand.

The modern log management solutions possess high granularity and complexities. These features enable the organizations to easily determine the root cause of potential anomalies from the logs that were never captured.

Capture Appropriate Data

The key for the successful implementation of log analytics includes having a large library of the actionable insights captured from the log files. To capture the actionable insights from the logs, the following set of questions must be asked.

- Who is accessing the network?
- What assets are they accessing?

- From where are they accessing the assets?
- When are they doing this?
- Are there established permissions to allow their activity?

Keep Applications Safe


Organizations should ensure that their log collection and management processes do not ruin the monitoring application (legacy-based or virtual application). This does not mean that the organizations require no extra efforts to ensure this. Occasionally, the need for continuous monitoring buries the application resources. To avoid this, organizations should ensure that they are appropriately configured because the parameters that control the frequency of log collection and distribution may impact server-resource utilization.

System Scalability

A problematic system generates more data than usual. This can lead to bursts in the log data. The amount of log data grows with the organization or the demand for an application. Therefore, it is important to ensure that the log analytics and management capabilities can scale accordingly.

hide01.ir

Compliance



- A clear idea about the **regulation standards** that an organization wants to comply with along with its associated requirements allows organizations benefit from the business agility and growth
- Compliance considerations** for the organizations to integrate their compliance programs with their cloud providers:
 - Know the requirements that impact an organization to know about the jurisdictions of an organization, industry, or activities employed by the organization to conduct business
 - Conduct regular compliance risk assessments to help the organizations to adopt the updated and revised risk assessment processes regularly
 - Monitoring and auditing the organization compliance program before a crisis hits helps organizations to determine the gaps and improving their compliance position

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Compliance

A clear understanding of the requirements of an organization and how compliance is achieved can enable the organizations to benefit from business agility and growth. Compliance failure can lead to regulatory fines, lawsuits, cyber security incidents, and reputational damage.

Following are the compliance considerations for an organization to integrate its compliance programs with its cloud providers.

- **Knowing the requirements that impact an organization** is important. These requirements are based on the jurisdiction of an organization, industry, or the activities employed by an organization for its operation.
- **Conducting regular compliance risk assessments** helps organizations to establish the foundation of a strong compliance program. This process allows organizations to adopt the updated and revised risk assessment processes regularly.
- **Monitoring and auditing the compliance program of an organization proactively** or before a crisis hits can help organizations to find gaps and improve their compliance position.



LO#04: Evaluate CSPs for Security before Consuming a Cloud Service

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#04: Evaluate CSPs for Security Before Consuming a Cloud Service

This section explains how to evaluate various CSP providers in terms of security before consuming a cloud service. It lists the various security features provides by AWS, Azure, and GCP.

Evaluating the CSPs



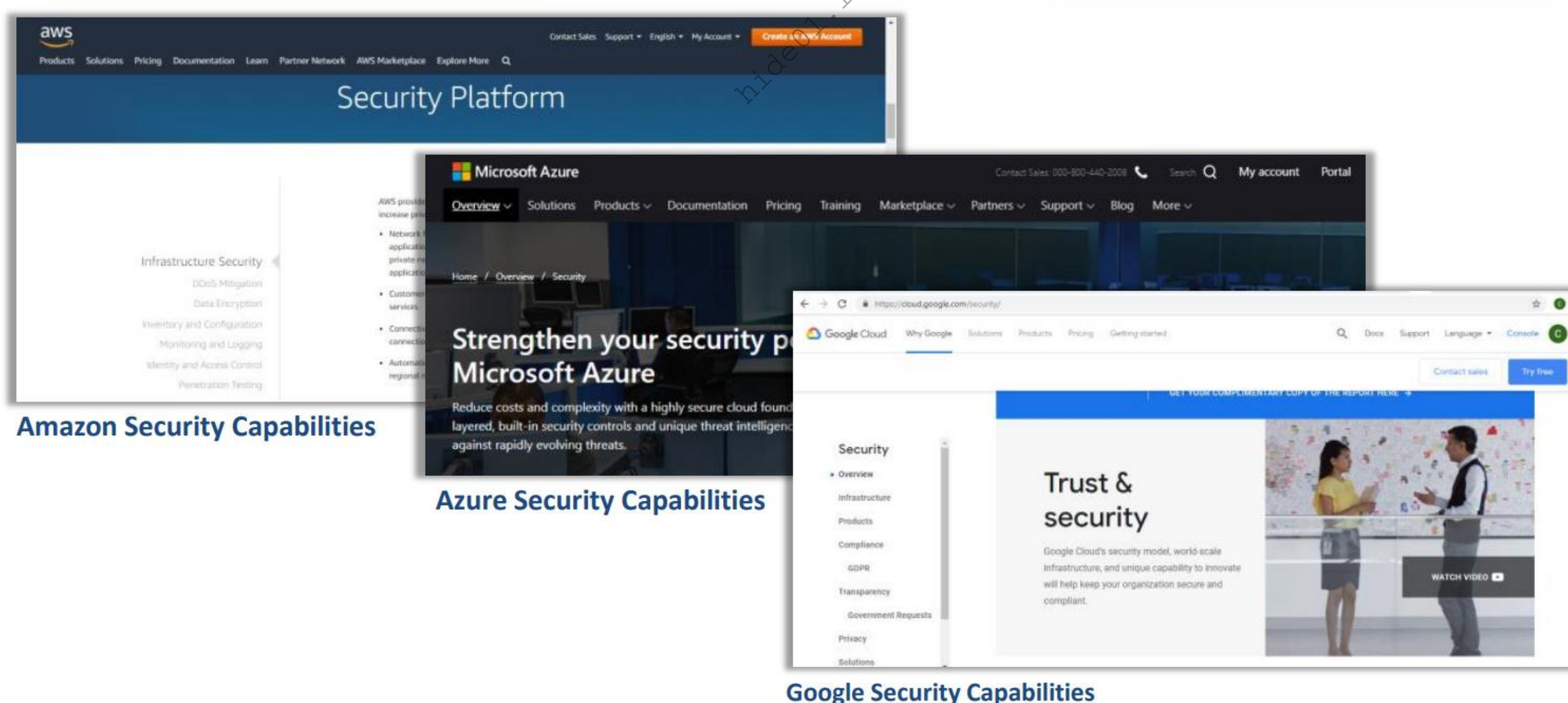
- Before consuming a cloud service, it is important to perform a **gap analysis** on the **security capabilities** and services provided by the cloud service providers
- It involves analyzing the platform capabilities of the cloud against maturity, transparency, compliance with enterprise security standards (e.g., ISO 27001), and regulatory standards such as PCI DSS, HIPAA, and SOX

The security maturity of the CSP should be evaluated based on:

- Disclosure of security policies, compliance, and practices
- Disclosure when mandated
- Security architecture
- Security automation
- Governance and security responsibility

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evaluating the CSPs (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evaluating the CSPs

Before consuming a cloud service, it is important to perform a gap analysis on the security capabilities and services provided by the cloud service providers. This gap analysis should benchmark the maturity, transparency, and compliance of a cloud platform with the enterprise security and regulatory standards such as PCI DSS, HIPAA, and SOX. Cloud security maturity models can help in accelerating the implementation of the migration strategy of applications to the cloud.

Security Features Provided By AWS, Azure, and GCP



Security Service Feature	AWS	AZURE	GCP
Identity and Access Management	IAM	Active Directory	Cloud IAM
Key Management	KMS	Key Vault	Cloud KMS
Network	VPC	Virtual Network, ExpressRoute	VPC
Security Check	Trusted Advisor, AWS Inspector	Security Center	Cloud Security Command Center
Storage Security	Data Encryption for S3	Storage Service Encryption (SSE)	Data Encryption Key (DEK)
Monitoring	Cloud Watch	Azure Monitor, Application insights	Google Cloud Monitoring, InfluxDB and Grafana, Stackdriver
Logging	CloudWatch Logs, Cloud Trail, Stackdriver Logging	Log Analytics, Security Event Logs	Stackdriver Logging
Compliance	CloudHSM	TrustCenter	Cloud HSM

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Features Provided By AWS, Azure, and GCP

Security Service Feature	AWS	AZURE	GCP
Identity and Access Management	IAM	Active Directory	Cloud IAM
Key Management	KMS	Key Vault	Cloud KMS
Network	VPC	Virtual Network, ExpressRoute	VPC
Security Check	Trusted Advisor, AWS Inspector	Security Center	Cloud Security Command Center
Storage Security	Data Encryption for S3	Storage Service Encryption (SSE)	Data Encryption Key (DEK)
Monitoring	Cloud Watch	Azure Monitor, Application insights	Google Cloud Monitoring, InfluxDB and Grafana, Stackdriver
Logging	CloudWatch Logs, Cloud Trail, Stackdriver Logging	Log Analytics, Security Event Logs	Stackdriver Logging
Compliance	CloudHSM	TrustCenter	Cloud HSM

Module 1.1: TABLE: Main Security Features Provided by AWS, Azure and GCP

On-premise vs. Third Party Security Controls Provided by Major CSPs



ON-PREMISE	AWS	AZURE	GOOGLE	ORACLE	IBM
Firewall and ACLs	Security Groups AWS Network ACLs	Network Security Groups (NSGs)	Cloud Armor VPC Firewall	VCN Security Lists	Cloud Security Groups
IPS/IDS	Third Party Only	Third Party Only	Third Party Only	Third Party Only	Third Party Only
Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Application Gateway	Cloud Armor	Oracle Dyn WAF	Cloud Internet Services
SIEM Log Analytics	AWS Security Hub Amazon GuardDuty	Advanced Log Analytics Azure Monitor	Stackdriver Monitoring Stackdriver Logging	Oracle Security Monitoring and Analytics	IBM Log Analysis Cloud Activity Tracker
Antimalware	Third Party Only	Microsoft Antimalware/ Azure Security Center	Third Party Only	Third Party Only	Third Party Only
Privileged Access Management (PAM)	Third Party Only	Azure AD Privileged Identity Management	Third Party Only	Third Party Only	Third Party Only
Data Loss Prevention (DLP)	Amazon Macie	Information Protection (AIP)	Cloud Data Loss Prevention API	Third Party Only	Third Party Only
Vulnerability Assessment	Amazon Inspector AWS Trusted Advisor	Azure Security Center	Cloud Security Scanner	Security Vulnerability Assessment Service	Cloud Security Advisor Vulnerability Advisor
Email Protection	Third Party Only	Office Advanced Threat Protection	Various controls embedded in G-Suite	Third Party Only	Third Party Only
SSL Decryption Reverse Proxy	Elastic Load Balancer	Application Gateway	HTTPS Load Balancing	Third Party Only	Cloud Load Balancer
VPN	VPC Customer Gateway AWS Transit Gateway	Virtual Network SSTP	Google VPN	Dynamic Routing Gateway (DRG)	IPSec VPN Secure Gateway
Key Management	Key Management Service (KMS)	Key Vault	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

On-premise vs. Third Party Security Controls Provided by Major CSP (Cont'd)



ON-PREMISE	AWS	AZURE	GOOGLE	ORACLE	IBM
Encryption At Rest	Elastic Block Storage	Storage Encryption for Data at Rest	Part of Google Cloud Platform	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services
DDoS	AWS Shield	Built-in DDoS defense	Cloud Armor	Built-in DDoS defense	Cloud Internet Services
IAM	IAM	Azure Active Directory	Cloud Identity Cloud IAM	Oracle Cloud Infrastructure IAM	Cloud IAM APP ID
MFA	AWS MFA	Azure Active Directory	Security Key Enforcement	Oracle Cloud Infrastructure IAM	App ID
Centralized Logging/Auditing	CloudWatch/S3 Bucket	Azure Audit Logs	VPC Flow Logs Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA
Load Balancer	Elastic Load Balancer/CloudFront	Azure Load Balancer	Cloud Load Balancing HTTPS Load Balancing	Cloud Infrastructure Load Balancing	Cloud Load Balancer
LAN	Virtual Private Cloud (VPC)	Virtual Network	VPC Network	Virtual Cloud Network (VCN)	VLANs
WAN	Direct Connect	ExpressRoute/MPLS	Dedicated interconnects	FastConnect	Direct Link
Endpoint Protection	Third Party Only	Microsoft Defender ATP	Third Party Only	Third Party Only	Third Party Only
Certificate Management	AWS Certificate Manager	Third Party Only	Third Party Only	Third Party Only	Certificate Manager
Container Security	Amazon EC2 Container Service (ECS)	Azure Container Service (ACS)	Kubernetes Engine	Oracle Container Services	Containers-Trusted Compute
Governance Risk and Compliance Monitoring	AWS CloudTrail AWS Compliance Center	Azure Policy	Cloud Security Command Center	Third Party Only	Third Party Only
Backup and Recovery	AWS Backup Amazon S3 Glacier	Azure Backup Azure Site Recovery	Object Versioning Cloud Storage Nearline	Archive Storage	IBM Cloud Backup

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

On-premise vs. Third Party Security Controls Provided by Major CSPs

On-premise security controls are provided by cloud platforms to ensure reliable customer service. Generally, third-party tools are required to secure the cloud infrastructure in terms of the security controls that are not provided by the CSP. Before taking any technology decisions, organizations should review their requirements and the existing tools provided by each CSP based on a self-check or requirement-driven approach. For example,

- How many security tools are currently required in the organization?
- What risks can the security tools reduce/address?
- Rationalize the existing security vendors and tools.

Matching the requirements with the solutions offered by the cloud vendor can help in making an effective technology decision regarding the selection of cloud provider. Additionally, it should be ensured that the third-party products can be integrated with the cloud platform. The security system should combine the third-party controls with the security controls provided by the CSP.

hide01.ir



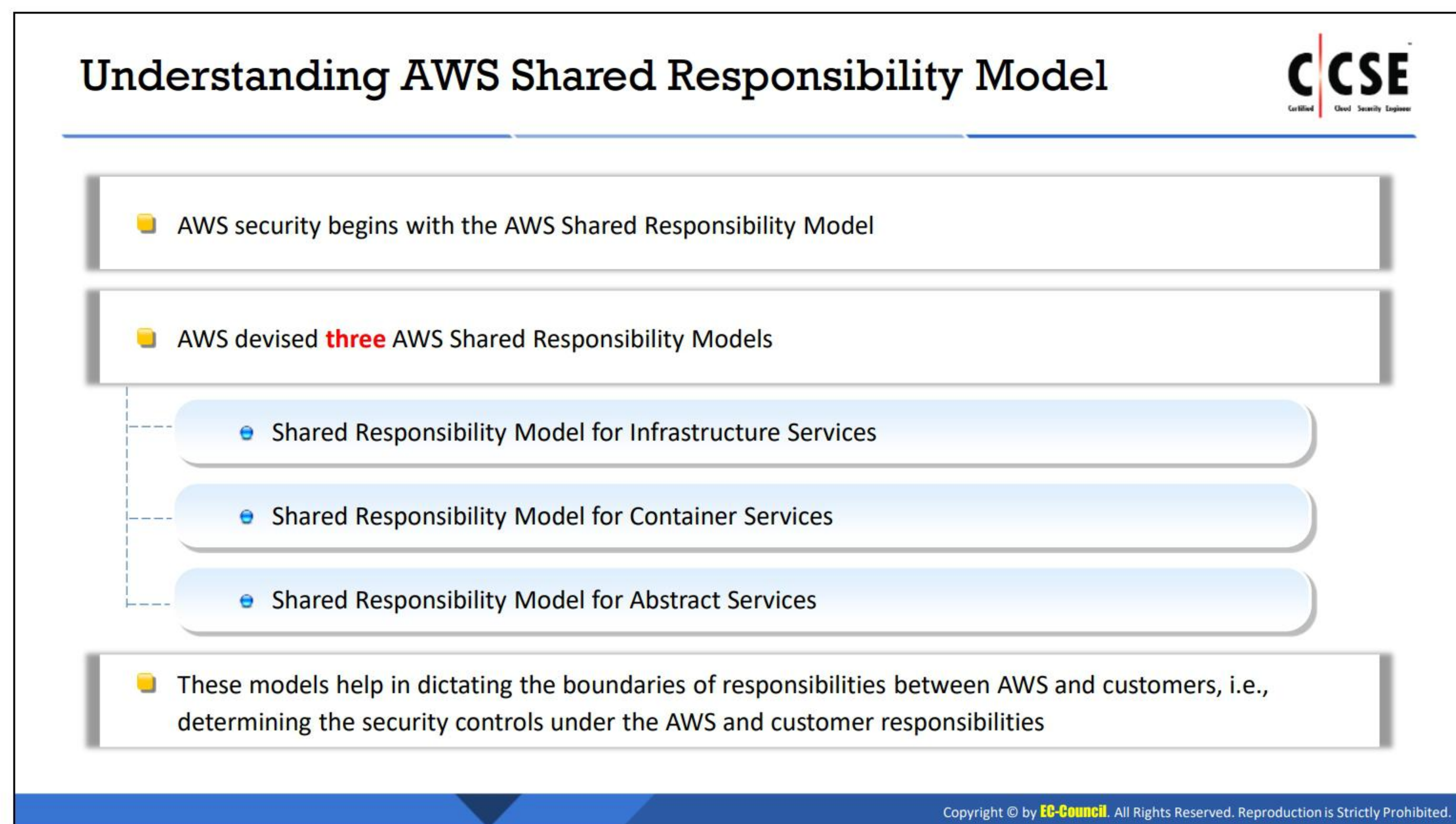
LO#05: Discuss Security Shared Responsibility Model in Amazon Cloud (AWS)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#05: Discuss Security Shared Responsibility Model in Amazon Cloud (AWS)

The objective of this section is to discuss Amazon cloud (AWS) Shared Responsibility Model and its secured solution design

hide01.ir



Understanding AWS Shared Responsibility Model

AWS security initially includes the AWS shared responsibility model that distinguishes the security controls between the AWS and customers. The customers decide the access levels he chooses to give from and to his resources, while AWS secures the cloud. A good understanding of the AWS shared responsibility model enables the building and maintenance of a highly secure and reliable environment.

AWS Security Responsibilities

AWS is responsible for the security of the cloud infrastructure that comprises the following elements.

- **AWS Global Infrastructure/Hardware**

Constant IT maintenance and physical security protection ensure the security of the AWS infrastructure, which includes regional, available, and edge zones.

- **AWS Software**

AWS security services that include encryption keys, network monitoring tools, and database protection secure the computation, storage, database, and networking in the cloud.

Customer Security Responsibilities

Customers are responsible for the security of their specific instances and their responsibilities are determined according to the selected AWS cloud service. Customers should perform all the required security configuration and management tasks if they select an Amazon IaaS (EC2, VP3, S3). This includes the following:

- **Customer Data**

Securing the business data on the network because they enter and exit the cloud service.

- **Platform, Applications, Identity and Access Management**

Managing and securing the platforms running on the cloud along with other elements of the platform such as application maintenance and IAM.

- **Client-Side Data Encryption**

Using either an AWS-managed encryption key or a personal key not provided by AWS.

- **File System Encryption**

Using an independent protection system or file system protection to secure the customer data at rest.

- **Network Traffic Protection**

Guarantee the security of all traffic entering and exiting the server.

- **Service and Communication Protection**

Routing and zoning data within specific security environments.

Shared Security Responsibilities

AWS provides customers with an infrastructure and the customers provide their own control implementation techniques under the AWS services.

- **IT Controls**

AWS and the customers share the responsibilities of IT operations along with the management and operation of these controls.

- **Patch Management**

- AWS is responsible for patching and fixing flaws within the infrastructure.
- Customers are responsible for patching their guest OS and applications.

- **Configuration Management**

- AWS is responsible for configuring the infrastructure devices.
- Customer is responsible for configuring their guest OSES, databases, and applications.

- **Awareness and Training**

- AWS trains the AWS employees.
- Customers train their employees.

- **Customer Specific**

Customers are responsible for the controls based on the applications they deploy within the AWS services.

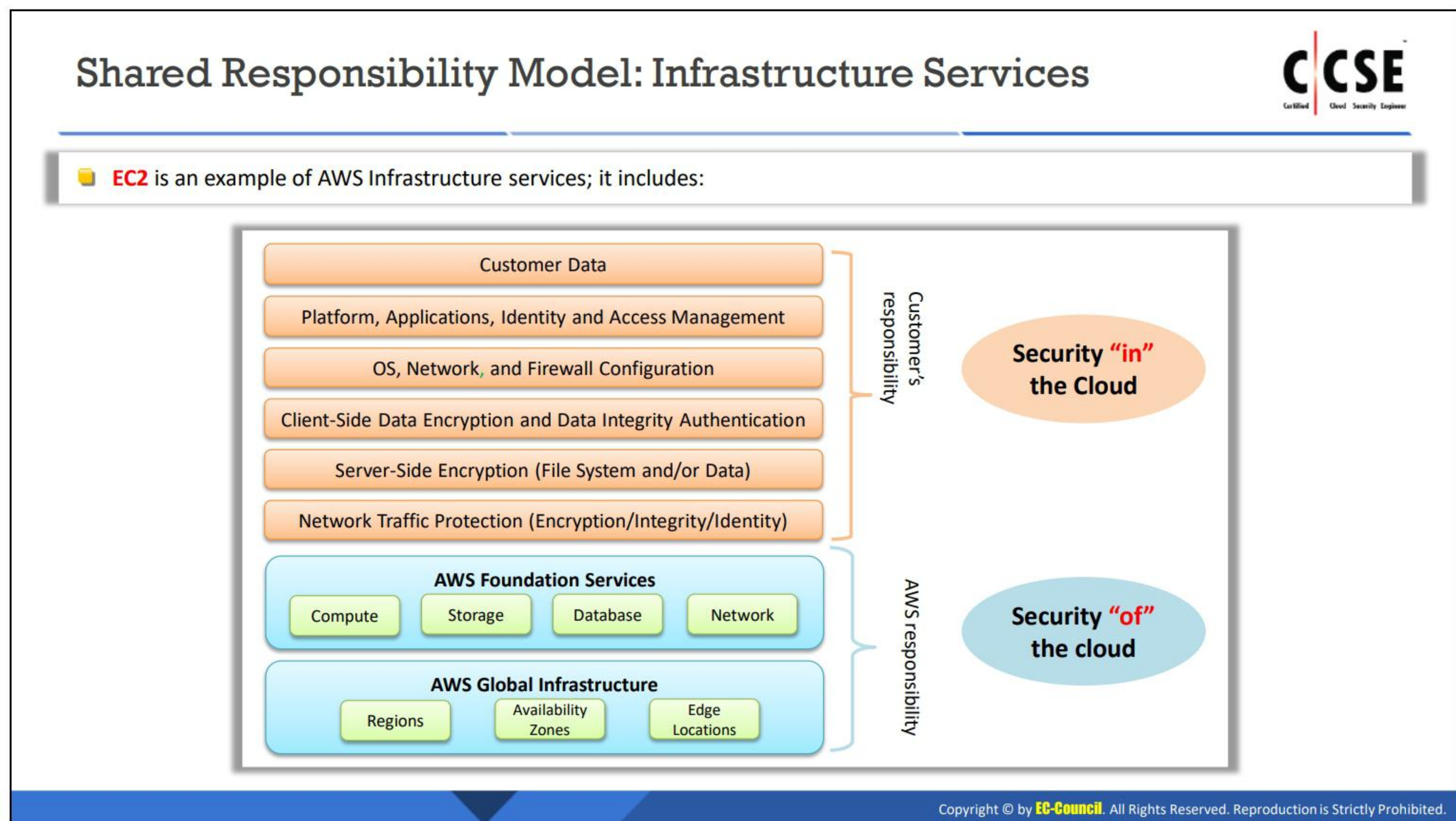
- **Service and Communication Protection/Zone Security**

Customers are responsible for routing or zoning data within specific security environments.

AWS devised three AWS shared responsibility models that represent the extent of AWS and customer responsibilities, and provide clear boundaries for each responsibility.

- Shared Responsibility Model for **Infrastructure Services**
- Shared Responsibility Model for **Container Services**
- Shared Responsibility Model for **Abstract Services**

hide01.ir



Shared Responsibility Model: Infrastructure Services

The AWS responsibility **Security "of" the Cloud** involves securing the infrastructure that runs the AWS cloud services. The infrastructure comprises hardware, software, networking, and other facilities/features that run the AWS cloud services. AWS is responsible for its global infrastructure elements that include

- Regions
- Availability Zones
- Edge Locations
- Foundation of AWS services such as compute, storage, database, and network.

AWS contains access controls to the data centers that store the customer data. It manages the components that constitute the cloud. Specifically, AWS includes controlling the physical access to

- Hardware components
- Networking components
- Generators
- Uninterruptible power supply (UPS) systems
- Power distribution units (PDUs)
- Computer room air conditioning (CRAC)
- Fire suppression systems.

Customer Responsibility – Security ‘in’ the Cloud

The customer manages the data in the cloud and is responsible for the cloud activities. The AWS cloud services determine the customer responsibilities. This helps in establishing the configuration work that should be performed by the customer as a part of their security responsibilities. For example, customers that deploy an Amazon EC2 instance are responsible for the management of the guest OS and applications installed on the instance along with the configuration of the AWS firewall on every instance. In the case of Amazon Simple Storage Service (S3) and Amazon DynamoDB abstracted services, customers access the endpoints to store and retrieve data, manage data, classify assets, and implement IAM tools for necessary permissions while AWS operates the infrastructure layer, OS, and platforms.

Specifically, the customer responsibilities include

- Client-side data encryption and data integrity authentication
- Server-side encryption (file system and/or data)
- Network traffic protection (encryption/integrity/identity)
- Security of OS, network, and firewall configuration followed by platform and application security, and IAM.

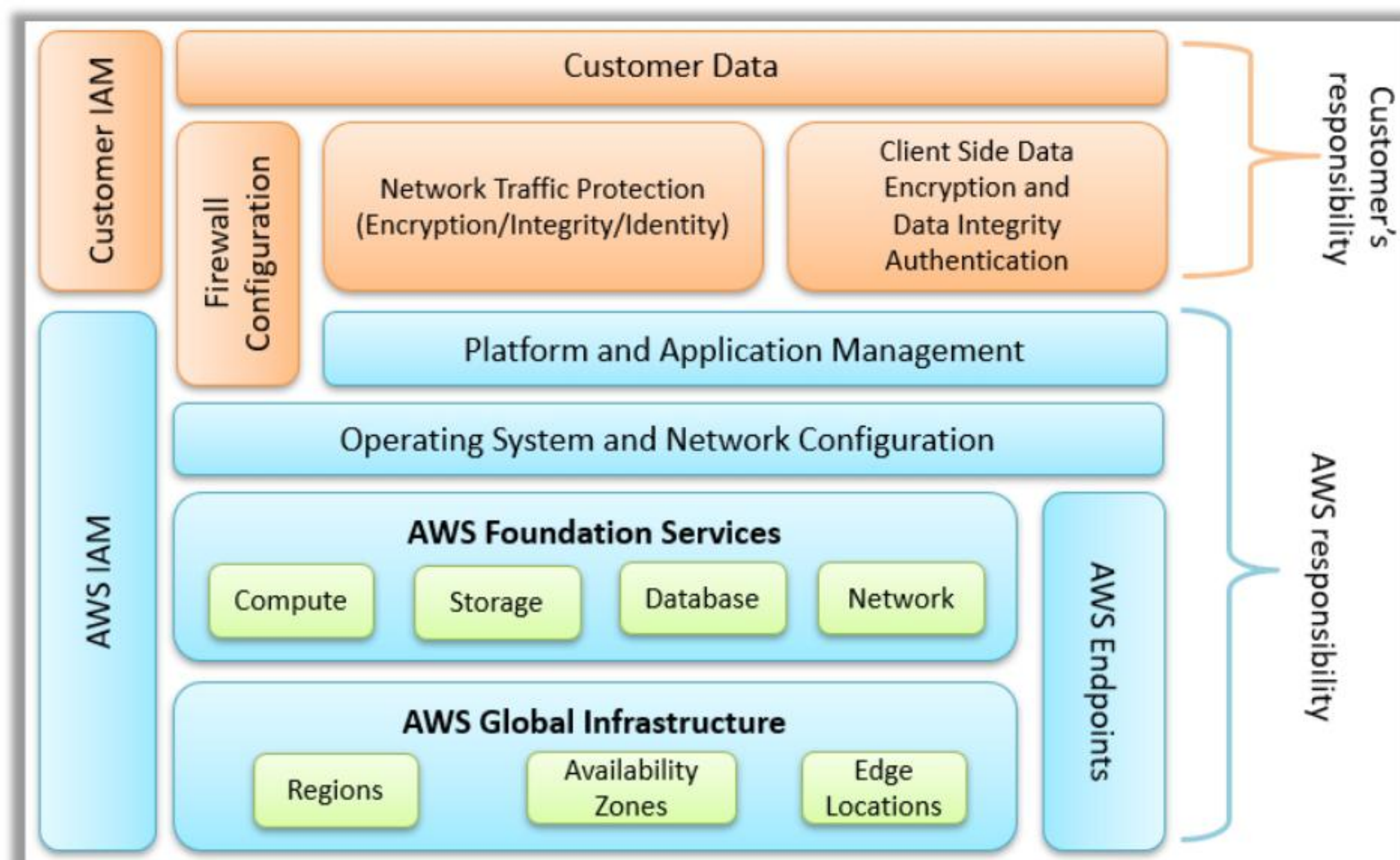
The implementation of additional security depends on the nature of the business, existing controls, and customer decisions. AWS provides its customers with several security controls; however, the application of these controls to a business depends on the customer.

Shared Responsibility Model: Container Services



Examples of AWS container services include:

- 1 AWS Relational Database Service (RDS)
- 2 AWS Elastic Map Reduce (EMR)
- 3 AWS Elastic Beanstalk



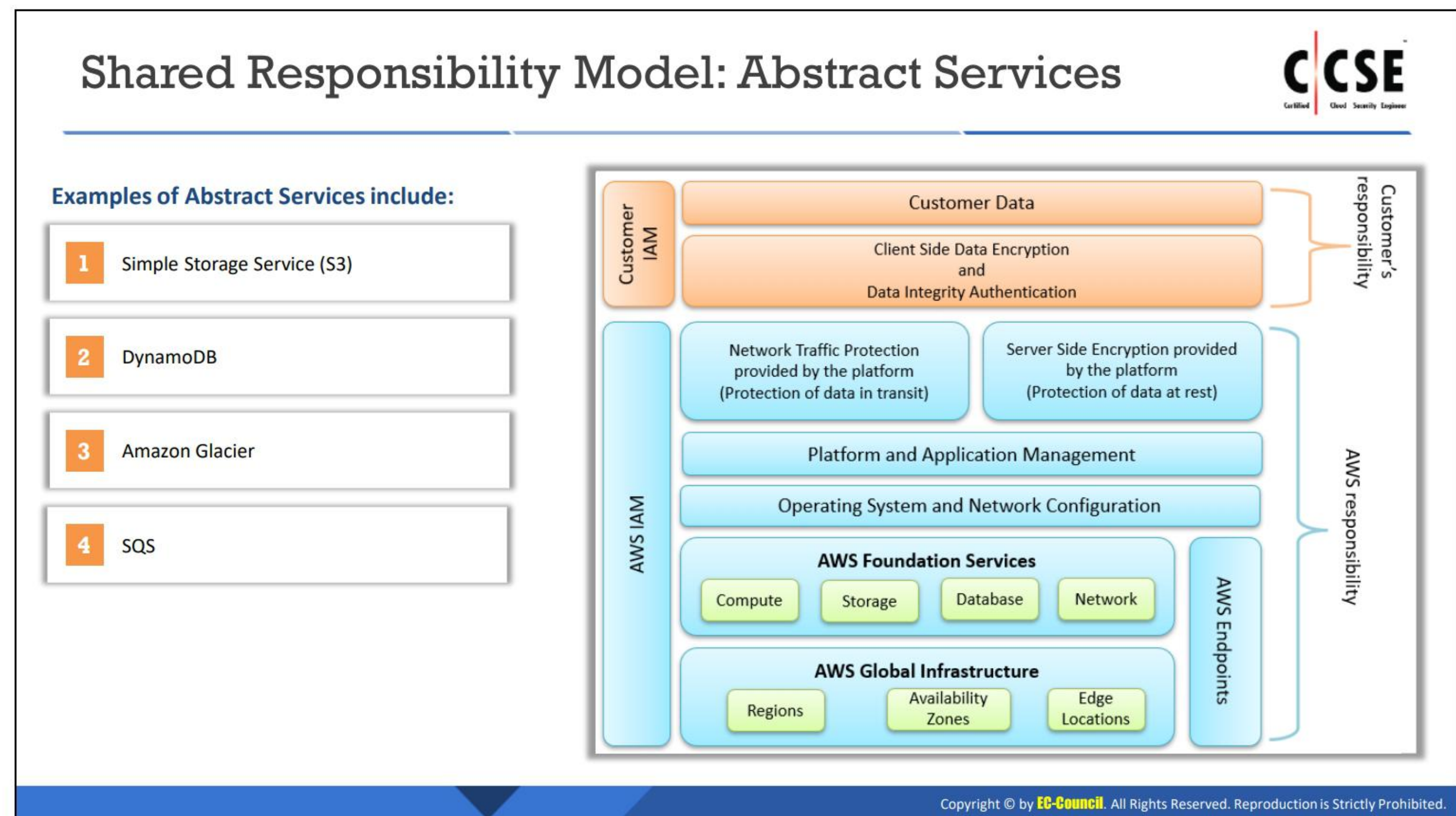
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Shared Responsibility Model: Container Services

The key difference between infrastructure-based and container services includes shifting the management of platform and application as well as the configuration of the OS and network to the AWS. The customer is responsible for the firewall configuration, which integrates at the platform and application management level.

Examples of AWS container services include:

- AWS relational database service (RDS)
- AWS Elastic MapReduce (EMR)
- AWS Elastic Beanstalk

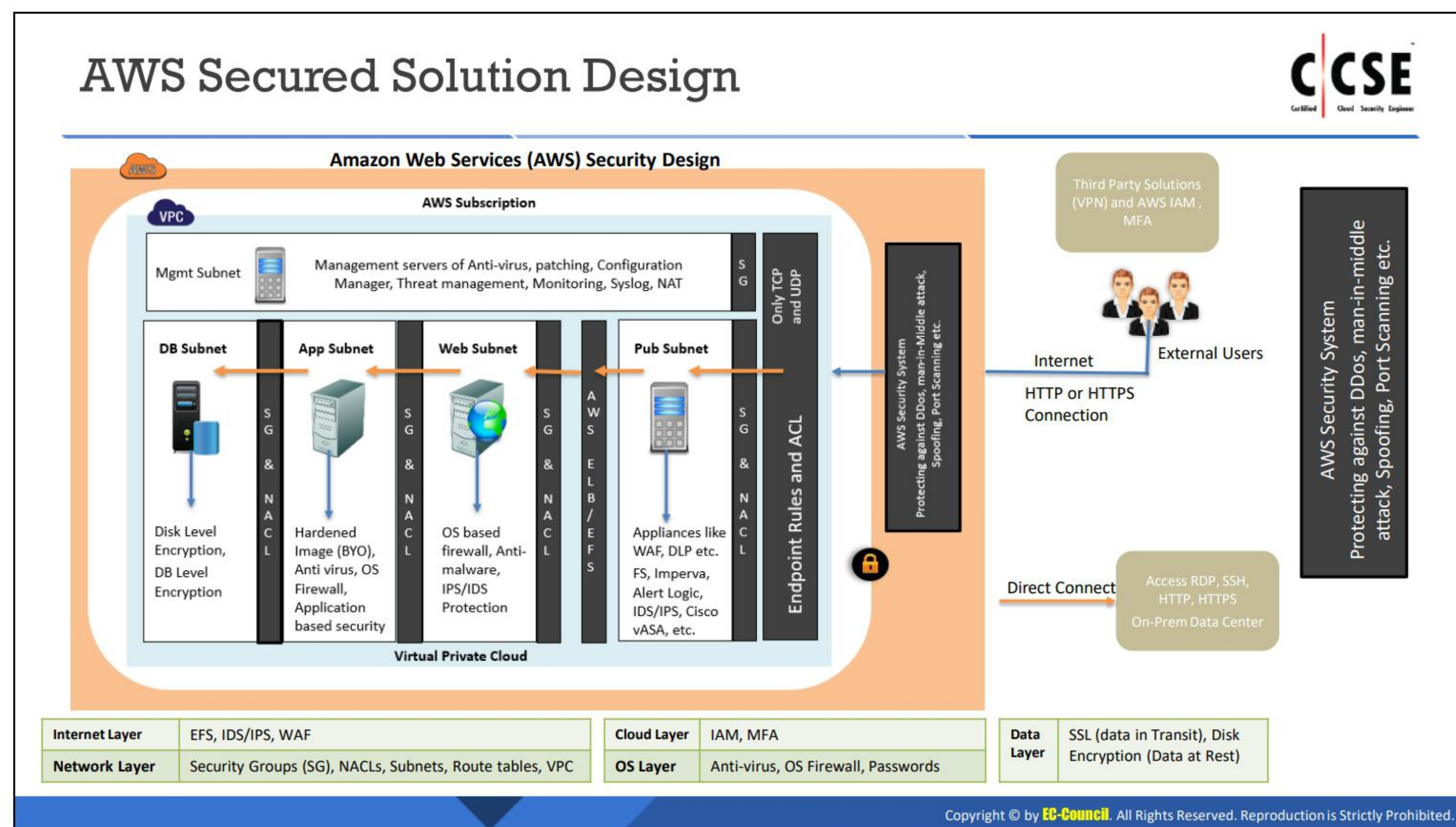


Shared Responsibility Model: Abstract Services

In the abstract service model, AWS takes more responsibilities such as network traffic protection. AWS manages network traffic protection through the platform by securing all data in transit using its own network. The customer is responsible for using IAM tools to implement necessary permissions on the platform and IAM user/group level. The responsibility and level of control shift more toward AWS with respect to each shared responsibility model.

Examples of abstract services include:

- Simple Storage Service (S3)
- DynamoDB
- Amazon Glacier
- SQS



AWS Secured Solution Design

Amazon Web Services (AWS) are based on the shared responsibility model between the AWS service providers and customer. AWS Security Measures encompass information security, system security, and asset security along with risk assessment and mitigation strategies to deliver business value.

Secured Solution Design

- Identity and Access Management:
 - To allow resource access to only authorized and authenticated users:
 - Define principals (users, groups, services, and roles that act in an AWS account).
 - Build policies aligned with the defined principals.
 - Implement strong credential management.
 - Use approaches such as
 - Protecting AWS credentials using multi-factor authentication (MFA)
 - Fine-grained authorization using IAM roles and policies.
- Detective Controls

As a key part of the governance frameworks, the detective controls (conducting inventory of assets and their detailed attributes, internal auditing, etc.) support:

 - Quality process
 - Legal and compliance obligation
 - Threat identification and response efforts

Consider the following approaches when addressing detective controls:

- Capture and analyze logs using AWS services such as CloudTrail, Amazon GuardDuty, AWS Config, and Amazon CloudWatch Logs.
- Integrate auditing controls with notification and workflow using AWS services such as CloudWatch events, AWS Config rules, and Amazon Inspector.

- Infrastructure Protection

Ensure the protection of the systems and services within the workload against vulnerabilities. Define:

- Trust boundaries (for example, network boundaries and packet filtering)
- System security configuration and maintenance (for example, hardening and patching)
- Operating system authentication and authorization (for example, users, keys, and access levels)
- Other policy-enforcement points (for example, web application firewalls and/or API gateways)

- Data Protection

To implement data protection in AWS and ensure the prevention of financial loss/compliance with regulatory obligations, consider approaches such as data classification, encryption/tokenization, data at rest security, data in transit security, and data backup/recovery.

- Incident Response

For incident response in AWS, consider approaches such as Clean Room using IAM, AWS CloudFormation, and AWS CloudTrail.



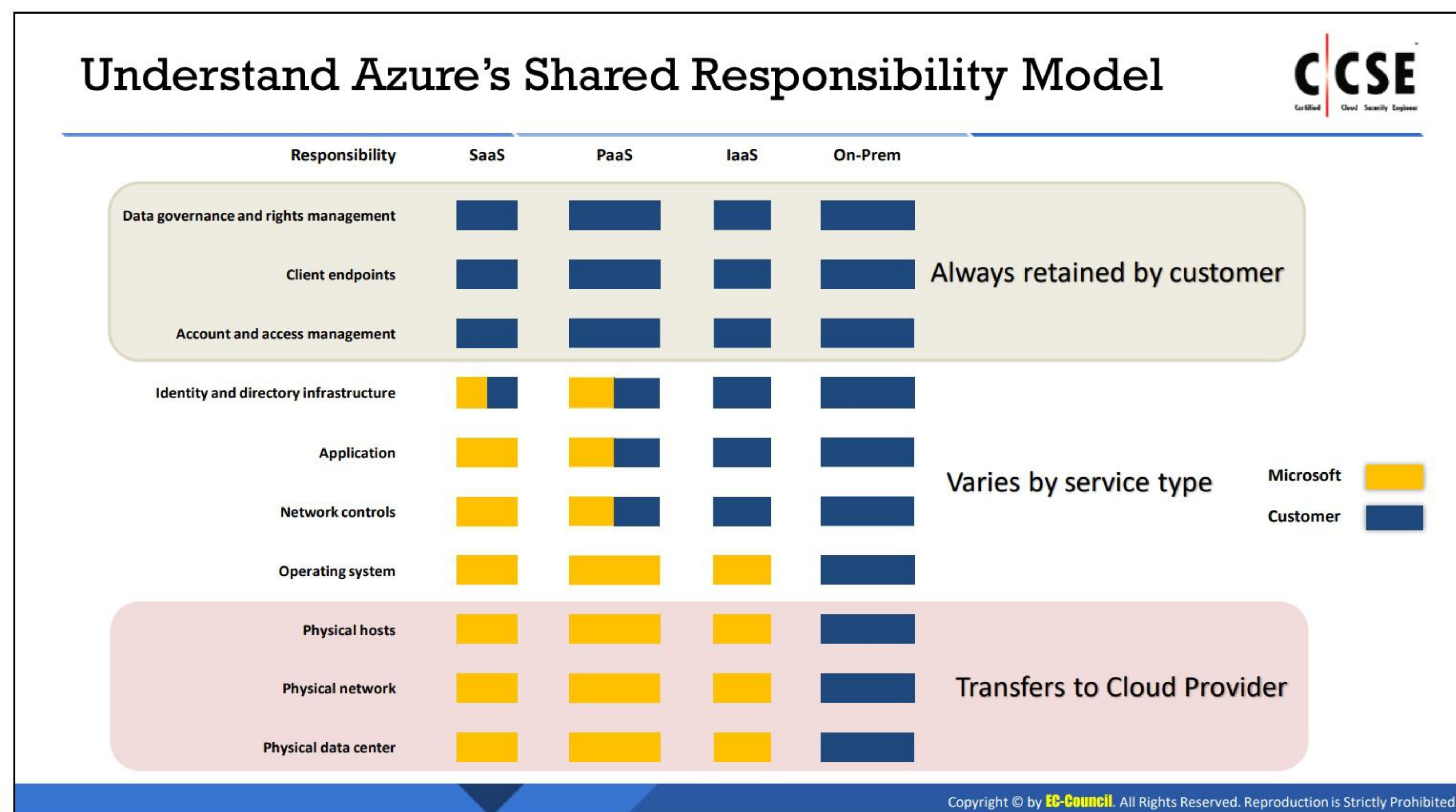
LO#06: Discuss Security Shared Responsibility Model in Microsoft Azure Cloud

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#06: Discuss Security Shared Responsibility Model in Microsoft Azure Cloud

This objective of this section is to explain Azure cloud Shared Responsibility Model and its secured solution design

hide01.ir



Understand Azure's Shared Responsibility Model

In the Microsoft Azure shared responsibility model, the customers and Microsoft Azure service providers share various responsibilities depending on the cloud service model (IaaS, PaaS, SaaS, or on-premise data center). The shared responsibilities include

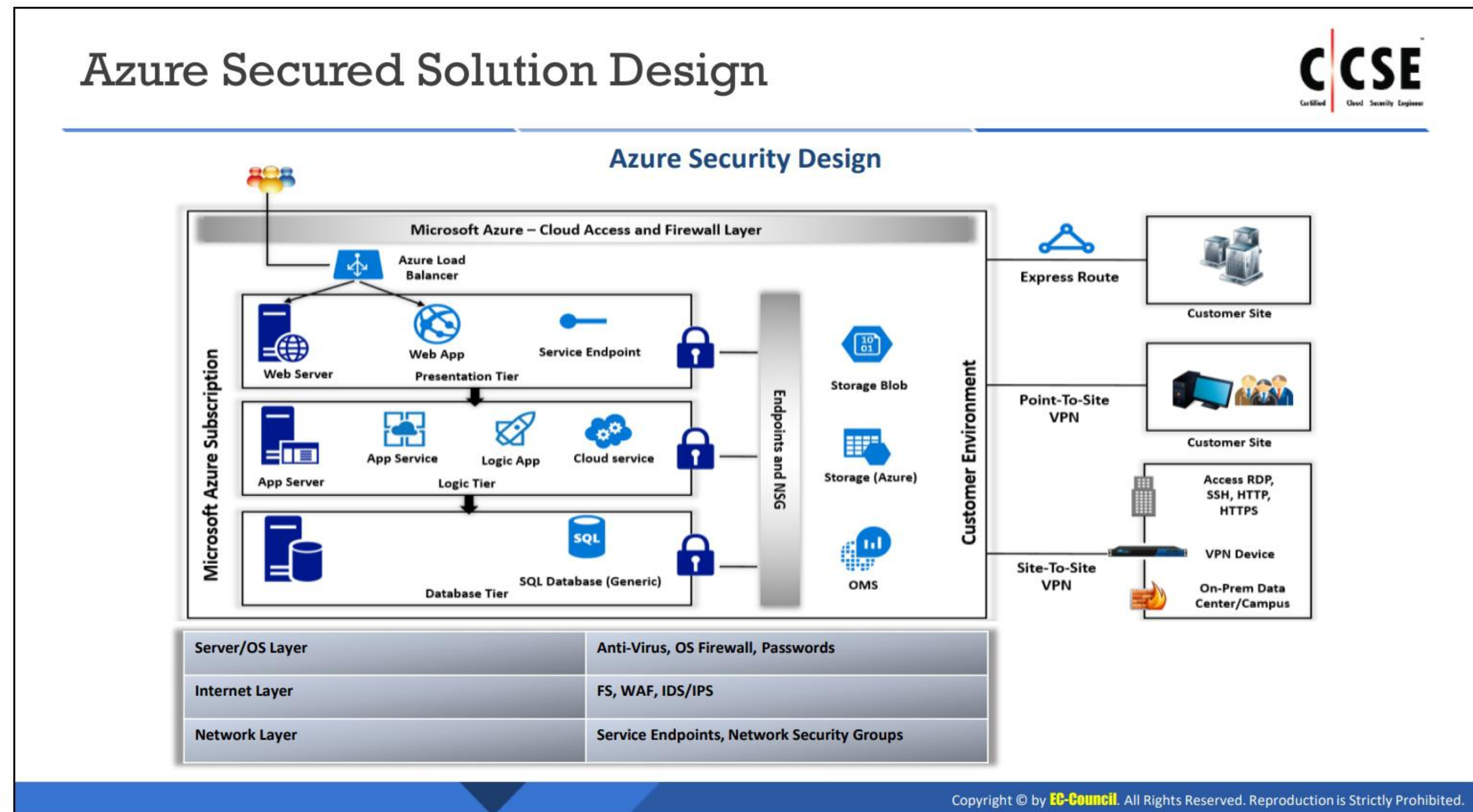
- Data classification and accountability
- Client and endpoint protection
- Identity and access management
- Application-level controls
- Network controls
- Host infrastructure
- Physical security

Cloud Service Model and Shared Responsibilities

- **SaaS:** The responsibilities of the information and data, devices (mobile and PCs), as well as accounts and identities are retained by the customer, whereas the responsibilities related to applications, network controls, operating systems (OSes), physical hosts, physical network, and physical data are owned completely by the Microsoft service provider. The identity and directory infrastructure responsibility is shared between the customer and Azure service provider. Because the customer owns the data and identities, it is the responsibility of the customer to secure the data and identities.

- **PaaS:** The responsibilities of information and data, devices (mobile and PCs), as well as accounts and identities are owned by the customer, whereas those related to the OS, physical hosts, physical network, and physical data are retained completely by the service provider. The responsibilities regarding the identity and directory infrastructure, applications, and network controls are shared between the customer and Azure service provider.
- **IaaS:** The responsibilities of information and data, devices (mobile and PCs), accounts and identities, identity and directory infrastructure, applications, network controls, and OS are completely retained by the customer, whereas those related to physical hosts, physical network, and physical data center are owned by the Azure service provider.
- **On-premises:** All responsibilities are retained by the customer.

hide01.ir



Azure Secured Solution Design

Microsoft Azure Cloud services are based on the shared responsibility model between the Azure service provider and customer.

Microsoft Azure Security Measures

- Secure data center against unauthorized access, interference, theft, fires, floods, etc.
- Infrastructure and services comply with critical protection laws.
- Maintain the Recovery Time Object (RTO), Recovery Time Point (RTP), and Failover in tier 3 or tier 4 data services.
- Continuous log audits.

Secured Cloud Design

Consumer Security Measures

The security measures on the customer cloud space should be satisfied and the Azure cloud service provider should take adequate security measures on-premise. The security measures aim to secure end-user access and end-to-end protection of the Azure cloud environment.

Identity management: For secure management, incorporate IAM with SSO and centralized AD. For the cloud root account, enable MFA.

Data encryption: Data encryption should be performed in the servers that host VMs, which provide encryption for the data in transit. The types of data that require encryption include

- Inactive data inside the cloud volume
- Entire cloud snapshots

- Total disk input/output

Network protection: Azure Endpoint and NSG provide protection at the network Level; however, the consumers are recommended to use an additional network layer of protection with Palo-Alto, Barracuda Solutions of WAF, and Firewall.

Secured solution design: Microsoft Azure ensures that the servers/services are placed in the following layers – Management, Public, Private, DMZ –to secure customer servers in the cloud.

hide01.ir



LO#07: Discuss Security Shared Responsibility Model in Google Cloud Platform (GCP)

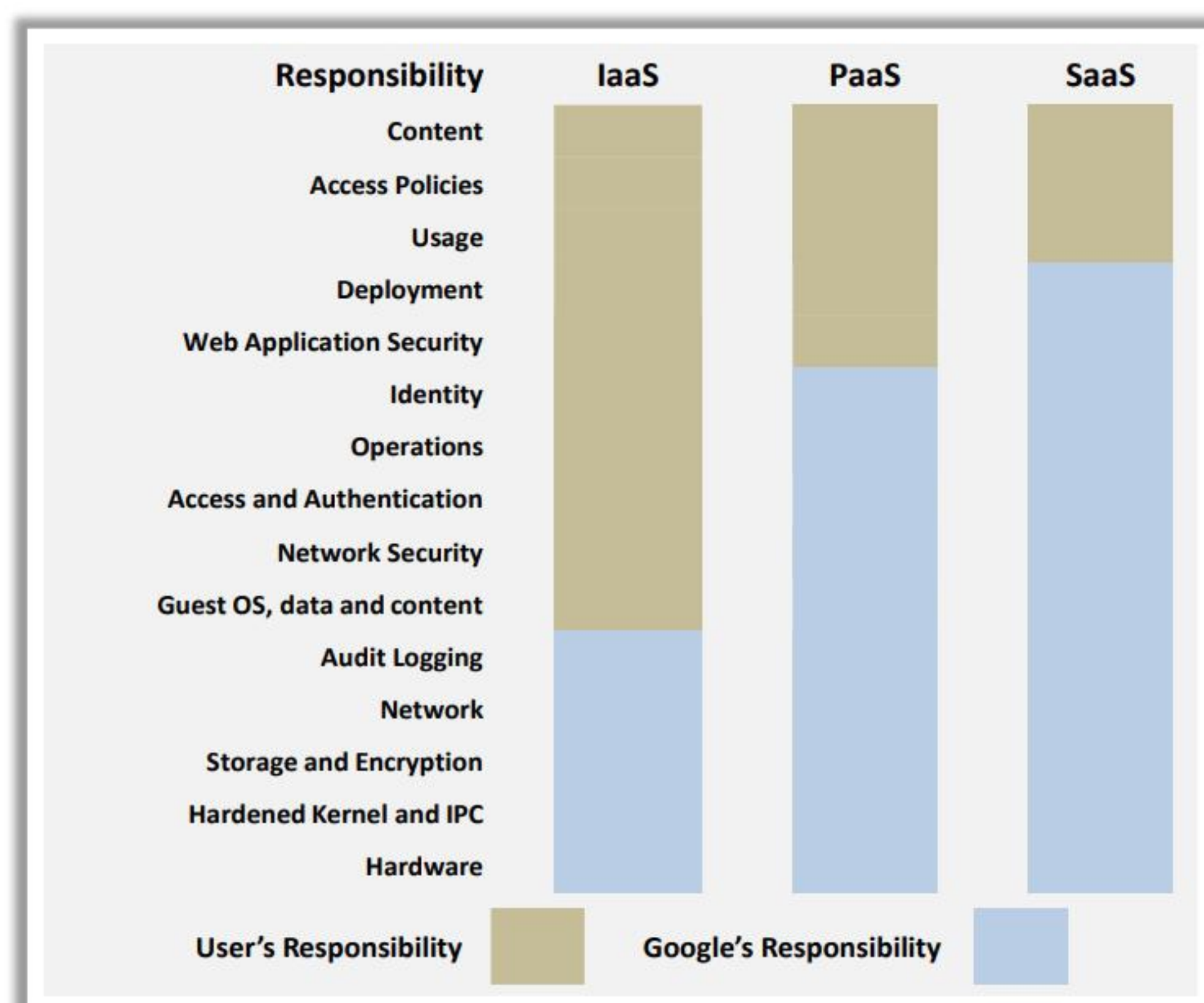
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LO#07: Discuss Security Shared Responsibility Model in Google Cloud Platform (GCP)

This section explains Google Cloud Platform (GCP) Shared Responsibility Model and its secured solution design

hide01.ir

Understanding Google Cloud Shared Responsibility Model



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Understanding Google Cloud Shared Responsibility Model

In the Google shared responsibility model, the users and Google cloud resource providers share the responsibilities based on the workload. The responsibilities are categorized as follows:

Infrastructure as a service layer: In the IaaS layer, the hardware, hardened kernel and IPC, storage and encryption, as well as network and audit logging are the responsibilities of the resource provider; meanwhile, guest OS, data and content, network security, access and authentication, operations, identity, web application security, deployment, usage, access policies, and content are the responsibilities of the user.

Platform as a service Layer: In the PaaS layer, the hardware, hardened kernel and IPC, storage and encryption, network, audit logging, guest OS, data and content, network security, access and authentication, operations, identity, and web application security are the responsibilities of the resource provider, whereas deployment, usage, access policies, and content are the responsibilities of the user.

Software as a service Layer: In the SaaS layer, the hardware, hardened kernel and IPC, storage and encryption, network, audit logging, guest OS, data and content, network security, access and authentication, operations, identity, web application security, deployment, and usage are the responsibilities of the resource provider, whereas access policies and content are the responsibilities of the user.

GCP Secured Solution Design



Google Infrastructure Security Layers

Operational Security			
Intrusion Detection	Reducing Insider Risk	Safe Employee Devices and Credentials	Safe Software Development
Internet Communication			
Google Front End		DoS Protection	
Storage Services			
Encryption at Rest		Deletion of Data	
User Identity			
Authentication		Login Abuse Protection	
Service Deployment			
Access Management of End User Data	Encryption of Inter-Service Communication	Inter-Service Access Management	Service Identity, Integrity, Isolation
Hardware Infrastructure			
Secure Boot Stack and Machine Identity	Hardware Design and Provenance		Security of Physical Premises

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

GCP Secured Solution Design

Google Infrastructure Security Layers are designed to secure internet services for the consumers and enterprises. They provide an overview of Google's holistic approach to explain the information processing lifecycle, which includes the hardware infrastructure at the lowest layer and the operational security layer as the highest layer consisting of various security measures to safeguard data security, privacy, and safety.

Hardware Infrastructure

- **Security of physical premises:** Google data centers implement strong physical security protection such as biometric identification, metal detection, cameras, vehicle barriers, laser-based intrusion detection systems, and access to a limited number of Google employees for certain roles and services.
- **Hardware design and provenance:** Google designed servers boards and networking equipment. For the identification and authentication of legitimate Google devices at the hardware level, Google designs include hardware security chips, which are deployed in the servers and peripherals.
- **Secure boot stack and machine identity:** BIOS, bootloader, kernel, and base operating systems image components of Google uses cryptographic signatures to validate at each boot or update. These components are built and controlled by Google. In Google data centers, the server machine has a specific identity for authenticating the API calls.

Secure Service Deployment

- **Service identity, integrity, and isolation:** For inter-service communication, Google uses cryptographic authentication and authorization.

- **Inter-service access management:** This feature of the GCP allows the service owners to specify the service that needs to be communicated with.
- **Encryption of inter-service communication:** The encryption of inter-service communication by Google provides security if the network is compromised.
- **Access management of end user data:** After receiving an end-user credential, Google passes it to the central identity service for verification. If the user credentials are verified, then the central identity service provides a short-lived end-user permission ticket, which is used for requests related to RPCs.

User Identity

- **Authentication/login abuse protection:** The Google central identity service provides a login page to users consisting of username and password. If Google identifies potential risks such as user login from unverified device, then it requests the user to provide additional information. After authenticating the user, the identity service allows access.

Secure Storage Services

- **Encryption at rest:** The Google storage service is configured to utilize keys from KMS for encrypting data before they are written on a disk.
- **Deletion of data:** Google does not delete the data directly; instead, it marks the data as scheduled for deletion to avoid unintentional deletions.

Secure Internet Communication

- **Google front end service:** It provides protection against Denial of Service (DoS) attacks, TLS termination, and public IP hosting of its public DNS name.
- **DoS protection:** The Google infrastructure has multilayer and multi-tier protection against DoS attacks that minimizes the risk of DoS impact on the services running behind the Google front end.

Operational Security

- **Safe software development:** Google creates infrastructure software securely by central source control, two-party review features, libraries preventing the release of security bugs, and manual security reviews.
- **Safe employee devices and credentials:** Google ensures that the infrastructure should be operated safely and protects the employee devices and credentials from vulnerabilities, sophisticated phishing, systems for scanning user-installed apps, downloads, and browser extensions.
- **Reducing insider risk:** Google monitors and limits the activities of employees with administrator roles in the infrastructure.
- **Intrusion detection:** The sophisticated data processing pipelines of Google are integrated with host-based signals on individual devices, monitoring points, and infrastructure service. The machine intelligence built on these pipelines provides warnings about the occurrence of incidents. The investigation and incident response team responds to the incident instantly.

Summary



- Cloud computing is an on-demand delivery of **IT capabilities** and provides Economic, Operational, Staffing, and Security benefits to the enterprise
- Data security, Compliance, Cost and Scalability are the core objectives of cloud security
- Risks arise according to **models employed**, operation models, and the technology used to enable the cloud service
- IAM is the management of the digital identities of users and their rights to access cloud resources
- Security logs are used for threat detection, data analysis, and compliance audits to enhance cloud security
- Before consuming a cloud service, it is important to perform a gap analysis on the security capabilities and services provided by the cloud service providers
- Cloud security is a shared responsibility, if the consumers do not secure their functions, the entire cloud security model will fail

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module described the features of enterprise cloud security. It provided insights about the various elements of cloud security that should be followed by an organization to secure the cloud. It highlighted the importance of evaluating the CSP before consuming cloud services and compared the security features provided by major cloud service providers. It discussed the security features provided by the Amazon cloud, Microsoft Azure cloud, and Google Cloud Platform.

This page is intentionally left blank.