EC-Council

C|CSE™

Certified Cloud Security Engineer

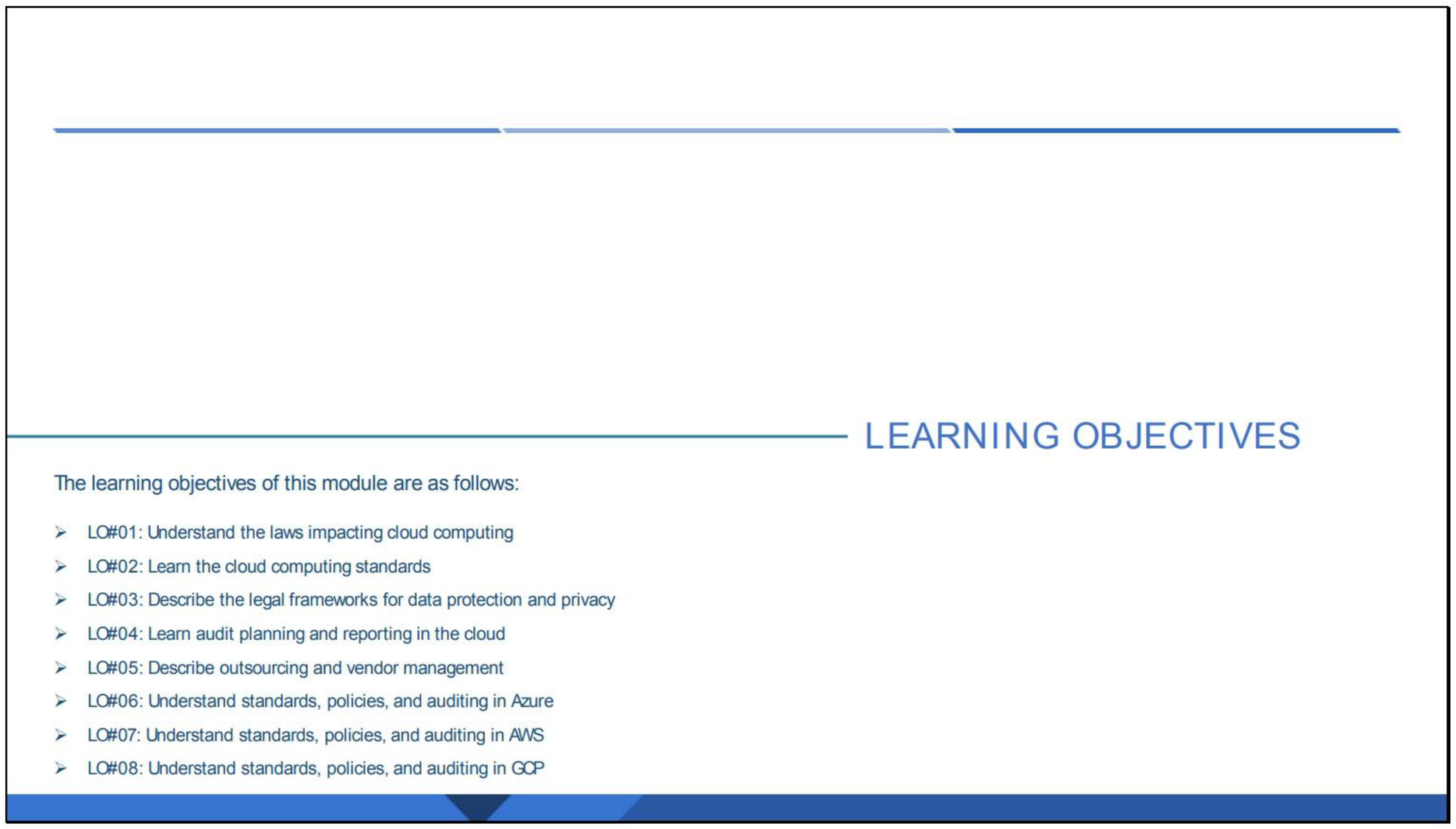

hide01.ir

Standards, Policies, and Legal Issues in Cloud

Module 11

This page is intentionally left blank.

hide01.ir



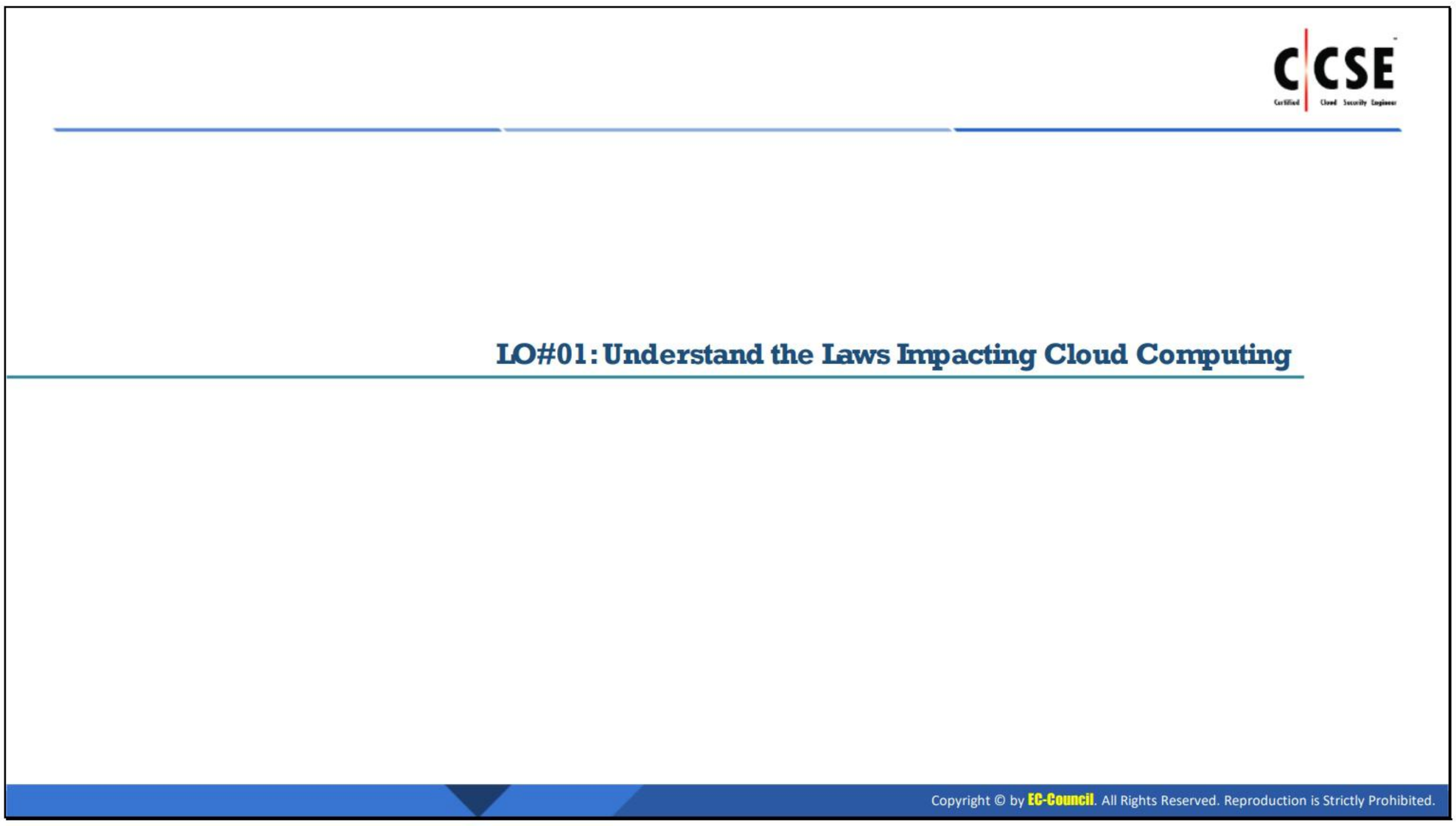
Learning Objectives

Every organization that adopts the cloud must adhere to the standards, policies, and regulations for managing the security risks, preventing any legal issues, and securing the cloud ecosystem. The regulations for cloud computing change continually, and cloud consumers should be aware of all the laws and standards related to cloud computing. This module helps cloud security engineers understand the laws impacting cloud computing and the various standards and policies applicable to the cloud. In addition, the module provides an understanding of cloud auditing and the standards, policies, and auditing in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

The learning objectives of this module are as follows:

- Understand the laws impacting cloud computing
- Learn the cloud computing standards
- Describe the legal frameworks for data protection and privacy.
- Learn audit planning and reporting in the cloud
- Understand standards, policies, and auditing in AWS
- Understand standards, policies, and auditing in Azure
- Understand standards, policies, and auditing in GCP
- Describe outsourcing and vendor management

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#01: Understand the Laws Impacting Cloud Computing

Every organization must follow certain laws and standards while using cloud platforms, and every cloud user must be aware of these laws and their impact on cloud computing. The objective of this section is to provide an overview of the laws that impact cloud computing and the legal risks associated with cloud computing. This section also demonstrates the legal challenges faced by the cloud user and cloud provider. Moreover, this section provides a checklist for protecting the data, contract termination, liability, and performance management.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Legal Risks in Cloud Computing

- Organizations using cloud platforms must satisfy/follow all legal standards, norms, and regulations related to cloud computing to avoid legal issues

Legal risks that impact cloud computing

Security procedures	Organizations that leverage cloud solutions and services without implementing proper security procedures face legal risks
Data ownership	Sensitive data hosted on the cloud can be accessed by the provider if the data center is located in a country without strong data privacy laws
Business continuity	Organizations using the cloud must be prepared for business continuity when they face a sudden disruption of their services. In such events, it is critical to provide continuous services to customers as per the SLAs and ensure their data security
Data privacy and data security	Failure to provide proper data security might cause several issues for the provider, including loss of customers, financial loss, lawsuits, and loss of reputation

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

Legal Risks in Cloud Computing (Cont'd)

hi0801.ir

Service levels	Failing to provide the level of services mentioned in the service-level agreement may result in legal risks
Service termination or suspension	Failing to notify customers regarding any violation of the agreement before service suspension or termination may cause legal risks for the provider
Jurisdictional issues	Different locations/countries have different laws regarding confidentiality and government access to data
Third-party access issues	The involvement of third parties in a multi-tenant shared cloud can be risky because they use the same admin interface to access cloud resources
Intellectual property rights	Intellectual property rights are not the same in all countries; therefore, there is ambiguity in the implementation of intellectual property laws to the cloud environment
Confidential data theft attacks	Cloud consumers must understand the disclosure policy of their cloud providers and determine how quickly the providers can alert their customers about a data breach

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

Legal Risks in Cloud Computing

While cloud computing provides multiple advantages to organizations, it is also associated with several legal risks or issues. Organizations should consider these legal issues while moving to a cloud environment. These issues/risks must be addressed effectively and in a timely manner to avoid legal penalties and actions. Organizations using cloud platforms must satisfy/follow all legal standards, norms, and regulations related to cloud computing to avoid legal issues.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are various legal risks that impact cloud computing.

- **Security Procedures**

  Organizations that leverage cloud solutions and services without implementing proper security procedures face legal risks. Organizations that do not have security measures to evaluate or approve cloud apps are also prone to legal risks. With the bring your own device (BYOD) trend, implementing such security procedures has become increasingly important. Organizations must establish security procedures to secure cloud data, apps, and services as per their objectives and workflows.

- **Data Ownership**

  Organizations must ensure that their customers' data hosted on the cloud cannot be accessed by unauthorized parties, including their staff. Customers are the only owners of their data, and their data must be protected at any cost. Cloud providers must follow all the applicable privacy laws of their countries to prevent any legal complications.

- **Business Continuity**

  Organizations using the cloud must be prepared for business continuity when they face a sudden disruption of their services. They should make proper arrangements to allow business operations to continue in case of unforeseen circumstances (e.g., a natural disaster, power outage, or hardware failure). In such events, it is critical to provide continuous services to customers as per the service-level agreements (SLAs) and ensure data security.

hide01.ir

- **Data Privacy and Data Security**

  Data privacy/security is the main concern for both the cloud provider and consumer as it can cause severe loss to their business and reputation. Insufficient data security can cause data breaches and expose critical information such as personally identifiable information (PII) and financial information. Failure to provide proper data security might cause several issues for the provider, including loss of customers, financial loss, lawsuits, and reputation loss.

- **Service Levels**

  A service-level agreement (SLA) is a contract between a cloud consumer and provider that establishes important service levels and expectations that are to be implemented without failure. Particularly, SLAs address important aspects such as availability, critical and noncritical outages, and planned outages. An SLA breach by the provider allows the consumer to receive a service credit to compensate for their loss and deter further SLA breaches.

- **Jurisdictional Issues**

  Data stored in a cloud data center located in a particular area are subject to the jurisdiction of that area. Any violation of rules regarding the stored data (such as a data breach or unauthorized data access) will be dealt with as per the jurisdiction of that area. However, storing the same data at multiple locations (having different jurisdictions and

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

legal systems) for better data usage and accessibility may result in many legal issues. Different locations/countries have different laws regarding confidentiality and government access to data. This can cause conflicting legal provisions for the data stored in different locations.

- **Service Termination or Suspension**

  Data stored or applications running in a cloud environment may be important/critical to an organization's business. In such a case, continuous access to the apps and data hosted on the cloud is crucial. The organization must ensure that the provider informs about each instance of violation of any agreement term before terminating or suspending the service. Moreover, the organization should confirm whether the provider gives an opportunity to fix or remedy any violation. The cloud service provider (CSP) must not restrict access to data for customers in the case of a service suspension.

- **Third-party Access Issues**

  The involvement of third parties in a multi-tenant shared cloud can be risky because they use the same admin interface to access cloud resources. In such cases, organizations should enhance security and implement multi-factor authentication (MFA) to improve protection. Furthermore, organizations that handle protected health information (PHI) must ensure that they work with providers complying with the Health Insurance Portability and Accountability Act (HIPAA) to meet privacy and security requirements. Consumers should always read the terms and conditions carefully before adopting a cloud service.

hide01.ir

- **Intellectual Property Rights (IPR)**

  Intellectual property rights (IPR) differ among countries; therefore, there is ambiguity in the implementation of intellectual property laws to a cloud environment. Organizations should be aware of the rights and regulations in the country where intellectual work is stored. Moreover, organizations should ensure that the CSP knows how to safeguard the stored intellectual property and prevent infringement pitfalls.

- **Confidential Data Theft Attacks**

  Most CSPs offer different security protection levels for their customers to protect their confidential data and apps, including encryption and the monitoring of data access. Cloud consumers must understand the disclosure policy of their providers and determine how quickly their providers can alert them about a data breach. Most countries (e.g., the US) have security breach disclosure laws that require CSPs to inform their customers about any breach when it occurs.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Laws Impacting Cloud Computing

- Various laws and regulatory standards are applicable to cloud computing environments because cloud computing is widely used and stores sensitive information such as customer details, credit/debit card details, PII, and PHI

The following are the most prominent laws that impact cloud computing

HIPAA	The Health Insurance Portability and Accountability Act (HIPAA) safeguards health-related data in cloud environments via its Privacy Rule and Security Rule
GLBA	The Gramm-Leach-Bliley Act (GLBA) applies to financial organizations that use the cloud to store financial data and regulates financial institutions via its Financial Privacy Rule and Safeguards Rule.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) applies to merchants and payment processors using the cloud to store and process payment-related information and specifies best practices for data privacy, perimeter security, and layered security
FERPA	The Family Educational Rights and Privacy Act (FERPA) safeguards student data gathered by educational organizations and the associated vendors
ISO 27018	This EU law, introduced by ISO, provides an auditable compliance framework for CSPs and promotes trust and wide adoption of cloud computing in all economic sectors to boost productivity

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

Laws Impacting Cloud Computing (Cont'd)

h1de01.ir

CLOUD	Clarifying Lawful Overseas Use of Data (CLOUD), a US law, allows **trans-border access** to communications data during criminal investigations
GDPR	The General Data Protection Regulation (GDPR) law obligates the party that holds and processes **personal data** for any purpose to take the **sole responsibility** of securing the data
UK Data Protection Act	This law requires data controllers to ensure that appropriate organizational and technical measures are used to process **personal data** to avoid unauthorized data processing or accidental data loss
USA PATRIOT Act	This US law enables gaining access to data stored under its jurisdiction for **anti-terrorism or e-discovery purposes**
ECPA	The Electronic Communications Privacy Act (ECPA) regulates the way US law enforcement officials can **access data stored in the cloud** and foreign countries
SCA	The Stored Communication Act (SCA) restricts the government's ability to force ISPs to **disclose information** that is stored with them
FISMA	The Federal Information Security Management Act (FISMA) highlights the importance of **information security** to the US's economic and national security interests

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

Laws Impacting Cloud Computing

Various laws and regulatory standards are applicable to cloud computing environments because of their prominence and wide use. Organizations store their corporate data in the cloud. Such data include sensitive information such as customer details, credit/debit card details, PII, and PHI.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Several countries have imposed laws and regulations on both the cloud providers and tenants to protect and secure data stored in the cloud.

Different laws and regulations apply to cloud computing environments. The most prominent laws that impact cloud computing are as follows.

- **HIPAA**: The Health Insurance Portability and Accountability Act (HIPAA) safeguards health-related data in cloud environments. It specifies the following two rules.
    - **Privacy Rule**: In the Privacy Rule, an entity (individual or organization) cannot reveal or utilize protected health information (PHI) of any individual unless the Rule allows it or the affected individual allows it through a written statement.
    - **Security Rule**: The Security Rule of HIPAA applies to electronic protected health information (EPHI) and compliments the Privacy Rule. For compliance, the rule needs three types of security safeguards: physical, technical, and administrative. In addition, different security standards are determined by the Rule for each type. Organizations should adapt and administer the required specifications as per the Rule.
- **Gramm–Leach–Bliley Act (GLBA)**: The GLBA applies to financial organizations that use the cloud to store financial data. It specifies two rules for financial organizations utilizing cloud ecosystems.
    - **Financial Privacy Rule**: This Rule requires financial organizations to update customers regarding the personal information that was collected, such as where the customers' personal information is stored, with whom the information is shared, how the information is secured, and how the information is utilized.
    - **Safeguards Rule**: This Rule requires financial institutions to create an information security plan that specifies actions and measures they will take to secure the private personal information of their clients.
- **Payment Card Industry Data Security Standard (PCI DSS)**: PCI DSS applies to merchants and payment processors that use the cloud to store and process payment-related information. Visa and MasterCard unitedly developed PCI DSS to make compliance easy for payment processors and merchants. This standard specifies best practices for layered security, perimeter security, and data privacy. Compliance with PCI DSS is mandatory for all organizations that handle and process payments and transactions.
- **Family Educational Rights and Privacy Act (FERPA)**: FERPA safeguards student information gathered by educational organizations and the associated vendors. This law states that educational institutions should take students' consent before disclosing personal information such as enrollment status, grades, and billing information. FERPA regulations protect students' information stored in cloud-based applications.
- **International Organization for Standardization (ISO) 27018**: It is a law of the European Union (EU) introduced by ISO that provides an auditable compliance framework for CSPs and promotes trust in and wide adoption of cloud computing in all economic sectors to boost productivity. It is the first privacy-specific international standard for cloud

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

computing that aims to create a common collection of security controls that public CSPs can easily implement as data processors. ISO 27018 helps cloud customers select CSPs by evaluating them against its privacy and data protection laws.

- **Clarifying Lawful Overseas Use of Data (CLOUD)**: CLOUD is a US law that allows trans-border access to communications data during criminal investigations. The data of a US resident can be accessed by other countries (having executive relations with the US), if stored outside the US. Under this law, foreign governments can request information on any US resident from US tech companies. US fintech companies have the right to cancel the request within 14 days if the person about whom the information is requested is not a US resident or the requested disclosure would create a risk of violating laws.
- **General Data Protection Regulation (GDPR)**: Under GDPR, the party that holds and processes personal data for any purpose has the sole responsibility to secure the data. Organizations that gather data of people living in EU countries must comply with GDPR rules to protect customer data. It holds data processors accountable for non-compliance or breaches. Here, processors refer to the organization as well as its partner (e.g., a cloud provider). Both will be penalized if even one of them is responsible for a breach. It places equal responsibility on data controllers (data owners) and data processors (that help manage data). GDPR requires organizations to inform their customers about their rights and create revised plans that define standard processes for managing and protecting data and reporting data breaches.
- **UK Data Protection Act:** This law obliges data controllers (data owners) to include certain provisions in their contracts with data processors (e.g., CSP). It requires the data controllers to ensure that appropriate organizational and technical measures are used to process personal data to avoid unauthorized data processing or accidental data loss.
- **USA PATRIOT Act:** This Act grants the US government access to data stored under its jurisdiction for anti-terrorism purposes. Under this law, the government must have a search warrant or subpoena to access data in the cloud. The CSP can respond to the search warrant depending on the case. Some CSPs cooperate without hesitation and provide access to data, whereas others object to search warrants.
- **Electronic Communications Privacy Act (ECPA):** ECPA regulates how US law enforcement officials can access data stored in the cloud and foreign countries. Under ECPA, compared to data stored in a PC, data stored in the cloud can be subject to a lesser standard for access through the enforcement of this law. Through terms of service (ToS) and SLAs, CSPs notify their customers that they can disclose information to law enforcement when requested via a legal process.
- **Stored Communications Act (SCA):** The SCA of the USA aims to promote the use and development of new methods of communications by securing the privacy rights of citizens. This law restricts the government's ability to force Internet service providers (ISPs) to disclose information stored with them. Under this law, service providers (including CSPs) are defined as electronic communications services (ECSs) and remote

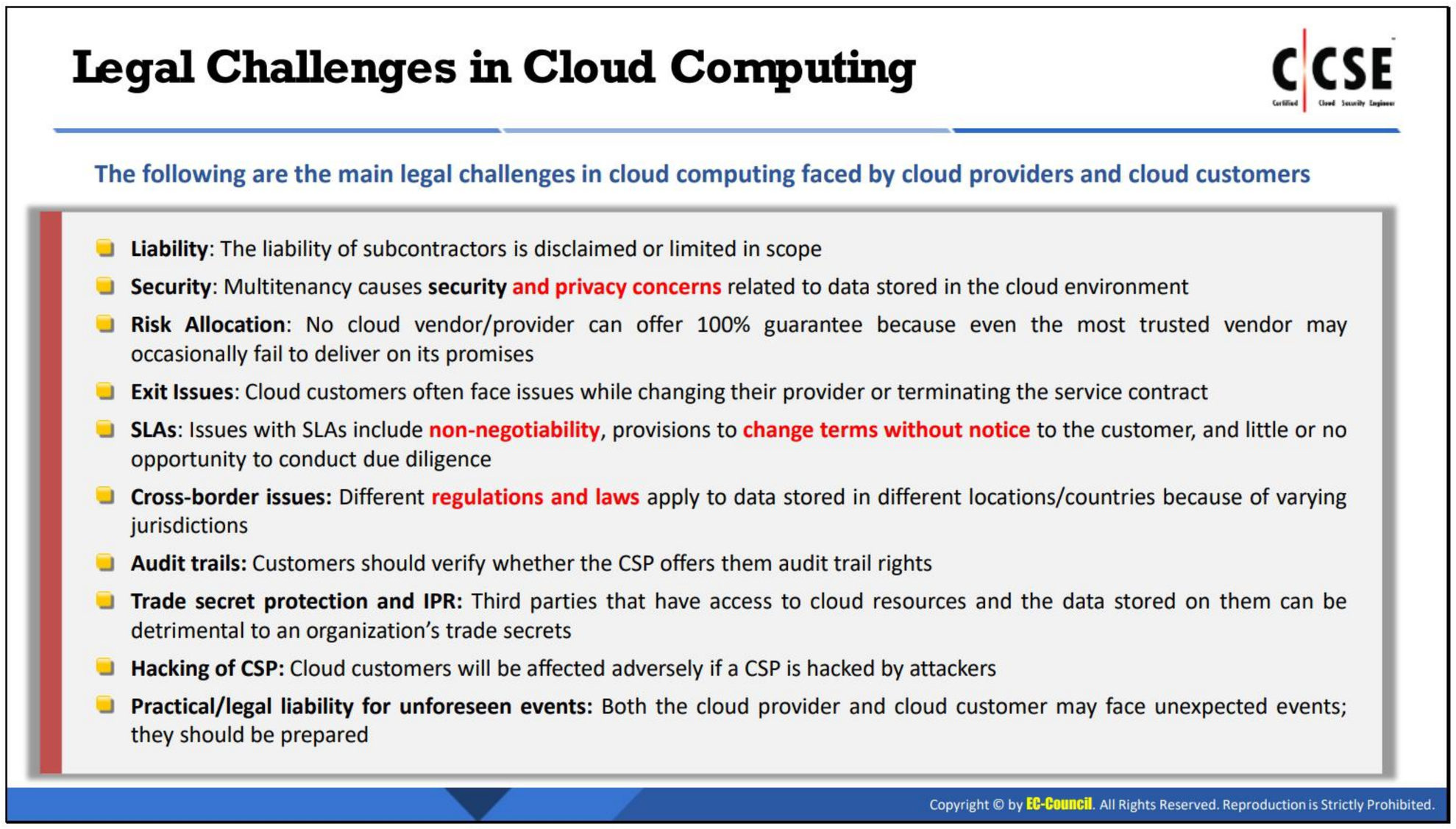
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

computing services (RCSs). Based on the category of the service provider and for how long the communication was stored, privacy protection is provided by this law.

- **Federal Information Security Management Act (FISMA):** FISMA was enacted in the US to highlight the importance of information security to the US's economic and national security interests. It offers a uniform system to address the risk levels that arise from both international and domestic sources. This law requires federal agencies to implement some programs to review information security and then report the results to the Office of Management and Budget (OMB). Through the Federal Cloud Computing Initiative, the program offers a standardized strategy for various security measures such as authorization, security assessment, and monitoring for cloud services.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Legal Challenges in Cloud Computing

In cloud computing, cloud providers and customers face various legal challenges. The following are the main legal challenges in the cloud.

hide01.ir

- **Liability**

  As multiple parties are involved in cloud services, the liability and responsibility of a breach are unclear. The liability of subcontractors is disclaimed or limited in scope. The client cannot bind a provider for a data or security breach owing to a lack of contractual privity between parties. Therefore, the agreement should include the liability of the CSP for acts performed by subcontractors. The customer must understand the service delivery model and exercise due diligence.

- **Security**

  In cloud computing, several virtual servers run on a single physical server, and there are multiple tenants on a server. A single virtual server hosts data of several users. This causes security and privacy concerns related to the data stored in the cloud environment. Data security and privacy are dependent on the integrity of virtualization.

- **Risk Allocation**

  Proper risk allocation is essential for managing and mitigating risks and minimizing losses and service outages. Cloud consumers must ensure that the contract agreement specifies the risk allocation terms. This helps both the provider and consumer know and implement their security as per the responsibilities defined in the agreement. No cloud vendor/provider can offer 100% guarantee because even the most trusted vendor may occasionally fail to deliver on its promises. Therefore, consumers must ensure that their

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

data are replicated, and applications are available at multiple sites. They can also opt for risk insurance in case their business shuts down because of any problem at the vendor end or the vendor getting hacked.

- **Exit Issues**

  Cloud customers often face issues while they change their provider or terminate the service contract. The options of interoperability and portability should be considered when a customer desires to change the CSP. While changing the CSP or service termination, the customer should consider the following questions:

  - Can the data records be accessed?
  - Can the data be extracted from the cloud?
  - What will be the obligations of both parties while exiting?

- **Service-level Agreements**

  Cloud providers and consumers sign a non-negotiable agreement known as a service-level agreement (SLA), based on which cloud services are provided to cloud consumers. The CSP must adhere to the terms and conditions in the SLA and is accountable if it cannot fulfill the SLA terms. SLAs must have options that allow the customer to terminate the contract if the CSP does not provide services as per the SLA, the CSP makes changes to the SLA terms, etc.

  Some common issues with SLAs are as follows:

  hidedl.ir

  - Non-negotiable
  - Little or no opportunity to conduct due diligence
  - Strong limits on liability
  - Risk is transferred to cloud users via provider-friendly agreements
  - Use of standard mass-market contracting terms
  - Terms can change without notice

- **Cross-border Issues**

  Different regulations and laws apply to data stored in different locations/countries owing to varying jurisdictions. Data can easily flow from one location to another in a cloud environment. The same data can have multiple legal provisions and regulations while stored, accessed, or used in various countries or locations. Cross-border data flow and potentially conflicting regulations may cause problems for the CSP. Complying with different regulations is also a challenge in cloud computing.

- **Audit Trails**

  Data move continuously between cloud services in a cloud environment. The cloud customer (data owner) has the right to know where their data travel; where is the data are stored; and who is accessing, transferring, or altering the data. This information can

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

be determined through audit trials. The cloud customer should verify whether the CSP offers audit trail rights to the customer.

- **Trade Secret Protection and IPR**

  In a cloud environment, various third parties have access to cloud resources and the data stored in it. This can be detrimental to an organization's trade secrets. To prevent third parties from disclosing trade secrets, the organization must make third-party vendors sign a non-disclosure agreement. Moreover, they must ensure via a written agreement that no intellectual property rights (IPR) are transferred to third-party vendors.

- **Hacking of CSP**

  Cloud environments are prone to cyber threats in the same manner as on-premises IT systems. If a CSP is hacked by attackers, cloud customers will be affected adversely. Such an incident may cause financial and reputational losses to the CSP. To address this issue, cloud consumers must ensure that the data controller (data owner) has the right to move against the CSP or vendor (legally) to raise a claim for the loss when cloud systems are hacked.

- **Practical/Legal Liability for Unforeseen Events**

  Both the cloud provider and cloud customer may face unexpected events and should be prepared for them. These events include natural disasters and unexpected hardware failure. During such an event, the following questions arise:

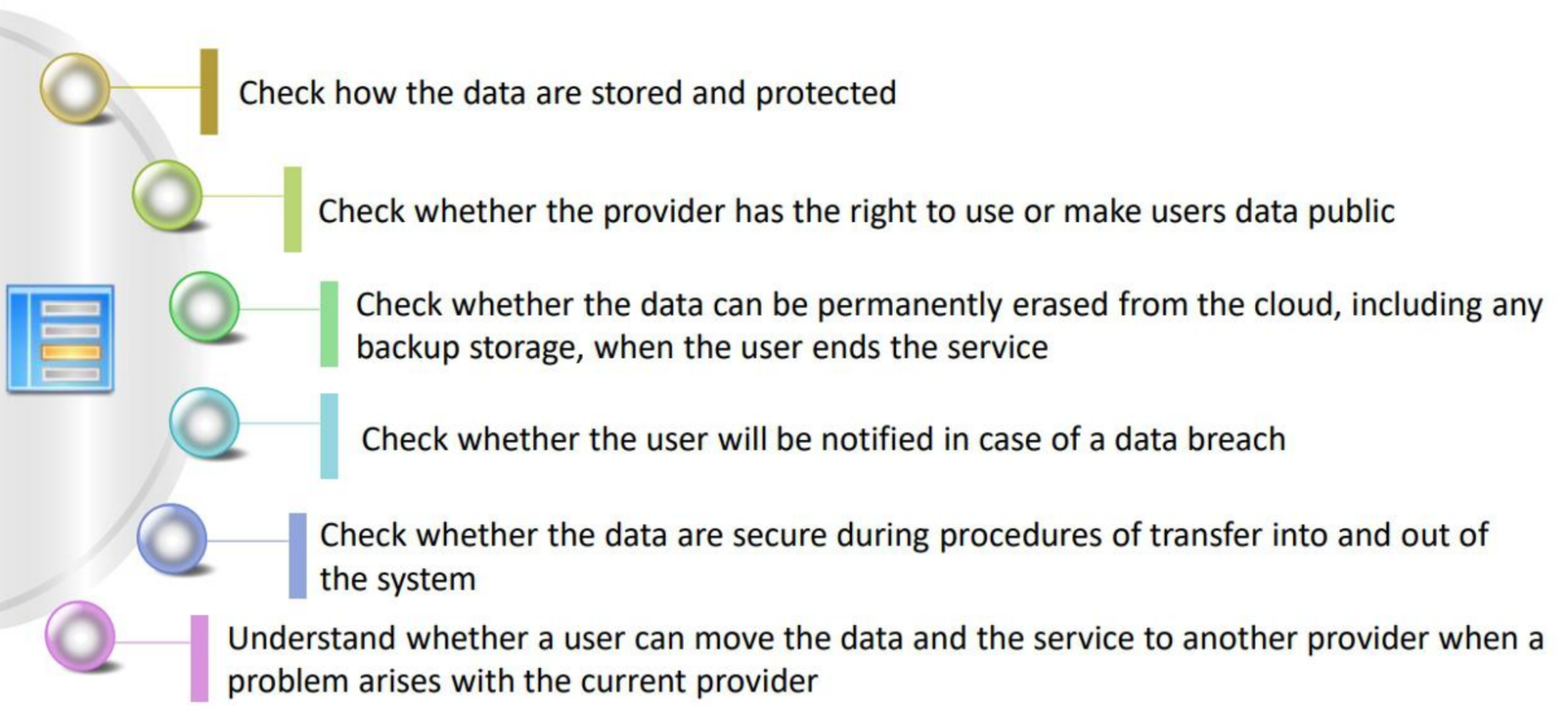
  - What will happen to the owner's data?
  - How much is the cloud provider responsible for the data recovery and restoration?
  - What backup mechanisms will be used to recover the data?

hidden01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Legal Checklist for Protection of Information

- Customers should question and clarify the following issues from a cloud provider prior to selecting the provider

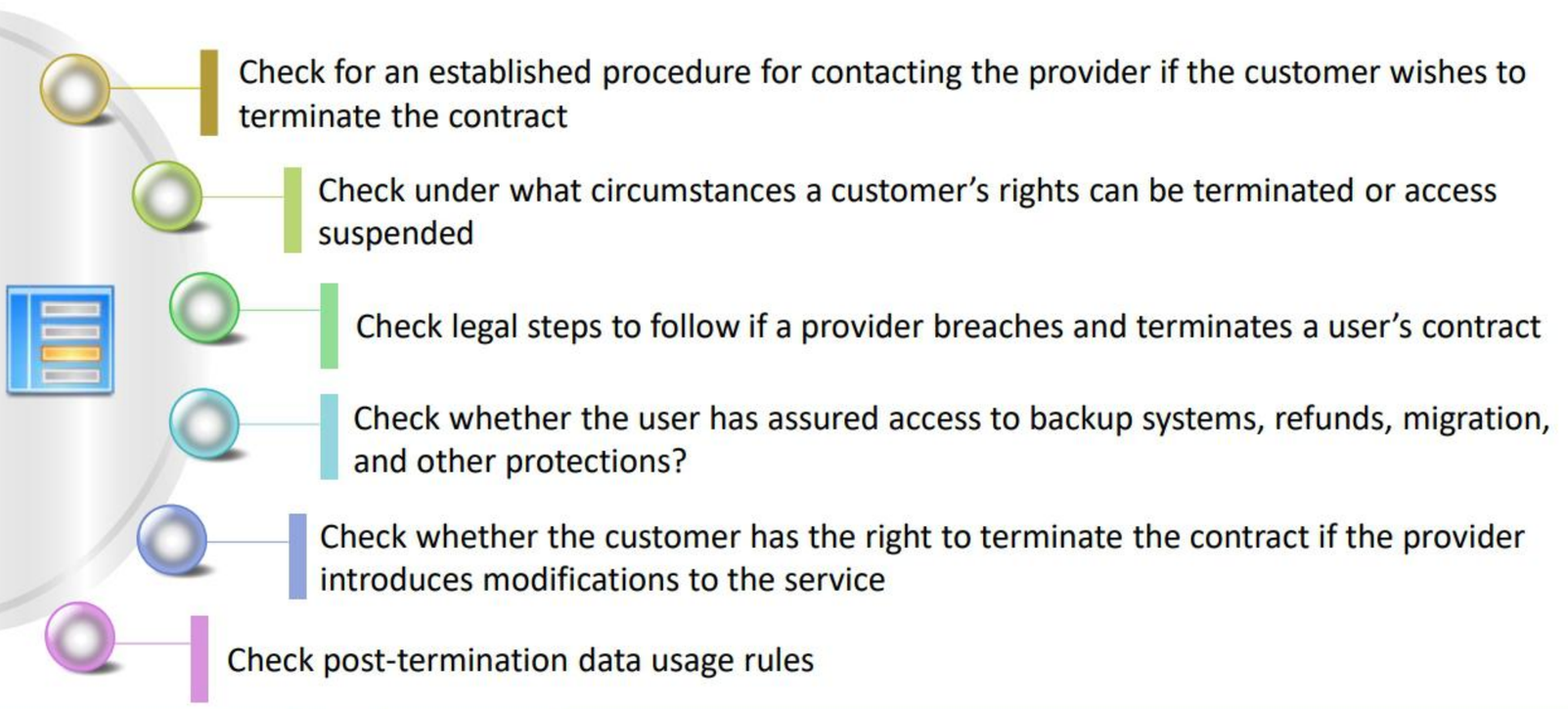


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Legal Checklist for Contract Termination

- Customers should question and clarify the following issues from a cloud provider prior to selecting the provider.

hide01.ir

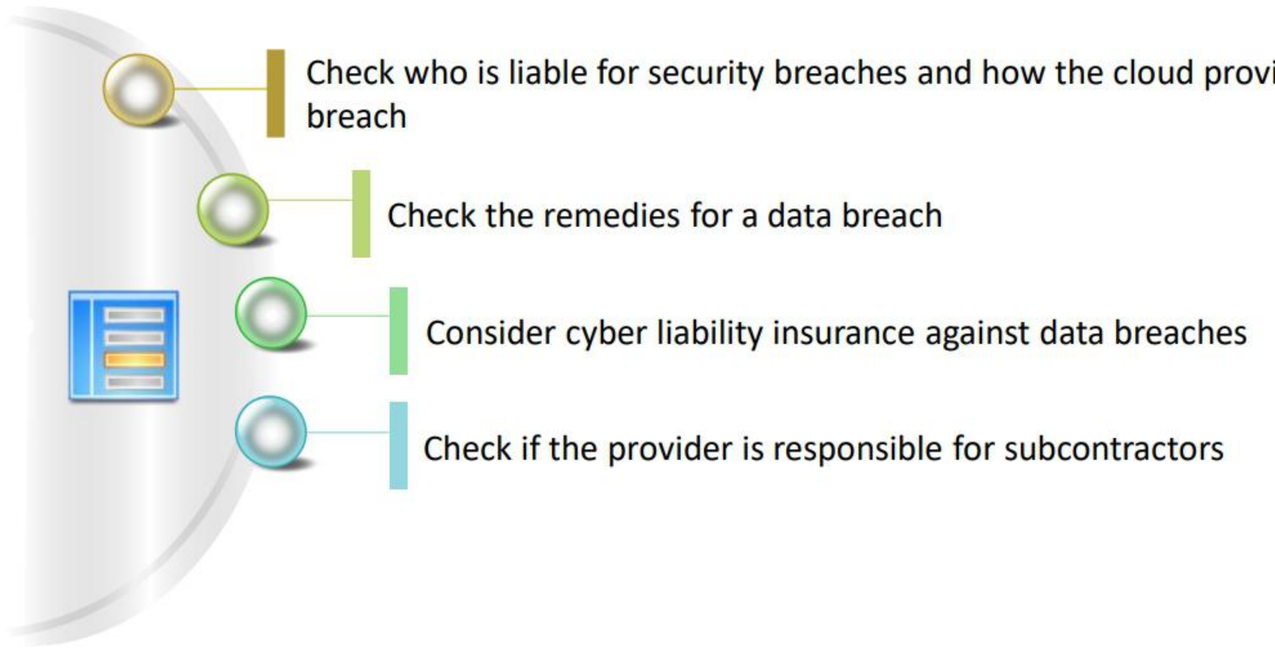


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Legal Checklist for Liability

- Customers should question and clarify the following issues from a cloud provider prior to selecting the provider

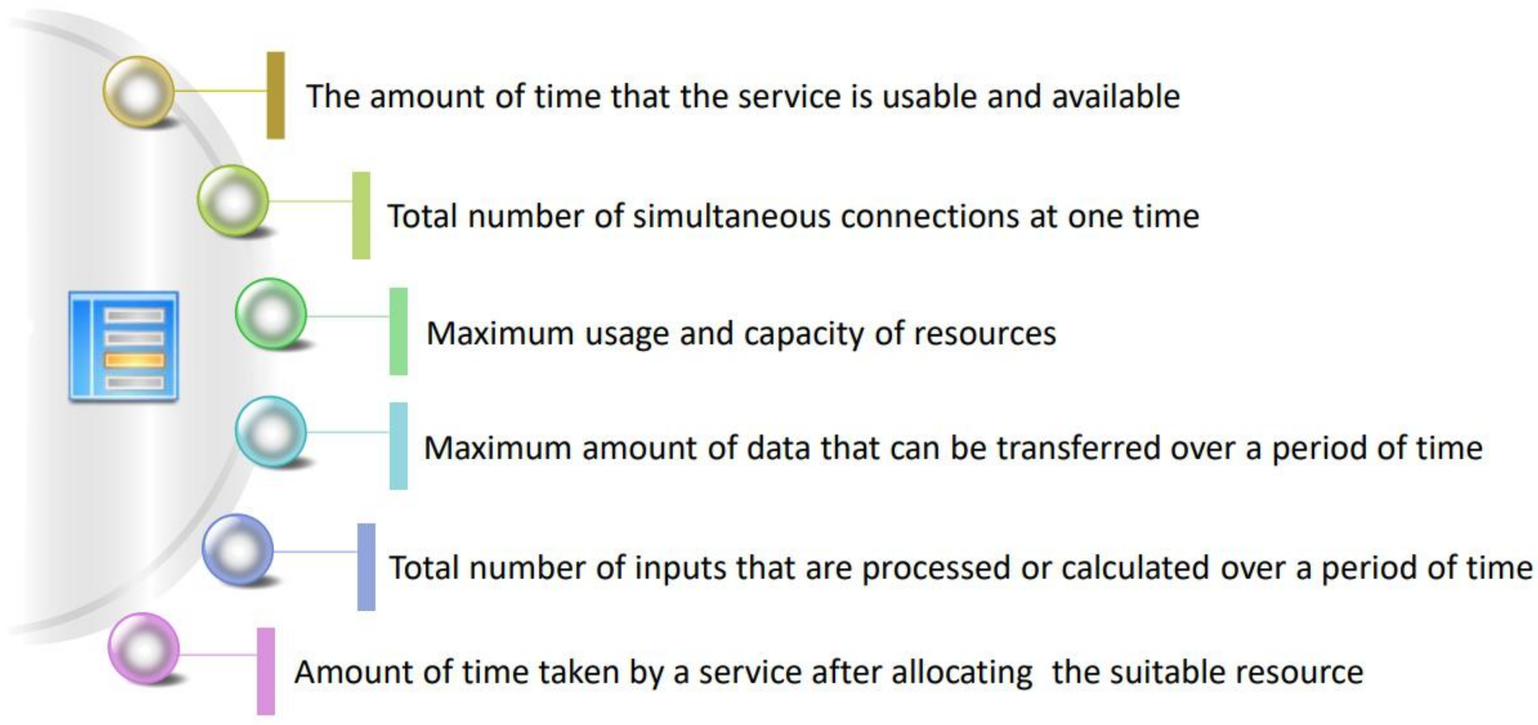


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Legal Checklist for Performance Management

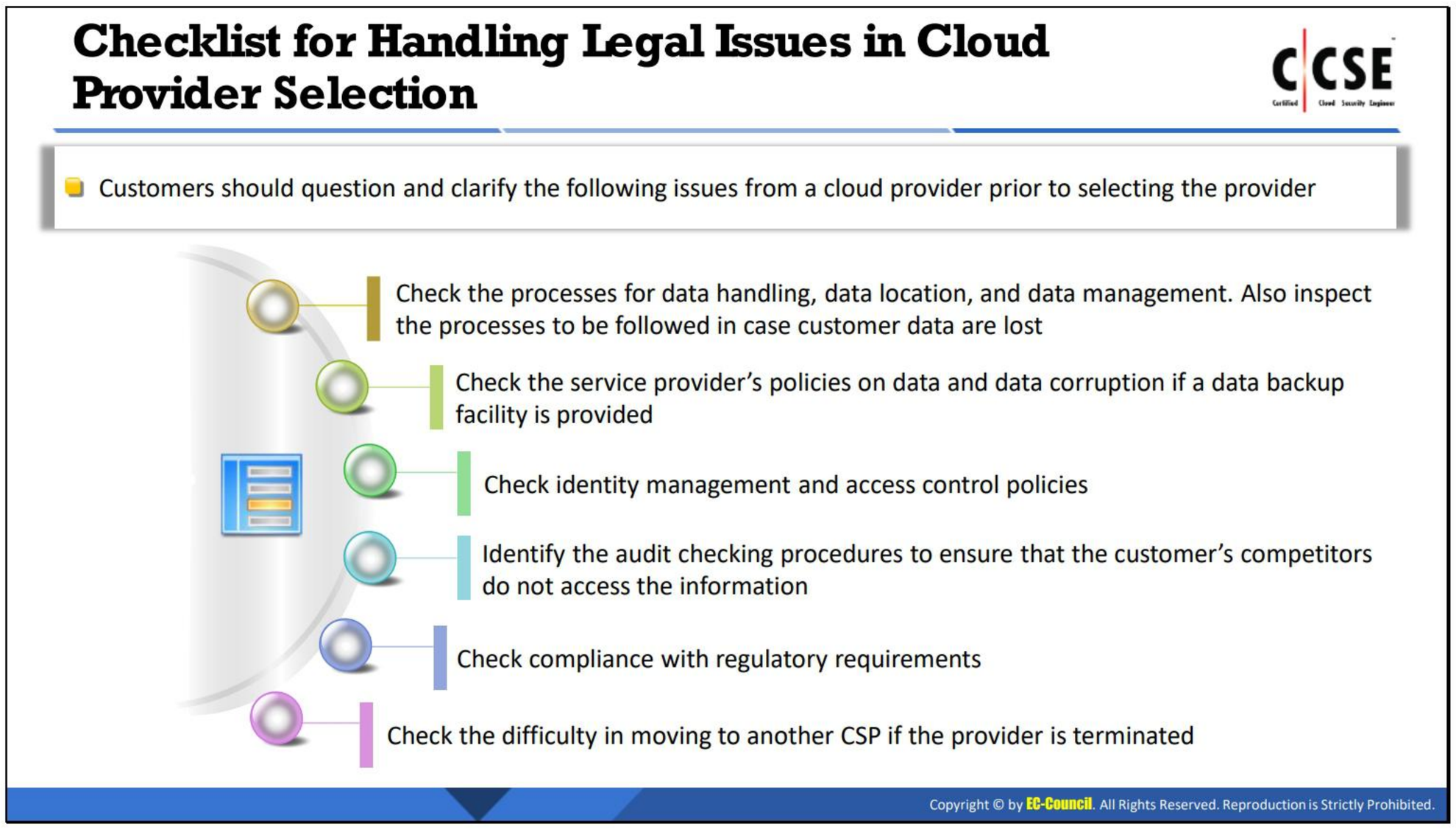
- Customers should obtain the following details from a cloud provider prior to selecting the provider

h1ee01.ir



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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Computing Legal Checklists

A cloud customer must use legal checklists to evaluate a CSP on various parameters by asking questions and clarifying doubts.

The following are the legal checklists that an organization must use as a cloud customer.

hade01.ir

Cloud Computing Legal Checklist for Protection of Information

Cloud customers should clarify the following from the CSP for information protection or data security.

- How are the data stored and protected by the CSP?
- Does the CSP have the right to use or make public users' data?
- Who is liable for handling, processing, storing, and accessing personal and sensitive information? Is the CSP responsible for subcontractors?
- Can the data be erased permanently from the cloud when the user ends the service?
- Who is responsible for security breaches and how will the CSP respond to them?
- Under what time frame will the CSP notify about a security breach?
- What due diligence is implemented for information security?
- How will the CSP handle the disposal of personal and sensitive information?
- What security measures (such as encryption, physical protection, and data backup) will the CSP take to ensure information security?
- Are the data secure while transferring in and out of the cloud.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Legal Checklist for Contract Termination

Cloud customers should clarify the following from the CSP before contract termination.

- Will the CSP notify the customer when it terminates the service?
- If the customer desires to terminate the contract, is there any established procedure to contact the CSP?
- In the event of contract termination, will the CSP transfer the data to the customer or to another CSP of their choice in an interoperable and usable format?
- Are the time, cost, and procedure for transferring/returning the customer's data at the termination of the contract clearly stated?
- Can the customer access the metadata created by the cloud service system at the end of the contract?
- Will the customer's data and metadata be permanently and immediately destroyed in a manner that data reconstruction and data restoration are not possible from the CSP after the contract termination?
- Before service termination, is there any option for the customer to confirm the deletion of metadata and records?
- If the cloud provider changes, is there any option for the customer to terminate the service agreement without penalty?
- Will the customer have the right to terminate the contract if the CSP introduces modifications in the service terms?
- Can the customer continue using the data in aggregate form after the termination of the contract?
- Will the customer receive the right to terminate the contract in the event of a material breach of applicable security and privacy obligations?
- Can the customer seek transition assistance to move data to another CSP if the contract is terminated? Will there be any obligation on the provider to return the customer's data?

hide01.ir

Cloud Computing Legal Checklist for Liability

Cloud customers should clarify the following from the CSP.

- Who is liable for security breaches and how will the CSP respond to a breach?
- What remedial measures will the CSP take for data breaches?
- Users should consider Cyber Liability Insurance against data breaches.
- Is the CSP responsible for subcontractors?
- How will the CSP address IP infringement by its system/service?
- Does the CSP disclaim consequential damages? Are there any exceptions to it?
- Has the CSP capped its total liability?

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing Legal Checklist for Performance Management

Cloud customers should obtain the following details from the CSP:

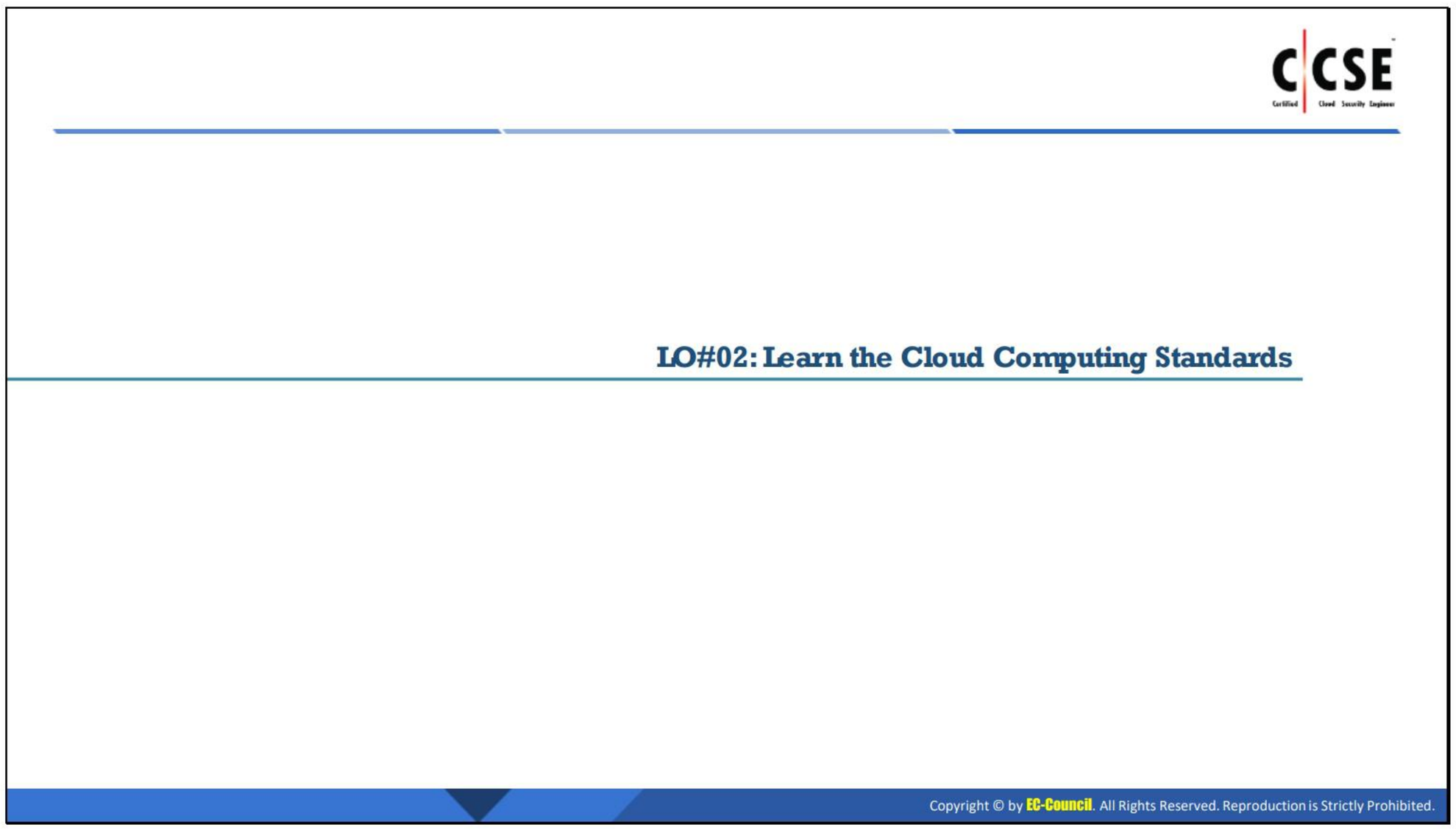
- Amount of time that the service is usable and available
- Total number of simultaneous connections
- Maximum usage and capacity of resources
- Maximum amount of data that can be transferred over a period of time
- Total number of inputs that are processed or calculated over a period of time
- Speed and accuracy with which the service can adjust to the amount of allocated resources

Checklist for Handling Legal Issues in Cloud Provider Selection

Before selecting a cloud service provider (CSP), cloud customers should consider the following actions.

- Check the data handling processes, the location of data, and how the data are managed. Inspect all the processes implemented for use in case customer data are lost.
- Check the CSP policies pertaining to data and data corruption. Ask the provider how data will be backed up and retrieved.
- Clarify policies related to identity management and access control. Ask who is authorized to do what activities under what circumstances and who will be responsible for the customer's data. Determine whether the CSP can view or access the data and identify the controls implemented to prevent the data from being copied or removed. Check whether the CSP has an audit trail.
- Ask whether the CSP has strong audit-checking procedures for data colocation to ensure that customer information is not accessed by a competitor hosted on the same hardware. In cloud computing, as several organizations' data are hosted on a single server, data security must be ensured.
- Check compliance with regulatory requirements such as corporate governance, data regulations, information provision requirements, banking regulations, and auditing standards. Carefully scrutinize the CSP's policies (e.g., data protection policy). Data checks might already be in place for data export to certain jurisdictions. For example, European data protection law restricts the export of any personal data to the US. However, cloud providers can take advantage of some legal exceptions to that restriction.
- Check how easy it will be to move or transfer to another CSP practically.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

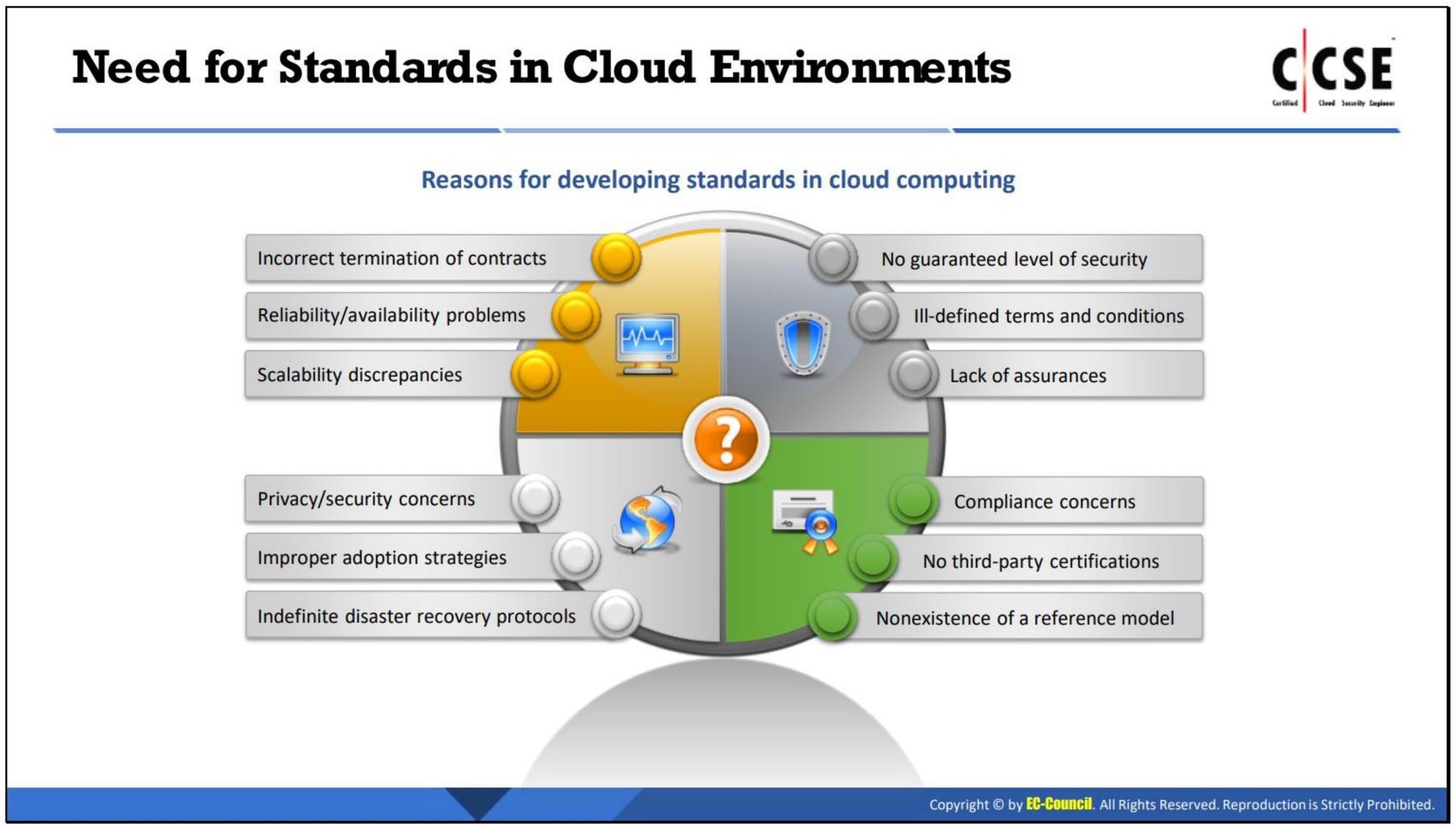


LO#02: Learn the Cloud Computing Standards

Cloud computing standards are essential to handle contract termination, security concerns, improper adoption strategies, compliance concerns, etc. The objective of this section is to explain various cloud computing standards such as PCI DSS, ITU-T X.1601, ISO/IEC 27017, NIST, CSA CCM, SAML 2.0, OVF, and OCCI. This section also demonstrates when the organization should follow cloud computing standards and explains the various cloud standard organizations and their roles.

hi10091.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Need for Standards in Cloud Environments

Cloud computing standards ensure that various cloud providers, customers, and applications work together without any operational issues. They are essential to increase the flexibility, security, and interoperability of cloud-based services. They are also required for the universal adoption of cloud services.

Cloud storage standards can help users and organizations address accessibility, security, and portability issues associated with the relentlessly growing pool of data. The cloud is a combination of diversified technical and business elements with high security risks. The implementation of standards in cloud computing practices and environments can minimize these risks.

Cloud computing standards are helpful in case of the below risks.

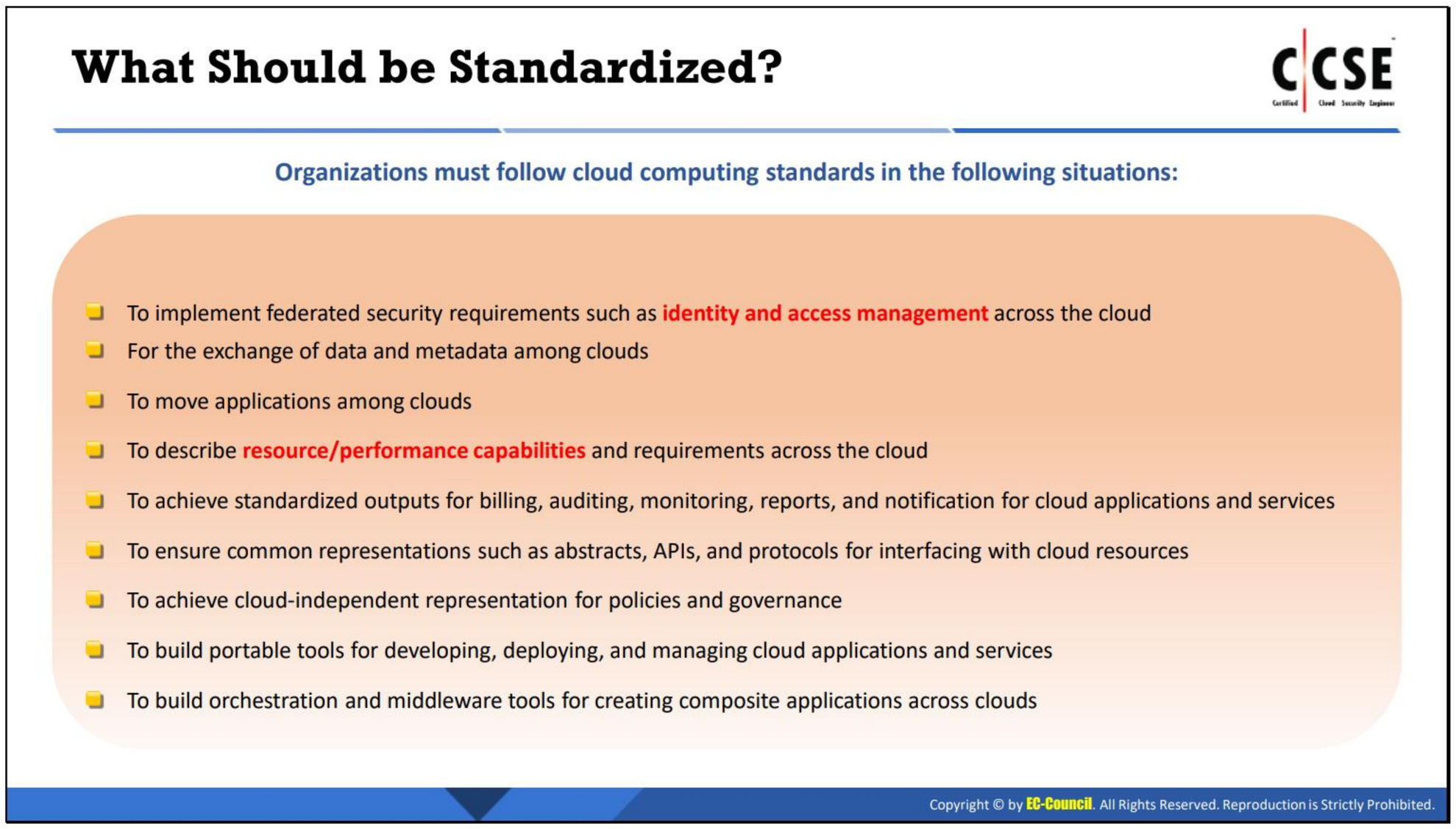
- Incorrect termination of contracts
- No guaranteed level of security
- Reliability/availability problems
- Scalability discrepancies
- Privacy and security concerns
- Improper cloud adoption strategies
- Indefinite disaster recovery (DR) protocols
- Non-defined terms and conditions
- Lack of assurances

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Compliance concerns
- No third-party certifications
- Nonexistence of a reference model

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



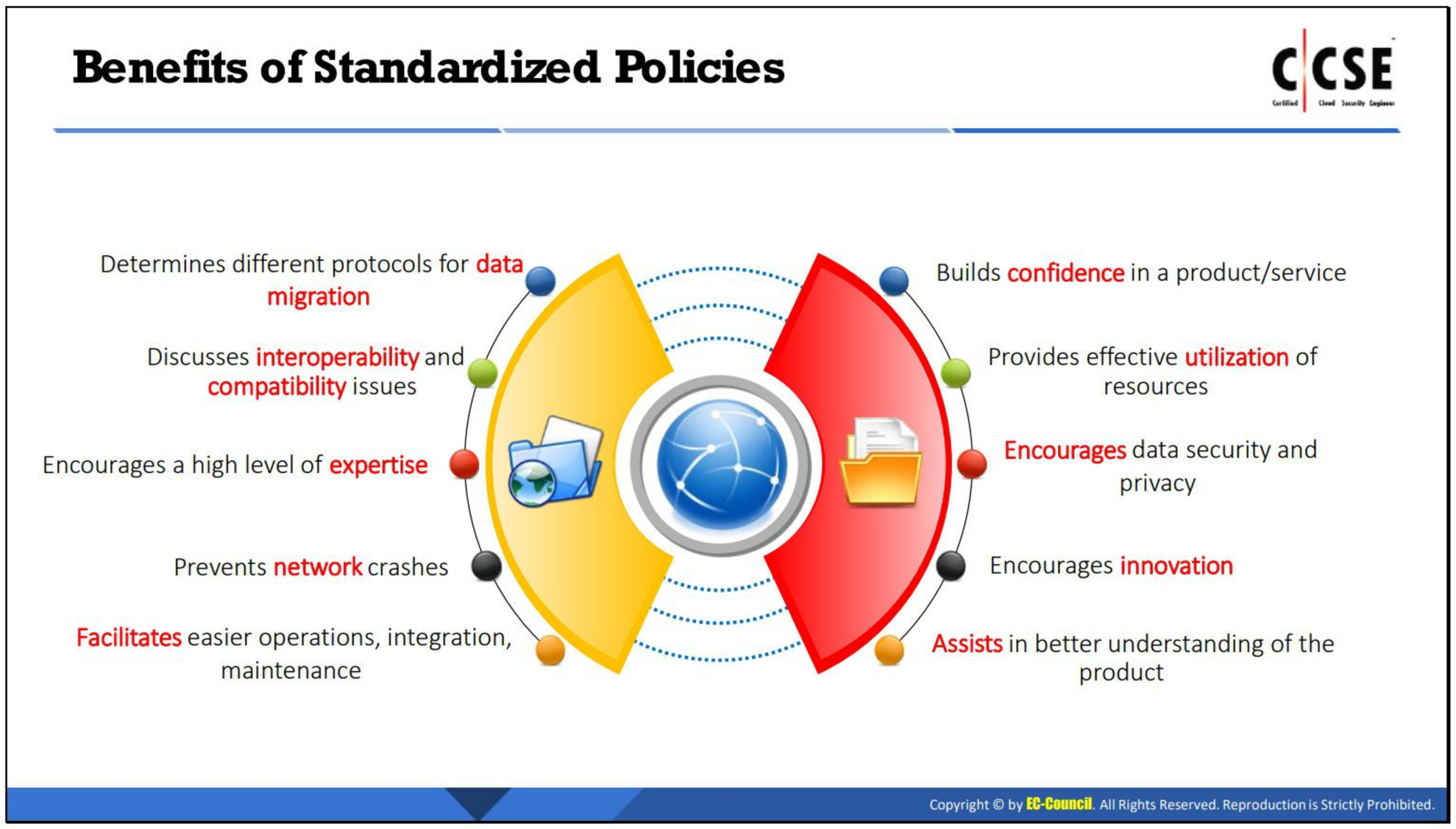
What Should be Standardized?

Organizations must follow cloud computing standards in the following situations.

hidedl.ir

- To implement federated security requirements such as identity and access management across the cloud
- For the exchange of data and metadata among clouds
- To move applications among clouds
- To describe resource/performance capabilities and requirements across the cloud
- To achieve standardized outputs for the billing, auditing, monitoring, reports, and notification of cloud applications and services
- To ensure common representations such as abstracts, application programming interfaces (APIs), and protocols for interfacing with cloud resources
- To achieve cloud-independent representation for policies and governance
- To build Portable tools for developing, deploying, and managing cloud applications and services
- To build orchestration and middleware tools for creating composite applications across clouds

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



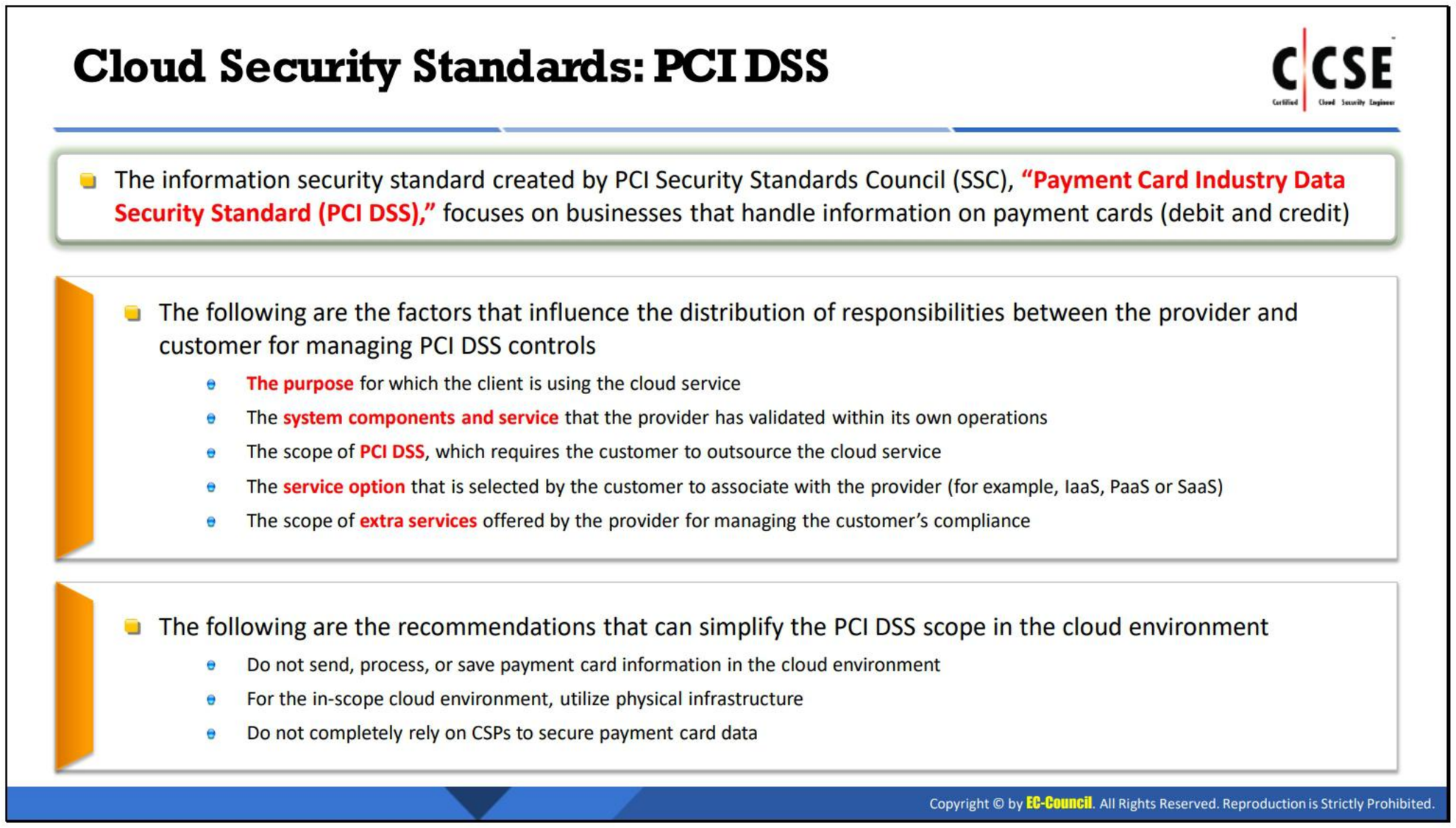
Benefits of Standardized Policies

There is a great demand from both cloud customers and providers for standardization in the cloud. Vendors promote standards to alleviate customers' fear in adopting the cloud to expand their business. Customers need standards to have the flexibility to switch to other service providers in case of poor vendor service or the presence of better deals. Technology-driven cloud offerings are changing on a monthly basis, and therefore, standards must address these new trends. Creating standards in haste for open-source distribution requires an effective standardized policy to eliminate the associated risks and/or challenges. Cloud standards increase efficiency and interoperability, minimize vendor lock-in, etc.

The following are the benefits of standardized policies in the cloud:

- Determines different protocols for data migration
- Discusses interoperability and compatibility issues
- Encourages a higher level of expertise and prevents network crashes
- Facilitates easier operations, integration, and maintenance
- Builds confidence in products/services and helps in the effective utilization of resources
- Encourages data security and privacy
- Encourages innovation and assists in providing a better understanding of the product

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security Standards: PCI DSS

The information security standard created by PCI Security Standards Council (SSC), called Payment Card Industry Data Security Standard (PCI DSS), focuses on businesses that handle information on payment cards (credit and debit cards).

The distribution of responsibilities between the cloud service provider (CSP) and the customer for managing PCI DSS controls are based on the following factors:

- The purpose for which the customer is using the cloud service
- The system components and service that the CSP has validated within its own operations
- The scope of PCI DSS, which requires the customer to outsource the cloud service
- The service option that is selected by the customer to associate with the provider (for example, SaaS, IaaS, or PaaS)
- The scope of extra services offered by the provider for managing the customer's compliance

The scope of CSP responsibility for all PCI DSS requirements must be clearly understood by the client.

Security as a service (SecaaS) is also a part of cloud security. SecaaS solutions may not be involved in storing and processing payment card data. A PCI DSS control is provided by SecaaS to the organization's environment. Therefore, it is not necessary to review SecaaS functionality.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scoping Recommendations

Organizations handling payment card data in a cloud environment must be aware of the impact of the cloud on the organization's PCI DSS scope. The following recommendations simplify the scope of PCI DSS in the cloud environment.

- Do not send, process, or save payment card information in the cloud environment.
- For the in-scope cloud environment, utilize physical infrastructure.
- Do not completely rely on CSPs to secure payment card data. If the CSP is responsible for more security controls, the cardholder data environment (CDE) will be greater, and it will increase complexity while defining and maintaining CDE boundaries.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Standards: ITU-T X.1601

- The standard ITU –T X.1601 divides the roles of an organization into the categories **cloud service provider (CSP), cloud service customer (CSC),** and **cloud service partner (CSN)**
- The framework for the cloud security **ITU-T X.1601 standard** covers the following

Security threats that arise in the cloud

Security threats for cloud service customers (CSCs)

- Data loss and leakage
- Insecure service access
- Insider threats

Security threats for cloud service providers (CSPs)

- Unauthorized administration access
- Insider threats

Source: https://www.itu.int/

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

Cloud Security Standards: ITU-T X.1601 (Contd.)

Security challenges and ways to reduce such risks in the cloud

hide01.ir

Security challenges for cloud service customers (CSCs)

- Ambiguity in responsibility
- Loss of trust
- Loss of governance
- Loss of confidentiality
- Service unavailability
- CSP lock-in
- Misappropriation of intellectual property
- Loss of software integrity

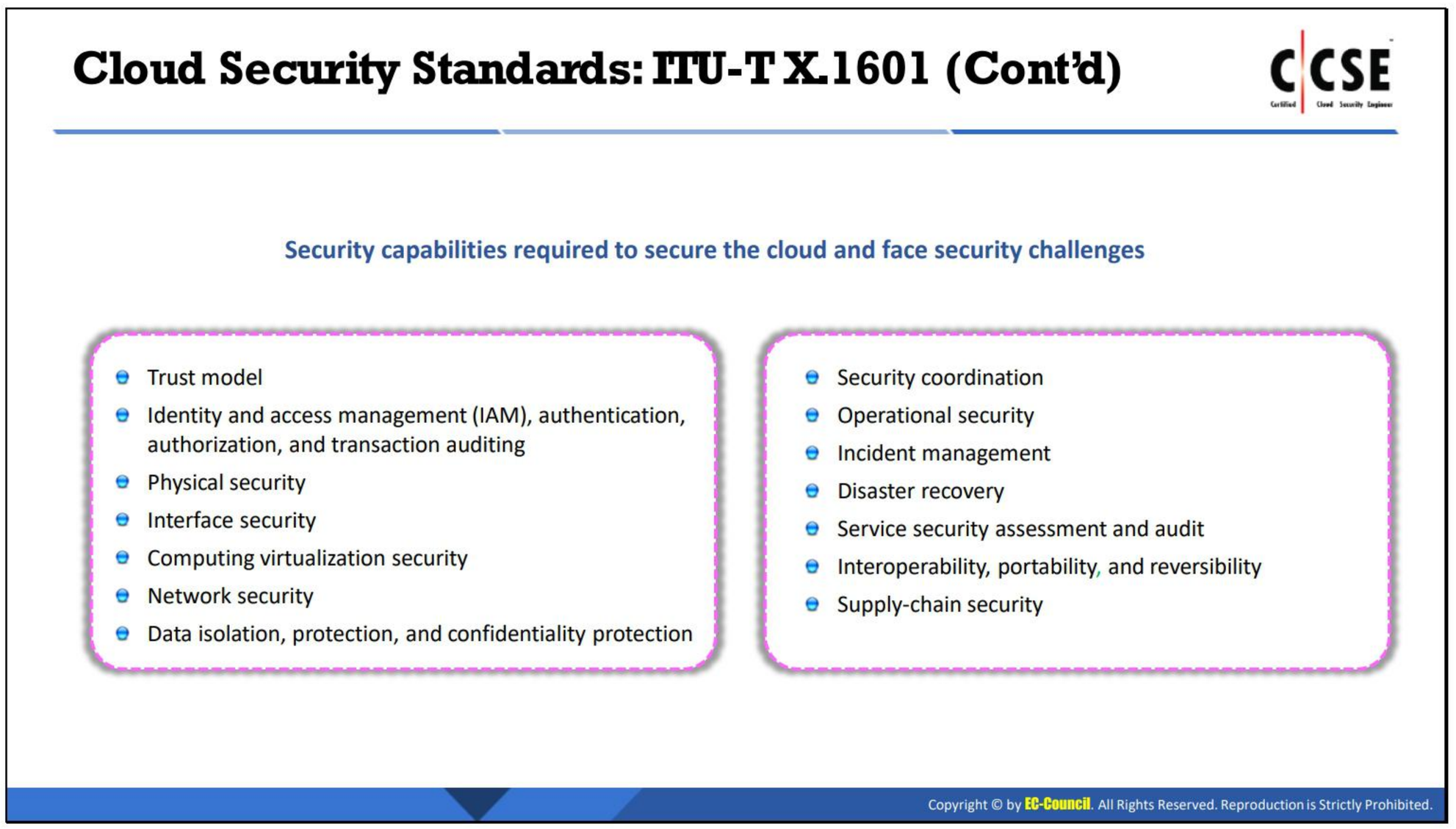
Security challenges for cloud service providers (CSPs)

- Ambiguity in responsibility
- Shared environment
- Inconsistency and conflict of protection mechanisms
- Jurisdictional conflict
- Evolutionary risks
- Bad migration and integration
- Business discontinuity
- CSN lock-in
- Supply-chain vulnerability
- Software dependencies

Security challenges for cloud service partners (CSNs)

- Ambiguity in responsibility
- Misappropriation of intellectual property
- Loss of software integrity

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



Cloud Security Standards: ITU-T X.1601

***Source**: https://www.itu.int/*

The framework for the cloud security standard "ITU-T X.1601" covers the following:

- Security threats that arise in the cloud
- Security challenges and ways to reduce such risks in the cloud
- Security capabilities required to secure the cloud and face security challenges

Security threats in cloud computing

The security threats that can arise in a cloud computing environment are discussed below.

- **Security threats for cloud service customers (CSCs)**

  The following threats directly affect CSCs.

  - **Data loss and leakage:** As the cloud service environment is typically a multi-tenant one, loss or leakage of data is a serious threat to the CSC. A lack of appropriate management of cryptographic information, such as encryption keys, authentication codes, and access privilege, could lead to significant damages, such as data loss and unexpected data leakage. Examples of such threats include insufficient authentication, authorization, and audit controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; unreliable data centers; and insufficient disaster recovery (DR).
  - **Insecure service access**: Identity credentials, including those of CSC administrators, are especially vulnerable to unauthorized users in the highly

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

distributed environment of cloud computing, since unlike traditional telecommunications, it is often difficult to rely on location (e.g., landline) or the presence of a specific hardware element (e.g., a mobile subscriber identity module (SIM)) to reinforce identity authentication. As most service offerings are remote, unprotected connections expose potential vulnerabilities. Even when the connections are protected or local, other attack methods (such as phishing, fraud, social engineering, and exploitation of software vulnerabilities) may succeed. If an attacker gains access to users' or administrators' credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information, and redirect a CSC's clients to illegitimate sites. Passwords are often reused across multiple websites and services, which amplifies the impact of such attacks, since a single break can expose multiple services. Cloud computing solutions also add a new threat to the landscape. The CSC's account or service instances may become a new base for an attacker. The attacker may leverage the CSC's reputation and resources to launch subsequent attacks.

- **Insider threats**: Insider threats include CSC employees who share "administrator" passwords or otherwise leave credentials unsecure (e.g., writing these on notes stuck to a screen), careless or inadequately trained users (or family members in a consumer setting), or malicious actions by disgruntled employees, all of which could pose significant threats.

- **Security threats for cloud service providers (CSPs)**

  The following threats are those that directly affect CSPs.

  - **Unauthorized administration access**: The cloud computing service includes interfaces and software components that allow the CSC's own staff to administer those aspects of the cloud computing service that are under its control, such as the addition or removal of CSC employee accounts, connections to the CSC's own servers, changes to service capacity, and updating the Domain Name System (DNS) entries and websites. Such administrative interfaces can become a target of choice for attackers who impersonate the CSC's administrators to attack a CSP. Because such cloud computing services must be accessible to the CSC's own staff, the protection of these services becomes a major concern for cloud computing security.
  - **Insider threats**: Insider threats include CSP employees who share "administrator" passwords or otherwise leave credentials unsecure (e.g., writing these on notes stuck to a screen), careless or inadequately trained users, or malicious actions by disgruntled employees, all of which pose a significant threat to any business.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security challenges in cloud computing

The challenges to be considered in the context of cloud computing services are described below.

- **Security challenges for CSCs**

  Security challenges associated with environmental difficulties or indirect threats that may give rise to more direct threats affecting the CSC's interests are as follows:

  - **Ambiguity in responsibility**: CSCs consume delivered resources through different service categories and deployment models. The customer-built information and communications technology (ICT) system thus relies on these services. The lack of a clear definition of responsibility among CSCs and CSPs may introduce conceptual and operational conflicts. Any contractual inconsistency of provided services could induce an anomaly or incidents.
  - **Loss of trust:** At times, it is difficult for a CSCs to recognize their CSPs' trust level due to the black-box feature of the cloud computing service. If there is no means of obtaining and sharing the provider's security level formally, CSCs have no means of evaluating the security implementation level achieved by the provider. Such lack of sharing at the security level with regard to the CSP could become a serious security threat for some CSCs in using cloud computing services.
  - **Loss of governance**: If CSCs migrate a part of their own ICT system to a cloud computing infrastructure, they give partial control to a CSP. This could be a serious threat to a CSC's data, notably in terms of the role and privilege assignment to the provider. Coupled with a lack of transparency regarding cloud computing provider practices, this may lead to misconfiguration or even enable a malicious insider attack. When adopting cloud computing services, some CSCs may have concerns about lack of control over their information and assets hosted in CSPs, data storage, reliability of data backup (data retention issues), countermeasures for business continuity plans (BCPs), disaster recovery (DR), etc.
  - **Loss of confidentiality**: When a CSP processes confidential information, confidentiality may become violated, which could also include a violation of applicable data protection regulations, certifications, or laws. This includes the leakage of confidential information or the processing of personally identifiable information (PII) for a purpose that is not authorized by the CSC and/or the data subject.
  - **Service unavailability**: Availability is not specific to the cloud computing environment. However, because of adopting a service-oriented design principle, service delivery may be impacted when upstream cloud computing services are not completely available. Moreover, the dynamic dependency of cloud computing offers more possibilities to an attacker.
  - **Cloud service provider lock-in**: High dependency on a single CSP could make it difficult to replace one CSP with another. A lock-in may occur when a CSP relies on non-standard functions or formats and does not provide interoperability. This

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

could become a security threat if the locked-in CSP fails to address known security vulnerabilities, thus leaving CSC vulnerable and unable to migrate to another CSP.

- **Misappropriation of intellectual property**: When the CSC's software is run or other assets are stored by the CSP, a challenge that arises is that this material could be leaked to third parties or misappropriated for unauthorized use. This could lead to a violation of copyright or the exposure of trade secrets.
- **Loss of software integrity**: Once the CSC's software is running in the CSP, the software may become modified or infected while it is out of the CSC's direct control, thus causing its software to misbehave in some way. Although this possibility exists outside the CSC's control, it could seriously affect its reputation and business.

- **Security Challenges for CSPs**

The security challenges associated with environmental difficulties or indirect threats that may give rise to more direct threats to the CSP's interests are descried below.

- **Ambiguity in responsibility**: Different roles (CSP, CSC, and cloud service partner (CSN)) may be defined in a cloud computing system. Ambiguity in the definition of responsibilities related to issues such as data ownership, access control, or infrastructure maintenance may impact business or legal disputes (especially when dealing with third parties, or when the CSP is also a CSC or a CSN). This ambiguity risk increases when the CSP is operating and/or offering services across multiple jurisdictions where contracts and agreements may exist in different languages or legal frameworks.
- **Shared environment**: Cloud computing offers potential cost savings through massive resource sharing on a very large scale. This situation, however, exposes many potentially vulnerable interfaces. For example, different CSCs consume services from the same cloud simultaneously. As a result, the CSC could potentially have unauthorized access to other tenants' virtual machines (VMs), network traffic, actual/residual data, etc. Any such unauthorized or malicious access to another CSC's assets might compromise integrity, availability, and confidentiality. For example, consider a situation in which multiple VMs co-hosted on one physical server share both the central processing unit (CPU) and memory resources that are virtualized by the hypervisor. This is an example of the failure of hypervisor isolation mechanisms, thus allowing unauthorized access to the memory or storage of other VMs.
- **Inconsistency and conflicts between protection mechanisms**: Due to the decentralized architecture of a cloud computing infrastructure, its protection mechanisms might be inconsistent among distributed security modules.
- **Jurisdictional conflict**: Data in the cloud can be moved around between data centers or even across international borders. Depending on the host country, the data will be governed by different applicable jurisdictions. Jurisdictional conflicts

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

can lead to legal complications that impact security, such as rules governing the lawful intercept of communications by law enforcement authorities, which in turn could affect decisions on cryptography.

- **Evolutionary risks**: One advantage of cloud computing is that it allows to postpone some choices from the system design phase to the execution phase. This means that some dependent software components of a system may be selected and implemented only when the function requiring them has been executed. However, conventional risk assessment methodology can no longer keep up with such a dynamically evolving system. For a system that has passed a security assessment during the design phase, new vulnerabilities might be introduced during its lifetime due to changes in software components.
- **Bad migration and integration**: Migrating to the cloud often implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an ICT system to an external CSP might require substantial changes in the system design (e.g., network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement might have both functional and non-functional impacts. For example, VMs that run behind a firewall in a private data center might accidently be exposed to the open Internet in the CSP's cloud.
- **Business discontinuity**: Cloud computing allocates resources and delivers them as a service. The whole cloud computing ecosystem is composed of many interdependent parts. Discontinuity in any part (such as a blackout, denial-of-service, or delay) might affect the cloud computing service availability connected with service unavailability and cause business discontinuity.
- **Cloud service partner lock-in**: The platform of the CSP is built using software and hardware components from various suppliers. Some components may include proprietary features or extensions that are useful to the CSP. However, relying on these proprietary features limits the CSP's ability to migrate to another component supplier. While lock-in is a business issue, it is not in itself a security threat. However, it can sometimes give rise to security concerns.
- **Supply chain vulnerability**: A CSP is at risk if hardware or software delivered to the platform through its supply chain undermines CSC or CSP security. For example, the accidental or deliberate introduction of malware or exploitable vulnerabilities.
- **Software dependencies**: When a vulnerability is detected, it may not be possible to apply updates immediately because doing so could break other software components (though those components may not otherwise require updating). This is particularly true if the dependency exists between components provided by one or more CSNs, rather than the CSPs themselves.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Security Challenges for CSNs**

  Challenges that directly affect CSNs are described below.

  - **Ambiguity in responsibility**: If a mix of CSP and CSN software is running in the service, it may not be easily apparent to the CSC where the responsibility for mitigation and handling of security incidents resides. Determining the responsible entity using technical analysis may be quite difficult. This could result in confrontation between the CSP and CSN(s) to determine who is at fault, resulting in further breaches if the root cause is not found.
  - **Misappropriation of intellectual property**: When partners submit software or other assets to the CSP for execution, the security challenge of the material being leaked to third parties or misappropriated for unauthorized use arises. This could include a violation of copyright or the exposure of trade secrets.
  - **Loss of software integrity**: Once the partner's software is running in the CSP, the software could be modified or infected while it is out of the CSN's direct control, thus causing its software to misbehave in some way. Although this possibility exists outside the CSN's control, it could seriously affect its reputation and business.

Security capabilities in cloud computing

This recommendation identifies the following security capabilities to defend against the identified cloud computing security threats and challenges.

- **Trust model**: A common trust model is necessary for any system where multiple providers cooperate to provide a trustworthy service. Because of the highly distributed and multi-stakeholder nature of cloud computing, the cloud computing environment needs to incorporate an overall trust model. This trust model will enable the creation of islands and/or federations of trusted entities, so that disparate elements of the system can authenticate the identity and authorized rights of other entities and components.
- **Identity and access management (IAM), authentication, authorization, and transaction audit:** IAM contributes to the confidentiality, integrity, and availability of services and resources and is thus essential for cloud computing. Furthermore, IAM may enable the implementation of single sign-on and identity federation for clouds using different authentication mechanisms or distributed in different security domains.
- **Physical security**: Access to premises containing CSP equipment is restricted to authorized persons and only to those areas directly necessary for their job functions; this is a part of the IAM process. However, the extent of physical security will depend on the value of the data and the extent to which multiple customers are provided access.
- **Interface security**: This capability secures interfaces open to CSCs and/or other contracted CSPs through which various kinds of cloud computing services are delivered and secures the communications based on these interfaces. Mechanisms available to ensure interface security include but are not limited to unilateral/mutual authentication, integrity checksum, end-to-end encryption, and digital signature.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Computing virtualization security**: Computing virtualization security refers to the security of the whole computing virtualization environment. It protects the hypervisor from attacks, protects the host platform from threats originating in the computing virtualization environment, and keeps VMs secure throughout the lifecycle. Specifically, this capability enables VM isolation and protects VM images and suspended VM instances in storage and during migration.
- **Network security**: In a cloud computing environment, network security enables both physical and virtual network isolation and secures communications among all participants. It enables network security domain partition, network border access controls (e.g., firewall), intrusion detection and prevention, and network traffic segregation based on security policies. It also protects the network from attacks in both the physical and virtual network environments.
- **Data isolation, protection, and confidentiality protection:** Data isolation may be realized logically or physically, depending on the required isolation granularity and the specific deployment of cloud computing software and hardware.

  Data protection ensures that CSC data and derived data held in a cloud computing environment are appropriately protected such that they can only be accessed or changed as authorized by the CSC (or according to applicable law). This protection may include some combination of access control lists, integrity verification, error correction/data recovery, encryption, and other appropriate mechanisms.

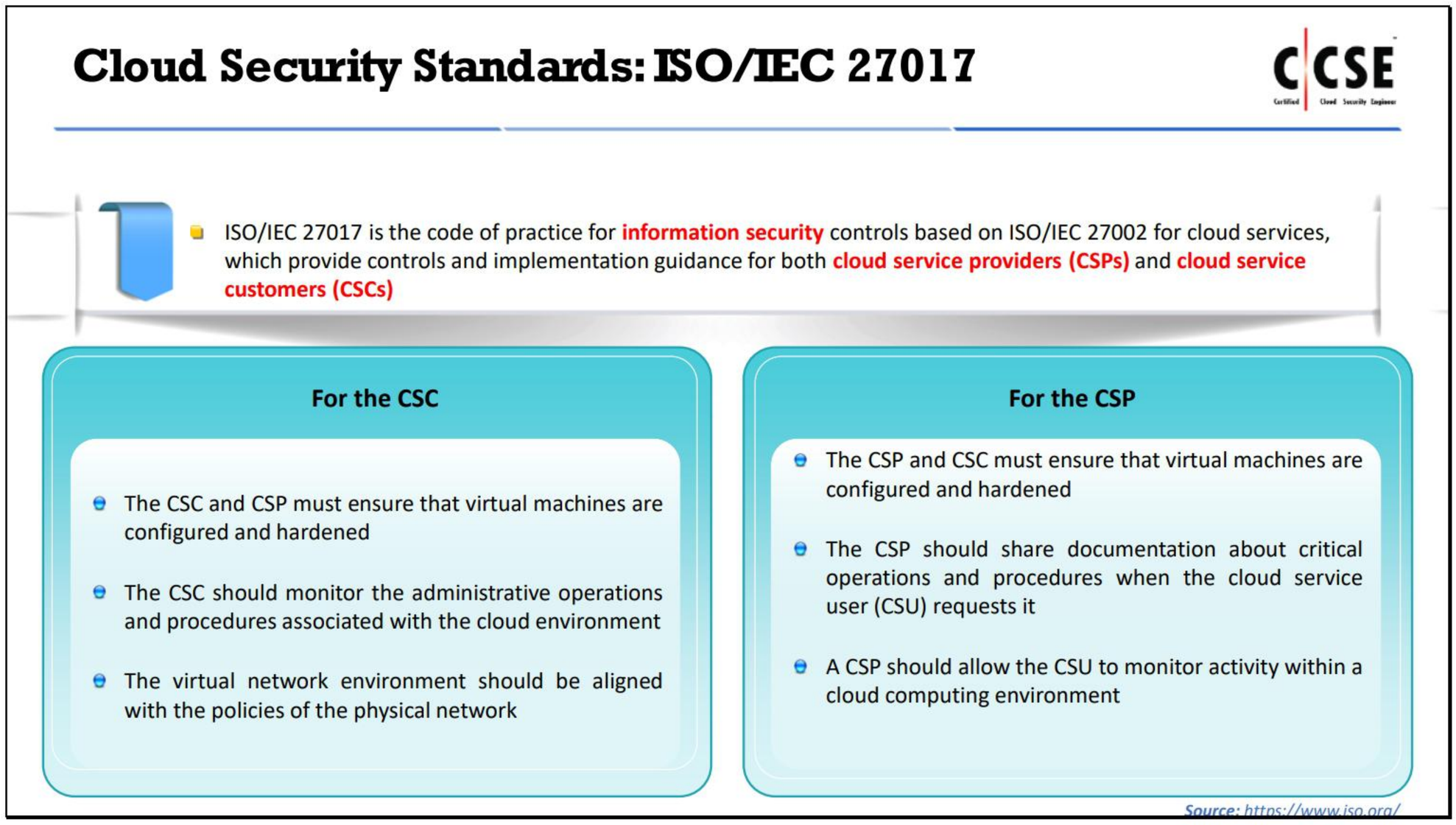
  A risk assessment of private information (noted as "confidentiality risk assessment") can assist a CSP in identifying the specific risks of confidentiality breaches involved in an envisaged operation. The CSP should identify and implement capabilities to address the confidentiality risks identified by the risk assessment and treatment of private information.
- **Security coordination**: Parties playing different roles in the cloud computing ecosystem, e.g., CSP, CSC, CSN, have different degrees of control over the physical or virtual resources and services, including security control. Each party will have various security mechanisms including hypervisor isolation, IAM, network protection, etc.
- **Operational security**: The operational security capability includes the following:
  - Defining sets of security policies and security activities (configuration management, patch upgrade, security assessment, incident response, etc. and ensuring that these security measures are correctly enforced to fulfil the requirements of applicable laws and contracts, including any security SLA
  - Monitoring the CSP's security measures and their effectiveness and providing appropriate reports to affected CSCs and applicable third-party auditors (acting as a CSN) to enable the CSC to measure whether a CSP is delivering on SLA security commitments
- **Incident management**: Incident management includes incident monitoring, prediction, alerting, and response. To know whether the cloud computing service is operating as

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

expected throughout the infrastructure, continuous monitoring is necessary (e.g., monitoring the real-time performance of virtualized platform and virtualized machine). This enables systems to capture the service security status, identify abnormal conditions, and provide early warnings about security system overloads, breaches, service discontinuity, etc.

- **Disaster recovery (DR)**: DR represents the capability to respond to catastrophic disasters, recover to a safe state, and resume normal operations as quickly as possible. This capability ensures continuity of provided services with minimum interruption.
- **Service security assessment and audit**: This capability enables the security evaluation of cloud computing services. It enables an authorized party to verify that a cloud service complies with the applicable security requirements. Security assessments or security audits could be performed by the CSC, CSP, or a third party (CSN), and security certification could be provided by an authorized third party (CSN).
- **Interoperability, portability, and reversibility**: This capability enables the coexistence and cooperation of heterogeneous components (interoperability). It enables CSCs to replace one CSP with another where appropriate (portability),and equips them to transfer their ICT system back from a cloud computing environment to a non-cloud computing ICT infrastructure (reversibility). This reversibility also enables the "right to be forgotten" if required by local laws or regulations.
- **Supply chain security**: A CSP uses many suppliers to build its services. Some of these are cloud industry participants, such as a CSN, while others are traditional IT equipment or service suppliers, such as hardware manufacturers with no direct relationship with cloud computing. This capability establishes a trust relationship between the CSP and all the participants in the supply chain through security activities. These supply chain security activities involve identifying and gathering information about the CSP's acquired components and services used to provide cloud computing services and enforce supply chain security policies.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security Standards: ISO/IEC 27017

***Source**: https://www.iso.org/*

hadeq_ir

ISO/IEC 27017 is a code of practice for information security controls based on ISO/IEC 27002 for cloud services; in other words, ISO 27017 suggests additional security controls for the cloud in areas that are not adequately addressed by ISO 27002.

ISO/IEC 27017:2015 establishes guidelines for information security controls applicable to the provision and use of cloud services by providing the following:

- Additional implementation guidance for relevant controls specified in ISO/IEC 27002
- Additional controls with implementation guidance that specifically relate to cloud services

Controls for CSC and CSP

ISO 27017 suggests controls that are compatible with the existing structure of ISO 27001/ISO 27002. The controls and implementation guidance included for CSC and CSP are as follows.

- **Cloud Service Customer (CSC)**
  - The CSC should agree with the CSP on an appropriate allocation of information security roles and responsibilities. Further, the CSC should confirm that they can fulfill the roles and responsibilities allocated to them.
  - The information security roles and responsibilities of both parties should be stated in an agreement.
  - The CSC should identify and manage their relationship with the customer support and customer care functions of the CSP.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The responsibilities shared between the CSC and CSP in terms of information security roles must be clearly understood and communicated.
- ISO 27017 addresses how assets are returned or removed from cloud services when the contract/agreement between the CSC and CSP is terminated.
- The CSC and CSP must ensure that virtual machines (VMs) are configured and hardened.
- The CSC should monitor the administrative operations and procedures associated with the cloud environment.
- The virtual network environment should be aligned with the policies of the physical network.

- **Cloud Service Provider (CSP)**
  - The CSP should agree to and document an appropriate allocation of information security roles and responsibilities with their CSCs, their CSPs, and their suppliers.
  - The CSP must protect and separate the CSC's virtual environment from other CSCs and external parties.
  - The CSP and CSC must ensure that VMs are configured and hardened.
  - The CSP must share documentation about critical operations and procedures when the cloud service user (CSU) requests it.
  - The CSP should allow the CSU to monitor the activity within a cloud computing environment.

hi4e01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Standards: ISO/IEC 27018

- The ISO/IEC 27018 standard provides guidance aimed at ensuring that CSPs offer suitable information security controls to protect the privacy of their customers' clients by securing personally identifiable information (PII) entrusted to them

Benefits of ISO/IEC 27018 for CSPs and CSCs

- Helps the CSP comply with obligations when acting as a PII processor
- Enables public cloud PII processors to be transparent in relevant matters
- Assists the CSC and the public cloud PII processor in entering into a contractual agreement
- Provides CSCs with a mechanism for exercising audit and compliance rights and responsibilities

Source: *https://www.iso.org/*

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

Cloud Security Standards: ISO/IEC 27018

Source*: https://www.iso.org/*

hidee.ir

ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect personally identifiable information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. This standard concentrates in the following ways on security controls for public cloud service providers (CSPs) that process PII.

- It builds on the existing ISO/IEC 27002 controls by adding specific items for cloud privacy.
- It provides new security controls for personal data.

As per the standard, a public CSP is a "PII processor" when it processes PII for and according to the instructions of a cloud service customer (CSC). The CSC can authorize one or more cloud service users (CSUs) associated with the use of the services made available to the CSC under their contract with the public cloud PII processor. The CSC has authority over the processing and use of the data. A CSC who is also a PII controller can be subject to a broader set of obligations governing the protection of PII as compared to a public cloud PII processor. Maintaining the distinction between the PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the CSC with respect to the PII they process and the operations necessary to achieve the CSC's objectives.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

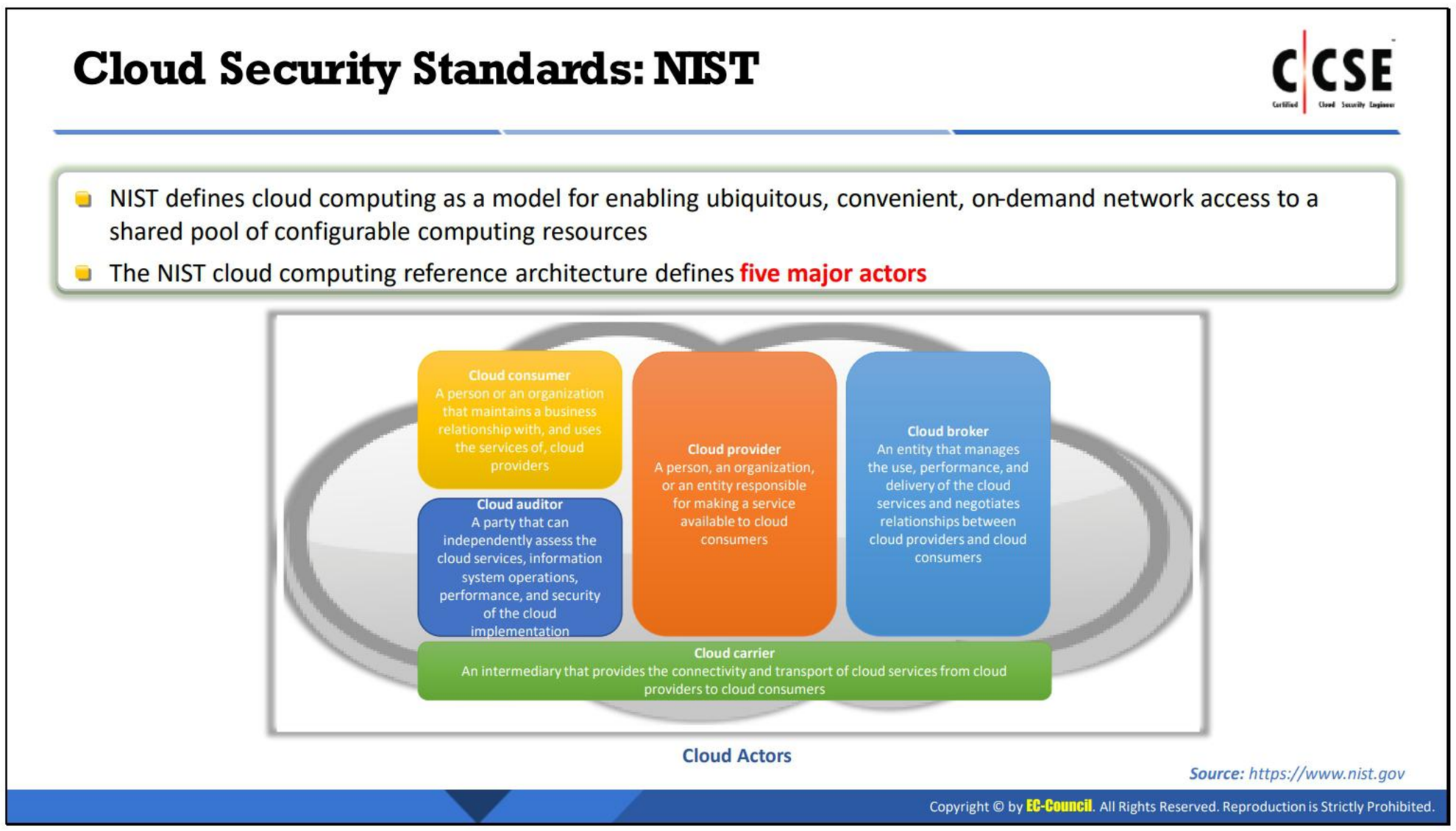
ISO 27018 Benefits

ISO 27018 benefits the CSC and CSP in the following ways.

- It helps the public CSP comply with applicable obligations when acting as a PII processor.
- It enables the public cloud PII processor to be transparent in relevant matters so that CSCs can select well-governed cloud-based PII processing services.
- It assists the CSC and the public cloud PII processor in entering into a contractual agreement.
- It provides CSCs with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual CSC audits of data hosted in a multi-party, virtualized server (cloud) environment are technically impractical and can increase risks to the physical and logical network security controls in place.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security Standards: NIST

***Source**: https://www.nist.gov/*

The National Institute of Standards and Technology (NIST), under the U.S. Department of Commerce, creates standards and guidelines pertaining to information security. NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The NIST cloud computing reference architecture is a generic high-level conceptual model that is a powerful tool for discussing the requirements, structures, and operations of cloud computing. The design of the NIST cloud computing reference architecture serves the following objectives:

- Illustrates various cloud services in the context of an overall cloud computing conceptual model
- Provides technical references to US Government (USG) agencies and other consumers to understand, discuss, categorize, and compare cloud services
- Communicates and analyzes security, interoperability, and portability candidate standards and reference implementations

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Factors Defined by the NIST Cloud Computing Reference Architecture

The NIST cloud computing reference architecture defines five major actors.

- **Cloud Consumer**

  A cloud consumer is a person or organization that maintains a business relationship with, and uses the service from, a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service.

- **Cloud Provider**

  A cloud provider can be a person, an organization, or an entity responsible for making a service available to cloud consumers. A cloud provider builds the requested software/platform infrastructure services, manages the technical infrastructure required for providing the services, provisions the services at agreed-upon service levels, and protects the security and privacy of the services.

- **Cloud Auditor**

  A cloud auditor is a party that can conduct an independent assessment of cloud services, information system operations, performance, and the security of a cloud computing implementation. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, and adherence to service-level agreement (SLA) parameters. For security auditing, a cloud auditor can assess the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the system's security requirements. The security auditing should include the verification of compliance with regulation and security policy.

hidoo1.ir

- **Cloud Broker**

  The NIST Reference Architecture, SP 500-292, 19, defines a cloud broker as an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. Cloud brokers provide services in the following three categories.

  - **Intermediation:** A cloud broker enhances a given service by improving a specific capability and providing value-added services to cloud consumers. The improvement can be the management of access to cloud services, identity management, performance reporting, enhanced security, etc.
  - **Aggregation:** A cloud broker combines and integrates multiple services into one or more new services. The broker provides data and service integration and ensures secure data movement between the cloud consumer and multiple cloud providers.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

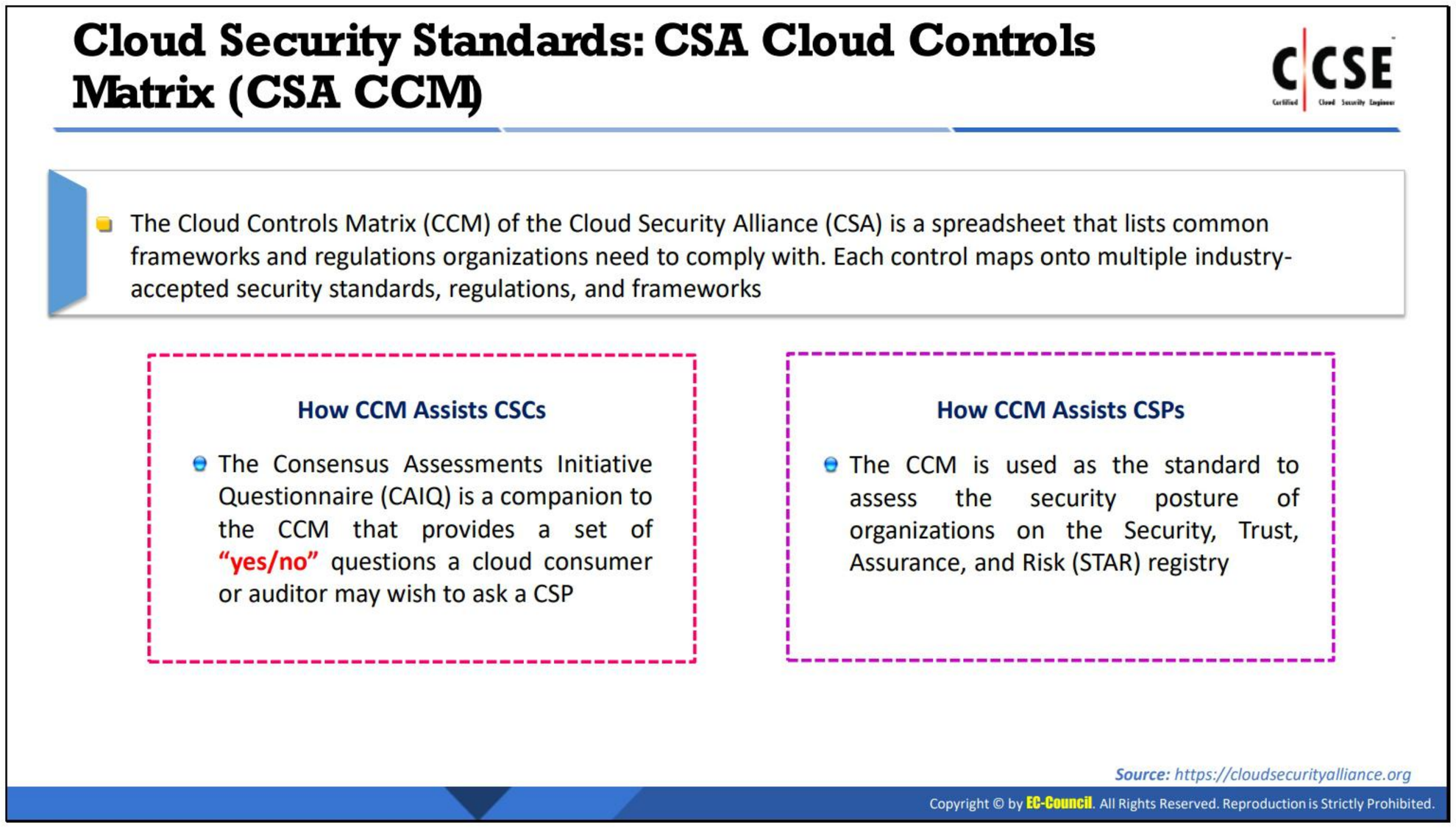
- **Arbitrage:** Service arbitrage is similar to service aggregation, except that the services being combined/consolidated are not fixed. Service arbitrage implies that a cloud broker has the flexibility to choose services from multiple service providers.

- **Cloud Carrier**

  A cloud carrier acts as an intermediary that provides the connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication, and other access devices. A cloud provider sets up service-level agreements (SLAs) with a cloud carrier to provide services consistent with the terms in the SLAs offered to cloud consumers. Further, the cloud provider may require the cloud carrier to provide dedicated and encrypted connections between cloud consumers and cloud providers.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Security Standards: CSA Cloud Controls Matrix (CSA CCM)

***Source**: https://cloudsecurityalliance.org/*

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing. It is a spreadsheet that lists 16 domains covering all key aspects of cloud technology. Each domain is broken up into 133 control objectives. The CCM can be used as a tool to systematically assess cloud implementation by providing guidance on which security controls should be implemented by which actor in the cloud supply chain. The controls in the CCM are mapped against industry-accepted security standards, regulations, and control frameworks including the following:

- ISO 27001/27002/27017/27018
- NIST SP 800-53
- AICPA TSC
- ENISA Information Assurance Framework
- German BSI C5
- PCI DSS
- ISACA COBIT
- NERC CIP

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Working of CCM

The Cloud Controls Matrix (CCM) is a spreadsheet that lists common frameworks and regulations organizations need to comply with. Each control maps onto multiple industry-accepted security standards, regulations, and frameworks, which implies that fulfilling the CCM controls also fulfills the requirements for the accompanying standards and regulations they map onto. This reduces the need for multiple frameworks and simplifies cloud security by allowing the user to view all of the common cloud standards in one place. For each control, the user can view all of the different requirements it fulfills. Each control in the CCM indicates who should fulfill the control (the CSP or CSC) as well as the type of cloud model (IaaS, PaaS, or SaaS) or cloud environment (public, hybrid, or private) the control applies to. The CCM clarifies the roles and responsibilities between a CSP and CSC by delineating the control guidance relevant to each party.

How CCM Assists CSCs

- **Use the CCM to assess cloud vendors or in place of a request for proposal (RFP):** The Consensus Assessments Initiative Questionnaire (CAIQ) is a companion to the CCM that provides a set of yes/no questions a CSC or auditor may wish to ask a CSP. Based on the security controls in the CCM, the questions can be used to document which security controls exist in a provider's IaaS, PaaS, and SaaS offerings. Organizations often use CAIQ to implement additional protection by building a request for proposal (RFP) with the information from CAIQ. Organizations can then verify the validity of a vendor's answers during the RFP interview.

hide01.ir

How CCM Assists CSPs

- **Use the CCM to submit to CSA's public registry:** The CCM is used as a standard to assess the security posture of organizations on the Security, Trust, Assurance, and Risk (STAR) registry. The STAR program promotes flexible, incremental, and multi-layered certifications that integrate with popular third-party assessments to avoid the duplication of effort and cost. Security providers can fill out the extended question set that aligns with the CCM and send it to potential and current clients to demonstrate compliance with industry standards, frameworks, and regulations. It is recommended that providers submit the completed CAIQ to the STAR registry so that it is publicly available to all clients.

Security Domains Covered by CCM

The domains covered in the current version of the Cloud Controls Matrix (CCM) are as follows.

- Application and interface security
- Audit and assurance
- Business continuity management and operational resilience
- Change control and configuration management
- Data security and privacy (DSP; previously DSI)
- Data center security
- Cryptography, encryption, and key management

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

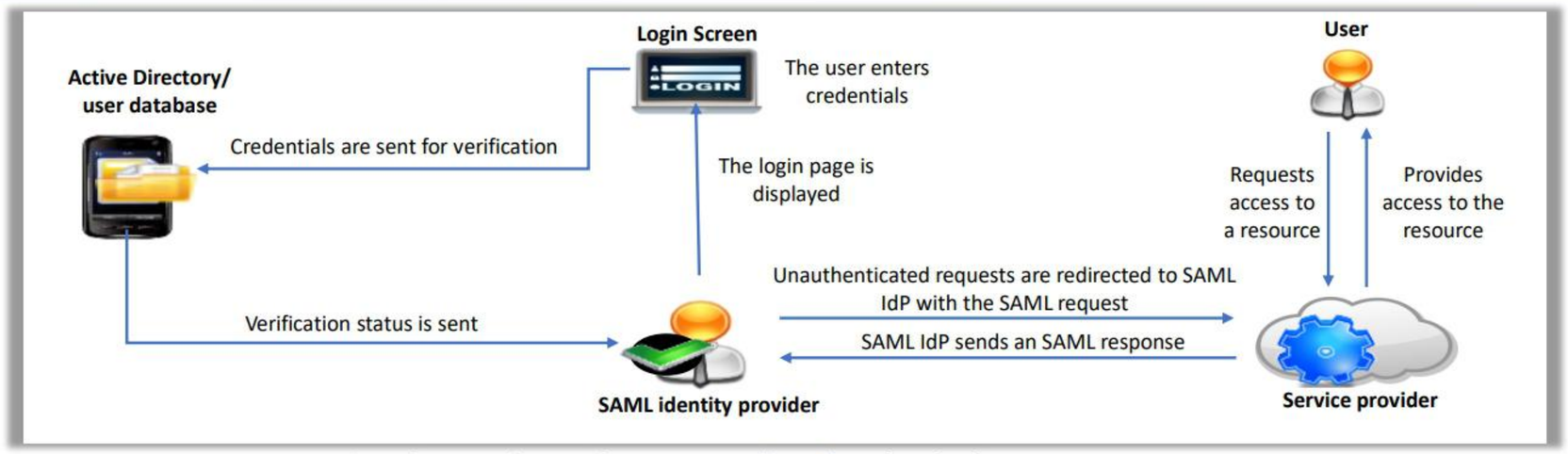
- Governance, risk management, and compliance
- Human resources security
- Identity and access management
- Infrastructure and access management
- Infrastructure and virtualization
- Interoperability and portability
- Universal endpoint management
- Security incident management, e-discovery, and cloud forensics
- Supply-chain management, transparency, and accountability
- Threat and vulnerability management

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Standards: SAML 2.0

- The OASIS **Security Assertion Markup Language (SAML) 2.0** standard defines an XML-based framework for describing and exchanging authentication and authorization information between an identity provider (IdP) and service provider (SP)
- The SAML framework defines three roles: **identity provider** (IdP), **service provider** (CSP), and **principal** (user)
- SAML provides the following two types of sign-in flows
  - **IdP-initiated flow**: In this sign-in flow, the principal accesses the SP from an intermediary IdP webpage
  - **SP-initiated flow**: In this sign-in flow, the principal accesses the resource directly from the SP's website



Security Assertion Markup Language (SAML) Authentication Process

Source: http://docs.oasis-open.org

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

Cloud Security Standards: SAML 2.0

***Source**: http://docs.oasis-open.org/*

The OASIS Security Assertion Markup Language (SAML) 2.0 standard defines an XML-based framework for describing and sharing information related to authentication and authorization information between an identity provider (IdP) and service provider (SP). SAML allows web-based single sign-on (SSO) and identity federation. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The OASIS SAML standard defines precise syntaxes and rules for requesting, creating, communicating, and using these SAML assertions.

Working of SAML

The SAML framework defines the following three roles:

- Identity provider (IdP)
- Service provider (SP): a CSP
- Principal: a user

SAML provides the following two types of sign-in flows.

- **IdP-initiated flow**: In this sign-in flow, the principal accesses the SP from an intermediary IdP webpage.
- **SP-initiated flow**: In this sign-in flow, the principal accesses the resource directly from the SP website.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The IdP is the central authority that grants access and exchanges identity and access information with an SP through SAML assertion. In IdP-initiated flow, the principal is authenticated with a single set of credentials provided to the IdP once and gains access to all the SAML applications. In SP-initiated flow, an unauthenticated principal is redirected to the IdP portal for sign-on before gaining access.

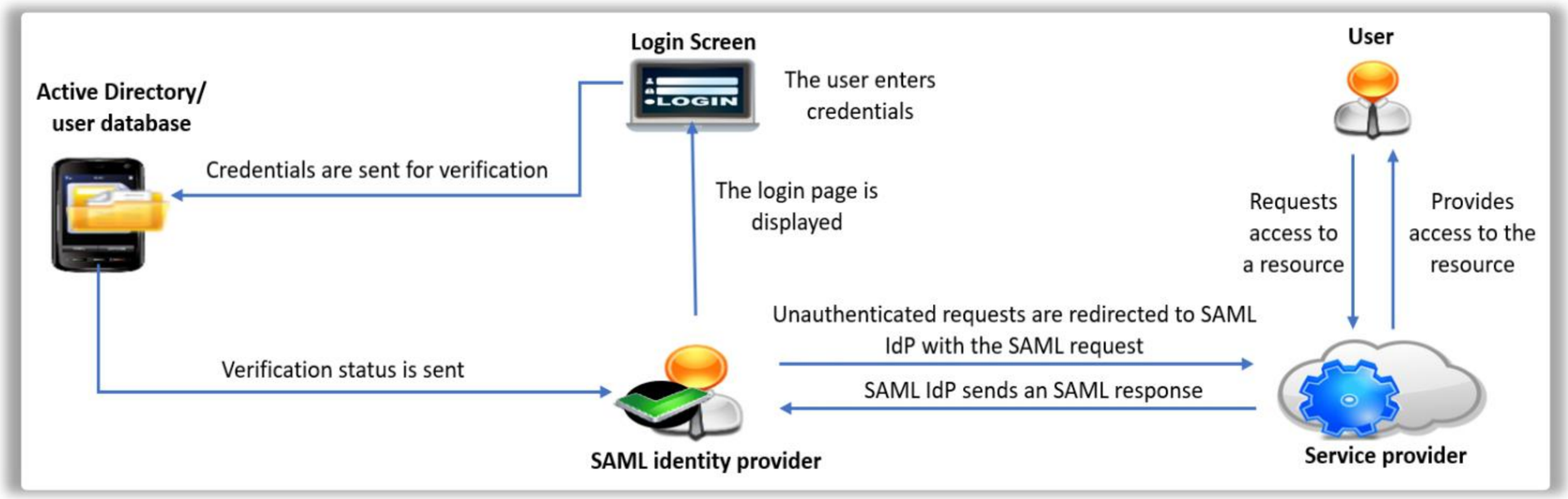
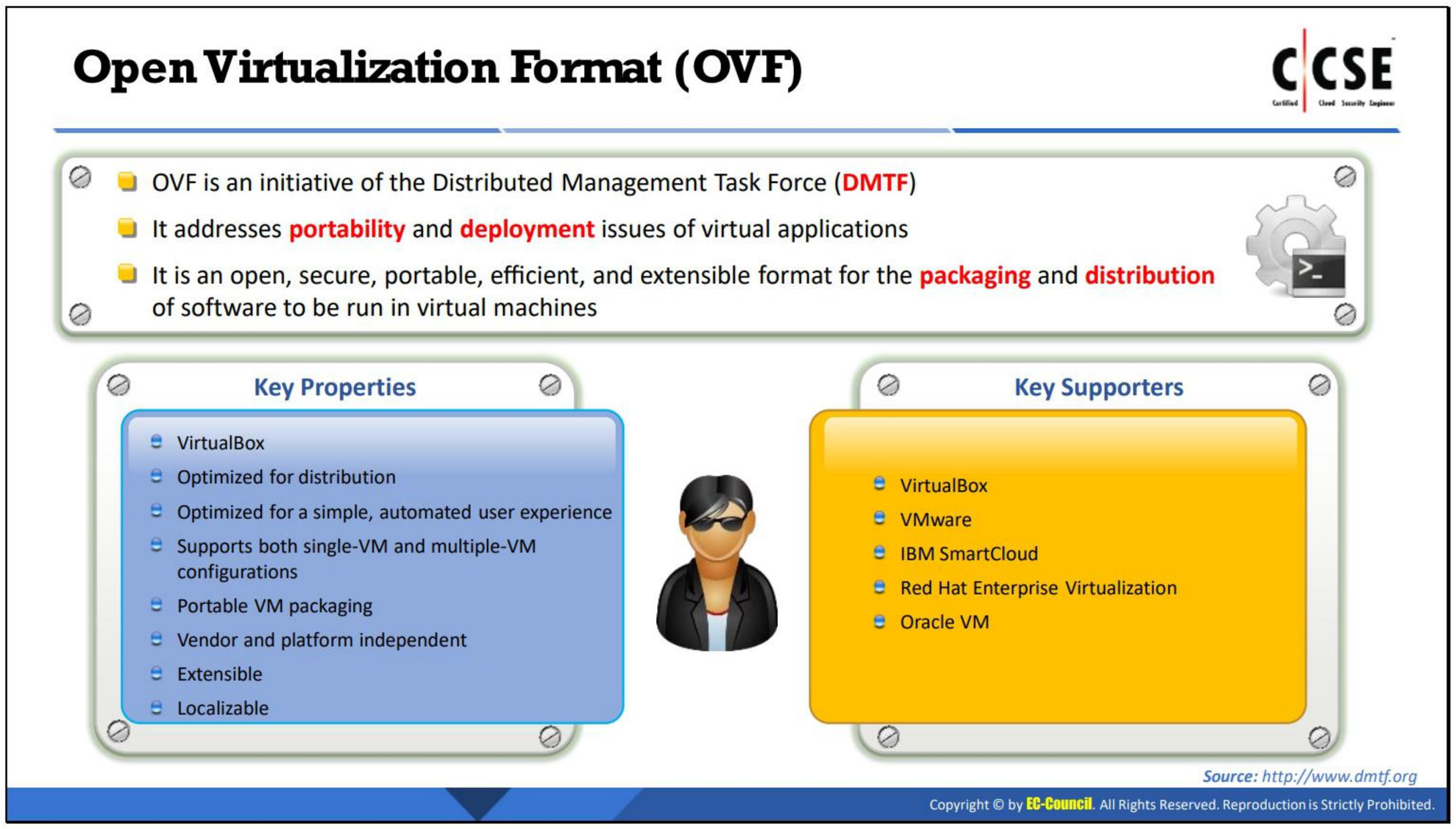


Figure 11.1: Security Assertion Markup Language (SAML) Authentication Process

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Open Virtualization Format (OVF)

Source: *http://www.dmtf.org*

OVF is an initiative of the Distributed Management Task Force (DMTF), which addresses portability and deployment issues in virtual applications. It is an open, secure, portable, efficient, and extensible format for packaging and distributing software to be run on virtual machines (VM).

The OVF specification improves the interoperability and portability of workloads for virtualization and cloud computing environments.

Key Focus Areas of OVF

- **Optimized for distribution:** OVF supports content verification and integrity checking based on industry-standard public key infrastructure (PKI), and it provides a basic scheme for the management of software licensing.
- **Optimized for a simple, automated user experience:** OVF supports the validation of an entire package and each VM or metadata component of the OVF during the installation phases of the VM lifecycle management process. It also focuses on the package of relevant user-readable descriptive information that a virtualization platform can use to streamline the installation experience.
- **Supports both single-VM and multiple-VM configurations:** OVF supports both standard single-VM packages and packages containing complex, multitier services consisting of multiple interdependent VMs.
- **Portable VM packaging:** OVF is a virtualization platform–neutral standard that also allows platform-specific enhancements to be captured. It supports the full range of virtual hard

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

disk formats used for hypervisors today and is extensible, i.e., it also supports formats that may emerge in the future. It captures VM properties concisely and accurately.

- **Vendor and platform independent:** OVF does not rely on the use of a specific host platform, virtualization platform, or guest operating system.
- **Extensible:** OVF is useful for present-day needs and can be extended even for future needs. It is designed to be extended as the industry moves forward with virtual computing technology. It also supports and permits the encoding of vendor-specific metadata to support specific vertical markets.
- **Localizable:** OVF is developed through a collaboration of the industry's key vendors. It is developed in an accepted industry forum as a future standard for portable VMs.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Open Cloud Computing Interface (OCCI)

- It is based upon **the Representational State Transfer (REST)** Protocol and **API** for all kinds of management tasks
- It provides a flexible API that focuses on integration, portability, interoperability, and innovation with a high **degree of extensibility**
- The current release of the OCCI is suitable to serve many models in addition to **IaaS**, **PaaS**, and **SaaS**
- The OCCI specification consists of an OCCI core specification, OCCI rendering specification, and OCCI extension specification

Key Supporters

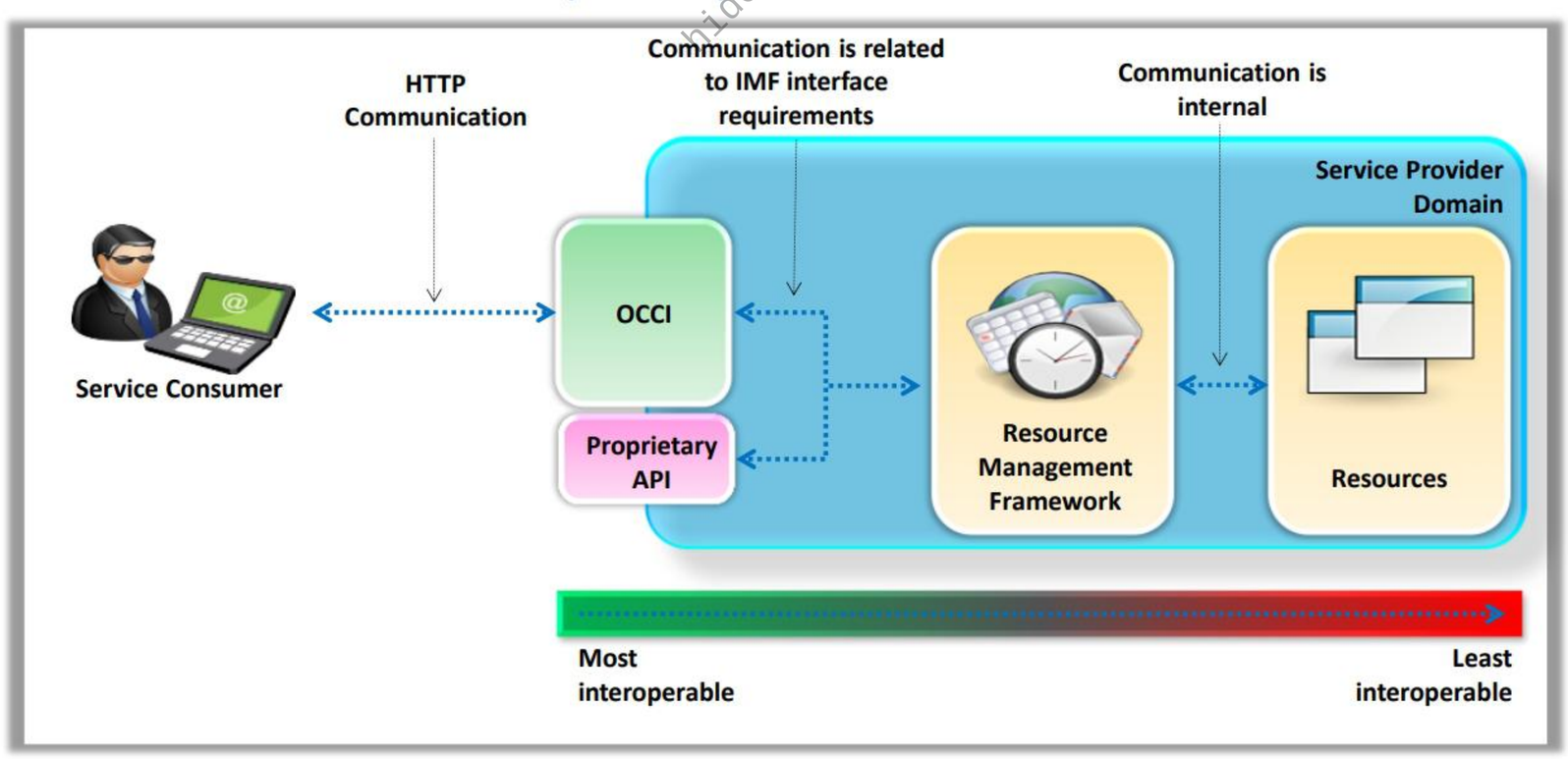


Source: http://occi-wg.org

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

Open Cloud Computing Interface (OCCI) (Cont'd)

OCCI's place in a provider's architecture



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

Open Cloud Computing Interface (OCCI)

***Source**: http://occi-wg.org*

OCCI is an open protocol for all cloud computing services. It comprises a set of open community-led specifications delivered through the Open Grid Forum, which defines how infrastructure service providers can deliver their compute, data, and network resource offerings through a standardized interface. OCCI aims at providing commonly understood semantics, syntaxes, and

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

a means of management in the domain of consumer-to-provider IaaS. OCCI's set of features includes implementation, protocol, and API stack, all of which provide management-level functionalities for the cloud service.

OCCI defines a set of specifications that define how infrastructure service providers can provide services that uphold certain universal standards. The aim of OCCI is the rapid development of clean, open, specific, and API-featured cloud offerings. It provides a flexible API that focuses on integration, portability, interoperability, and innovation with a high degree of extensibility.

The Cloud Computing Architectural Framework is based on the requirements of cloud computing stakeholders and is custom-made with respect to the needs of organizations, networks, service providers, customers, and security professionals.

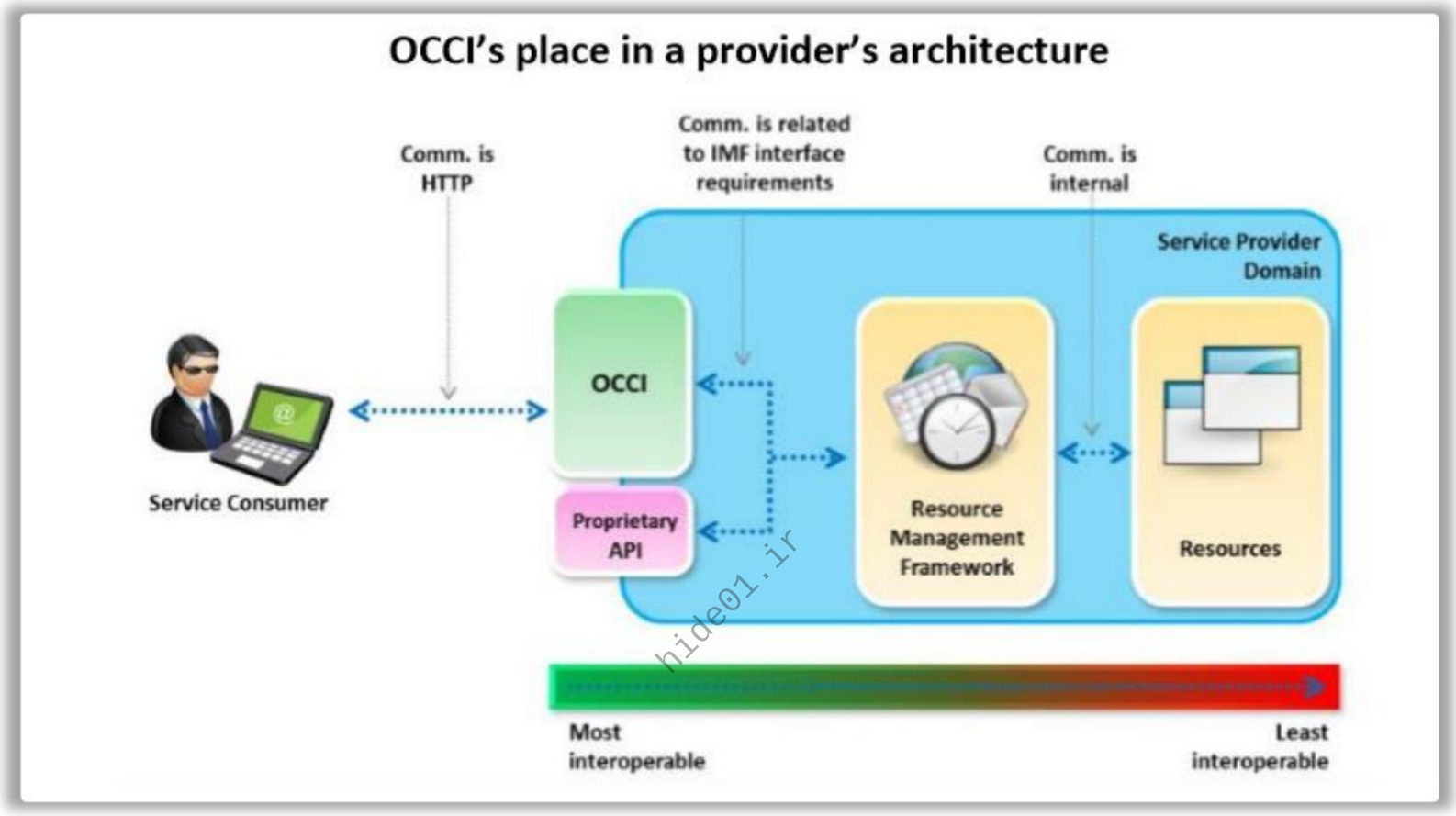


Figure 11.2: OCCI's Place in Provider's Architecture

The OCCI specification is released as a suite of complementary documents that together form the complete specification. OCCI specifications are divided into three categories:

- OCCI Core specification
- OCCI Rendering specifications
- OCCI Extension specifications

The OCCI Core specification defines the OCCI core model that interacts with rendering and is explained through extensions. The OCCI Core specification consists of a single document defining the OCCI Core Model.

OCCI Rendering specifications define each rendering of the Core Model and how multiple renderings interact with the same instances of the OCCI Core Model automatically while supporting extension rules. OCCI Rendering specifications consist of multiple documents, each describing a particular rendering of the OCCI Core Model.

The Extension documents describe additions to the OCCI Core Model defined within the OCCI specification suite.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Data Management Interface (CDMI)

- CDMI provides a **functional interface** based on RESTful principles that applications use to create, retrieve, update, and delete data elements from the cloud
- This interface provides client with capabilities to view the cloud **storage** offering and manage container data

Key Supporters

- Microsoft Azure Storage API
- Rackspace cloud files API

Main Tasks

- Gives details about all the **services** provided to the client in the cloud storage
- Describes how data are **managed** or **stored** in containers
- Specifies how **metadata** are connected with containers and the objects associated with them

Helps Administrators in Certain Domains

- Clearly defines how user credentials are mapped to principals used in an **access-control list** (ACL)
- Grants special **privileges** to certain cloud users or groups
- Allows allocation of resources to external **user authorization** systems (e.g., LDAP or Active Directory)

Source: http://www.snia.org/cdmi

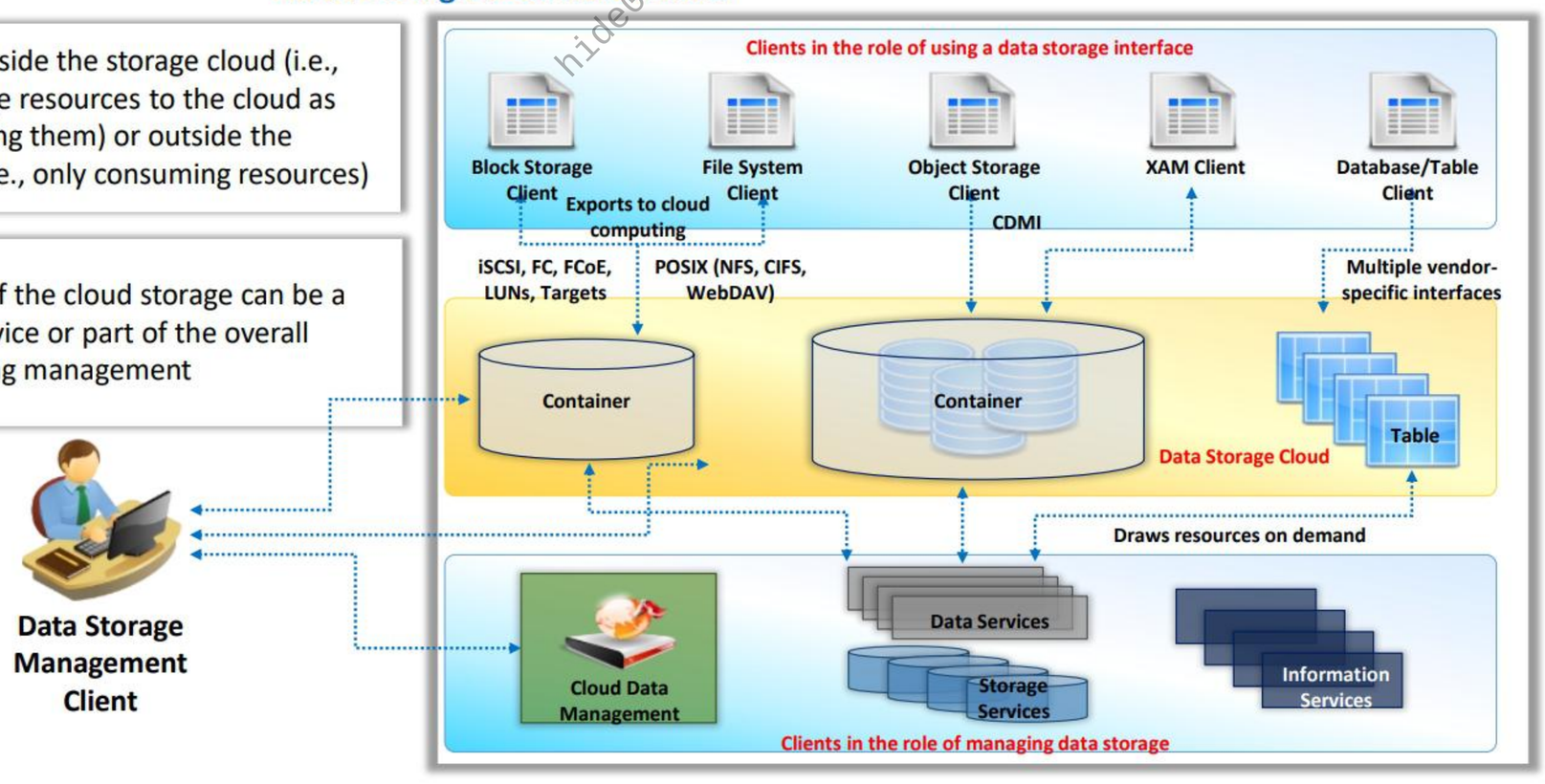
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Data Management Interface (CDMI) (Cont'd)

Cloud Storage Reference Model

Clients can be inside the storage cloud (i.e., providing storage resources to the cloud as well as consuming them) or outside the storage cloud (i.e., only consuming resources)

Management of the cloud storage can be a standalone service or part of the overall cloud computing management



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

Cloud Data Management Interface (CDMI)

Source: *http://www.snia.org/cdmi*

The Cloud Data Management Interface (CDMI) is a technical workgroup developed by the Storage Networking Industry Association (SNIA) to create a framework for interoperability between clouds and standards associated with the cloud computing industry. CDMI cloud storage

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

standards can be implemented by cloud service providers (CSPs) in both public and private clouds.

CDMI defines applications that are used to create, retrieve, update, and delete data from the cloud. This interface provides clients with capabilities to view the cloud storage service and manage container data.

CDMI provides a functional interface based on RESTful principles that applications abide by to create, retrieve, update, and delete data elements from the cloud. Metadata can be set on containers and the data elements they contain through this interface. Administrative and management applications can manage containers, accounts, security access, and monitoring/billing information, even for storage accessible by other protocols.

- **CDMI Metadata**

  CDMI allows users to place metadata directly in the storage object. The metadata can be archived, backed up, protected, and retained, along with the actual data. CDMI uses many types of metadata such as data system metadata, Hypertext Transfer Protocol (HTTP) metadata, storage system metadata, and user metadata. Metadata specify the data requirements based on individual data elements or groups of data elements.

- **Data System Metadata**

  Data system metadata are metadata specified by a CDMI client and are a component of objects. Data system metadata abstractly specify the data requirements associated with data services that are deployed in the cloud storage system.

- **HTTP Metadata**

  HTTP metadata are metadata related to the use of the HTTP protocol (e.g., ContentLength, and Content-Type). HTTP metadata are not specifically related to this international standard but should be discussed to explain how CDMI uses the HTTP standard.

- **Storage System Metadata**

  Storage system metadata are metadata generated by the storage services in the system (e.g., creation time and size) to provide useful information to a CDMI client.

- **User Metadata**

  User metadata consist of client-defined JavaScript Object Notation (JSON) strings, arrays, and objects that are stored in the metadata field. The namespace used for user metadata names is self-administered, and user metadata names cannot begin with the prefix “cdmi_”.

CDMI defines both a means to manage the data and a means to store and retrieve the data. The means to store and retrieve the data is called a data path. The means to manage the data is called the control path. CDMI specifies both a data path interface and control path interface.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The main functions of CDMI are as follows:

- Allows clients to discover the capabilities of the cloud storage offering
- Manages containers and the data placed in them
- Allows metadata to be associated with containers and the objects they contain

It supports domains that allow administrators to:

- Determine how user credentials are mapped to principals used in an access-control list (ACL)
- Allow the granting of special cloud-related privileges
- Allow delegation to external user authorization systems (e.g., Lightweight Directory Access Protocol (LDAP) or Active Directory)

Cloud Storage Reference Model

The cloud storage reference model hosts multiple types of cloud data storage interfaces that support legacy and new applications. Data storage interfaces are provided based on the demand of the resource pool, and the storage capacity is drawn from a pool provided by storage services.

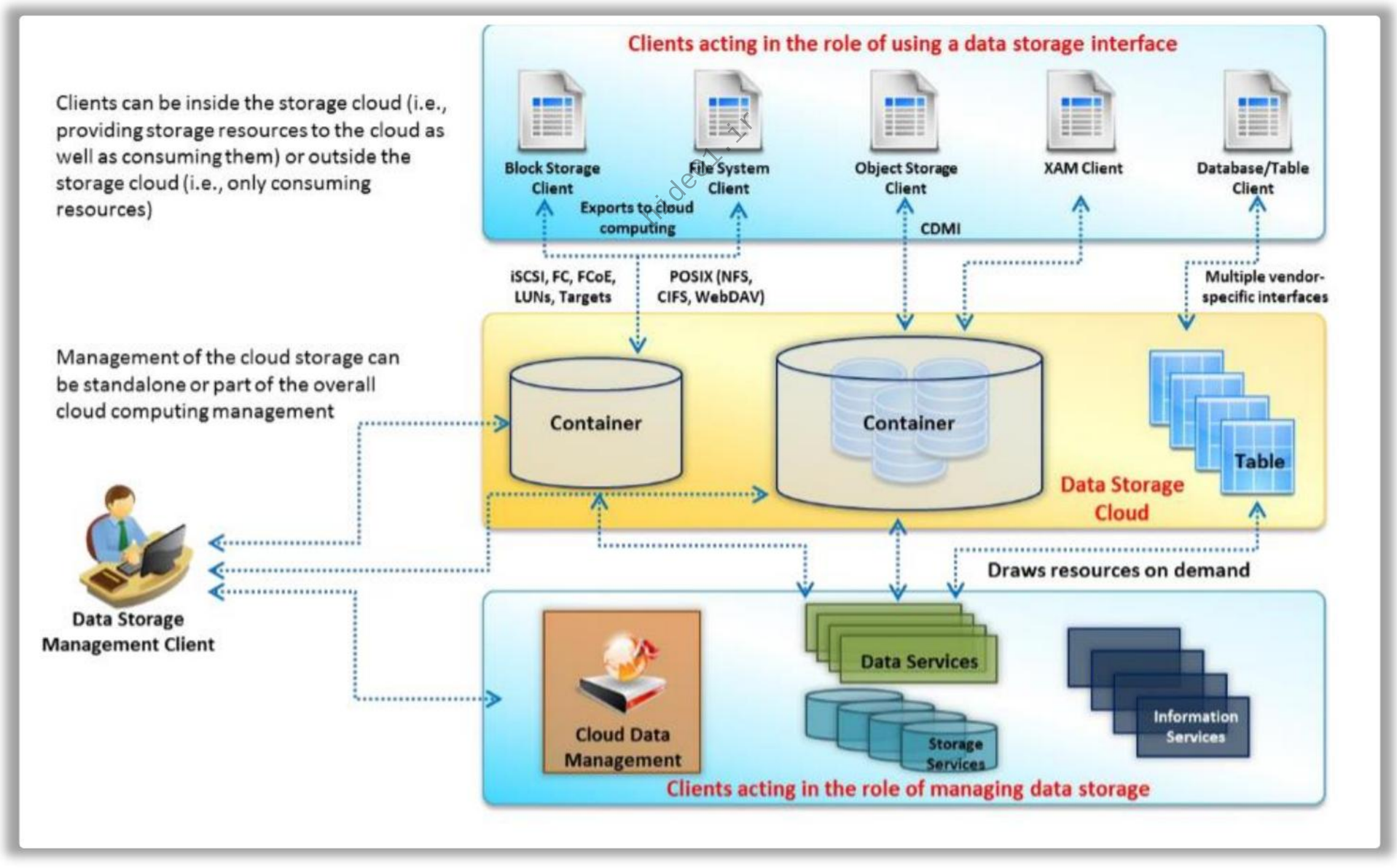
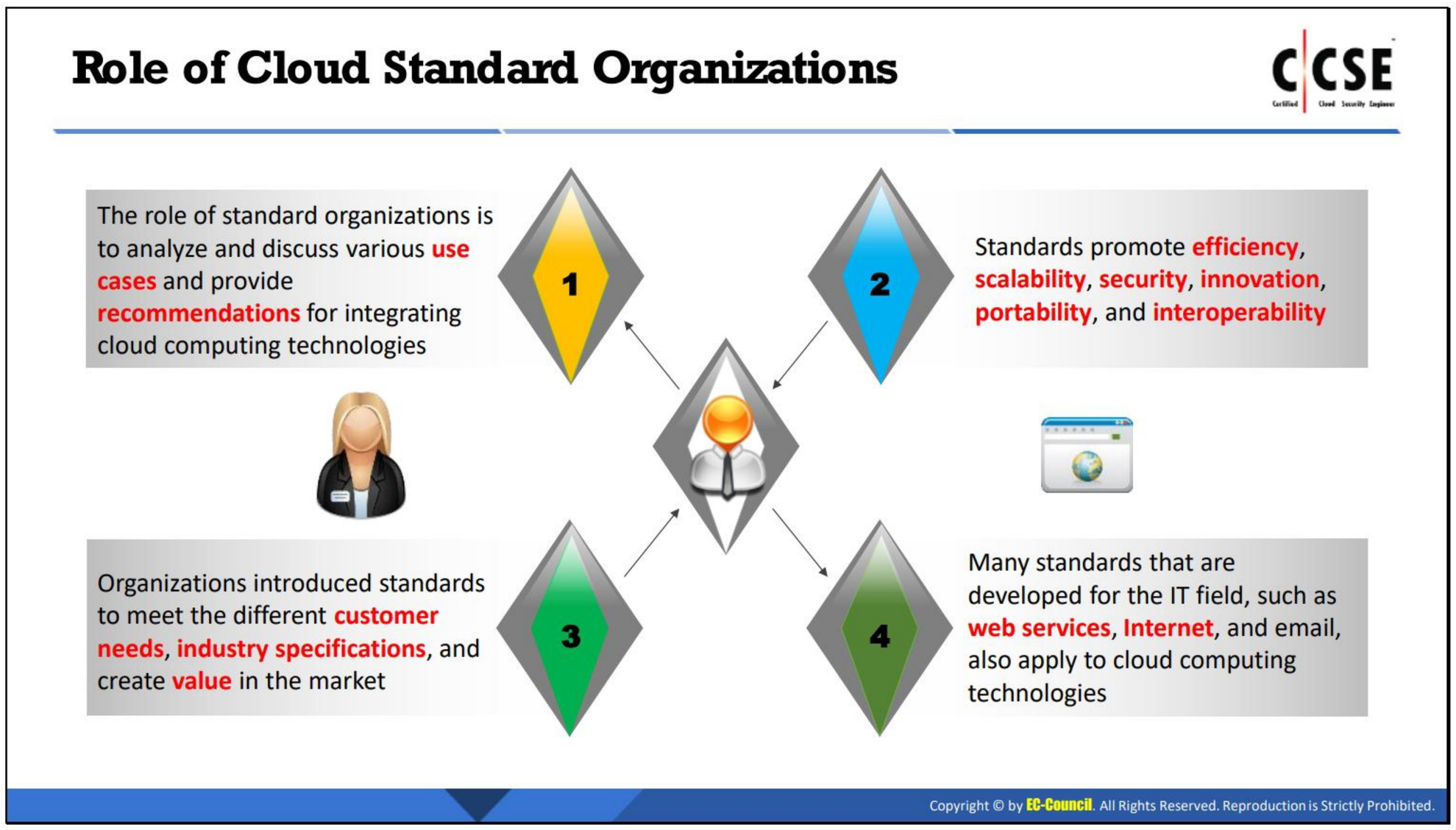


Figure 11.3: Cloud Storage Reference Model

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Role of Cloud Standard Organizations

The roles of cloud standard organizations are as follows.

hide01.ir

- Cloud computing standards promote efficiency, scalability, security, innovation, portability, and interoperability.
- Cloud standard organizations analyze and discuss various use cases and provide recommendations for integrating cloud computing technologies.
- Many organizations have introduced standards to meet different customer needs and industry specifications as well as create value in the market.
- Some standards are still in the evolving phase, and standard organizations develop them explicitly to support cloud computing functions and specifications.
- Many standards developed for information technologies such as web services, Internet, and email also support cloud computing technologies.
- Many organizations such as NIST, DMTF, SNIA, and IEEE are developing standards and providing best practices for cloud computing.
- Standard developing organizations (SDOs) are working on devising benchmarking tools and key indicators for measuring the products, solutions, and services available in the cloud.
- The main areas of focus for most SDOs are interoperability, portability, and security.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Activities of Different Cloud Standard Organizations

	SaaS	PaaS	IaaS	DaaS
Provisioning			OGF/DMTF	SNIA
Metering and Billing				SNIA
Security			OGF/DMTF/CSA	SNIA (IETF)
Privacy				
Quality of Service			DMTF	SNIA
Identity		OASIS		
Client Application Interface				
Development Platform				
Virtual Machine Interface			DMTF	
Data Storage Interface				SNIA

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

Activities of Different Cloud Standard Organization

The table below presents target cloud areas of cloud standard organizations for different cloud service delivery models.

hide01.ir

	SaaS	PaaS	IaaS	DaaS
Provisioning			OGF/DMTF	SNIA
Metering and Billing				SNIA
Security			OGF/DMTF/CSA	SNIA (IETF)
Privacy				
Quality of Service			DMTF	SNIA
Identity		OASIS		
Client Application Interface				
Development Platform				
Virtual Machine Interface			DMTF	
Data Storage Interface				SNIA

Figure 11.4: Target Cloud Areas of Cloud Standard Organizations

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Organizations Involved in Development of Standards for Cloud Computing

Cloud computing standards are practices widely accepted by many cloud organizations to maintain homogeneity in cloud operations. For example, CPU speeds measured by providers vary in terms of terminology and measurement units and lack consistency in standards. Amazon Web Services (AWS) defines CPU speeds with the Elastic Compute Unit, Google with the Google Compute Engine Unit, and Microsoft with clock speed. Homogeneity in cloud services facilitates the simplification of the migration process from one service provider to another. Interoperability between CSPs can be simplified when a common set of cloud standards is followed.

Cloud standard development organizations have drafted best practices and standards for the critical areas in cloud computing services.

The following are some of the important organizations in the world that are developing standards for cloud computing.

- National Institute of Standards and Technology (NIST)
- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- Open Cloud Consortium (OCC)
- Open Grid Forum (OGF)
- The Object Management Group (OMG)
- Storage Networking Industry Association (SNIA)
- Institute of Electrical and Electronics Engineers (IEEE)
- European Telecommunications Standards Institute (ETSI)
- Organization for the Advancement of Structured Information Standards (OASIS)

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: National Institute of Standards and Technology (NIST)

Source: *http://www.nist.gov*

hide01.ir

NIST published the Cloud Computing Standards Roadmap to evaluate the landscape of existing cloud computing standards for security, portability, and interoperability using different models, studies, use cases, etc. NIST identified areas of standardization gaps and prioritized key areas where standards need to be developed.

NIST defines cloud computing as a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST created the following working groups to provide guidance and standards for federal cloud computing initiatives:

- Cloud Computing Reference Architecture and Taxonomy Working Group
- Cloud Computing Security Working Group
- Cloud Computing Target Business Use Cases Working Group
- Cloud Computing Standards Roadmap Working Group
- Cloud Computing Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) Working Group

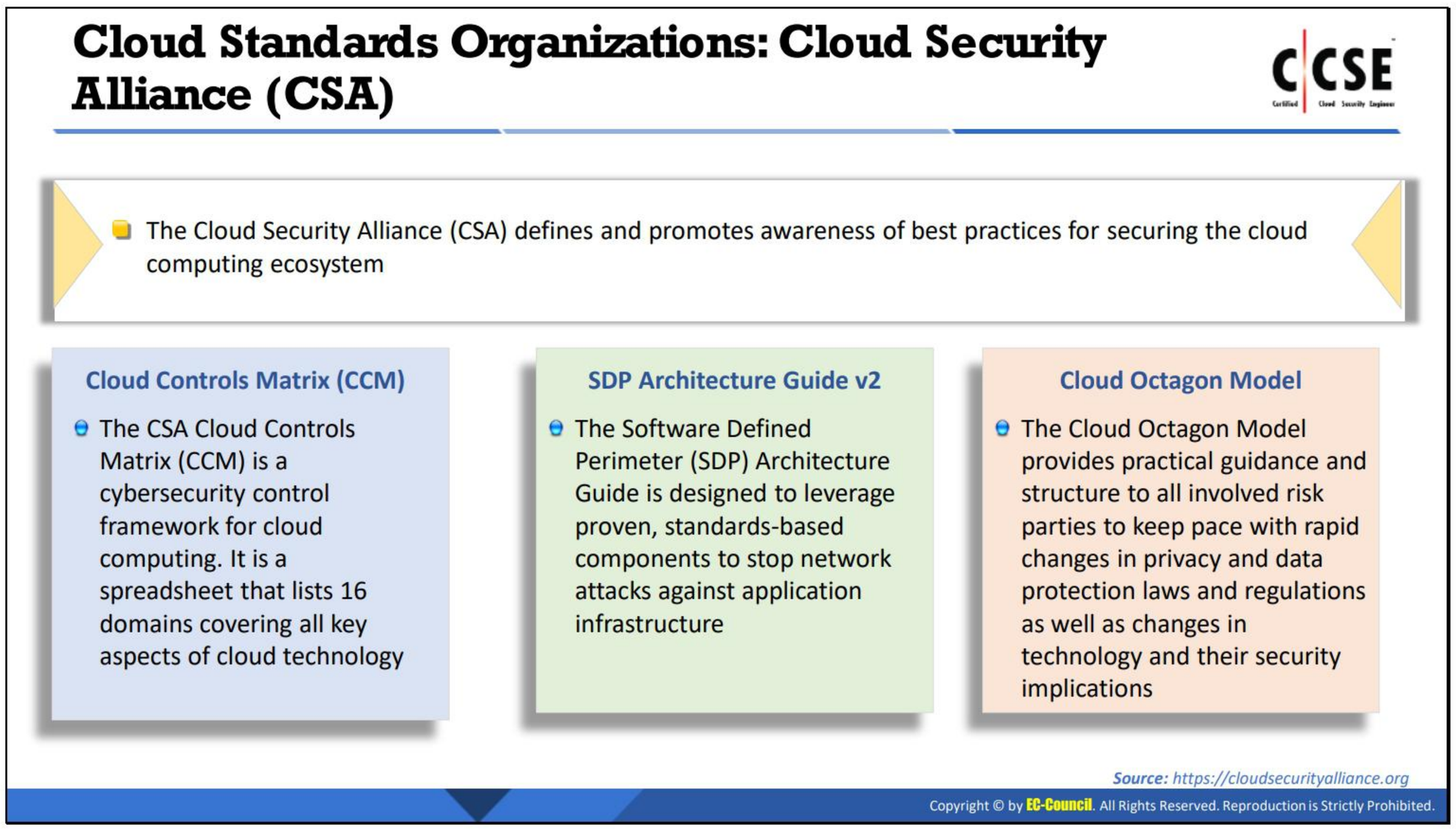
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NIST has finalized its first set of guidelines for managing security and privacy issues in cloud computing. The key guidelines include the following.

- Carefully plan the security and privacy aspects of cloud computing solutions before implementing them.
- Understand the public cloud computing environment offered by the cloud provider.
- Ensure that a cloud computing solution—i.e., both cloud resources and cloud-based applications—satisfies organizational security and privacy requirements.
- Maintain accountability over the privacy and security of data as well as applications implemented and deployed in public cloud computing environments.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: Cloud Security Alliance (CSA)

***Source**: https://cloudsecurityalliance.org/*

The Cloud Security Alliance (CSA) is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject-matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security–specific research, education, certification, events, and products. CSA's activities, knowledge, and extensive network benefit the entire community impacted by the cloud from providers to customers, governments, entrepreneurs, and the assurance industry. Further, it provides a forum through which diverse parties can create and maintain a trusted cloud ecosystem. CSA's Security Guidance for Critical Areas of Focus in Cloud Computing provides a practical, actionable roadmap to adopt the cloud paradigm safely and securely.

Leverage Frameworks and Architectures Specific to the Cloud

It is recommended to adopt core tools used by the government and regulated industries for the use and management of cloud services. Enterprises should build a foundation for secure cloud environments with proven models for mitigations, countermeasures, and capabilities specific to cloud computing.

The following tools have been used by enterprises to implement frameworks, architectures, and approaches.

- **Cloud Controls Matrix (CCM)**

  The CSA CCM is a cybersecurity control framework for cloud computing. It is a spreadsheet that lists 16 domains covering all key aspects of cloud technology. Each domain is subdivided into 133 control objectives. The CCM can be used as a tool to

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

systematically assess cloud implementation by providing guidance on which security controls should be implemented by which actor within the cloud supply chain.

- **Benefits of CCM**
  - **Strengthens information security in control environments:** The CCM delineates control guidance for the service provider and consumer. It also differentiates according to the cloud model and environment.
  - **Reduces audit complexity:** Controls map onto multiple industry-accepted security standards, regulations, and controls frameworks. Fulfilling the CCM controls also fulfills the requirements for the accompanying standards and regulations they map onto.
  - **Normalizes cloud deployment:** The CCM normalizes security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.
  - **Integrates with the STAR registry:** The CCM is used as the standard to assess the security posture of organizations on the Security, Trust, Assurance and Risk (STAR) registry. The STAR program promotes flexible, incremental, and multi-layered certifications that integrate with popular third-party assessments to avoid the duplication of effort and cost.

- **SDP Architecture Guide v2**

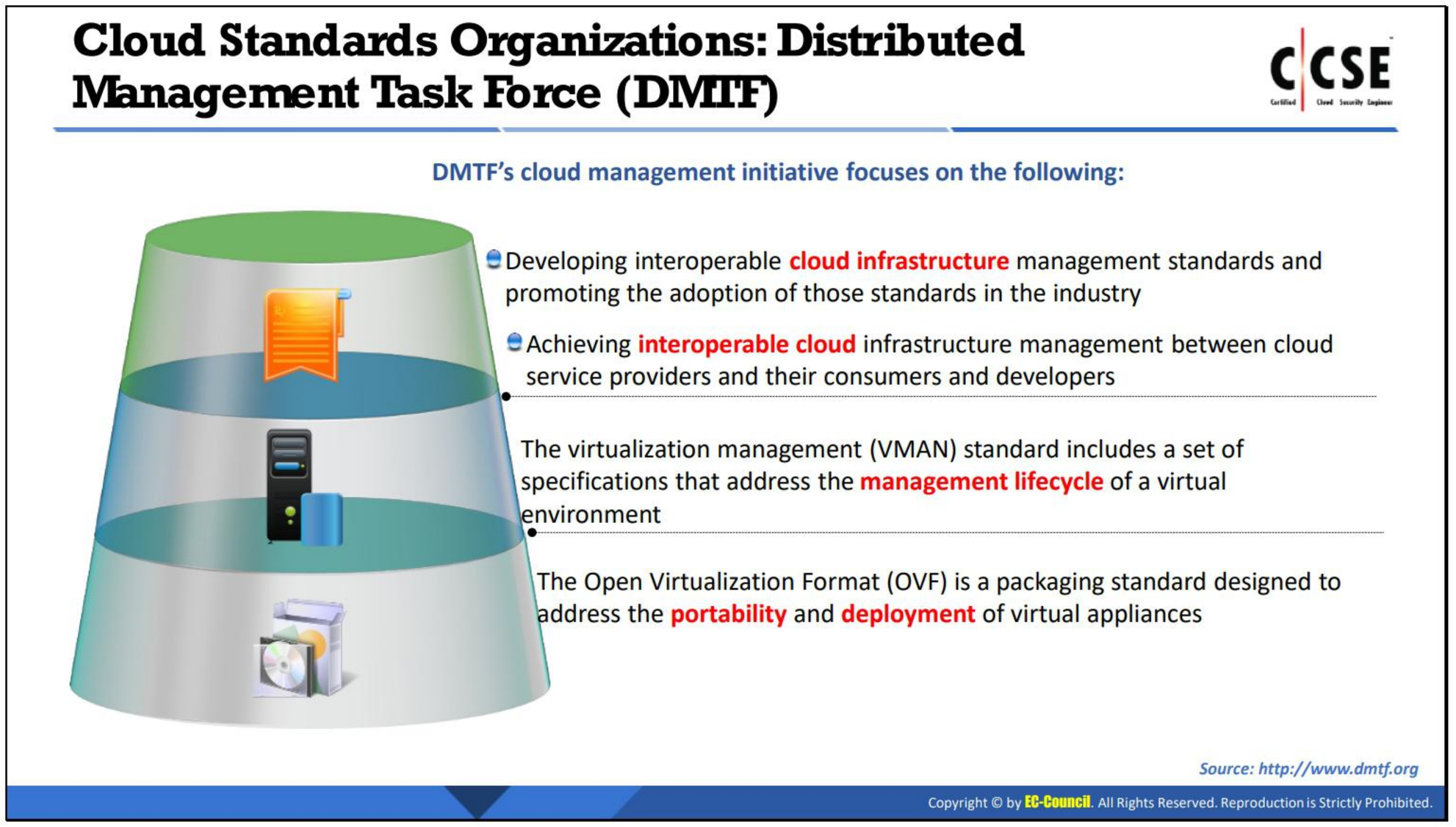
  The Software Defined Perimeter (SDP) architecture guide is designed to leverage proven, standards-based components to stop network attacks against application infrastructure. The architecture guide helps increase the awareness and adoption of SDP, improves the understanding of SDP usage in different environments, and helps enterprises successfully deploy SDP solutions based on the architecture recommendations.

- **Cloud Octagon Model**

  CSA provides an approach to assess risk in SaaS cloud computing. The Cloud Octagon Model stems from an approach conceptualized and implemented by the Cloud Security Group within the Technology & Engineering department, Corporate Information Security Office (CISO), ABN AMRO Bank NV (Netherlands). It counts such aspects as procurement, IT governance, architecture, development and engineering, service providers, risk processes, data classification, and country. The model provides practical guidance and structure to all involved risk parties to keep pace with rapid changes in privacy and data protection laws and regulations, as well as changes in technology and their security implications. The model aims to:

  - Reduce risks associated with cloud computing
  - Improve the effectiveness of the cloud risk team
  - Improve the manageability of the solution
  - Improve security

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: Distributed Management Task Force (DMTF)

Source: *http://www.dmtf.org*

The Distributed Management Task Force (DMTF) brings the IT industry together to collaborate on systems management, standards development, validation, promotion, and adoption, addressing the need for open management standards for cloud computing.

DMTF's Cloud Management Work Group (CMWG) focuses on standardizing interactions between cloud environments by developing cloud resource management protocols, packaging formats, and security mechanisms to facilitate interoperability.

The DMTF working groups promoted by the Cloud Management Initiative focus on achieving interoperable cloud infrastructure management between CSPs and their consumers and developers.

Cloud Working Groups

- Cloud Management Working Group (CMWG)
- Cloud Auditing Data Federation Working Group (CADF)
- Software Entitlement Working Group (SEWG)
- System Virtualization, Partitioning, and Clustering Working Group (SVPC)
- Cloud Management Working Group (CMWG)

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Management Working Group (CMWG)

CMWG is focused on standardizing interactions between cloud environments through specifications to achieve interoperable cloud infrastructure management between CSPs and their consumers and developers.

Cloud Auditing Data Federation Working Group (CADF)

CADF develops specifications for federating audit event data, including interface definitions and a compatible interaction model that describes interactions between IT resources for cloud deployment models. CADF is associated with CMWG to reference their resource model and interface protocol work. CADF develops open standards for audit data, which can be federated from cloud providers to evaluate customers' trust in cloud-hosted applications.

Software Entitlement Working Group (SEWG)

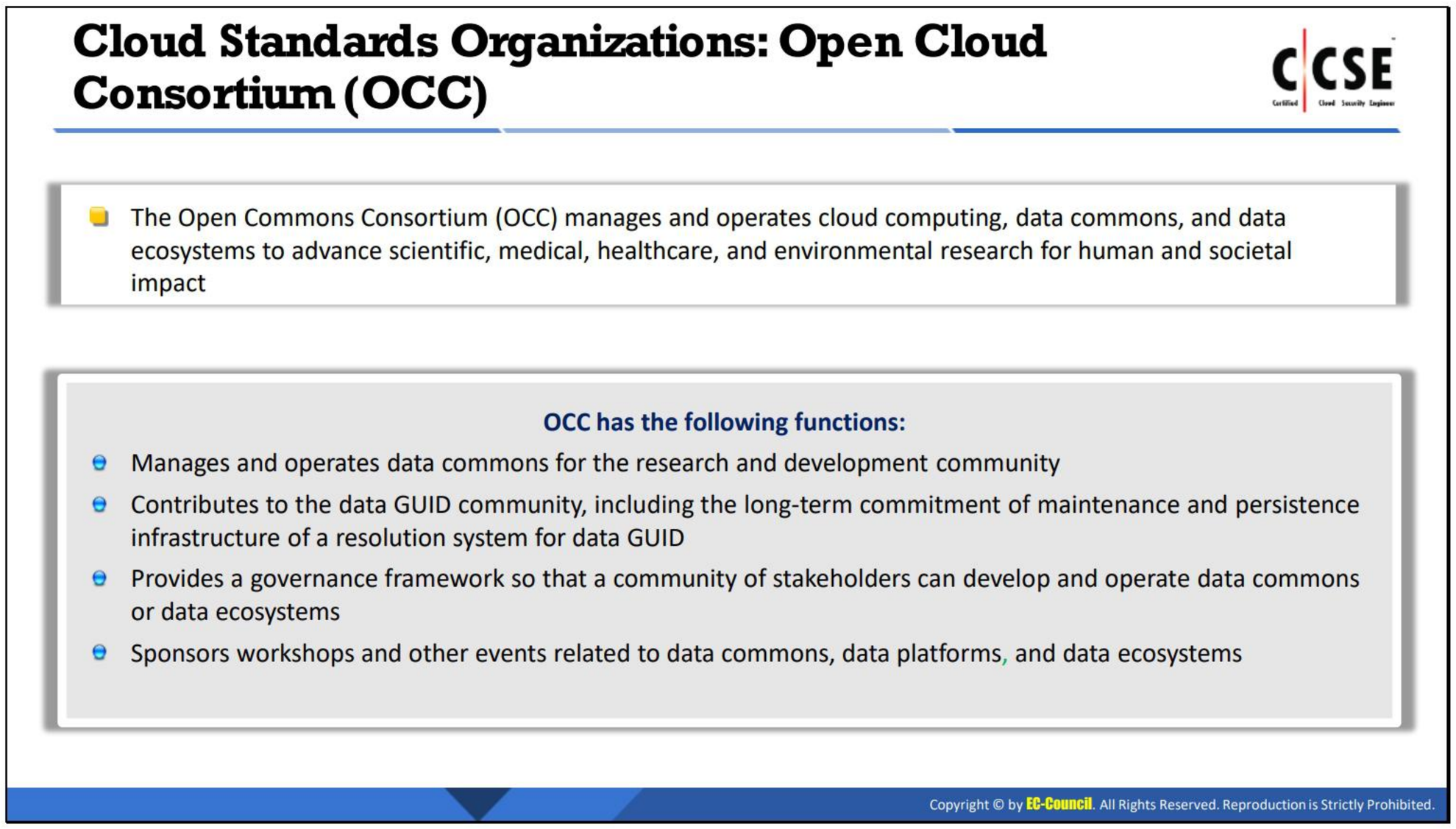
SEWG focuses on addressing software license management challenges in cloud systems and virtual environments. This group is working to develop a set of recommendations to guide the future industry standardization of software license management in these environments.

System Virtualization, Partitioning, and Clustering Working Group (SVPC)

SVPC develops DMTF standards for virtualization management. This includes the discovery, configuration, and active management of virtual computer systems. SVPC develops specifications for the packaging and distribution of virtual appliances composed of one or more virtual computer systems.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: Open Cloud Consortium (OCC)

***Source**: https://www.occ-data.org/*

OCC manages and operates cloud computing, data commons, and data ecosystems to advance scientific, medical, healthcare, and environmental research for human and societal impact.

OCC provides the following:

- Consortium and project management
- Legal agreements and governance structure
- Management and operation of cloud computing infrastructure
- Management of security and the required compliance

Activities of OCC

OCC is involved in the following activities:

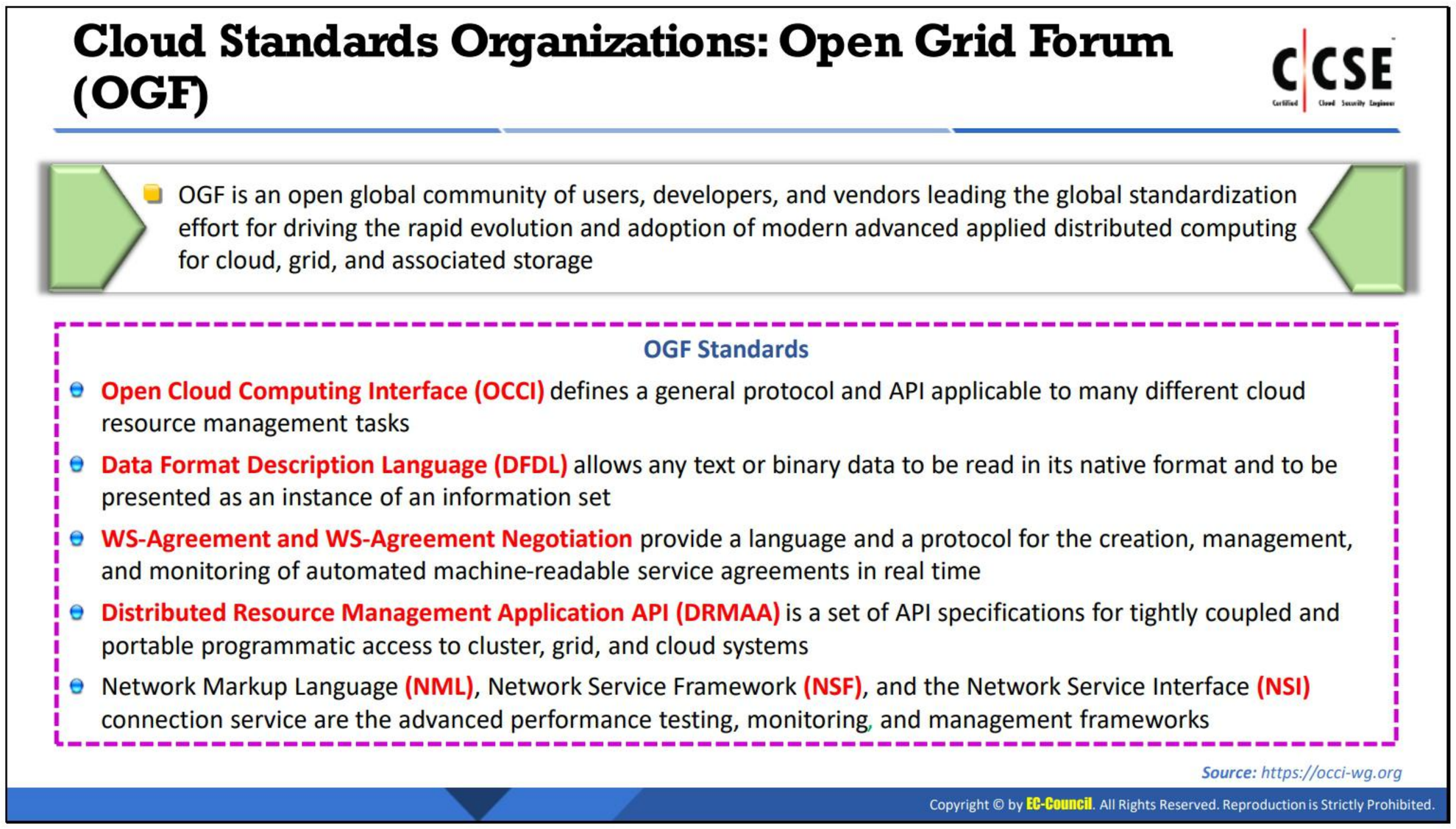
- Manages and operates data commons for the research and development community
- Develops and operates framework services so that a research community can develop and operate a data ecosystem containing data commons, data platforms, and data resources and a collection of applications over them
- Contributes to the data globally unique identifier (GUID) community including the long-term commitment of maintenance and persistence infrastructure of a resolution system for data GUID. Data GUID provides persistent data identifiers for data
- Provides a governance framework so that a community of stakeholders can develop and operate data commons or data ecosystems

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Sponsors workshops and other events related to data commons, data platforms, and data ecosystems
- Participates in working groups that develop and operate many data platforms, including the following:
    - The BloodPAC Data Commons
    - The OCC Environmental Data Commons
    - The BRAIN Commons
    - The Veterans Precision Oncology Data Commons

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: Open Grid Forum (OGF)

***Source**: https://occi-wg.org/*

OGF is an open global community of users, developers, and vendors leading the global standardization effort for driving the rapid evolution and adoption of modern advanced applied distributed computing for cloud, grid, and associated storage. OGF is focused on developing and promoting innovative, scalable techniques, applications, and infrastructures to improve productivity in the enterprise and within the international research, science, and business communities. OGF accomplishes these objectives through open forums, interactions, and events that build the community, explore trends, share optimal approaches, document findings, and consolidate these results into standards, where appropriate. The output of this process is the documentation and codification of best practices and standards that provide the basis for some of the largest and most powerful operational computing infrastructure systems.

OGF Standards

- **OCCI**: The Open Cloud Computing Interface (OCCI) specification set defines a general protocol and API applicable to many different cloud resource management tasks. OCCI began as a remote-management API for IaaS model–based services, allowing for the development of interoperable tools for common tasks, including deployment, autonomic scaling, and monitoring. OCCI is suitable to serve many other models in addition to IaaS, including PaaS and SaaS.
- **DFDL**: The Data Format Description Language (DFDL) is a language for describing text and binary data formats. A DFDL description allows any text or binary data to be read in their native format and to be presented as an instance of an information set. DFDL also allows

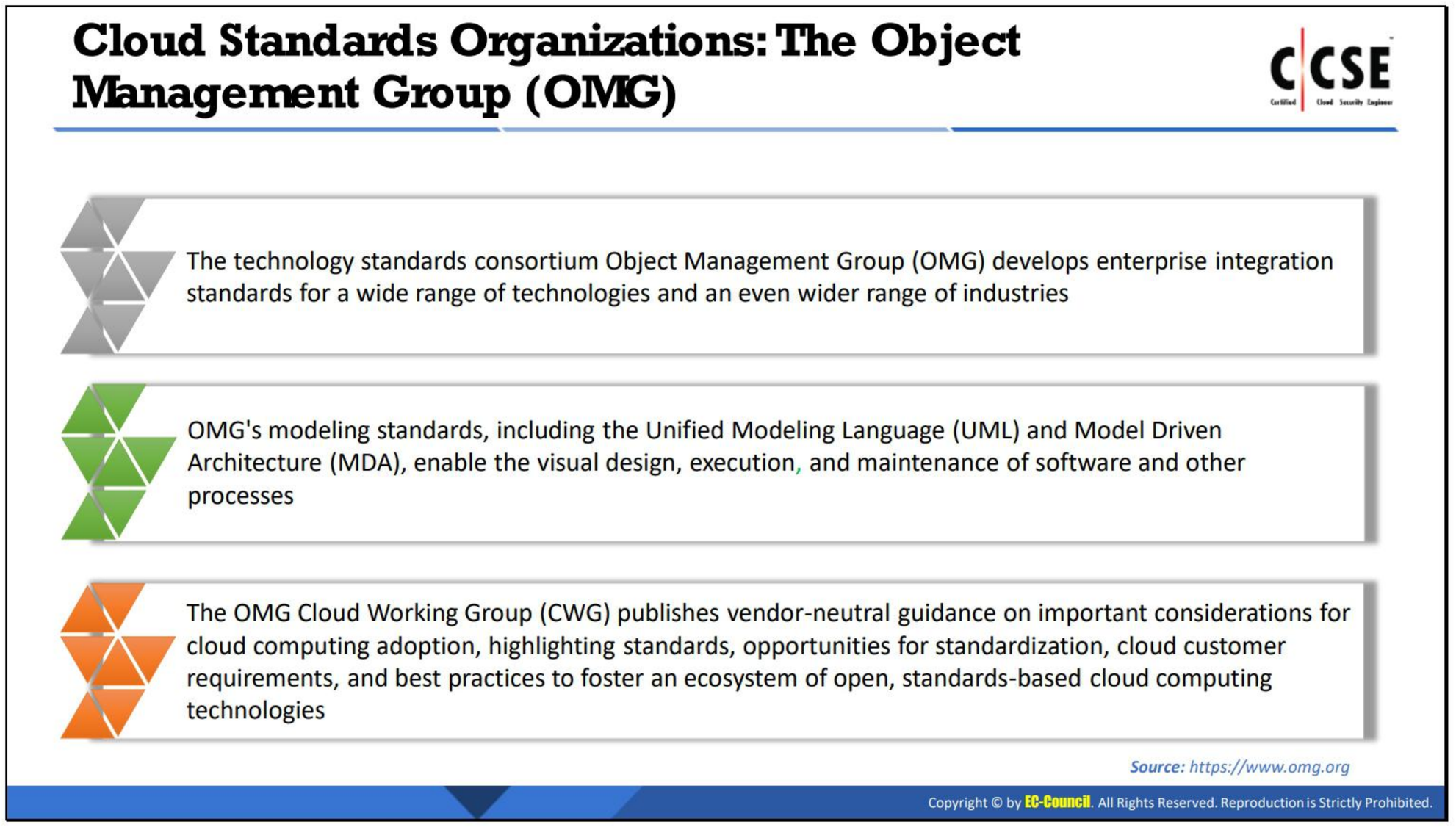
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

data to be taken from an instance of an information set and written out to their native format.

- **WS-Agreement and WS-Agreement Negotiation**: The WS-Agreement and WS-Agreement Negotiation family of specifications provides a language and a protocol for the creation, management, and monitoring of automated machine-readable service agreements in real time. This specification set includes provisions for advertising the capabilities of service providers and creating agreements based on templates, as well as for monitoring agreement compliance at runtime.
- **DRMAA**: The Distributed Resource Management Application API (DRMAA), with an accompanying C language binding, is a set of API specifications for tightly coupled and portable programmatic access to the cluster, grid, and cloud systems with widespread adoption in batch scheduling and other implementations.
- **NML, NSF, and NSI**: The Network Markup Language (NML), Network Service Framework, Network Service Interface (NSI) Connection Service, and other products of OGF's networking-oriented infrastructure groups enjoy widespread adoption and are some of the most advanced performance testing, monitoring, and management frameworks in the industry.

OGF performs extensive work on authentication and authorization in distributed environments. Examples include the Grid Certificate Profile and related documents produced by the Certificate Authority Operations (CAOPS) working group and the products of the Federated Security community group. The latter products are used, for instance, by the Interoperable Global Trust Federation (IGTF) and supports projects worldwide in cloud computing.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



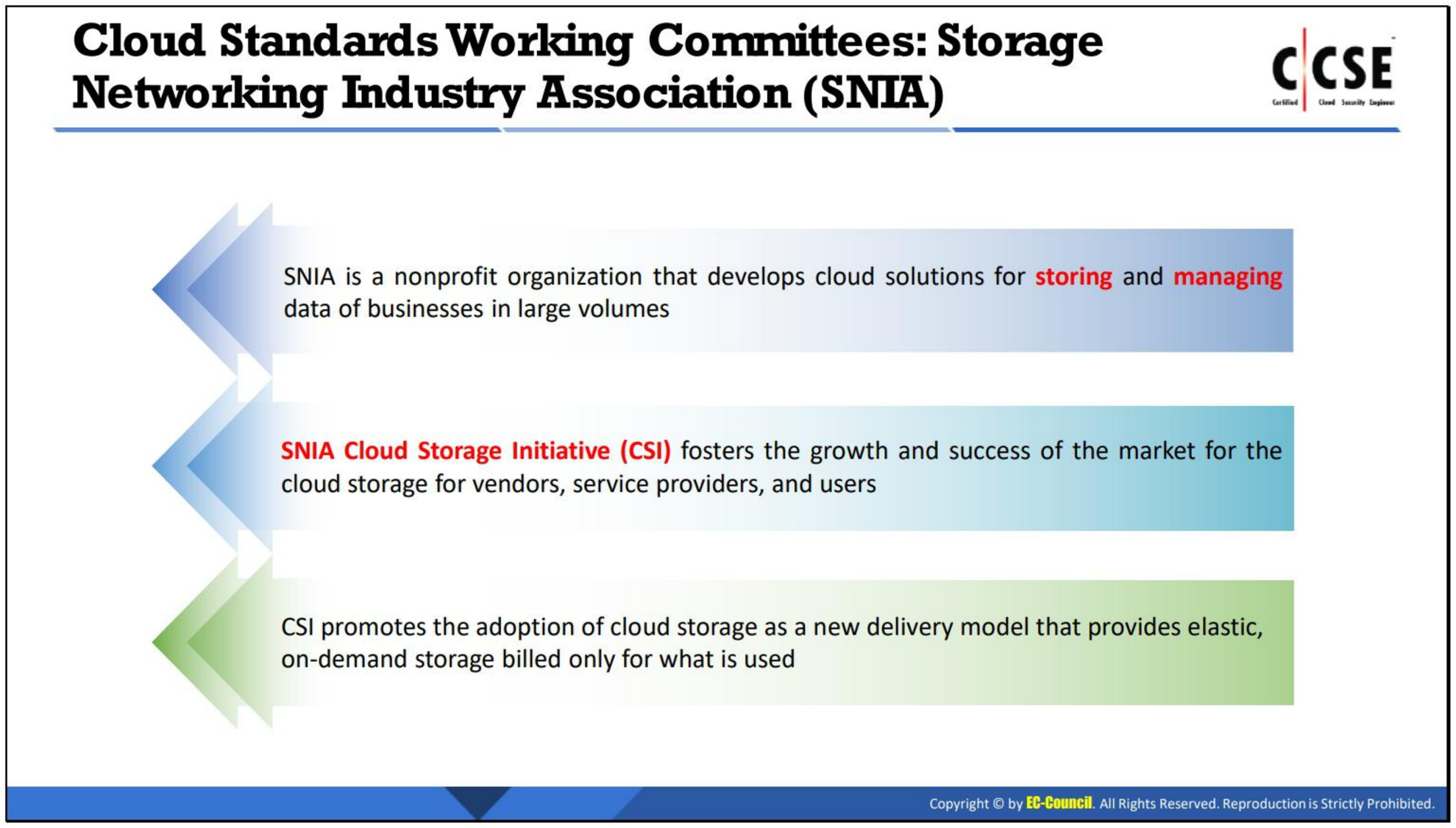
Cloud Standards Organizations: The Object Management Group (OMG)

***Source**: https://www.omg.org/*

OMG is an international, open-membership, not-for-profit technology standards consortium. OMG standards are driven by vendors, end users, academic institutions, and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. OMG's modeling standards, including the Unified Modeling Language (UML) and Model Driven Architecture (MDA), enable powerful visual design, execution, and software maintenance, in addition to other processes. OMG also hosts organizations such as the Consortium for Information & Software Quality (CISQ), the DDS Foundation, and BPM+ Health. Furthermore, OMG manages the Industrial Internet Consortium (IIC), the Industry IoT Consortium, and Digital Twin Consortium.

The OMG Cloud Working Group (CWG) publishes vendor-neutral guidance on important considerations for cloud computing adoption, highlighting standards, opportunities for standardization, cloud customer requirements, and best practices to foster an ecosystem of open, standards-based cloud computing technologies. The CWG takes over the mission of the Cloud Standards Customer Council™ (CSCC™), an OMG-managed program.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

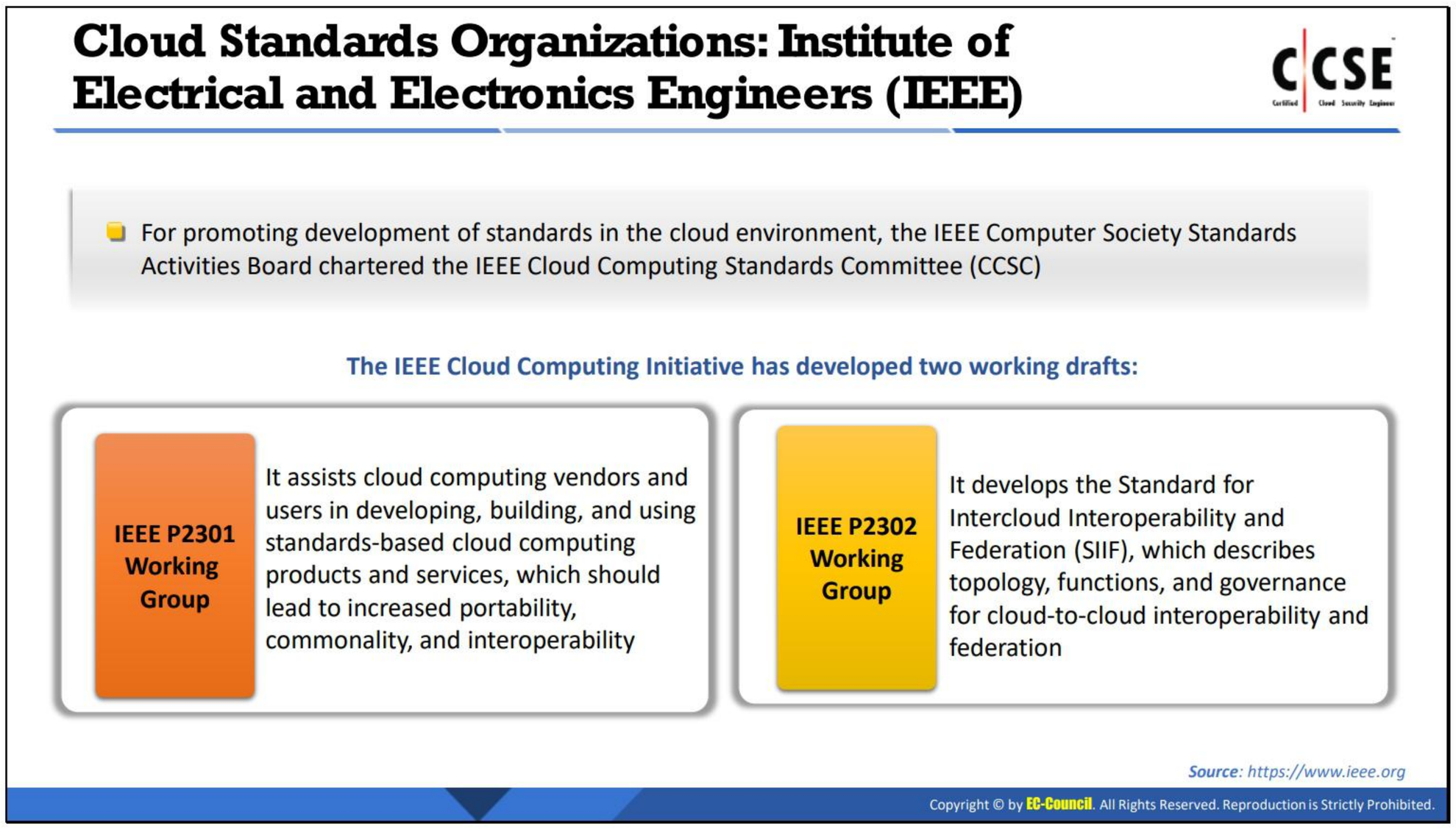


Cloud Standards Working Committees: Storage Networking Industry Association (SNIA)

SNIA is a non-profit organization that develops robust cloud solutions for storing and managing data of businesses in large volumes. The SNIA Cloud Storage Initiative (CSI) fosters the growth and success of the market for cloud storage for vendors, service providers, and users. CSI promotes the adoption of cloud storage as a new delivery model that provides elastic, on-demand storage billed only for what is used.

The SNIA Cloud Data Management Interface (CDMI) is an ISO/IEC standard that enables cloud solution vendors to meet the growing need for interoperability for data stored in the cloud. The CDMI standard is applicable to all types of clouds: private, public, and hybrid. CDMI provides end users the ability to control the destiny of their data and ensures hassle-free data access, data protection, and data migration from one cloud service to another.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: Institute of Electrical and Electronics Engineers (IEEE)

***Source**: https://www.ieee.org*

hzle01.ir

The Institute of Electrical and Electronics Engineers (IEEE) is a technical professional organization dedicated to advancing technology. For promoting the development of standards in the cloud environment, the IEEE Computer Society Standards Activities Board chartered the IEEE Cloud Computing Standards Committee (CCSC), which brings together a broad range of individuals and organizations from a wide range of technical and geographic points of origin to facilitate standards development and standards-related collaboration.

The IEEE Cloud Computing Initiative has originated two working drafts:

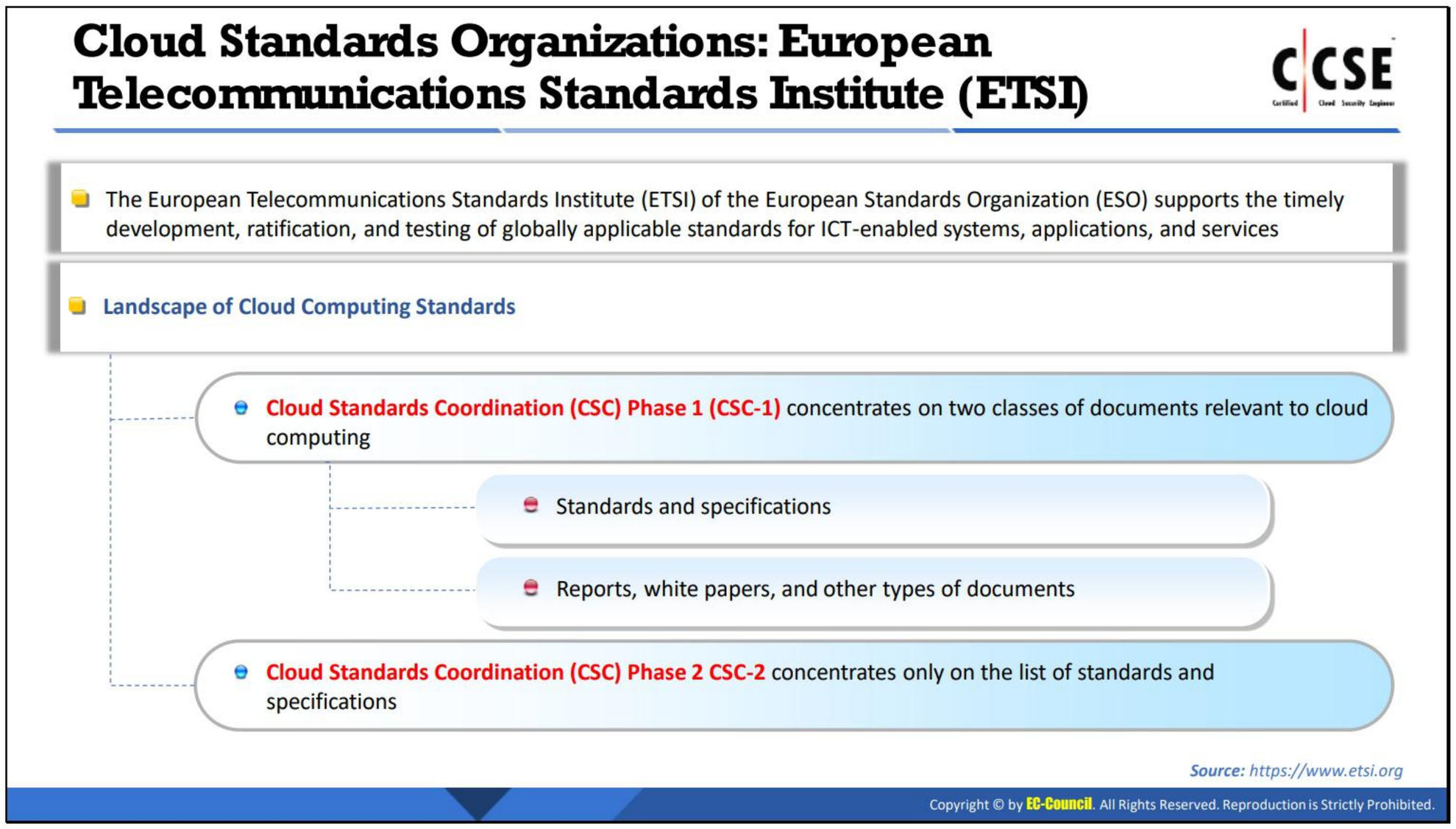
- P2301
- P2302
    - **IEEE P2301 Working Group**: This working group develops a guide aimed to assist cloud computing vendors and users in developing, building, and using standards-based cloud computing products and services, which should lead to increased portability, commonality, and interoperability. Cloud computing systems contain many disparate elements. There are often multiple options for each element, each with different externally visible interfaces, file formats, and operational conventions. In many cases, these visible interfaces, formats, and conventions have different semantics. This guide enumerates options, grouped logically into “profiles,” for such definitions of interfaces, formats, and conventions from various sources. In this manner, cloud ecosystem participants tend towards greater portability, commonality, and interoperability, growing the overall adoption rate of cloud computing.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IEEE P2302 Working Group:** This working group will develop the Standard for Intercloud Interoperability and Federation (SIIF). This standard defines topology, functions, and governance for cloud-to-cloud interoperability and federation. Topological elements include clouds, roots, exchanges (which mediate governance between clouds), and gateways (which mediate data exchange between clouds). Functional elements include namespaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust infrastructure. Governance elements include registration, geo-independence, trust anchor, and potentially compliance and audit. The standard address neither intra-cloud (within cloud) operation, which is cloud implementation–specific, nor proprietary hybrid-cloud implementations.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: European Telecommunications Standards Institute (ETSI)

***Source**: https://www.etsi.org/*

hade01.ir

European Telecommunications Standards Institute (ETSI) provides members with an open, inclusive, and collaborative environment, which supports the timely development, ratification, and testing of globally applicable standards for ICT-enabled systems, applications, and services. ETSI is a European Standards Organization (ESO). Cloud Computing is increasingly used as the platform for the ICT infrastructure provisioning, application/systems development, and end-user support of a wide range of core services and applications for businesses and organizations. ETSI launched Cloud Standards Coordination, which develops a standard for cloud computing. The Cloud Standards Coordination Phase 2 (CSC-2) was launched to address issues left open after the work of Cloud Standards Coordination Phase 1 (CSC-1) was completed, with a particular focus on the perspective of cloud computing users.

The main objectives of ETSI are to:

- Provide an updated list of identified cloud computing standards
- Analyze the progress of coverage of the cloud service lifecycle
- Analyze the main concerns of customers and users and how standards help their resolution
- Identify areas of maturation and areas where standards must progress in the future
- Provide conclusions based on the analyses

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

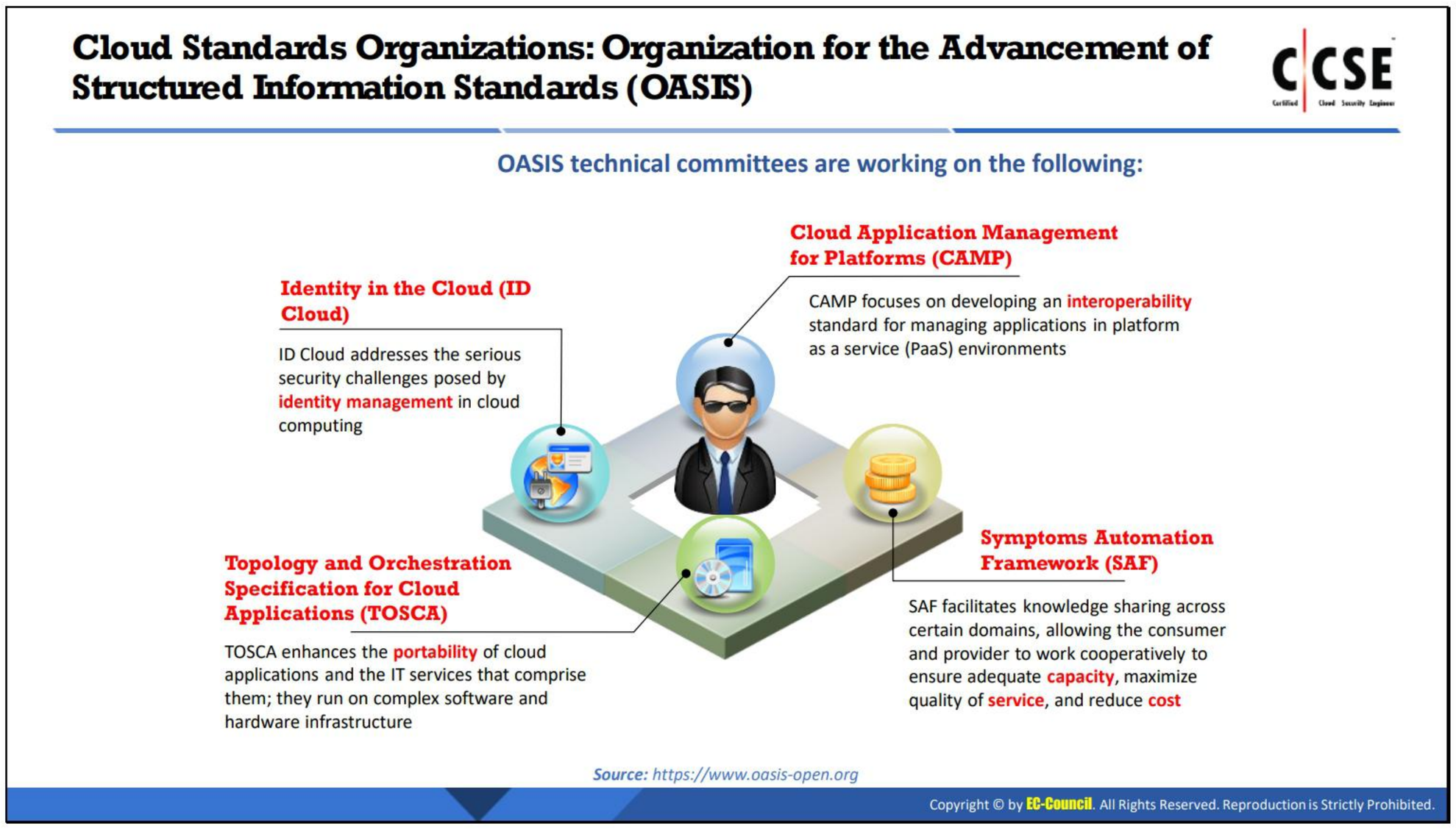
Cloud Computing Standards Landscape

- CSC-1 identified the following two classes of documents relevant to cloud computing.
    - Standards and Specifications: A Standard is an output from a formally recognized SDO (such as ETSI or ITUT), and a Specification is an output from any other form of SDO that becomes a Standard when ratified by a recognized SDO.
    - Reports, White Papers, and other types of documents.
- CSC-2 concentrated only on the list of Standards and Specifications and used the same approach as CSC-1 for mapping Standards and Specifications to the cloud computing service lifecycle. To achieve comparability across the two, the cloud computing service lifecycle framework developed for Cloud Standards Coordination has been largely reused for this new maturity assessment.

  The service lifecycle is divided into three major phases.
    - Phase 1: The acquisition of a cloud service
    - Phase 2: The operation of a cloud service
    - Phase 3: The termination of a cloud service

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Standards Organizations: Organization for the Advancement of Structured Information Standards (OASIS)

Source: *https://www.oasis-open.org*

hade01.ir

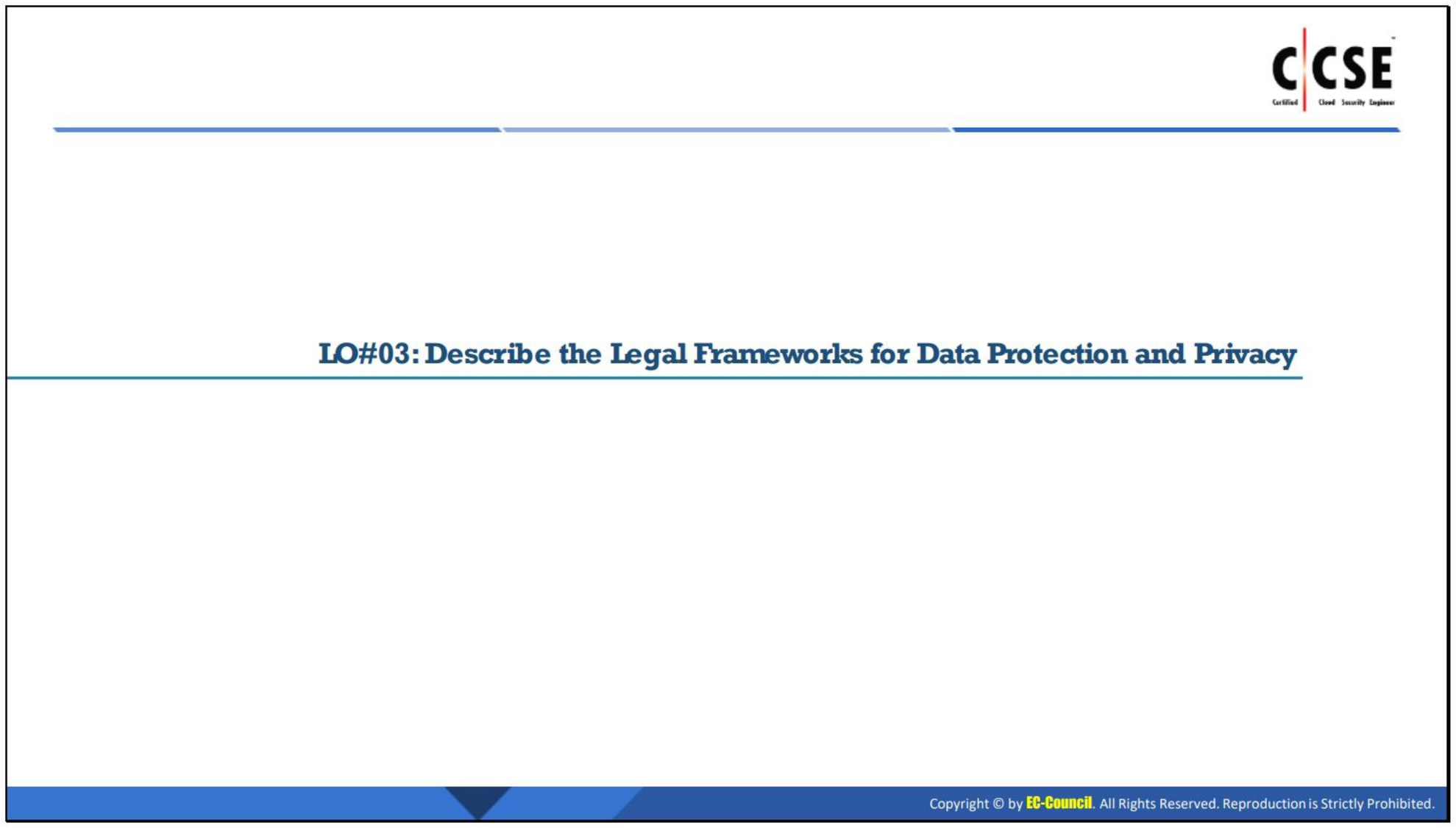
The Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit consortium that drives the development, convergence, and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, cloud computing, SOA, web services, the Smart Grid, electronic publishing, emergency management, and other areas.

The OASIS technical committees are working on the following.

- **Identity in the Cloud (ID Cloud)**: ID Cloud addresses the severe security challenges posed by identity management in cloud computing.
- **Cloud Application Management for Platforms (CAMP)**: CAMP is focused on developing an interoperability standard for managing applications in Platform as a Service (PaaS) environments.
- **Topology and Orchestration Specification for Cloud Applications (TOSCA)**: TOSCA enhances the portability of cloud applications and the IT services that use them and run on complex software and hardware infrastructure.
- **Symptoms Automation Framework (SAF):** SAF facilitates knowledge sharing across certain domains, allowing consumers and providers to work cooperatively to ensure adequate capacity, maximize the quality of service, and reduce cost.

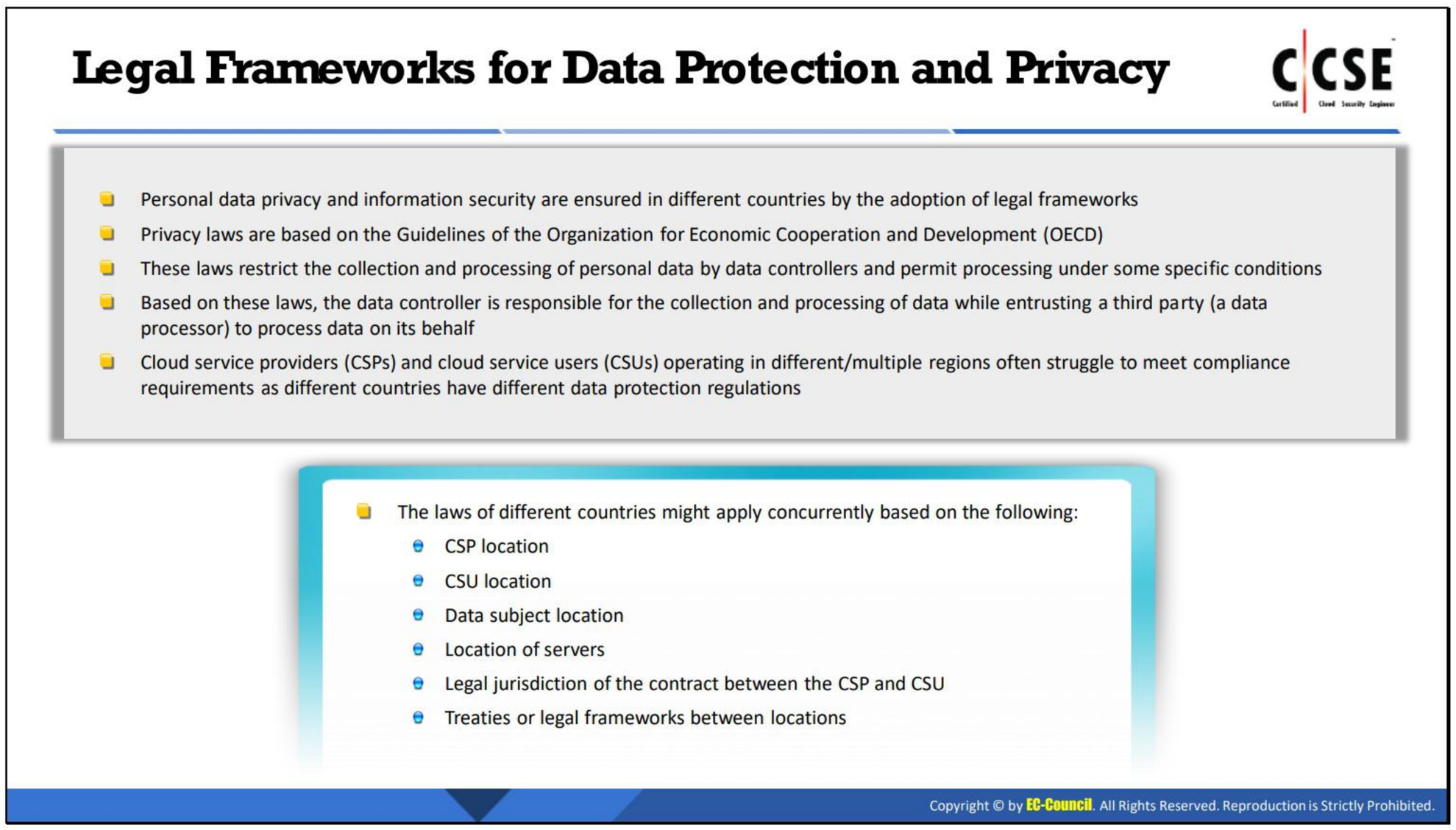
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#03: Describe the Legal Frameworks for Data Protection and Privacy

To address the privacy and security concerns related to data stored in the data centers of cloud providers, cloud security engineers must understand the different laws formulated in various countries to protect data stored in the cloud. Organizations must follow these laws and regulations to ensure data protection and privacy in the cloud. This section explains the various legal frameworks for data protection and privacy in various countries.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Legal Frameworks for Data Protection and Privacy

Cloud computing has introduced various privacy and security concerns related to data stored in the data centers of cloud providers. Organizations use cloud platforms to store non-sensitive as well as sensitive information. Sensitive information stored in the cloud may include business-critical information, personal information of their customers/employees, and financial information. Laws or legal frameworks are created to keep sensitive data stored in cloud data centers secure.

Different countries have different laws to protect data stored in the cloud. Organizations must follow these laws and regulations to ensure data protection and privacy in the cloud. As cloud providers have data centers located in multiple countries and their customers' data are stored in these data centers, various laws and regulations apply to the same set of data stored in different locations/geographies. Organizations face issues when they use cloud platforms to store data because they must comply with various laws and regulations.

CSPs and customers that operate in more than one region must meet compliance requirements from different contexts because different rules are enforced in different countries to safeguard customers' data. These rules require CSPs and their customers to implement different security measures for cloud data protection and privacy, which is often not easy.

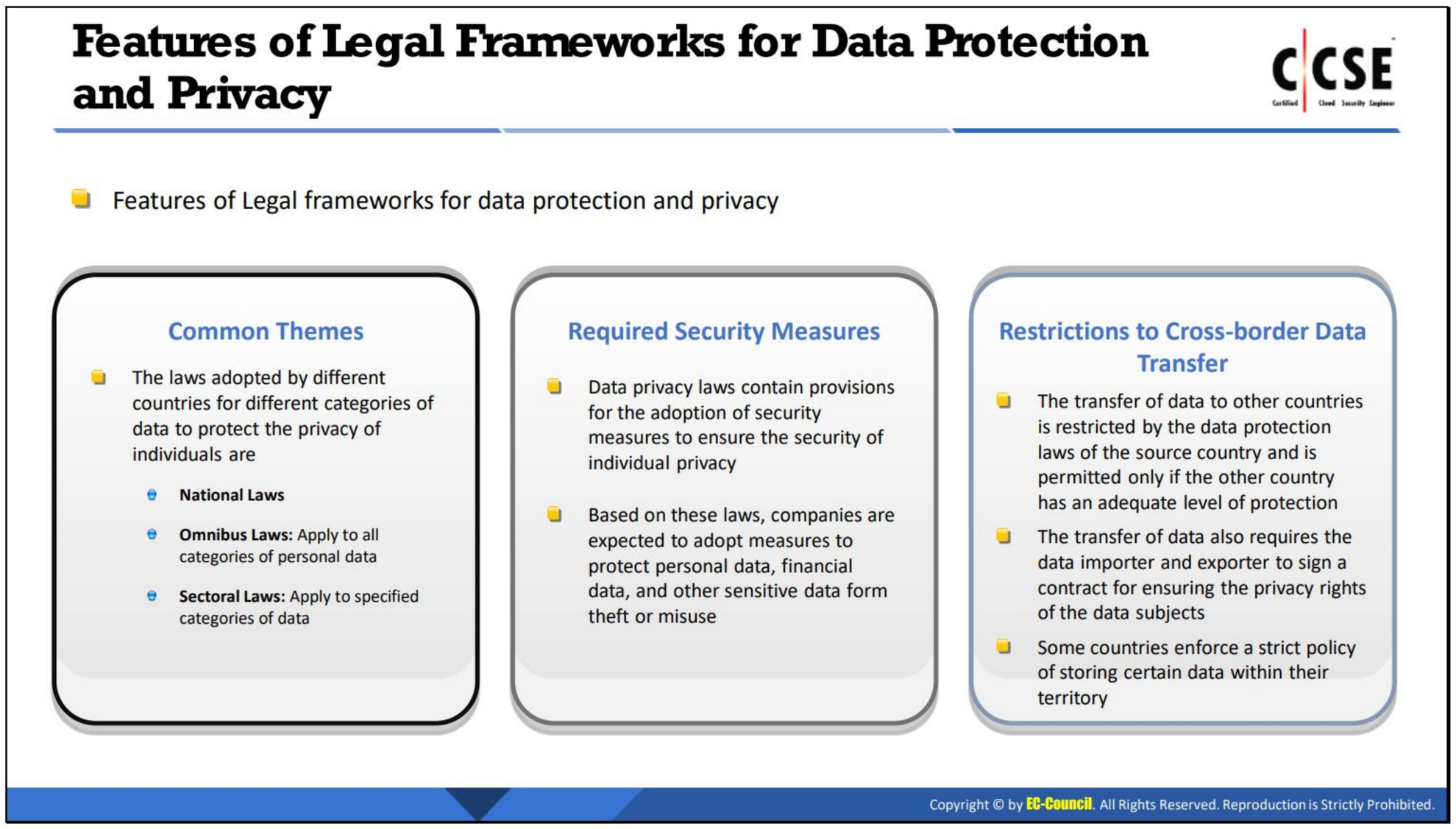
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The laws of different countries might apply simultaneously in certain circumstances based on the following:

- The CSP's location (where the provider is located)
- The cloud user's location (where the customer organization resides)
- The data subject's location (where the data subject, the individual whose data is collected and processed, resides)
- The location of servers (where the data centers of the provider are located)
- Contractual legal jurisdiction between the CSP and CSU
- Treaties or legal frameworks that exist between various locations

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Features of Legal Frameworks for Data Protection and Privacy

Data privacy laws are created by countries to protect the personal information of their citizens against individuals, corporates, or government authorities that can access the personal information without any limitations. These laws specify certain conditions related to accessing and transferring information that must be followed. These laws apply to data stored in the cloud as well.

Data privacy laws govern how individuals and entities can collect and process the data of others. Data protection is important in cloud computing because the data stored in the cloud are spread over multiple data centers located in different regions having different data protection laws. CSPs and customer organizations must follow the applicable laws while collecting, processing, and storing data of others.

Common Themes

Different countries have adopted laws for different categories of data to protect the privacy of individuals. These laws include the following:

- **National or omnibus laws**: These laws are applicable to all kinds of personal data.
- **Sectoral laws**: These laws are applicable to specified groups of data.

Required Security Measures

These data privacy laws often include provisions for adopting security measures to protect individuals' privacy. Simultaneously, organizations must also implement suitable physical, technical, and administrative measures for protecting a wide range of data from alteration, misuse, and loss. These data include financial data, personal data, trade secrets, and other sensitive data.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Restrictions to Cross-border Data Transfers

Many countries have implemented data protection laws that restrict the transfer of data beyond their boundaries. These laws allow the transfer of information only when the country to which the information will be transferred provides an adequate level of protection to secure the personal information and privacy rights of the individuals affected, as specified in the relevant national law. This implies that personal data cannot be transferred to countries that do not have adequate data protection laws. The main objective of this adequacy requirement is to ensure that individuals whose data are transferred are protected in the same manner as they were through policies provided to them prior to the data transfer.

Furthermore, it may be essential for the data exporter and importer to sign an agreement that ensures the maintenance of privacy rights for data subjects. The requirements to ensure adequate data protection might be stringent and complex depending on the country. In some cases, transferring data inside or outside the country may require the prior permission of the local data protection commissioner.

Moreover, laws in some countries require certain data to be stored within their territory, and such data may not be transferred outside such countries. For example, China and Russia have new data localization laws that require specified personal data of individuals residing in these countries to be stored inside the country borders.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Regional Legal Frameworks: Asia-Pacific Region

- The following are examples of laws and legal frameworks in information privacy and security in the Asia-Pacific region

Australia

- The two laws that provide protection to cloud service users in Australia are the **Privacy Act** and the **Australian Consumer Law (ACL)**
- The Privacy Act includes the following:
  - 13 Australian Privacy Principles (APPs) that apply to private sectors and nonprofit organizations with an annual turnover of more than AUD 3 million, private health service providers, and small businesses
  - Based on the Privacy Act, organizations must notify Australian residents and the Australian Information Commissioner regarding security breaches.
  - Security breaches include unauthorized access and loss of personal information
  - Even if the CSP is based abroad, the Privacy Act is applicable to Australian consumers
- ACL includes the following:
  - Protection of cloud service users from false contracts and poor CSP conduct

China

- The 2017 Cyber Security Law governs critical information infrastructure operators
- The security responsibilities of operators who handle critical information infrastructure are as follows:
  - Internal organization and training
  - Data backup
  - Emergency response
  - Security inspection of risks
  - Reporting potential risks to relevant authorities
- The Cyber Security Law also includes a data localization provision so that personal information and sensitive data are stored within Chinese territory
- Draft Regulations on Cross-Border Data Transfers, which supplement the Cyber Security Law, include the following:
  - Enforcement of security review requirements on organizations that plan to transfer data outside the border
  - Expand data localization and the types of information to be stored within Chinese territory

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

Regional Legal Frameworks: Asia Pacific Region (Cont'd)

hide01.ir

Japan

- The Act on the Protection of Personal Information (APPI) in Japan requires the private sector to protect personal information
- Law on the Protection of Personal Information Held by Administrative Organs is a national data protection law
- Japan also includes profession-specific laws and laws specific to certain sectors to maintain data confidentiality
- Amendments to the APPI laws restrict the transfer of personal data to third parties

Russia

- Russian data protection laws impose restrictions on the processing of personal data
- The handling of personal information is regulated by the **data localization law**, which requires the personal data of Russian citizens to be stored within the country
- **Roskomnadzor**, the Russian data protection regulator, ensures the confidentiality of personal data

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

Regional Legal Frameworks: Asia-Pacific Region

Prominent countries in the Asia-Pacific region such as Australia, China, Japan, and Russia have enforced data protection laws that allow the data owner to take sufficient physical, technical, and administrative measures for securing personal data from misuse, alteration, and loss.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Australia

Australia has two key laws that protect the data and privacy of customers who use cloud services. These two laws are described below.

- **Privacy Act**

  This Act was enacted in 1988 to ensure the data security and privacy of Australian citizens. The following are the key aspects of the Privacy Act.

  - It includes 13 Australian Privacy Principles (APPs) that apply to some small businesses, all private health service providers, and all private-sector and non-profit organizations with an annual turnover greater than AUD 3 million.
  - Organizations must notify the Australian Information Commissioner and affected Australian residents regarding security breaches.
  - Security breaches must be reported if the organization detects unauthorized access or personal information disclosure that may cause serious damage to affected individuals or the loss of personal information due to possible information disclosure or unauthorized access that is likely to cause serious harm to affected individuals.
  - The Privacy Act defines how to manage personal information to protect information or opinion about an individual and ensures that the person cannot be traced or identified using the information.
  - Even if the CSP is located overseas, the Privacy Act can be applied for Australian customers.

hade01.ir

- **Australian Consumer Law (ACL)**

  The ACL is enacted to protect the rights of Australian customers The following are the key aspects of the ACL.

  - It protects customers from false or misleading contracts and poor conduct from providers.
  - The ACL safeguards the rights of cloud consumers by prohibiting unconscionable conduct while using cloud services. Unconscionable conduct occurs when customers are pressurized by the CSP using questionable tactics to purchase a service that does not suit their needs.
  - The ACL provides consumer guarantees to cloud customers that entitle them to ask for a refund if the provider fails to offer services as per the agreed service availability or quality.

China

China recently introduced new legislation that governs information systems to address the security and privacy issues of personal and corporate information. In 2017, China introduced the Cyber Security Law, which governs the operations of critical information infrastructure operators and network operators.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Under the Cyber Security Law, network operators must comply with a list of security requirements including the following:

- Creation of cyber-security emergency response plans
- Design and implementation of information security measures
- Provision of necessary support to investigative authorities for investigating crimes and protecting national security (when needed)

This law requires the providers of network services and products to update their users regarding known bugs and security defects and to report such issues to the relevant authorities.

The Cyber Security Law has imposed several security obligations on critical information infrastructure operators. These obligations include the following:

- Internal organization
- Training
- Emergency response requirements
- Data backup
- Security inspections and annual risk assessments
- Reporting the risks to the relevant authorities

Under the Cyber Security Law, a provision called data localization requires personal information and important data to be stored within the boundaries of China. This law also restricts the transfer of business data and personal information overseas and is a challenge for organizations that work globally and normally need to transfer data outside the country. According to this law, all sensitive information should be stored within the country. Failing to comply with the law may lead to hefty fines for the organization and the discontinuation of its business activities due to the cancellation of its business licenses or the suspension of its business activities.

hidden1.ir

China has also introduced some draft regulations on the cross-border transfers of sensitive information and important data. Draft Regulations on Cross Border Data Transfers that supplement the Cyber Security Law include the following:

- Implementing new security review requirements on organizations that plan to transfer data outside the national borders
- Expanding data localization requirements and increasing the types of information to be stored within the country's territory

Japan

Japan has a data protection law called the Act on the Protection of Personal Information (APPI), which requires private sector enterprises to safeguard data and personal information. It is the principal law that obligates organizations to be transparent and protect the personal information of Japanese residents, failing which they may face criminal penalties.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Various other laws in Japan ensure data protection and privacy; examples include the Law on the Protection of Personal Information Held by Administrative Organs and sector-specific laws. For instance, in the healthcare industry, there are profession-specific laws such as the Act on Public Health Nurses, Midwives, and Nurses; the Medical Practitioners' Act; and the Pharmacist Act. These acts require all registered health professionals to ensure the confidentiality of patient information.

Japan made certain amendments in the APPI that have restricted the ability to transfer personal information to third parties. The law now requires the consent of the data subject for the transfer of their personal information to third parties. If the information is transferred to another country that has an established framework for personal information protection, consent for data transfer is not required. However, the country's framework for personal information protection must meet the standard specified by the Personal Information Protection Commission.

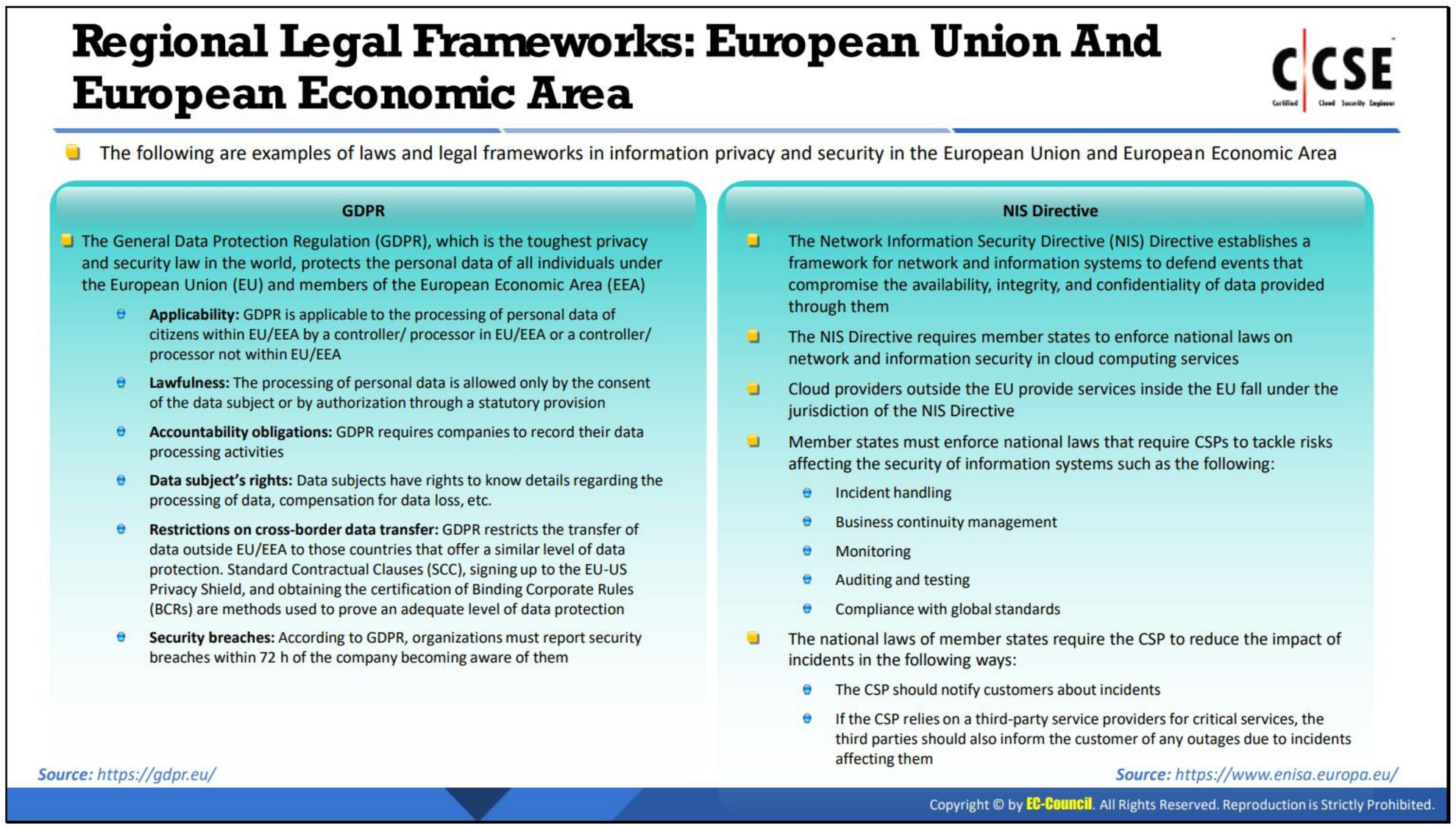
Russia

Russia has its own data protection laws that ensure data security and privacy in the cloud. Russian data protection laws impose various restrictions on data processing. These laws require taking consent before processing most forms of data. The data localization law regarding the handling of personal information is the most important aspect of the Russian legal framework.

Companies operating in Russia are required to store the personal data of their citizens within Russia. Companies that are located outside Russia and do not have a physical presence in the country cannot provide services. Roskomnadzor is the federal executive body in Russia that serves as the data protection regulator in Russia, and it is responsible for ensuring compliance with the law. Roskomnadzor blocks websites that are non-compliant with the country's laws. Recently, it has blocked access to a foreign social media network that had no physical presence in Russia but was providing services.

Under the data localization law, organizations must perform all data processing activities (from collecting the data of Russian citizens to storing the data in a database) inside the country, and the data should be stored locally. Organizations that fail to comply with this law will be penalized by imposing fines that increase if they fail to comply with the law multiple times.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Regional Legal Frameworks: European Union and European Economic Area

Source: *https://www.enisa.europa.eu/*

ide01.ir

GDPR

The General Data Protection Regulation (GDPR), which is the toughest privacy and security law in the world, protects the personal data of all individuals under the European Union (EU) and members of the European Economic Area (EEA)

- **Applicability**: GDPR is applicable to the processing of personal data of citizens within EU/EEA by a controller/ processor in EU/EEA or a controller/ processor not within EU/EEA
- **Lawfulness**: The processing of personal data is allowed only by the consent of the data subject or by authorization through a statutory provision
- **Accountability obligations**: GDPR requires companies to record their data processing activities
- **Data subject's rights**: Data subjects have rights to know details regarding the processing of data, compensation for data loss, etc.
- **Restrictions on cross-border data transfer**: GDPR restricts the transfer of data outside EU/EEA to those countries that offer a similar level of data protection. Standard Contractual Clauses (SCC), signing up to the EU-US Privacy Shield, and obtaining the certification of Binding Corporate Rules (BCRs) are methods used to prove an adequate level of data protection
- **Security breaches**: According to GDPR, organizations must report security breaches within 72 h of the company becoming aware of them

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NIS Directive

The Network Information Security (NIS) Directive establishes a framework for networks and information systems to defend against actions that can compromise the authenticity, availability, confidentiality, or integrity of (processed, transmitted, or stored) data or related services provided via these networks and information systems. The Directive was enforced in August 2016, and every EU/EEA member state implemented it in its national legislation.

According to the Directive, national laws of every member state must enforce network and information security requirements on essential service operators. Essential service operators provide services that are necessary for maintaining critical societal and/or economic activities, and incidents impacting the networks and information systems of such services can damage the provision of these services. The Directive suggests the following requirements to be implemented in national laws.

- Implementing organizational and technical measures to secure network and information systems that are used in the operations of essential services
- Implementing suitable measures to prevent or minimize the impact of incidents that affect the security of networks and systems utilized for provisioning essential services and to enable business continuity
- Notifying the relevant authority about the incidents that impact the continuity of essential services without any undue delay
- Providing the information required to assess the networks and system security
- Providing evidence of effective security policy implementation

As per the NIS Directive, national laws of member states must impose network and information security requirements on digital service providers (e.g., cloud computing services, e-commerce platforms, and online search engines). The scope of this Directive includes the digital service providers that provide services inside the EU but are located outside the EU.

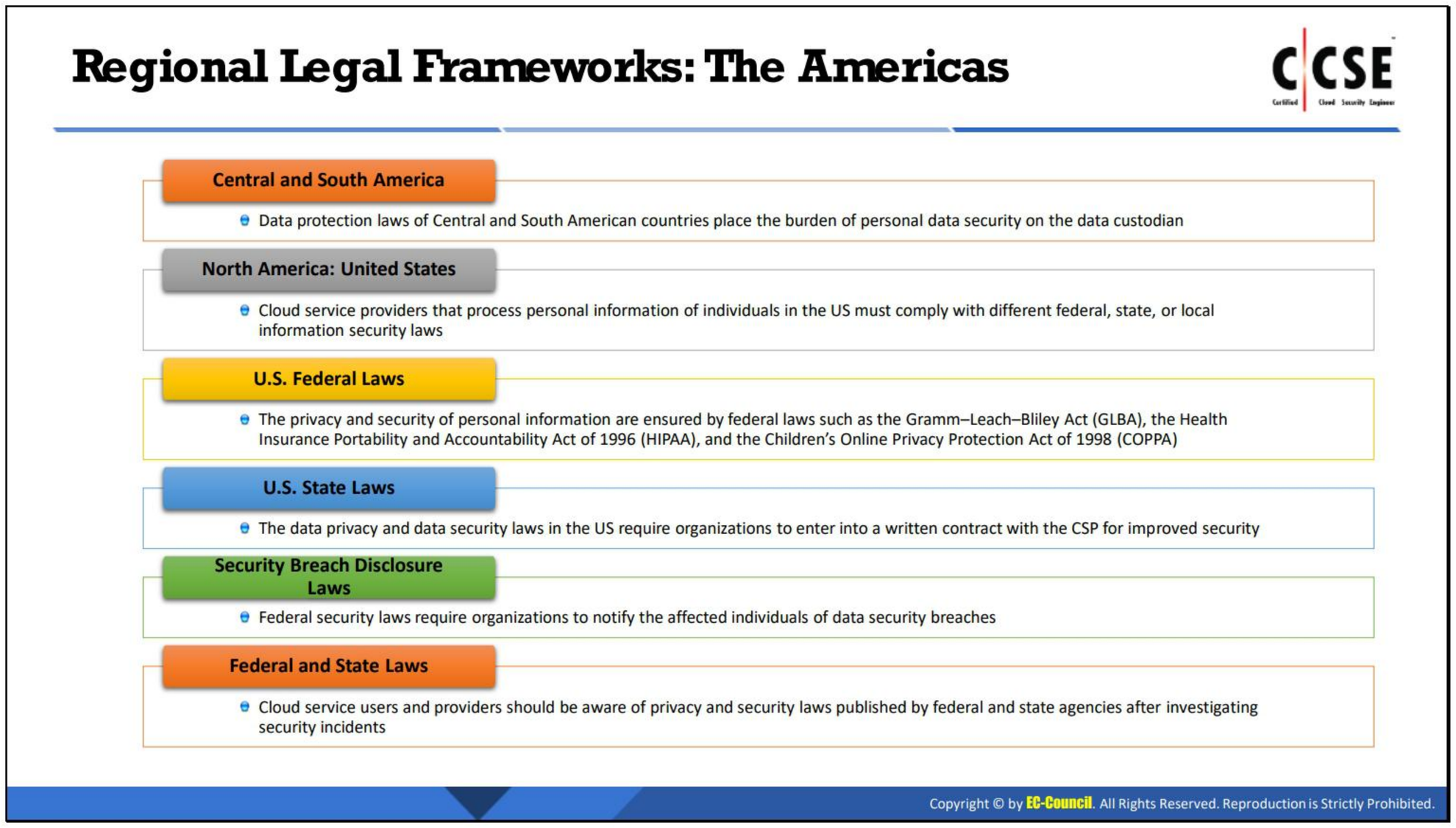
National laws of member states should also require digital service providers (e.g., CSPs) to implement measures to handle risks affecting the security of information systems they use. They must include the following measures to manage risks properly:

- Incident handling
- Monitoring
- Auditing and testing
- Business continuity management
- Compliance with global standards

According to the Directive, national laws of member states must require CSPs to prevent or reduce the impact of incidents. It requires the following.

- CSPs should notify competent authorities about incidents and provide the necessary information to the authorities.
- If CSPs rely on a third-party service provider for critical services, the CSP should inform competent authorities about any outages or service disruptions that may occur because of incidents affecting the third-party provider.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Regional Legal Frameworks: The Americas

Central and South America

Central and South American countries are adopting various data protection laws that define the necessary security requirements and responsibilities of a custodian (CSP). Data protection laws of Central and South American countries make the custodian responsible for ensuring the security and privacy of personal data, irrespective of where the data are stored. The custodian is also responsible for the data transferred to third parties.

Inspired by the European Directive 95/46/EC, countries such as Chile, Argentina, Peru, Mexico, and Uruguay have enacted data protection laws. These laws may also have references to the Asia-Pacific Economic Cooperation (APEC) Privacy framework. Security breach disclosure provisions are included in Mexico's federal data protection law.

North America: United States

The US has several federal, state, and local regulations regarding data protection and privacy. Organizations that conduct business in the US or gather or process the personal information of individuals or companies in the US must follow multiple laws and regulations, including local and federal privacy laws or information security laws. Owing to the complexity and variety of laws, complying with these laws is challenging for CSPs and cloud users as well as service providers and subcontractors who help provision cloud services.

The various laws that ensure data protection and privacy are as follows.

- **US Federal Laws**

  The privacy and security of personal information are ensured by federal laws such as the Gramm–Leach–Bliley Act (GLBA), the Health Insurance Portability and Accountability Act

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(HIPAA) of 1996, and the Children's Online Privacy Protection Act (COPPA) of 1998. These laws contain security and privacy-related provisions that require organizations to implement sufficient security measures while processing personal data.

In addition, these laws bind organizations to take necessary precautions while hiring service providers and contractors. These laws may consider organizations responsible for the actions of their subcontractors. For example, certain privacy and security rules of HIPAA and GLBA require organizations to ensure that their subcontractors take reasonable security measures and follow data privacy provisions.

- **US State Laws**

  Apart from federal laws, many US states have laws related to data security and privacy. These laws are applicable to organizations involved in collecting or processing personal information of state residents, irrespective of the location in the US where the data are stored. Most of these state laws require such organizations to have a written contract with the service provider (e.g., CSP) incorporating suitable security measures. Moreover, these organizations and the service providers working with them must provide adequate privacy protection and security for personal data.

- **Security Breach Disclosure Laws**

  If entities or organizations suffered a security breach that exposed protected and sensitive data of individuals, multiple federal security laws and most state laws require them to notify the affected individuals about the breach. Moreover, they often need to inform the state or federal agencies regarding the breach. Both cloud providers and customers need to have a good understanding of these laws to avoid the risk of class-action lawsuits.

- **Federal and State Agencies**

  Cloud service users (CSUs) and cloud service providers (CSPs) should also understand the common law of privacy and security that was published by federal and state agencies based on investigations into security events and incidents. Cloud providers must update their public documentation when there is a change in the way of their working to avoid actions that may result in the breach of Section 4 of the Federal Trade Commission (FTC) act. FTC performs enforcement actions against organizations having security and privacy practices that are inconsistent with their claims in public disclosures.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Contracts and Provider Selection

- Cloud customers have a contractual commitment to ensure the security of client data
- Examples of such contracts include the following:
  - Terms and Conditions statement posted by companies on their website
  - Data processor agreement to process personal data only for specific purposes
- Organizations must ensure that when data are stored in the cloud, and the commitments made in the privacy notice should be fulfilled
- When data are hosted in the cloud, the responsibility for securing the data remains with the data custodian
- These commitments can be fulfilled by due diligence before the signing contract and conducting security audits during the negotiation of the contract

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

Contracts and Provider Selection (Cont'd)

Internal Due Diligence

- The cloud service provider and cloud service customer must verify the practices and restrictions to identify the legal and compliance requirements before entering into an agreement
- The cloud customer should analyze whether they entered into any agreements that restrict the transfer of data to other parties

Monitoring, Testing, and Updating

- Periodic monitoring, testing, and evaluation of cloud services ensure that all the privacy and security measures are followed
- Cloud customers and service providers must ensure that they comply with the changing legal and regulatory requirements

External Due Diligence

- Before entering into an agreement, due diligence should be conducted to review the operations of the cloud service provider
- Due diligence includes evaluating the nature and completeness of services, service stability, availability of support or maintenance, customer service, and data-center location
- The cloud customer should evaluate service levels, end-user and legal agreements, etc.

Third-party Audits and Attestations

- Third-party audits are conducted to ensure the compliance of CSP infrastructure
- Customers should consider the scope of assessments and the services included in assessments when evaluating assessments published by the cloud provider

Contract Negotiations

- Customers should carefully review the proposed contract to reduce exposure to legal risks
- Customers should ensure that the contracts can be negotiated to reduce risks

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

Contracts and Provider Selection

Cloud customers can use contractual terms to protect the information of their users, employees, and contacts. Organizations can have certain terms in their contracts with their CSPs that prevent them from using the information for secondary purposes or sharing it with third parties. Customer organizations are obligated to protect the data of their clients and are responsible for any data misuse or exposure.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations must uphold promises made via different means such as a Privacy Statement and Terms and Conditions posted on their websites as well as contracts signed with third parties. For instance, as per a service agreement, a data processor might be allowed to process the data of its clients for certain purposes only. Similarly, an organization may have certain obligations to meet because of a contract with its customers regarding the protection of their data, restriction of data usage, data security, etc.

When hosting data in the cloud, an organization must assure its customers/data subjects that it would meet the commitments and promises mentioned in its privacy notice or other contracts. They must ensure that the customer's data stored in the cloud environment will be utilized for the stated purpose. If the privacy notice of the organization allows data subjects to access, modify, or delete their information stored in the cloud, the CSP must also allow them to have these permissions.

When moving data or operations to the cloud, the data custodian or collector remains responsible for protecting and securing the data. Although the custodian hosts the data using a third-party provider (CSP), the custodian is accountable for any misuse, loss, and damage of the data. Thus, it is essential for the data custodian to enter into a formal agreement with the CSP that regulates data usage, roles, and other activities. Before executing the contract and performing security audits during the contract period, the data custodian should ensure that these obligations are fulfilled through due diligence.

Internal Due Diligence

ide01.ir

As organizations are the custodians of data entrusted to them by data subjects, they are obliged to follow regulations and laws that restrict the disclosure and transfer of the data to third parties. If it is necessary to transfer the data to third parties, organizations must impose certain obligations on the third parties to ensure data security and privacy.

Both parties (the data custodian and CSP) must identify legal requirements and compliance obstacles before starting to use the cloud service. For example, the cloud customer must determine whether their business model supports the use of cloud services and under what conditions. Similarly, the cloud provider must evaluate the risk of doing business in certain (unfamiliar) markets that are subject to various legal requirements.

The organization must identify whether it had entered into a data use agreement or confidentiality agreement with its customers that prohibits them from transferring the data to third parties. If it had signed such an agreement, the organization cannot use cloud services, which involve the transfer of the customers' data to cloud providers. In such cases, the organization must take specific consent from the customers (the data owners) before transferring the data to the cloud. Transferring the data without the consent of the data owners would result in a breach of the confidentiality/data use agreements signed with the customers.

Monitoring, Testing, and Updating

As the cloud environment keeps changing and evolving, it is essential to evaluate whether cloud services and other security measures are consistently working as expected. This can be achieved by regularly monitoring, testing, and updating cloud services and security measures over time.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To ensure that all the privacy and security measures are properly implemented, organizations should perform the periodic monitoring, testing, and evaluation of cloud services. If the cloud services are not tested regularly, control efficacy may be compromised without getting noticed.

Cloud customers and service providers must ensure that they comply with the changing legal and regulatory requirements. As the regulatory, legal, and technical landscape changes rapidly over time, both parties should know and understand the applicable laws and regulations and how to comply with them. This will help them address new security threats, compliance requirements, and laws promptly and ensure that both parties remain compliant. In addition, regular monitoring, testing, and updating will help ensure that the implemented security and privacy measures continue to evolve as new technologies are introduced.

External Due Diligence

As part of external due diligence, an organization must review all the relevant aspects of the CSP's operations before signing a contract with a provider. The organization must ensure that it understands everything about the service or application it will acquire from the provider. Furthermore, the organization should perform due diligence in evaluating all the important aspects of the provider's service, even if it takes several days to do so.

Depending on the nature of the proposed project, due diligence may include the following:

- Assessing the completeness and nature of the provided services
- Assessing service stability
- Assessing the availability of support or maintenance
- Assessing the responsiveness of customer service
- Determining the locations of data centers
- Validating the network speed

h1d001.ir

The organization can talk to other customers of the provider who are using the same services to gain more insights into aspects of the service. In addition, the organization can review reports of ligations filed against the provider and research online to better understand the reputation of the provider.

Most cloud customers evaluate at least the following aspects to ensure that a provider is suitable for them:

- Applicable service level
- Privacy policies
- Security disclosures
- End-user and legal requirements
- Proof of compliance with applicable legal requirements

The organization can investigate or evaluate the provider and its services depending on the intensity and depth of due diligence. Furthermore, the organization must review all terms and

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

conditions of the provider's service agreement as part of due diligence to understand what the provider will and will not offer. Reviewing the service agreement will help the organization make informed decisions.

Contract Negotiations

Contracts in cloud computing precisely describe the understanding or agreement of the parties involved. While negotiating contracts, both parties can have multiple measures and precautions to avoid or minimize their exposure to commercial, legal, and reputational risk with respect to the use of cloud services.

Organizations must review the proposed contract carefully before signing it (even if it is non-negotiable). A careful review of the contract has the following two benefits.

- The contract terms can be changed to accommodate their requirements.
- If the contract is non-negotiable, organizations can at least have a clear understanding of the consequences and implications of service engagement.

A non-negotiable contract may not have all the protections or contractual requirements that cloud customers would need. This can be risky for customers. In such cases, customers should identify other risk mitigation techniques that can be used to alleviate the risk.

Reliance on Third-party Audits and Attestations

As cloud customers cannot physically conduct audits to evaluate CSPs, they must rely on third-party audit reports and attestations for compliance purposes. Third-party audits and attestations are often used to prove that a particular CSP's infrastructure is compliant with the applicable standards and laws. This helps customers decide whether to choose a particular provider.

It is essential for a cloud customer to evaluate the published audit reports to understand the scope of the assessment and what services and features were audited under the assessment. This will help them better understand the services and features offered by the provider. Attestations should be based on well-defined industry standards with clearly defined scopes and the list of specific controls that were evaluated.

Third-party attestations and audit reports help cloud customers know which service of the cloud provider complies with which applicable standards. For instance, a new storage provision of a CSP could be non-compliant with the HIPAA standard, but its other offerings may be HIPAA compliant. Customers can make informed decisions by choosing the relevant and suitable services with the help of these third-party attestations and audit reports.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Electronic Discovery

- Discovery refers to the process by which the opposing party collects private documents for litigation
- The cloud is a repository of electronically stored information (ESI) that is crucial for investigations
- Cloud service providers and users must be able to identify all the documents required for a case
- Cloud service providers and users must know the issues occurring when a user is subject to a discovery request and the relevant data are with the provider

Electronic Discovery Issues

Issues	Description
Possession, Custody, and Control	The responsibility of either the CSP or user to produce information is limited to documents within its possession, custody, or control Data that are available and not available to the user are based on the agreements between the CSP and CSU
Relevant Cloud Applications and Environment	In cases where the cloud application or environment itself can resolve a dispute, a subpoena or other discovery processes can be directly served to the cloud service provider
Searchability and e-Discovery Tools	In the cloud environment, the organization may not be able to apply e-discovery tools that the organization uses on their on-premises environment Users may not have administrative access to access all the cloud data Negotiating the service agreement can solve this issue

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

Electronic Discovery (Cont'd)

hide01.ir

Issues	Description
Preservation	The complexity of data preservation in the cloud environment depends on the cloud service and the deployment model Prevention of the destruction or modification of data under the possession of a particular party is the responsibility of that party
Data Retention Laws and Record-keeping Obligations	Data retention laws require the covered entities to keep the data for a certain period **Scope of preservation:** The party that requests the data is not authorized to all the data in the cloud Relevant information is over-preserved if the user cannot preserve the relevant information granularly Examination of the over-preserved is called document review or privilege review, which is performed by client-paid attorney staff **Dynamic and shared storage:** Preservation of data is difficult with cloud storage The client must work with the provider to decide on ways to store the relevant data
Collection	The collection of data by the user from the cloud is difficult because of the lack of administrative control over the data **Access and bandwidth**: Clients and service providers must ensure that access to large amounts of data by the client during litigations requires a protocol, which should be included in SLAs **Forensics**: Acquiring bit-by-bit images of cloud data is difficult because the CSP may not provide access to the hardware in most cases, particularly in multi-tenant environments **Reasonable integrity**: A client subject to a discovery request must ensure that the collection of data from the CSP is complete and accurate **Limits to accessibility**: The cloud customer may not be able to collect all their data in the cloud, because of differences in data storage or data access rights and privileges. The cloud user and provider must analyze the discovery request as well as the relevance and accessibility of data structures while responding to requests

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

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Electronic Discovery (Cont'd)

Issues	Description
Direct Access	Cloud providers may not be able to provide direct access to the cloud infrastructure because the hardware resources might be out of their possession or control
Native Production	The data in the native cloud format may not be suitable to the requesting customer To address this situation, the information can be exported with standard protocols within the cloud environment
Authentication	Authentication in e-discovery refers to the forensic authentication of evidence data Questions arise in the court regarding the integrity of data
Cooperation Between the Provider and Client in e-Discovery	Cloud customers and providers must consider including the complications caused by e-discovery in their SLAs while beginning their relationship to reasonably cooperate with each other
Response to a Subpoena or Search Warrant	If the cloud service provider receives a request for personal client data from a third party in the form of a subpoena or a court order, the CSP has the responsibility to protect the sensitive client data SLAs should include provisions to notify the users about any subpoena as well as the time given to the company to fight the request for access

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

Electronic Discovery

Information stored electronically is called electronic information. It is intangible in nature and can be accompanied by metadata (e.g., timestamps). These factors differentiate electronic information from information on paper. In a court of law, electronic information can be produced as evidence in a legal case.

hidden1.ir

Discovery in US law refers to the process by which the prosecuting party collects private documents to be used in litigation. Electronic discovery (e-discovery) involves identifying, collecting, and producing electronically stored information (ESI) as evidence in response to a legal request from a court of law. ESI in the context of e-discovery includes emails, databases, presentations, documents, audio and video files, websites, voicemails, and social media. All these can be produced as evidence in court in a legal case or investigation.

To avoid claims of tampering with evidence in court at a later stage, it is essential to preserve the original content and metadata of ESI. Once the ESI is identified by parties, relevant documents are kept under legal custody, where they cannot be modified or deleted. This ensures that evidence is tamperproof and admissible in court.

With organizations moving to the cloud at a rapid rate, the cloud will become a repository of most ESI that will be required in investigations or litigations as evidence. Therefore, CSPs and their clients must be able to identify all the documents that are relevant and required for a legal case.

Electronic Discovery Issues

Cloud service providers and customers must know the following issues in legal cases when a customer/client is subject to a discovery request and the provider has the potentially relevant data on its cloud platform.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Possession, Custody, and Control**

  In most jurisdictions of the US, an organization/client (party in litigation) is obligated to produce information in court that is relevant and under its possession or control. When the organization uses a cloud provider for storage, this obligation remains. Upon request, the provider is responsible for producing the data (documents, files, etc.) relevant to the litigation and under its control.

  However, the organization does not have control over all data hosted on the cloud platform. This includes disaster recovery (DR) systems and certain metadata used by the provider. The responsibility of the CSP for producing such data in court is unclear, especially for international cases.

- **Relevant Cloud Applications and Environment**

  In cases where a cloud application or environment itself can resolve a dispute, a subpoena or other discovery processes can be directly served to the CSP. This is because the client or organization has no control over the artifact (application or environment) to produce it in the court.

Searchability and e-Discovery Tools

A cloud customer or client may not be able to use e-discovery tools in a cloud environment that it uses in its on-premises environment. The cloud customer may also not have the administrative rights to access all the data stored in the cloud environment. For example, the client could easily access the email accounts of its employees on its on-premises server, but it may not have the same ability to access email accounts that are hosted in the cloud.

This limited access and potential additional time required to access information on the cloud may create problems for the client. Therefore, the inability to use conventional e-discovery tools on the cloud and limited searchability are issues faced by the client in the context of e-discovery. If the client can supplement or negotiate the cloud service agreement, this issue can be addressed in advance; else, the client must address issues separately on a case-by-case basis and buy additional services from the provider.

Preservation

Preservation refers to securing potential evidence (data that can be used by a party in a legal case) from destruction, modification, or deletion. The complexity of data preservation in a cloud environment depends on the cloud service and deployment model selected by the client. Preservation in the cloud environment can be as simple as in conventional IT infrastructure or more complex depending on the cloud service and deployment model used by the client.

As per US law, a party is responsible for taking suitable steps to preserve evidence that is under its control or possession for a legal case or investigation. Similar laws for evidence preservation exist in other countries such as European countries, South Korea, Japan, and Singapore.

Data Retention Laws and Record-keeping Obligations

Data retention laws require covered entities to keep the data for a certain time period. In the US, there are various data retention requirements for different types of data. Furthermore, privacy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

laws place limitations on data retention. In cases of conflicting requirements on the same data, case law and guidance should be used to resolve such conflicts. The following are some important aspects of data-retention laws and record-keeping obligations.

- **Costs and storage**: When using cloud storage for evidence preservation, storage requirements must be weighed against SLA requirements and costs because preservation may require retaining large volumes of data.
- **Scope of preservation**: The party that requests the data is not allowed to access all the data in the cloud environment. The party is only entitled to the data relevant to the legal case being reviewed. The client must be able to preserve only the relevant information to be produced as evidence in court. If the client lacks the ability to identify and preserve the relevant information, it may need to over-preserve the cloud data. Later, this over-preserved information must be examined to identify what information is relevant as part of the e-discovery process. The examination of over-preserved information is called document review or privilege review, which is performed by client-paid attorney staff or emergency expert systems.
- **Dynamic and shared storage**: The preservation of data is difficult with cloud storage. If the client has sufficient space to store relevant data, knows how to preserve data, and limits access to only a few people, modest data preservation in the cloud can be achieved. However, data preservation is still practically difficult in cloud environments because of the elastic nature of the cloud. Thus, the client may need to consult the provider for ways to store the relevant data.

hide01.ir

Collection

Since the client does not have administrative access to its data hosted on the cloud, data collection is difficult, expensive, and time-consuming. In addition, the client does not have a uniform level of visibility across all of its data, further increasing the difficulty of data collection. The following are some aspects related to data collection in the cloud.

- **Access and bandwidth**: The SLA signed between a client and a cloud provider determines the client's access to its data. The SLA should allow the customer to have instant access to a large quantity of data in a forensically sound manner. Before beginning the relationship, both the client and the provider must establish a protocol for special access to the data stored in the cloud in the case of litigation. If any such agreement was not signed, the client will be responsible for the extra time and cost incurred on collecting the relevant data from the cloud. However, if a litigant can prove that the requested information is not accessible, the law excuses the litigant.
- **Forensics**: Acquiring a bit-by-bit image of a cloud data source is not possible or is complicated, because CSPs do not provide access to their hardware in most cases, particularly in a multi-tenant environment. When multiple tenants use the same hardware, the provider cannot allow the client access to its hardware, because doing so may provide the client access to other tenants' data. Similarly, it is difficult in even a private cloud to perform forensics. The client should inform the court or the opposing

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

counsel about these limitations. Owing to the various limitations of cloud computing, such forensic analysis is very rarely warranted.

- **Reasonable integrity**: A client subject to a discovery request must ensure that the collection of data from the CSP is complete and accurate by taking the necessary steps. This is especially important when litigation-specific measures are utilized for collecting the information.
- **Limits to accessibility**: In some cases, the client may not be able to collect all of its data stored in the cloud, because of differences in data storage options, data access rights, and privileges. When responding to a discovery request, the cloud provider and the client must analyze the relevance of the request before implementing further steps to obtain the data.

Direct Access

A party's request to directly access the IT environment of the responding party outside the cloud environment is not usually entertainment. However, some courts allow the requesting party direct access to the responding party's IT environment to collect and preserve evidence. In a cloud environment, direct access to collect evidence and perform forensic analysis is impossible because CSPs typically do not provide direct access to their hardware infrastructure. For gaining such access, the requesting party must directly negotiate with the CSP, as some providers may not have possession of their hardware and facilities.

hide01.ir

Native Production

CSPs normally store data in highly proprietary applications and systems that are not controlled by clients. If any relevant information is lost with conversion, the electronically stored information (ESI) can usually be produced in standard formats (e.g., PDF for electronic documents). If the data are produced in the cloud-native format, the requesting party cannot read the information produced. Thus, it is best for all parties (the requester, provider, and producer) to export relevant information via standard exporting or reporting protocols used inside the cloud environment with proper care to ensure that the information is preserved.

Authentication

Authentication in e-discovery refers to the forensic authentication of evidence data. Data stored in the cloud can be considered evidence unless its integrity is lost. Merely storing data in the cloud does not impact the admissibility of the data in court. Information stored in the cloud is credible and admissible until tampering or modification occur. The main aspect that determines a document's credibility is its integrity (it should be what it claims to be).

Cooperation Between Provider and Client in e-Discovery

Cloud users and providers must consider including the provisions of discovery requests in SLAs to reasonably cooperate with each other. Before starting their relationship, both parties must consider the complications that may arise from discovery. CSPs can include discovery services in their cloud offerings while designing them to attract customers.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

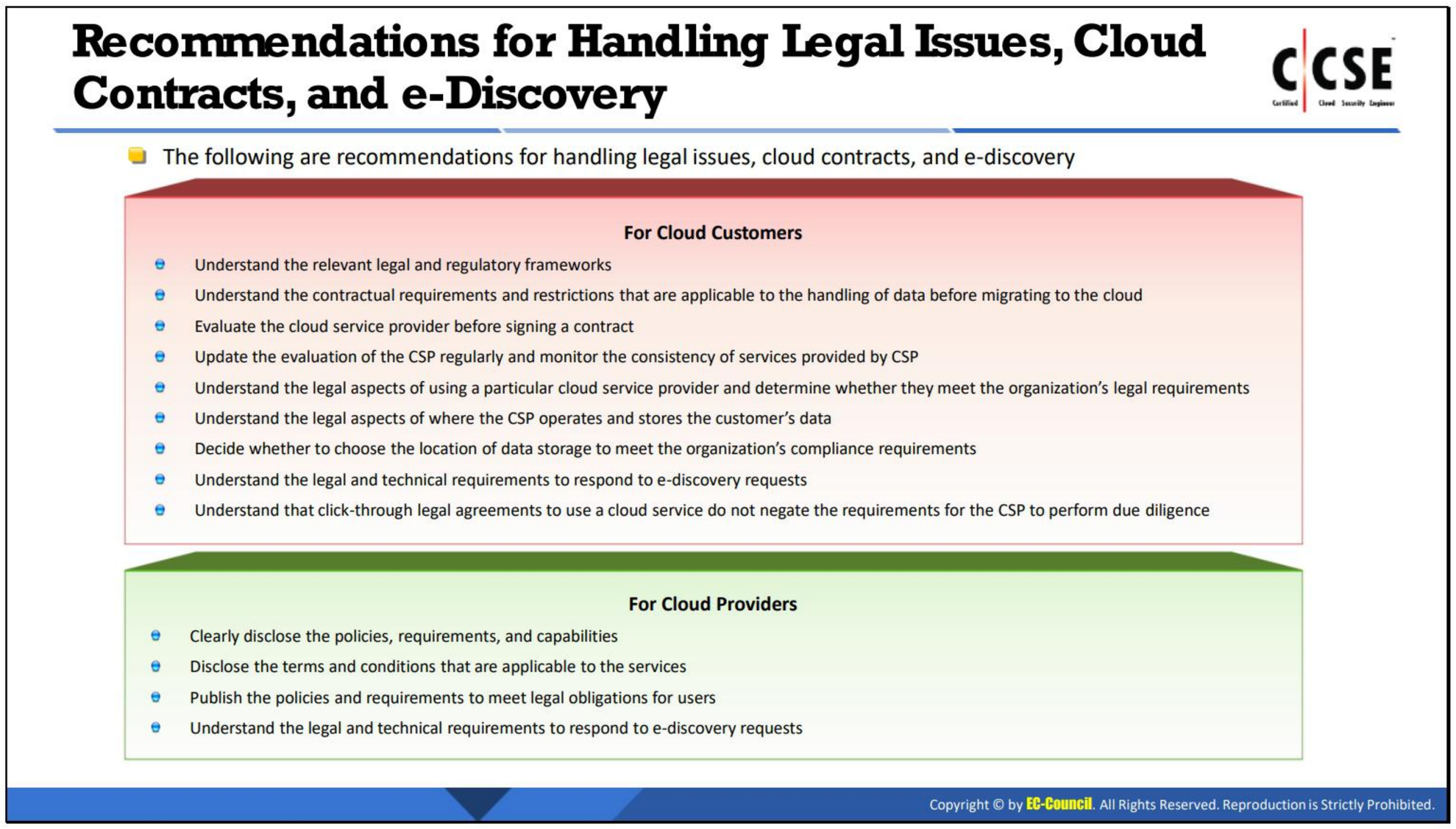
Response to a Subpoena or Search Warrant

When a CSP receives a request from a third party to access client information stored in the cloud, the provider must notify the client before providing access to its data. The request to access client information can be in the form of a warrant, subpoena, or court order. The client whose information was requested in the warrant or subpoena can contest the request to protect the secrecy of the data sought. This is possible only when the provider notifies the client before providing access. Thus, SLAs should include provisions that require the provider to inform the client about any subpoena so that the client has enough time to protect their information stored in the cloud.

Before responding to any warrant by providing access to the requested information, the CSP must consult the counsel to confirm the validity and strength of the legal request. The provider must then analyze the request and consider if it can disclose the requested information while meeting its obligations to the client.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recommendations for Handling Legal Issues, Cloud Contracts, and e-Discovery

The following are the recommendations for handling legal issues, cloud contracts, and e-discovery.

hide01.ir

Recommendations for Cloud Customers

- Before moving systems and data to the cloud, cloud customers must understand the following:
  - The relevant legal and regulatory frameworks
  - The contractual requirements and limitations that are applicable to the handling of data
- Cloud customers should evaluate cloud service providers (CSPs) before signing a contract.
- Cloud customers should regularly monitor the nature, scope, and consistency of the services purchased from the provider and update the provider's evaluation.
- Cloud customers should understand the legal implications of using certain CSPs and match those implications with their (customers') legal requirements.
- Cloud customers should understand the legal implications of the location where the CSP operates and stores data physically.
- If the option is available, customers should decide the location where their data must be hosted in order to comply with their jurisdictional requirements.
- The cloud consumer should comprehend the legal and technical requirements to provide a response to e-discovery requests.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

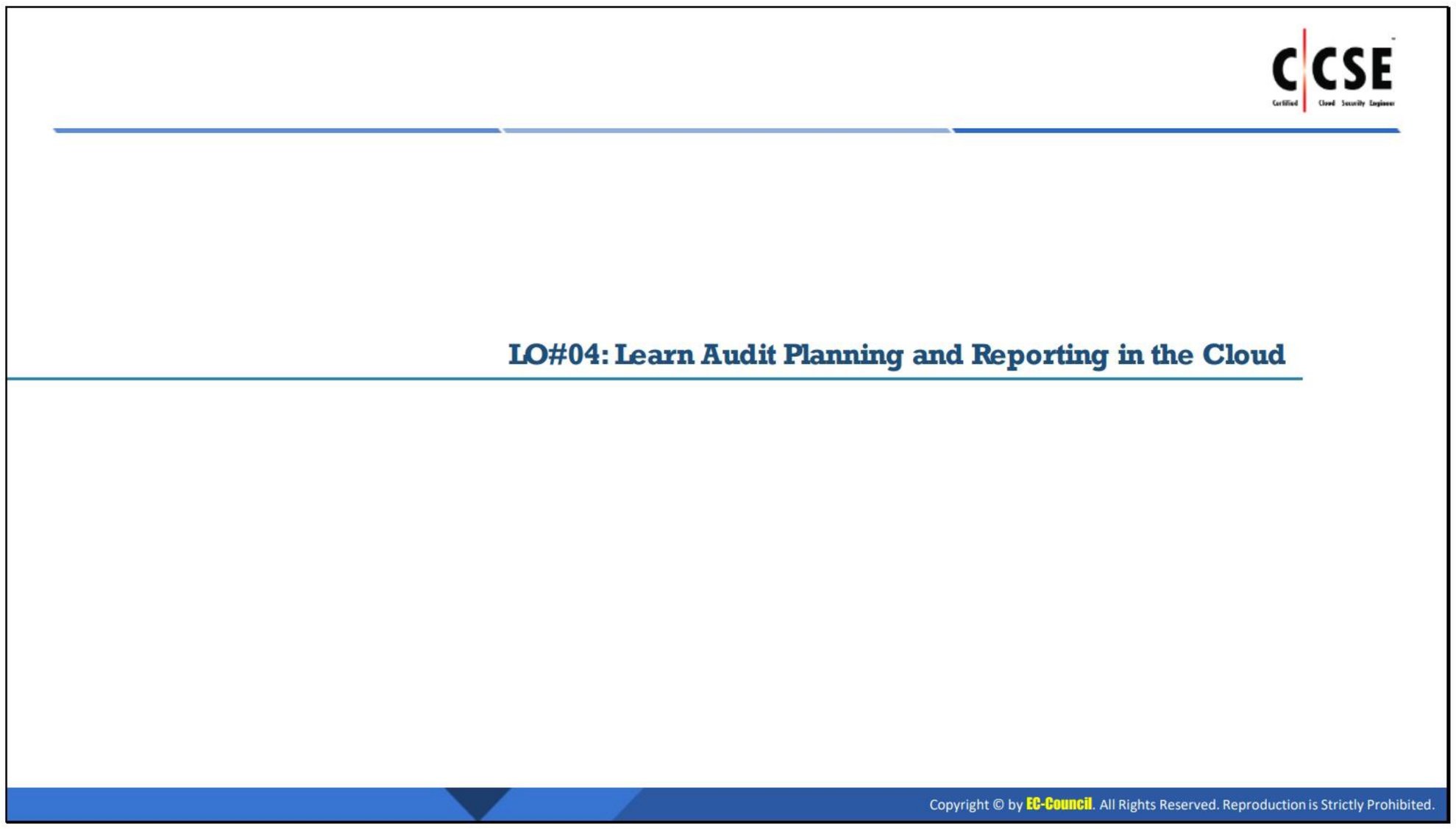
- The cloud consumer should understand that click-through legal agreements do not invalidate the provider's responsibility of performing due diligence.

Recommendations for Cloud Providers

- Cloud service providers (CSPs) should clearly and precisely disclose the requirements, policies, and capabilities of the services they offer. This allows customers to compare the services provided by various providers and decide the provider that best meets their requirements.
- CSPs should disclose the terms and conditions that are applicable to their services. This will help customers attain a clear picture of the services offered by CSPs.
- CSPs should publish their policies, capabilities, and requirements to meet cloud customers' legal obligations such as e-discovery. Customers can use the information published by the provider to make informed decisions about their future alliance with the provider.
- CSPs should understand the legal and technical requirements to respond to e-discovery requests.

hide01.ir

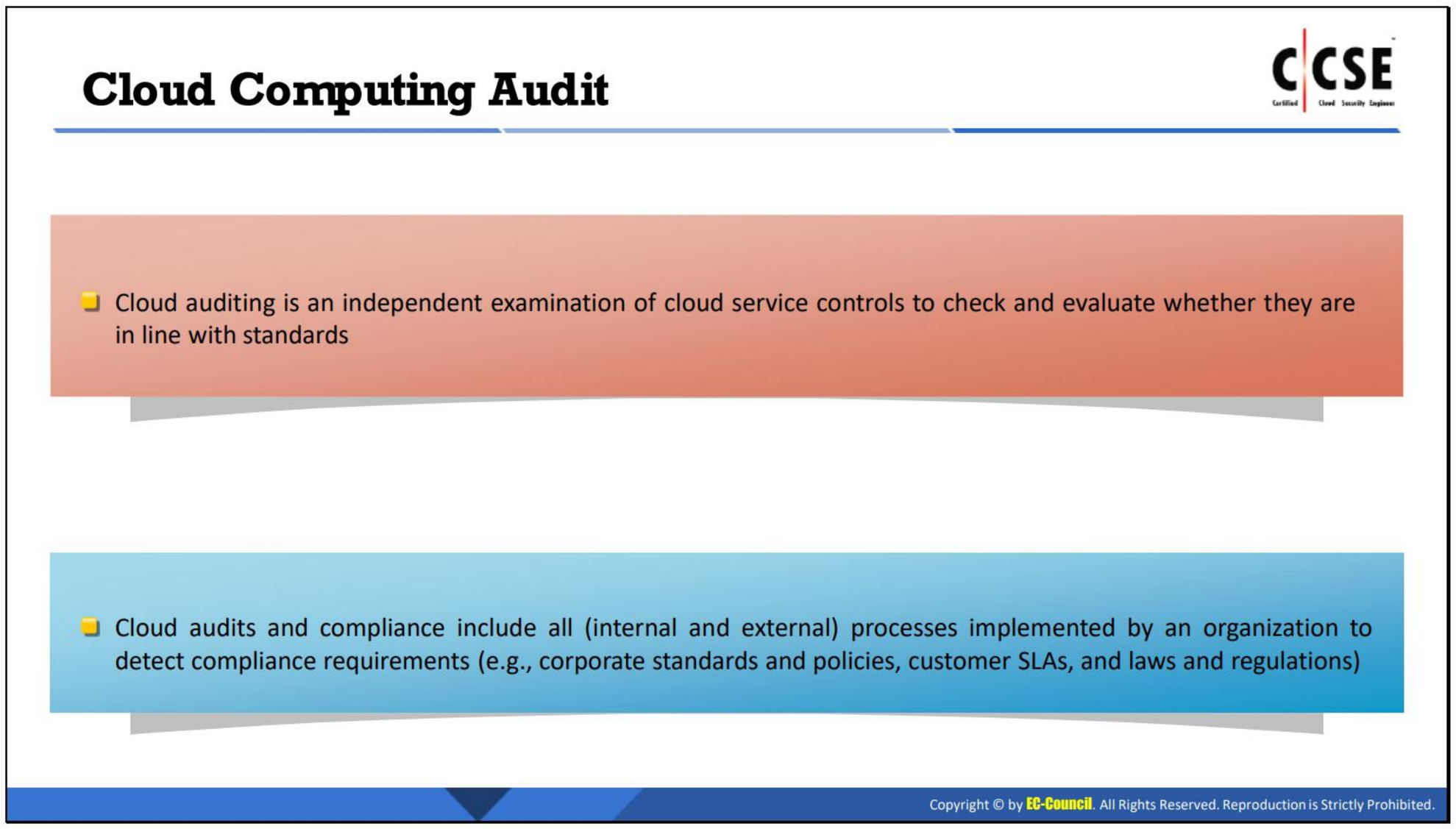
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Learn Audit Planning and Reporting in the Cloud

Cloud service controls should be examined to evaluate and check whether they meet the applicable standards. Auditing should be performed regularly to ensure that all the compliance requirements are met and to monitor the processes, policies, and procedures in a n organization. This section focuses on explaining cloud computing audits and their impact on the organization, as well as the scope, objectives, and testing methods of cloud auditing. It also explains internal audit and internal auditor objectives. In addition, this section illustrates cloud-specific auditing challenges, various standards applicable to cloud security auditing, and gap analysis.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Computing Audit

Cloud auditing is an independent examination of cloud service controls to check and evaluate whether they are in line with the applicable standards through a review of objective evidence. Cloud auditing is different and more complicated than conventional IT auditing. It can be external or internal. Internal audits are conducted by internal auditors to assess and analyze data and processes for enhancing an organization's efficiency and effectiveness. External audits are performed by third-party expert auditors or auditing firms.

Usually, auditing involves hiring an independent, third-party group/organization to verify how well all standards, procedures, and policies are followed through physical inspection, inquiry, observation, analytics procedures, confirmation, and/or re-performance. In cloud computing auditing, some of these steps are used to form an opinion of the design and operational effectiveness of controls present in the following areas:

- Network security
- Security incidents
- Communication
- Risk management
- Data management
- Change management
- Vulnerability and remediation management

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

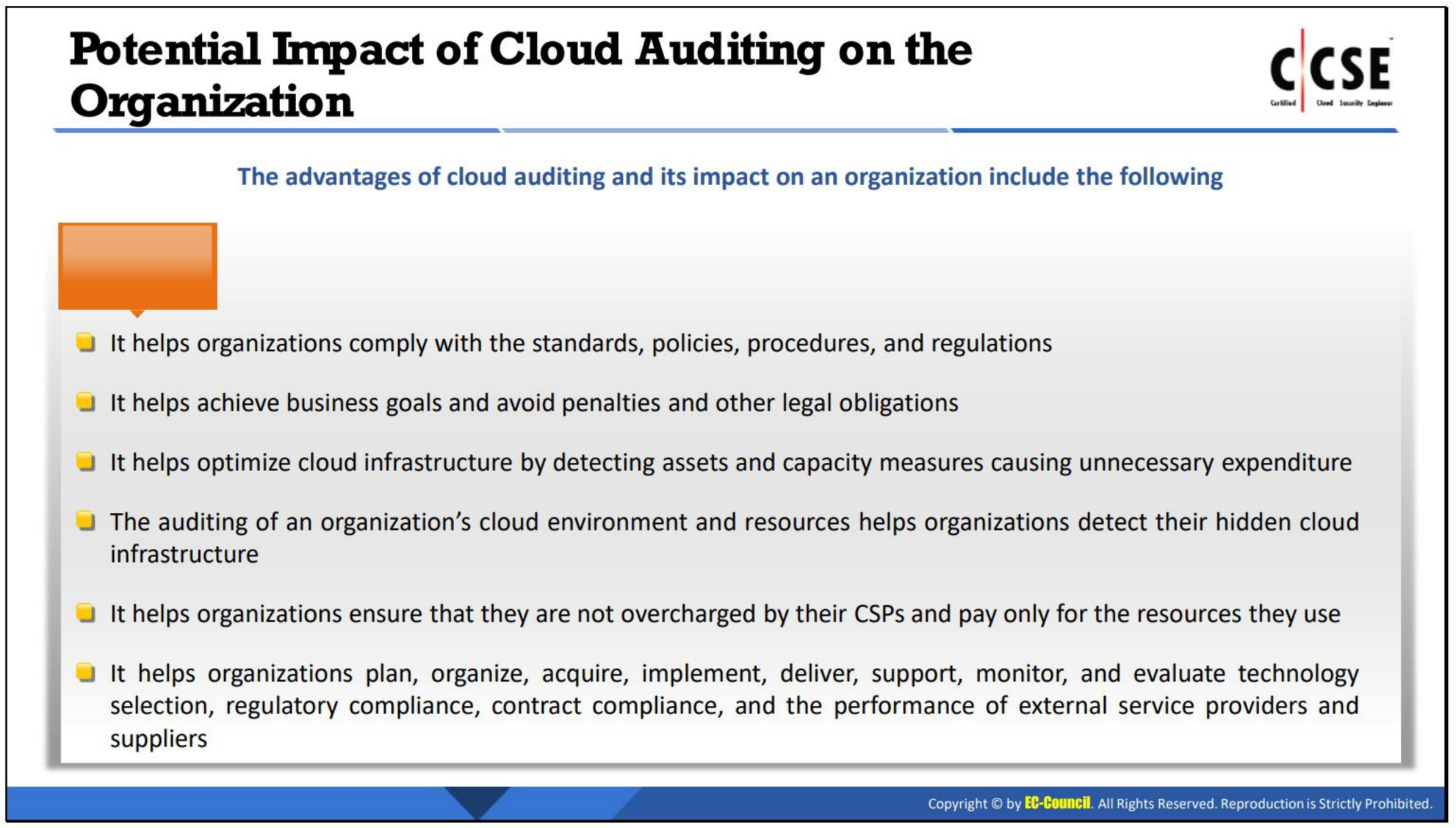
Cloud auditing includes security auditing or the auditing of security controls. Security controls are technical, operational, and management safeguards or countermeasures that an organization enforces to protect the availability, confidentiality, and integrity of information systems. In security auditing, the cloud auditor checks the security controls in the information system to determine whether they are implemented appropriately, working as per requirements, and providing the expected output as per the security requirements of the system.

Cloud audits and compliance include all (internal and external) processes implemented by an organization to detect compliance requirements (e.g., corporate standards and policies, customer SLAs, and laws and regulations). Cloud auditing helps organizations to:

- Implement processes, policies, and procedures to meet those compliance requirements
- Monitor these processes, policies, and procedures to check whether they are followed diligently

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

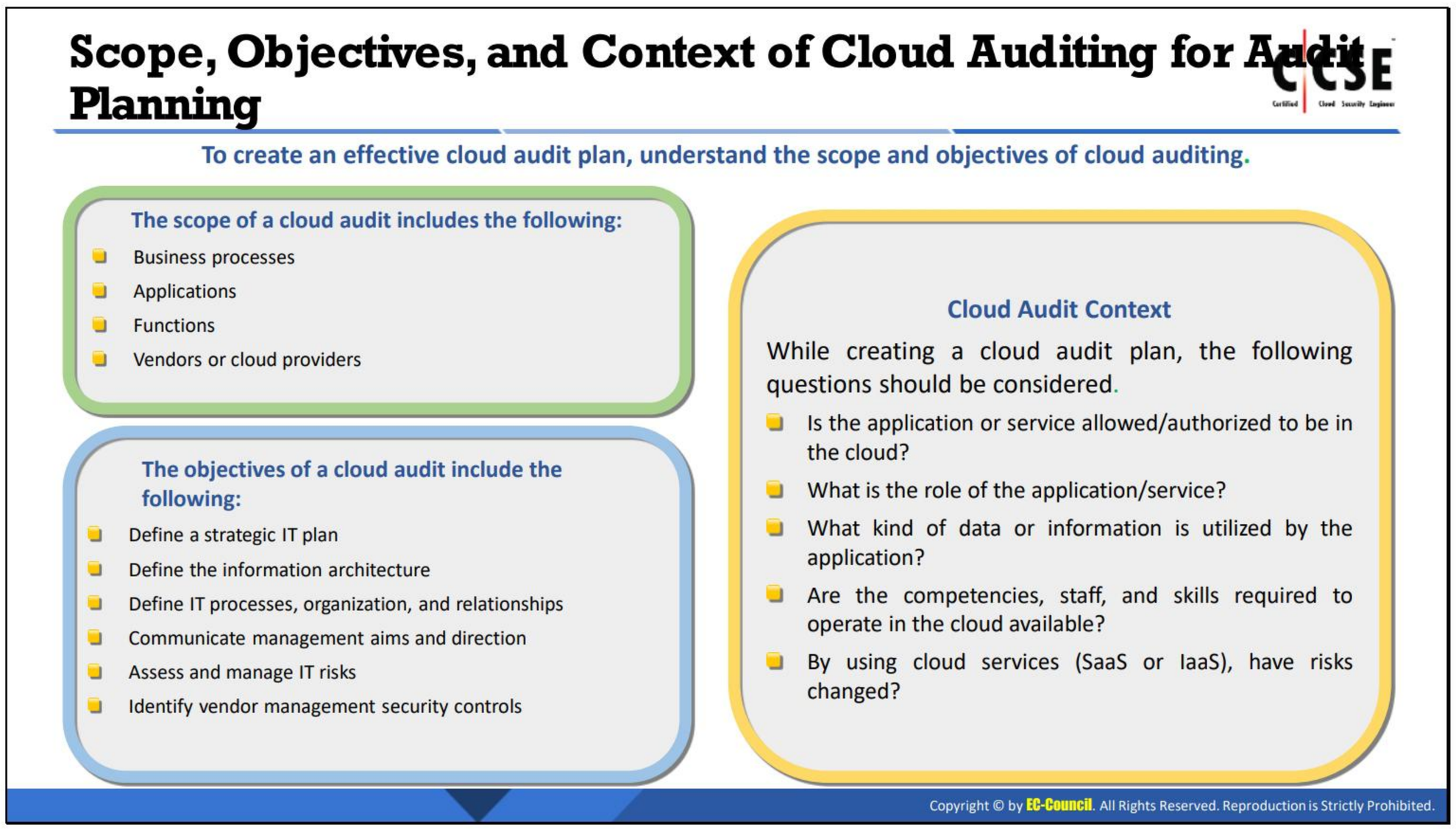


Potential Impact of Cloud Auditing on the Organization

Cloud computing audits help organizations ensure that they comply with the applicable standards, policies, procedures, and regulations. This ensures that organizations can achieve their business goals and avoid penalties and other legal obligations. Cloud auditing offers the following advantages to organizations:

- It helps optimize cloud infrastructure by detecting assets and capacity measures causing unnecessary expenditure. This helps organizations achieve better control over finances and gain greater visibility over their cloud estate.
- Organizations can detect what hidden cloud infrastructure they have by auditing their cloud environment and resources. This can help them shut down unused/unwanted workloads to save cost and minimize security risks as well as optimize their cloud inventory.
- By performing regular cloud audits, organizations can ensure that their CSPs do not overcharge them and that they pay only for the resources they use. This is because cloud auditing helps them detect unused resources and gain complete control over capacity management (by identifying extraneous capacity) in their cloud environment.
- Performing an in-depth analysis of cloud inventories can help organizations reduce/eliminate additional costs.
- It helps organizations plan, organize, acquire, implement, deliver, support, monitor, and evaluate technology selection, regulatory compliance, contract compliance, and the performance of external service providers and suppliers.
- Cloud audit checks can be used to test data integrity, confidentiality, availability, security, etc.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scope, Objectives, and Context of Cloud Auditing for Audit Planning

To create an effective cloud audit plan, understanding the scope and objectives of cloud auditing is essential. Having a clear understanding of the cloud auditing objectives will help organizations align their business objectives with the audit objectives. This will ensure that the resources and time spent by the organizations will help them achieve a strong, well-controlled environment.

Scope of Cloud Auditing

The scope of a cloud audit includes all procedures specific to the subject of audit and IT controls related to risk assessment, organization and administration, monitoring activities, communication, system operations, logical and physical access, and change management. An auditor can review and obtain evidence for any of the controls within these areas to be assured that these controls are designed and operated effectively. The scope of a cloud computing audit does not include the controls maintained by a vendor.

The scope of a cloud audit includes the following:

- Business processes
- Applications
- Functions
- Vendors or cloud providers

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Objectives of Cloud Auditing

Objectives are used as a way of concluding the evidence obtained by cloud auditors. With well-defined objectives for a cloud audit, organizations can easily align their business objectives with the audit objectives.

The following is a list of sample cloud computing audit objectives that are useful for both auditors and businesses.

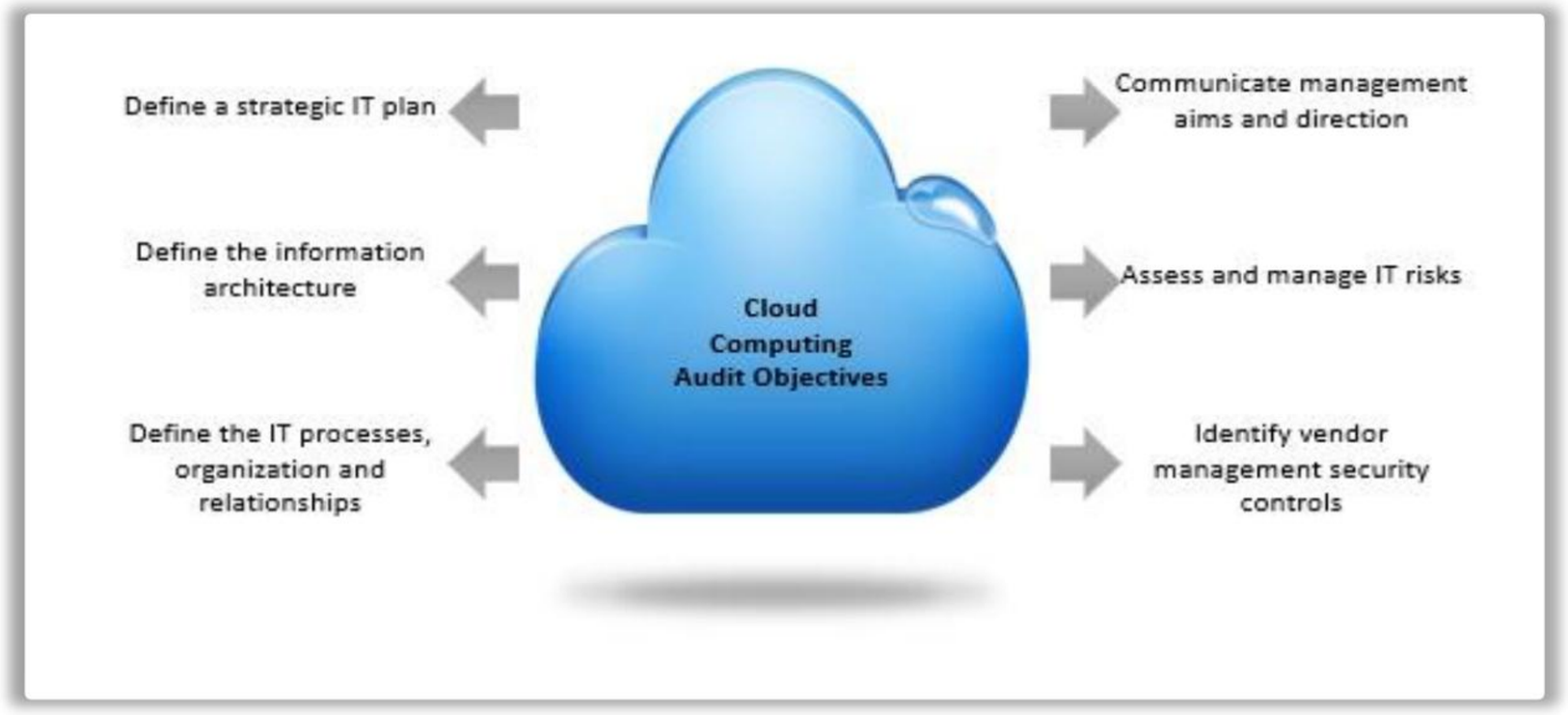


Figure 11.5: Cloud Computing Audit Objectives

- **Define a strategic IT plan**: Defining a strategic IT plan is essential because the use of IT resources must align with the business objectives of the organization. Organizations should check whether IT investments are supported by a strong business case and identify what training/education is required during the new IT investment rollout while defining a strategic IT plan.
- **Define the information architecture**: The information architecture involves all system, network, and security requirements essential to protect the security and integrity of information. The information must be secured at all stages: at rest, in transit, and during processing.
- **Define IT processes, organization, and relationships**: An IT environment with improved stability can be created by making and implementing standardized, repeatable, and documented processes. Organizations must create procedures and policies that include the organizational structure, system ownership, roles and responsibilities, information security, risk management, incident management, change management, segregation of duties, and disaster recovery.
- **Communicate management aims and direction**: The management of an organization must ensure that its mission, policies, and objectives are clearly communicated across the organization.
- **Assess and manage IT risks**: The organization must assess and document all IT risks that can potentially affect its objectives. These risks can be laws and regulations, security vulnerabilities, unauthorized access to sensitive information, etc.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identify vendor management security controls**: Organizations that rely on third-party vendors (e.g., AWS for hosting their infrastructure and Automatic Data Processing (ADP) for payroll processing) must detect the risks that can potentially affect the accuracy, reliability, and safety of sensitive information.

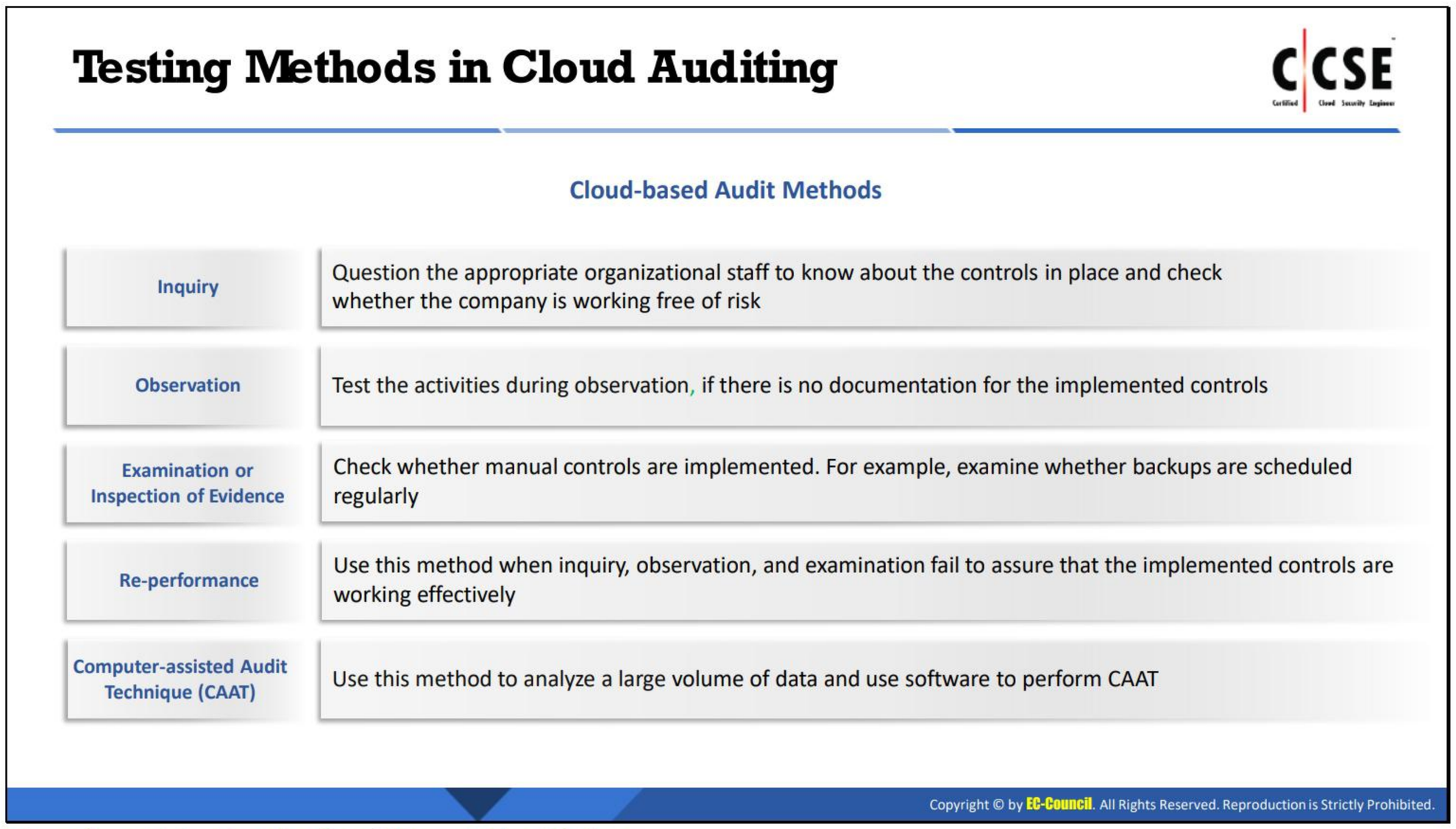
Cloud Audit Context

While creating a cloud audit plan, the following questions should be considered:

- Is the service or application allowed/authorized in the cloud ecosystem?
- What role is played by the application or service?
- What kind of data is used by the application?
- Does the organization have the necessary competencies, staff, and skills for operating in the cloud environment?
- While utilizing cloud services (SaaS or IaaS), have the risks changed?

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



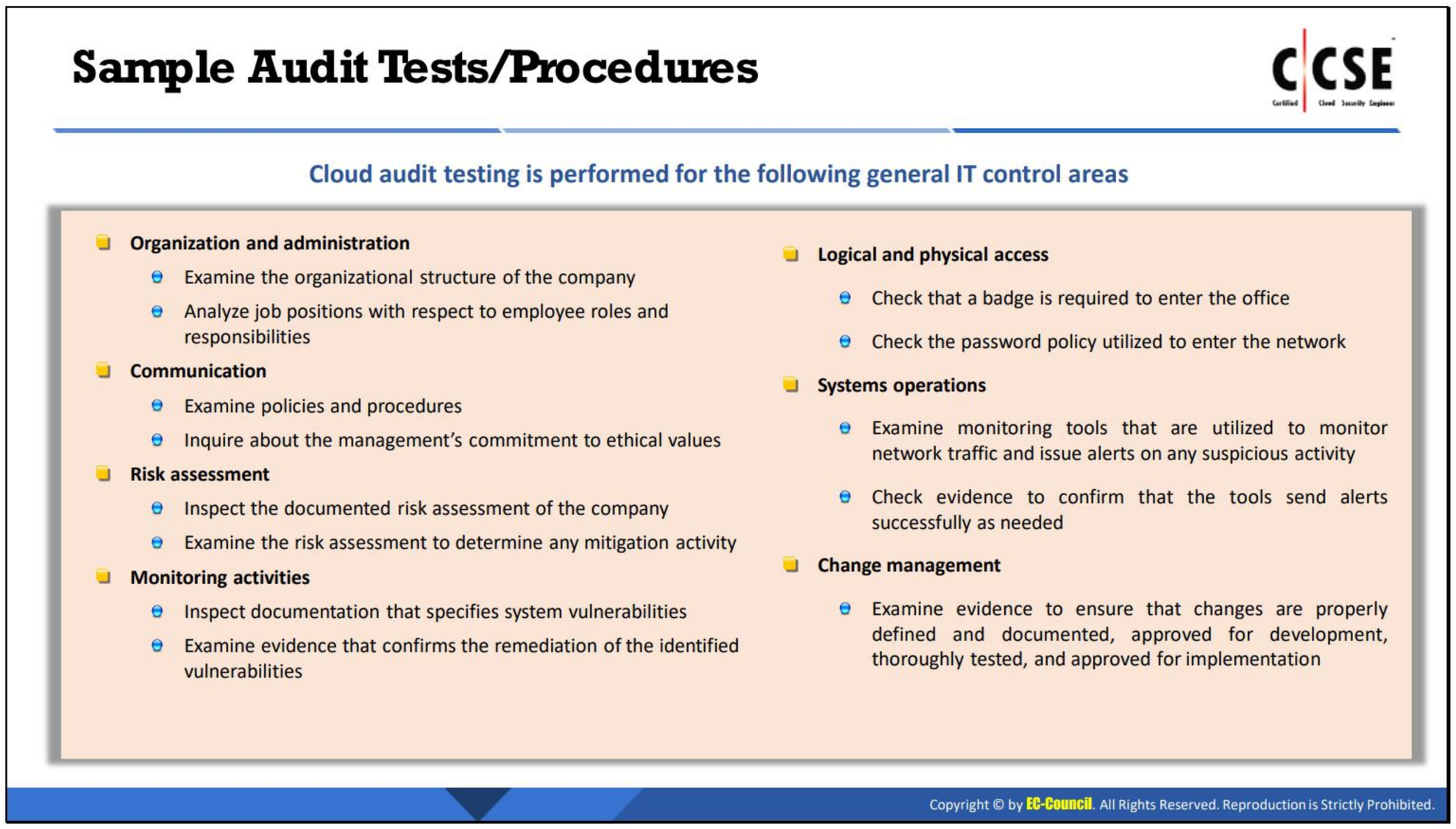
Testing Methods in Cloud Auditing

Various types of tests are performed in cloud auditing to collect objective evidence. These tests or procedures help in gathering evidence and in forming an opinion about the service under audit by using a combination of procedures to collect evidence.

The following are cloud-based audit methods used to confirm the answers and facts that an organization receives during an audit.

- **Inquiry:** Question the appropriate staff of the organization to know about the implemented controls and check whether the company is working without risk. For example, the auditor may inquire whether the management's data center is safe from visitors. This is the most relevant method of auditing.
- **Observation:** Test the activities during observation. Use this method if there is no documentation for the operation of the implemented controls. For example, observe whether a security camera is installed for the data center.
- **Examination or inspection of evidence:** Examine whether manual controls are implemented. For example, examine whether backups are scheduled regularly.
- **Re-performance:** Use this method when the above three methods fail to assure that the implemented controls are working effectively. In this method, the auditor manually executes the implemented controls.
- **Computer-assisted audit technique (CAAT):** Use this method to analyze a large volume of data. Use software to perform CAAT. For example, use spreadsheets, databases, and data analyzing software. Both re-performance and CAAT are considered the strongest cloud auditing methods.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sample Audit Tests/Procedures

The following are some sample tests that are performed for general IT control areas.

- **Organization and Administration**

  For the organization and administration control area, the following procedures are used.

  - Examine the organizational structure of the company.
  - Analyze job positions with respect to employee roles and responsibilities.
  - Analyze the interview process to identify the technical competencies of the company's test.
  - Examine the evidence of completed background checks.

- **Communication**

  For the communication control area, the following procedures are used.

  - Examine policies and procedures.
  - Inspect evidence to verify that policies and procedures are available for reference to all employees.
  - Examine the company's "Terms of Use" or privacy documentation to determine whether they specify responsibilities and commitments.
  - Inquire about the management's commitment to ethical values.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Risk Assessment**

  For risk assessment, the following procedures are used.

  - Inspect the documented risk assessment of the company.
  - Examine the risk assessment to determine whether any mitigation activity is found, as required.

- **Monitoring Activities**

  For monitoring activities, the following procedures are used.

  - Inspect documentation that specifies system vulnerabilities.
  - Analyze system configurations to check whether notifications are provided when failures and vulnerabilities are identified.
  - Examine evidence that confirms the remediation of the identified vulnerabilities.

- **Logical and Physical Access**

  For auditing logical and physical access, the following procedures are used.

  - Check whether a badge is required to enter the office.
  - Inspect evidence to ensure that individuals that have administrator-level access are authorized.
  - Examine the password policy used to enter the network.

hidden.ir

- **Systems Operations**

  For auditing system operations, the following procedures are used.

  - Inspect monitoring tools that are used to monitor network traffic and issue alerts on any suspicious activity.
  - Check evidence to confirm that the tools send alerts successfully as needed.
  - Examine evidence to confirm that notifications are followed up on and remediated as required.

- **Change Management**

  For auditing change management, the following procedure is used.

  - Examine evidence to ensure that changes are properly defined and documented, approved for development, thoroughly tested, and approved for implementation.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Internal Audit

- Internal Audit (IA) is a process that helps the board and management of an organization detect and consider the key risks of using cloud computing
- Internal audits are performed by internal auditors of an organization to evaluate and analyze the data and processes in order to improve the organization's effectiveness and efficiency
- Organizations can conduct an internal audit for creating a cloud risk framework equipment tool that will help in determining the root causes of risks by providing a view on the evolving, pervasive, and interconnected behavior of cloud computing risks

Proactive steps for IA

Step	Explanation
Engage stakeholders	Encourage business and IT executives to have a conversation about migrating to the cloud Make stakeholders understand the potential of rouge IT environments Identify which applications or data should be moved to the cloud and the possible risk implications after they are moved
Review the framework of the organization	Modify the current risk framework of the company based on the new identified risks Use the new or modified risk framework tool to measure the current cloud capability state of the organization across various cloud risk domains
Develop a risk-mitigation plan or strategy	Ensure that IA is part of the risk equation so that it can help the organization create a risk-based approach for using the cloud This step involves understanding the involved risks as well as suggesting ways to reduce risk
Review data governance	IA must review the existing enterprise data governance program and implementation across different systems to confirm whether policies are implemented for compliance with the applicable regulatory laws The management can make risk-informed decisions regarding the migration of data and services to the cloud by understanding the data governance program and its implementation inside the organization
Evaluate potential cloud vendors	The IT staff should know many vendors and business leaders that can meet the objectives of moving to the cloud IA must be involved in risk discussions with compliance, security, and risk groups Internal auditors may help the enterprise develop an assessment profile for vendors. This profile must explore issues such as DR capabilities and vendor controls

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

Internal Audit

An internal audit (IA) is a process that helps the board and management of an organization to detect and consider the key risks of using cloud computing. It also helps the organization determine whether the risks are mitigated appropriately. IAs are performed by internal auditors of an organization to evaluate and analyze the data and processes to improve the organization's effectiveness and efficiency.

IAs can help organizations develop a framework to assess and mitigate the risks related to cloud computing. Through IAs, organizations can be assured of the effectiveness of their risk mitigation efforts in the cloud control environment. For example, before signing an agreement with cloud vendors or cloud customers, an IA must be conducted for thoroughly assessing the current vendor procurement process to determine how the company can mitigate cloud risks that it may face. Internal auditors within an organization can check the effectiveness of the control environment once the information security group of the organization builds cloud monitoring capabilities.

Organizations can conduct IAs for creating a cloud risk framework equipment tool that will help in determining the root causes of risks by providing a view on the evolving, pervasive, and interconnected behavior of cloud computing risks. Such a tool can assist the organization in improving efficiency in its compliance and risk management efforts as well as in developing risk event scenarios. The elements of the framework include delivery strategy, data management, infrastructure security, identity and access management, and business resilience and availability.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

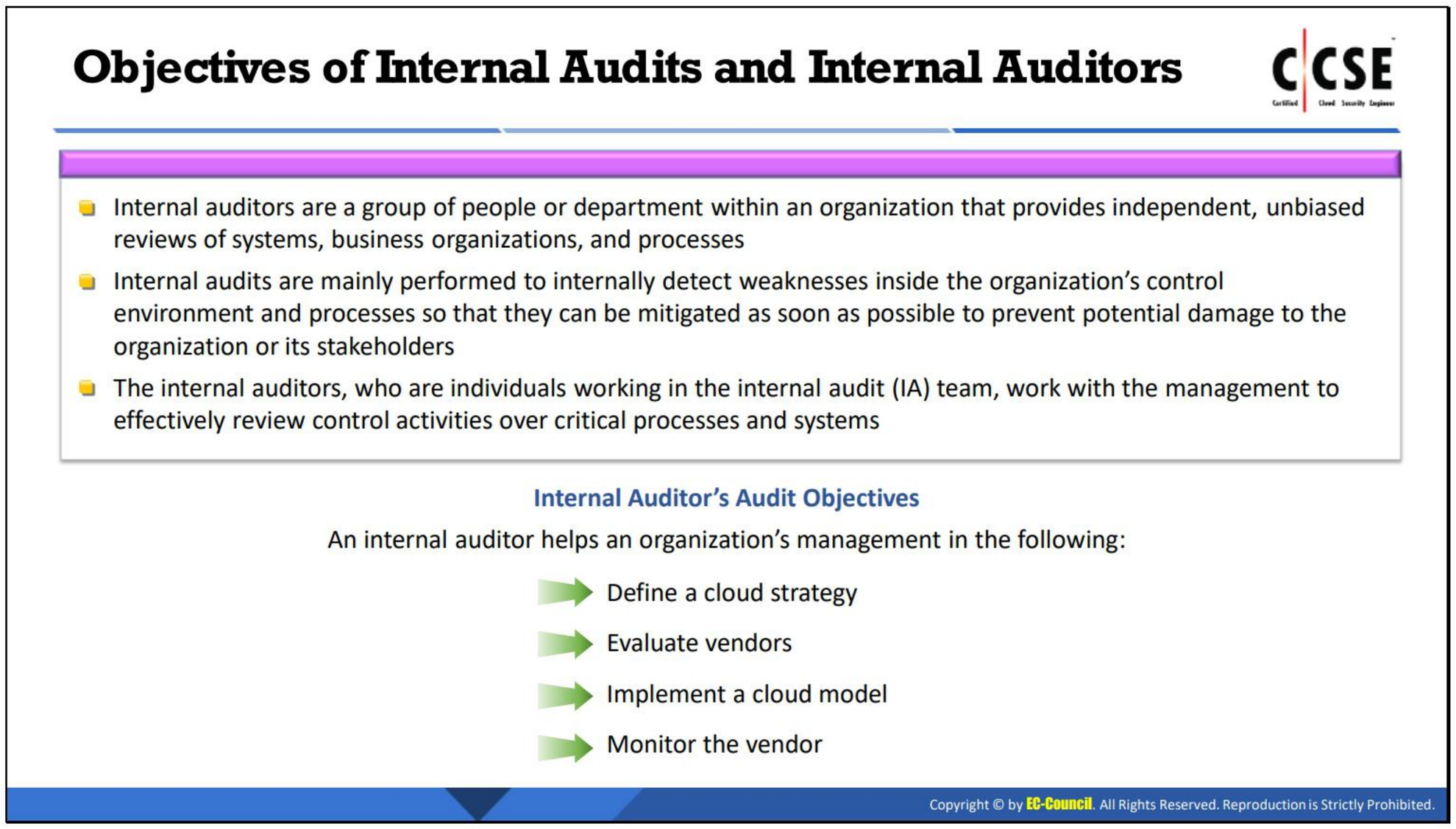
Proactive steps for IA

Implement the following steps to address issues related to cloud computing.

Step	Explanation
Engage stakeholders	▪ Encourage business and IT executives to have a conversation about migrating to the cloud. ▪ Make stakeholders understand the potential of rouge IT environments. ▪ Identify which applications or data should be moved to the cloud and the possible risk implications after they are moved.
Review the framework of the organization	▪ Modify the current risk framework of the company based on the newly identified risks. ▪ Use the new or modified risk framework tool to measure the current cloud capability state of the organization across various cloud risk domains.
Develop a risk-mitigation plan or strategy	▪ Ensure that IA is part of the risk equation so that it can help the organization create a risk-based approach for using the cloud. ▪ This step involves understanding the involved risks as well as suggesting ways to reduce risk.
Review data governance	▪ IA must review the existing enterprise data governance program and implementation across different systems to confirm whether policies are implemented for compliance with the applicable regulatory laws. ▪ The management can make risk-informed decisions regarding the migration of data and services to the cloud by understanding the data governance program and its implementation inside the organization.
Evaluate potential cloud vendors	▪ The IT staff should know many vendors and business leaders that can meet the objectives of moving to the cloud. ▪ IA must be involved in risk discussions with compliance, security, and risk groups. ▪ Internal auditors may help the enterprise develop an assessment profile for vendors. This profile must explore issues such as disaster recovery (DR) capabilities and vendor controls.

Table 11.1: Proactive Steps for Internal Audit

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Objectives of Internal Audits and Internal Auditors

Internal auditors are a group of people or departments within an organization that provides independent, unbiased reviews of systems, business organizations, and processes. The internal auditor's role is to offer an objective source of information to the governing bodies and senior leaders of the organization regarding the organization's control environment, risks, operational effectiveness, and compliance with the applicable regulations and laws.

Internal audits (IAs) are mainly performed to internally detect weaknesses inside the organization's control environment and processes so that they can be mitigated as soon as possible to prevent potential damage to the organization or its stakeholders. IAs are the reviews performed by the IA team. The internal auditors, who are individuals working in the IA team, work with the management to effectively review control activities over critical processes and systems. As cloud services evolve, internal audit and compliance play a crucial role to help organizations assess and manage risks, especially for third-party compliance.

Objectives of Internal Auditors

The objectives/roles of internal auditors include the following.

- **Define a cloud strategy:** With the help of the management, internal auditors must ensure that a cloud computing strategy is well defined and communicated. If a strategy has not been defined yet, internal auditors can help the management address the following questions.
    - **What is the business case for migrating to the cloud?**

      The organization must have a clear understanding of the value it desires to gain by migrating to the cloud and determine if it can completely accept or mitigate

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the risks associated with the cloud environment. A cloud hosting solution is suitable for the business if it seeks to increase scalability and efficiency significantly while reducing costs.

- **Will this decision align with the business requirements?**

  The organization must determine whether the decision to move to the cloud aligns with its overall business needs. Choosing a cloud solution would be appropriate if the organization is striving to reduce labor or operational costs.

- **Are you aware of the current state of systems and data to be moved to the cloud?**

  Understand the current state of system data that the organization desires to move to the cloud. The organization must determine what exactly is to be moved to the cloud environment. The organization must also consider whether it will move critical/sensitive data to the cloud and whether it will be able to comply with the applicable data retention requirements.

- **Evaluate vendors:** The organization must choose an appropriate cloud vendor after evaluating the risks and benefits of moving to the cloud. Choosing an appropriate vendor is of utmost importance. Internal auditors must help the organization evaluate vendors by addressing the following questions.

  - **Who will be responsible for managing vendor relationships?**

    Organizations that use third-party cloud providers must determine who will be the link between them and vendors. This ensures clear communication between the organization and the vendor's IT department, legal department, and account managers.

  - **How are assets secured?**

    Organizations must understand how the vendor manages the (physical and logical) security by asking for security policies, results of vulnerability tests and penetration tests, and attestations. The vendor must be capable of describing the data security controls it provides to secure data.

  - **How will the responsibility be divided?**

    The organization must understand who is mainly responsible for securing data as well as monitoring and controlling apps, servers, and data that are hosted in the cloud. Moreover, the organization must determine who will be legally and financially responsible for the security, uptime, and data.

  - **How will DR planning be affected by moving to the cloud?**

    The organization must ask the vendor about its business continuity/disaster recovery (BC/DR) plans and verify whether they align with the organization's business objectives and recovery needs.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **How are multiple tenants managed by the vendor?**

  Data of the organization may be stored in a physical machine containing other tenants' data. The organization must know what controls are implemented by the vendor to physically and logically separate its data from other tenants' data.

- **How will this decision change the technology environment?**

  The organization's technology environment may change once it implements a cloud-based solution. This includes the change in the interaction between systems, network topology, and flow of data. In addition, the organization must identify which data resides on and flows between which devices or components, who owns these devices, and who is responsible for governing this environment.

- **Where is the data stored physically?**

  Organizations must know where its data are stored physically because the CSP may store data internationally, causing additional international, regulatory, and ownership risks depending on the location of data storage.

- **How will the risks and controls of the organization align with the prospective vendor?**

  Through a gap analysis, the organization must determine whether the vendor has implemented any process or control gaps that may make the organization prone to additional risk.

hade01.ir

- **Implement a cloud model:** After the vendor is selected, internal auditors must evaluate the implementation process. The internal auditors must evaluate all implementation activities to ensure that they adhere to the organization's system development lifecycle, change management, and project management methodologies. Internal auditors help determine whether the level of planning is sufficient to minimize project risk and provide independent feedback on the mitigation process.

  While implementing a cloud computing model, consider the following.

  - **Service-level agreements (SLAs) and operating-level agreements (OLAs)**: The organization must understand the SLAs and OLAs provided by the CSP.
  - **Compliance responsibilities**: Both the organization and the CSP should understand their compliance responsibilities.
  - **Incident management**: The organization should understand the existing processes and escalation procedures for incident management. Moreover, it should know the expected time to resolve incidents.
  - **User access rights**: The organization should know who can determine the user access rights to data.
  - **Data backup frequency**: The organization should understand who is responsible for backup and recovery processes and their frequency.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

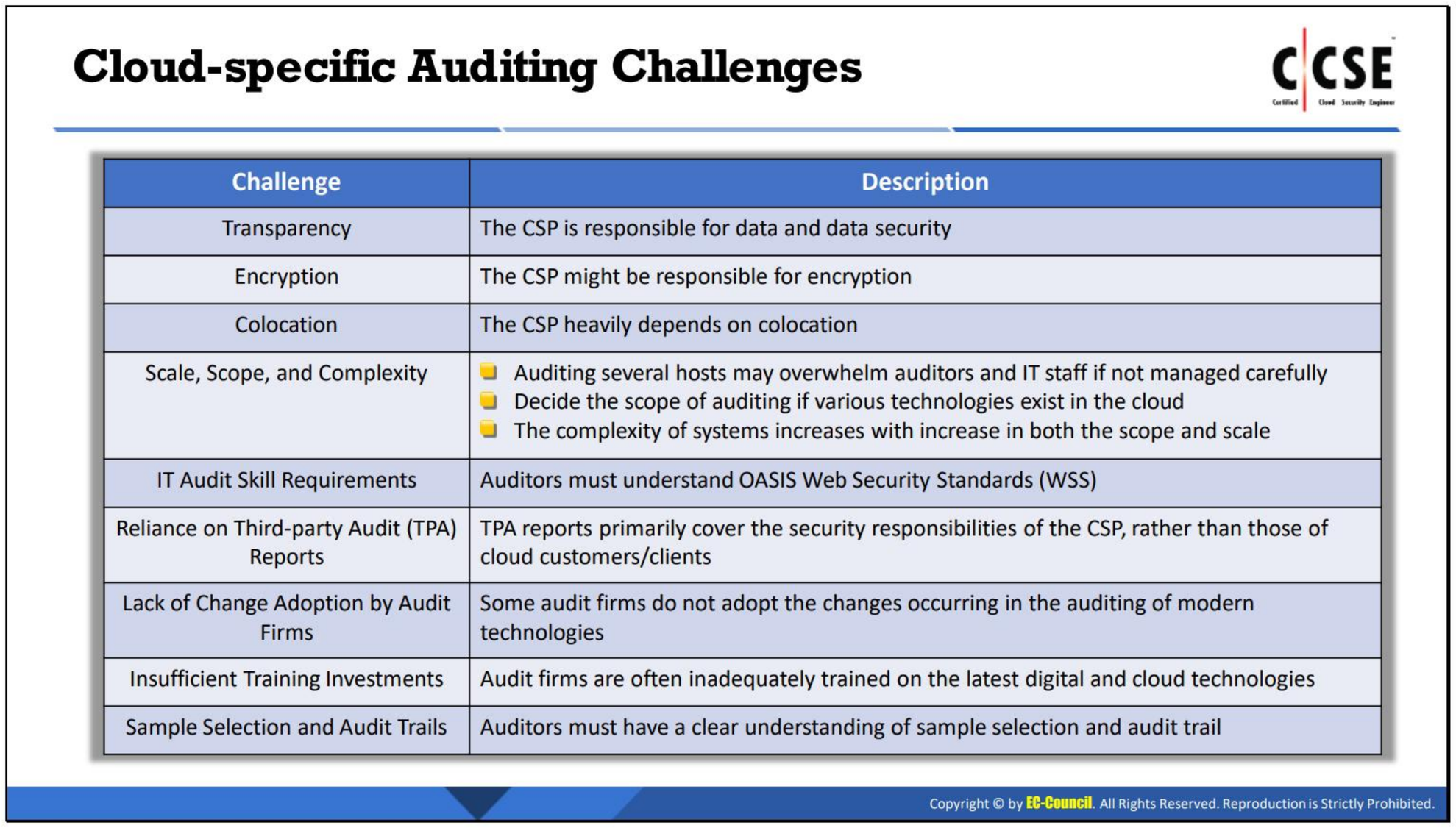
- **Monitor the vendor:** After integrating the planned systems and data into the cloud, internal auditors evaluate whether the defined owner can monitor and control the vendor relationship. The organization, by this time, must formally monitor and report on the agreed-upon service levels while investigating and resolving variances (if present).

  While monitoring the vendor relationship, confirm the following.

  - **Relationship management**: The organization must understand how the relationship between the organization and the vendor is managed. It must ensure that a single person is designated as the primary point of contact with the provider and that person should communicate regularly with their counterpart at the provider.
  - **Invoice accuracy**: The organization must obtain independent reports to confirm the accuracy of invoices.
  - **Monitoring and reviewing SLAs and OLAs**: All SLAs and OLAs between the provider and the organization must be monitored and reviewed to ensure that they are delivered accurately as promised.
  - **Monitoring contractual control requirements**: Contractual control requirements (e.g., security, privacy, regulatory, etc.) should be monitored through the means articulated in the contract, such as assessment reports and audits.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud-specific Auditing Challenges

Various challenges exist in a cloud environment that make cloud auditing a challenge. These challenges serve as barriers that prevent effective cloud auditing. The following are some cloud-specific auditing challenges.

hide01.ir

- **Transparency**

  Transparency in cloud security audits not only helps an organization identify potential risks and threats easily but also develops the appropriate security countermeasures and recommendations. A good cloud security audit must determine whether the CSP offers a good balance between end-user access and security controls. Audits must determine whether the provider is transparent about the access-control mechanisms it uses. Transparency is more crucial in a cloud environment because the CSP, rather than the cloud user, controls most of the data. A comprehensive understanding of the data location, CSP assets, and data security policies is essential in cloud security audits.

- **Encryption**

  Storing unencrypted information in the cloud is risky for user organizations. The customer's data will be exposed if the cloud is compromised. Organizations can encrypt their data before sending the data to the cloud, but this may allow system administrators to abuse their privileges. However, it is also risky to leave encryption solely to the CSP. In such a case, if one storage system is breached, all other storage systems can also be breached. Cloud auditors may wish to keep their queries secret, and the organization under audit might also want to preserve the privacy of its encrypted data. However, such a collaboration is not easy or possible in a cloud system where the organization's data are

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

stored in third-party infrastructure. The CSP may not disclose certain cryptographic information even for auditing purposes.

- **Colocation**

  In cloud computing, several user organizations share a single provider's physical systems. This helps them reduce costs significantly, but the sharing of technology infrastructure causes security concerns. The CSP must prevent user systems from gaining admin access to the hardware so that other users' data cannot be accessed and services are not abused. The provider must balance the colocation systems' and hypervisor's business needs as well as security issues. No official standard exists to address the need to standardize the security and structure of colocation.

- **Scale, Scope, and Complexity**

  Many virtual machines (VMs) are hosted on a single machine in cloud computing. This increases the number of hosts that must be audited. Auditing several hosts may overwhelm auditors and IT staff if not managed carefully. Auditors should ensure that standardization is implemented to make this process smoother and faster.

  Various technologies exist in cloud computing. Therefore, the scope of auditing must be considered. For instance, when dealing with cloud providers with a colocation problem, inspecting hypervisor security is important. A hypervisor vulnerability may threaten the isolation between VMs, which may cause concern for cloud users about their data privacy and security.

  Video01.ir

  The complexity of systems increases with the increase in both the scope and scale. Cloud auditors must consider this complexity so that they can invest more time and resources than they do in a conventional IT auditing process. They must also know about the physical location where the CSP stores customers' data because various laws apply to data depending on the storage location.

- **IT Audit Skill Requirements**

  Various IT processes are involved in cloud computing. As cloud auditing mainly focuses on IT management, information governance, data, network, contingency, and encryption controls, the audit and assurance staff must know these issues. They should have demonstrated proficiency in the information security components of IT infrastructure, risk assessment, risk management, and vulnerabilities and threats of cloud computing. Cloud IT auditors must understand OASIS Web Security Standards (WSS) because cloud computing depends on web services. They should determine whether the existing risk assessment process can capture risks accurately.

- **Reliance on Third-party Audit (TPA) Reports**

  Organizations primarily rely on third-party audit reports for assurance on cloud-based systems. If the organization does not use an updated IT questionnaire for auditing IT systems, its outdated questionnaires cannot effectively audit cloud technologies. Therefore, it must rely on third-party audit (TPA) reports. TPA reports primarily cover the security responsibilities of the CSP but not that of cloud customers/clients.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of Change Adoption by Audit Firms**

  Audit firms do not easily adopt changes when auditing modern technologies. Some audit firms still use the standard IT questionnaire that was developed more than 20 years ago. They use outdated questionnaires for auditing modern technology without using any automated tools for IT audits. This results in ineffective cloud auditing.

- **Insufficient Training Investments**

  Audit firms make inadequate investments in training their staff (IT auditors) in the latest digital and cloud technologies. One of the reasons for this is the fear that their staff would leave them if they are trained in modern technologies. Although these firms conduct various awareness sessions for their auditors, they do not provide sufficient training in highlighting the risks, mitigating the risks, testing the controls that are relevant to these risks, and the latest technology tools that help in effective auditing.

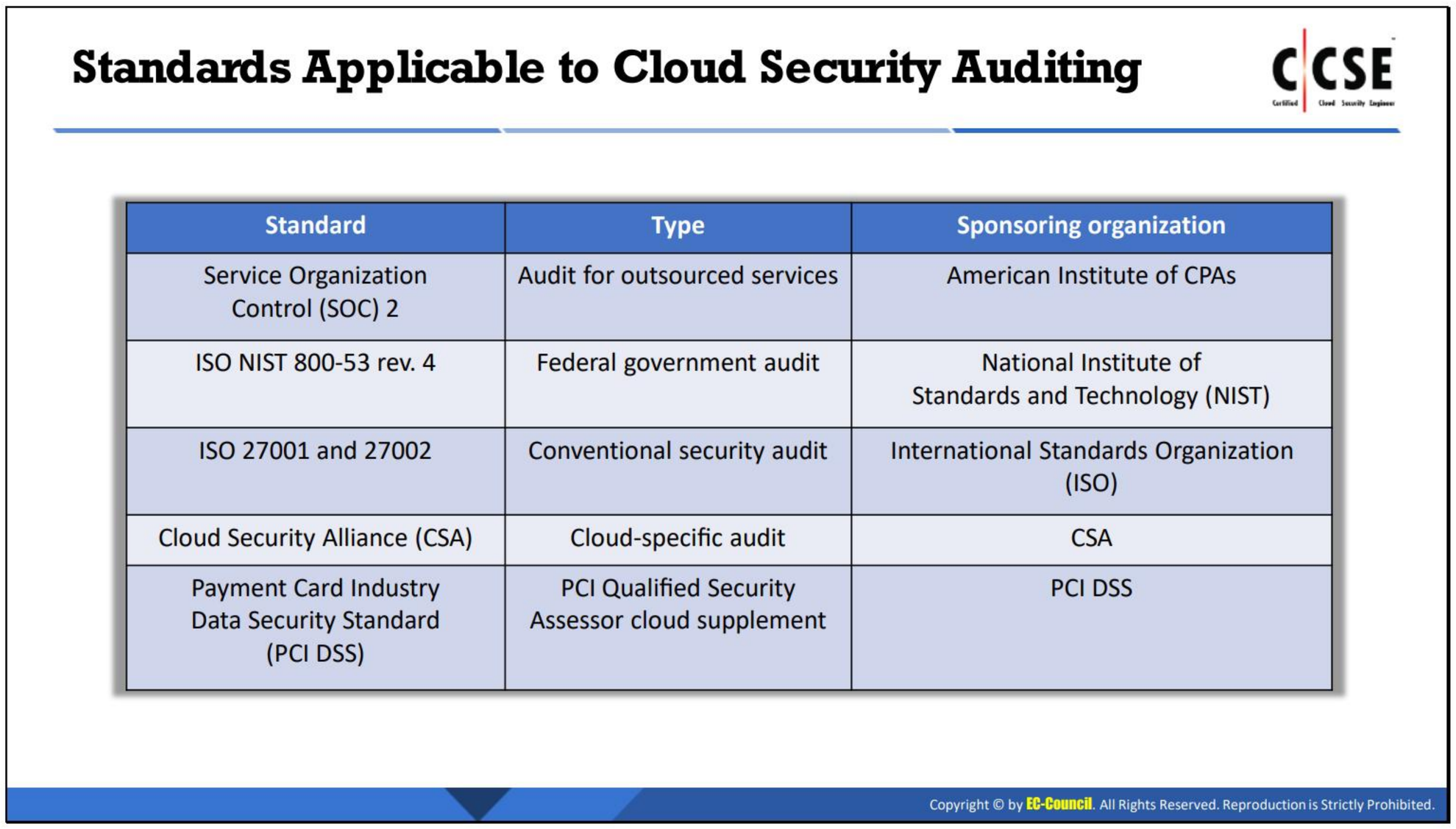
- **Sample Selection and Audit Trails**

  Sample selection and audit trails play a crucial role for auditing a cloud environment. Auditors must attain a clear understanding of the following.

  - What will be the universal population from which a sample will be selected?
  - In a highly dynamic environment, what will be the sample selection method?
  - When no audit trail is provided by the CSP, how will historical data be tested?

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Standards Applicable to Cloud Security Auditing

The following are the standards applicable to cloud security auditing.

Service Organization Control (SOC) 2

cside01.ir

SOC 2 is a standard developed by the American Institute of Certified Public Accountants (CPAs). It defines the criteria for managing customer data as per five trust-service principles: privacy, security, availability, confidentiality, and processing integrity. The audit information of SOC 2 is used by internal management and regulators. SOC 2 is mainly used to audit governance, risk management, and compliance (GRC) programs. The criteria for evaluating and reporting on issues related to the five trust-service principles can be defined as follows.

- **Security**: The system is secured from (logical and physical) unauthorized access.
- **Availability**: The system is available for use or operation as agreed.
- **Privacy**: Personal information is gathered, utilized, stored, and destroyed in accordance with the commitments in the privacy notice of the entity and with the criteria of Generally Accepted Accounting Principles (GAAP).
- **Confidentiality**: Confidential information is protected as agreed.
- **Processing integrity**: System processing is timely, accurate, complete, and authorized.

SOC 2 applies when an entity outsources the collection, transmission, processing, organization, storage, and disposal of the entity's information. A SOC 2 report should be obtained by the following:

- CSPs
- Fintech companies

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Intellectual property protection
- Salesforce automation
- Healthcare providers and payers
- Service providers hosting data center

ISO 27001 and 27002

ISO 27001 and 27002 are standards developed by ISO. ISO 27001 is used when the foundations of information security have to be built and a framework is to be created in an organization. ISO 27002 is used for implementing controls. ISO 27001 and 27002 are used as the most commonly used IT security auditing standards. These standards apply to both conventional IT and cloud environments.

NIST SP800-53 rev 4

NIST SP800-53 rev 4 is a standard developed by NIST that offers a catalog of privacy and security controls for US federal information systems. The procedures offered by this standard are used for assessing security and privacy controls in federal information systems. This standard is technology-neutral and is applicable to both conventional IT and cloud environments. Its procedures can be customized and easily tailored to offer organizations the required flexibility to perform privacy control assessments and security control assessments. These assessments support the risk management processes of the organizations and are aligned with the organizations' committed risk tolerance.

hide01.ir

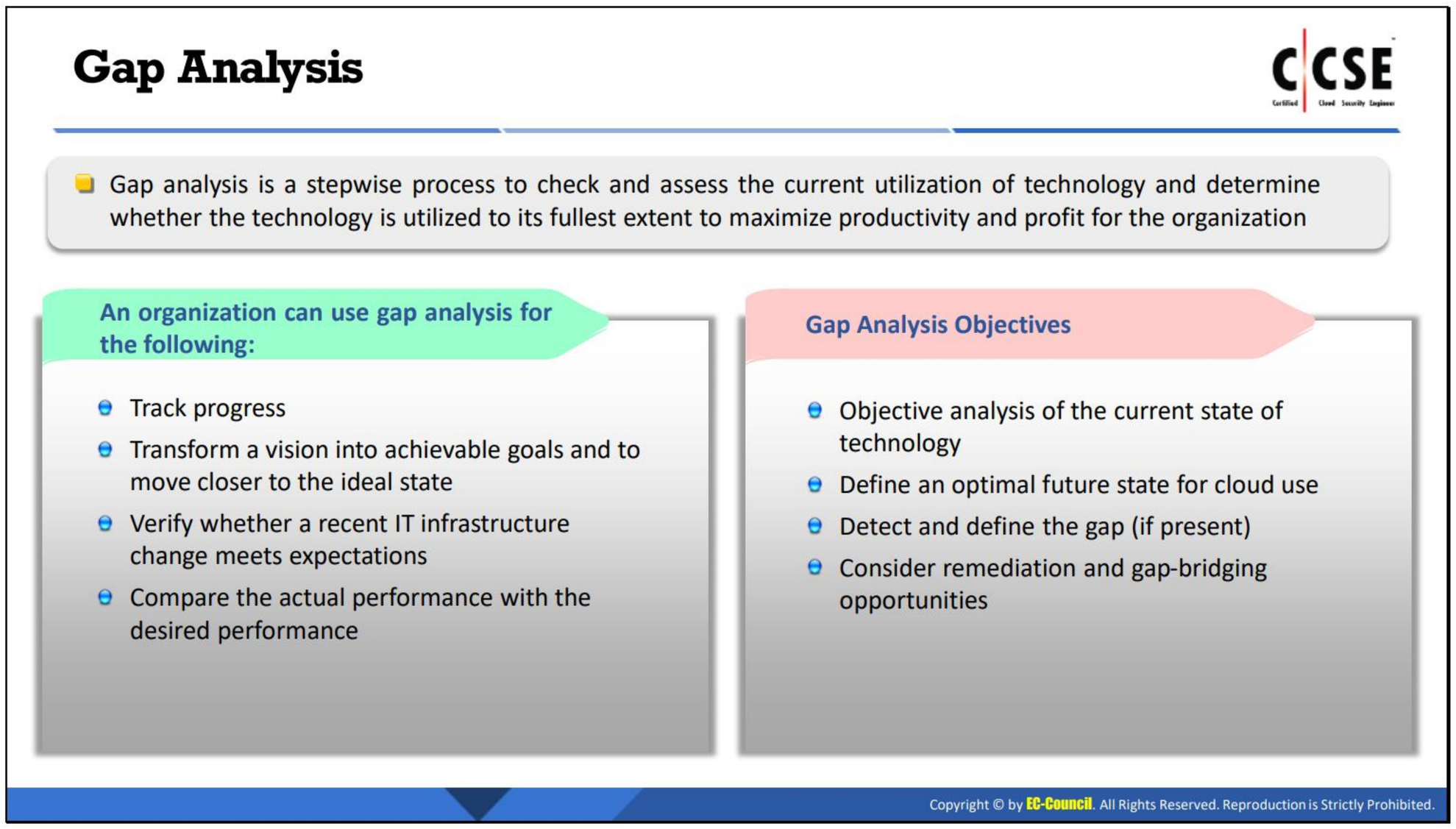
Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) develops cloud-security auditing standards. The CSA Cloud Control Matrix (CCM) is a standard designed specifically for cloud environments to provide basic security principles to guide CSPs and to help prospective cloud consumers in evaluating the overall security risk of a CSP. It is the only meta-framework of cloud-specific security controls mapped to leading standards, regulations, and best practices. It offers organizations the required structure, clarity, and detail related to information security in cloud environments. Currently, this standard is considered the de-facto standard in cloud environments for cloud security assurance and compliance.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a standard applicable to cloud providers and SaaS vendors that store or process cardholder data (e.g., credit card and payments-related data) in cloud environments. This standard ensures that the organization's credit card processing system is secure and the transactions are protected from the beginning to the end. The effectiveness of the cloud information security controls is evaluated during a PCI audit by a qualified security assessor (QSA). The PCI DSS Cloud Special Interest Group (SIG) offers some recommendations for multitenancy to address security concerns related to colocation. It has a QSA cloud supplement that guides cloud auditors that handle PCI DSS certifications in cloud environments.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gap Analysis

Gap analysis is a stepwise process to check and assess the current utilization of technology and determine whether the technology is utilized to its fullest extent to maximize productivity and profit for the organization. With the adoption of cloud-based technologies, organizations need to conduct a gap analysis to optimize their productivity and profit levels. A gap analysis bridges the gap between current technology use and optimal technology use to increase productivity and profits.

The gap in a gap analysis simply shows the distance between the current and desired states. Gap analysis helps organizations establish a baseline to determine how they have improved over time.

Benefits of Gap Analysis

A gap analysis offers the following benefits.

- Businesses can track their progress via a gap analysis.
- Organizations can use a gap analysis to transform their vision into achievable goals and move closer to their ideal state.
- A technology gap analysis can help organizations verify whether a recent IT infrastructure change meets expectations.
- It helps organizations compare their actual performance with the desired performance.
- It assists enterprises in identifying the best cloud practices, platform capabilities, processes, and niche features that can help them meet their cloud objectives.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Core Principles of Gap Analysis

Although different organizations perform different types of gap analysis depending on the organization's size, industry, and pre-existing IT infrastructure, the following four core principles must be followed by all organizations using cloud-based software to perform a gap analysis.

- **Objective analysis of the current state of technology:** An objective analysis of the present technology status forms the first step for an effective gap analysis for cloud technologies.

  Consider the following steps to perform an analysis:

  - Examine the latest balance sheet, profit/loss statements, and other financial documents.
  - Compare the current numbers to those of the months before cloud implementation.
  - Assess the organization's use of cloud technology to improve productivity and profitability after considering changes impacting revenue such as a seasonal customer decline.
  - Check whether employees use the cloud to accomplish their work.

- **Define an optimal future state for cloud use:** Identifying and defining an optimal future state of cloud use (or correct state for cloud use) is the second step for an effective gap analysis. This step helps identify future cloud goals and how to realize them.

  A correct state for cloud use commonly involves the following.

  - **Saves money spent on storage space**: Using the cloud assuredly saves money in the future, which otherwise would have been spent on on-premises storage.
  - **Reduces operational costs**: The cloud requires less bandwidth and energy to operate then on-premises infrastructure, reducing the overall operational cost. Operational costs can be substantially reduced if all the information of the organization is moved to the cloud because dividing time and functions between other business-conducting methods and the cloud can be expensive to the organization in terms of interoperability, collaboration, and productivity.

- **Detect and define the gap (if present):** To detect, define, and close the performance gap with the cloud, an organization should observe the activities of other organizations in similar industries to effectively use the cloud. The performance gap mainly arises from interoperability failures between the cloud and existing technologies/servers.

  An example is tracking whether all employees are using the cloud services the organization has implemented. One of the common causes of performance gaps is employees who use outdated working methods, despite their organization's cloud adoption. This brings difficulty in file sharing within teams and adds confusion to file storage methods.

  Organizations should ensure that employees have access to the technology they have implemented. When employees are not trained in the use of cloud services, they tend to

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

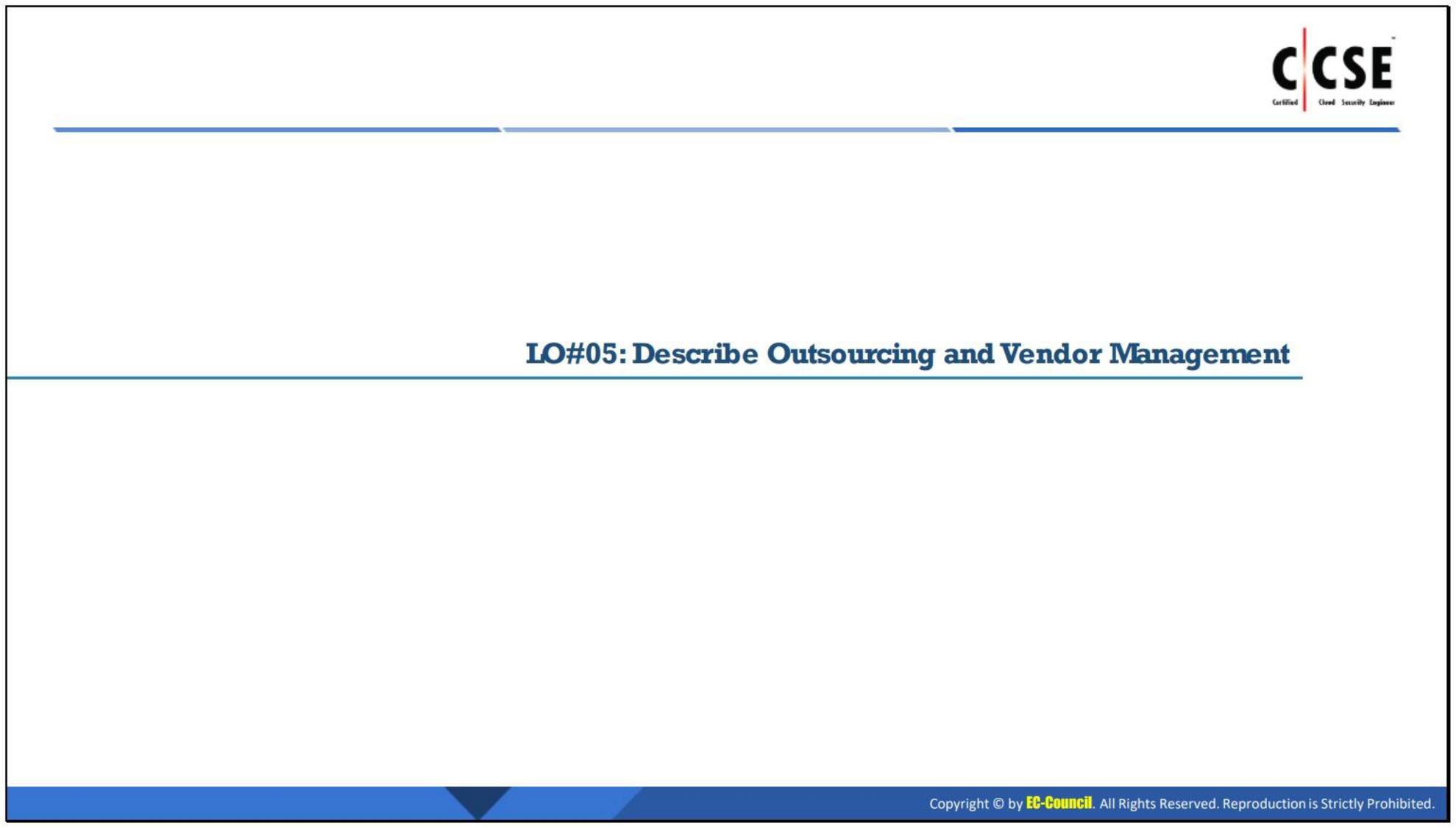
fail in understanding the importance of technology and the functions provided by it. This gap can be filled by conducting quarterly training to educate them on cloud technologies and services. Employees should also be made aware that the use of cloud services is secure because some people tend to avoid using cloud services owing to a misconception that it is insecure.

- **Consider remediation and gap-bridging opportunities:** This step involves careful planning as it attempts to fix the identified gap. An enterprise-wide plan should be implemented to eliminate profit and performance gaps in cloud-based software. This can be achieved by creating a plan that helps in eliminating the gaps. This plan must include the following:
    - Identifying a solution to the gap
    - Finding an actionable roadmap to close the gap

If organizations perform a gap analysis using these four core principles, they can realize the full potential of cloud technology. Moreover, they can achieve greater mobility, scalability, better collaboration, easier access to files/documents, low-cost data and information storage, and reduced operating costs.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

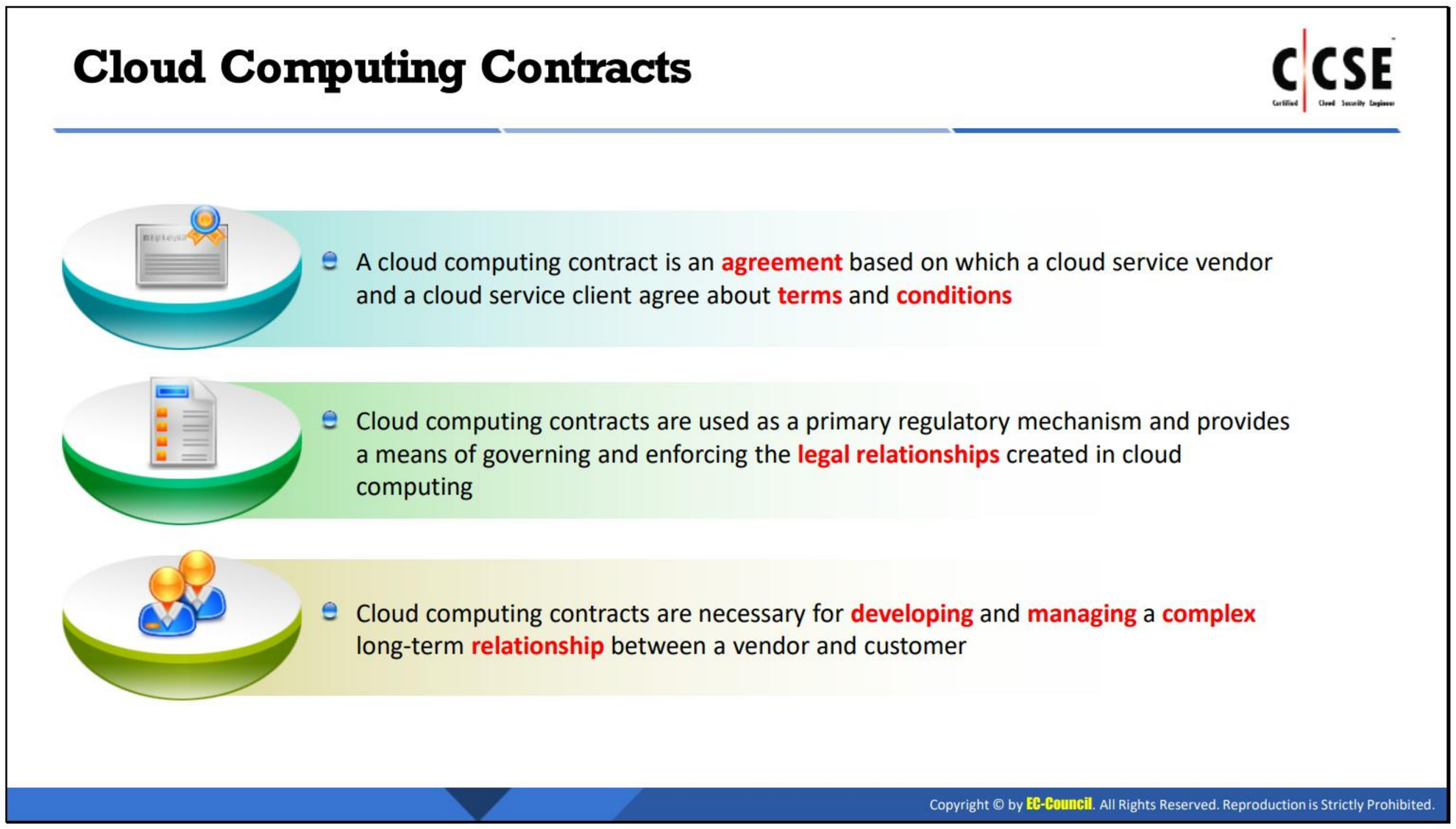


LO#05: Describe Outsourcing and Vendor Management

As cloud environments often store sensitive information on cloud customers, it is important to consider various factors before signing a cloud computing contract. The objective of this section is to provide pertinent information related to cloud computing contracts, questions to ask before signing a cloud computing contract, various issues with subcontracts, non-negotiable contracts, and the best practices for cloud computing contracts. This section also explains contract requirements for cloud security, SLA, and how customers can change their vendors when dissatisfied with the services. This section aims to increase awareness among cloud users regarding cloud computing contracts and help prevent legal, compliance, or security issues with cloud service providers.

hid01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Computing Contracts

In a cloud computing contract, the cloud service provider (CSP) and cloud service customer mutually agree to the operational terms and conditions. Cloud computing contracts are used as a primary regulatory mechanism and provides a means of governing and enforcing the legal relationship created in cloud computing. Cloud computing contracts are necessary for developing and managing a complex long-term relationship between a vendor and customer. Contracts differ in contractual terms, which are drafted according to the requirements of the CSP and cloud consumer. Cloud computing contracts should clearly state that the client will have complete authority over the data stored in the cloud environment, and during the closure of the contract, the provider should hand over all the data to the client and destroy all copies of the data stored in the cloud environment.

General Terms Used in Cloud Contracts

A cloud computing contract addresses many issues between a CSP and cloud consumer in cloud operations, including the following:

- Acceptable use policy
- Auditing rights
- Changes to the terms
- Confidentiality
- Cloud infrastructure
- Compensation
- Compliance with laws

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Data confidentiality
- Data privacy
- Data security
- Data retention schedules
- Data storage and restrictions
- Dispute resolution
- Emergency security issues
- Freedom to move
- Governing law and jurisdiction
- Indemnity
- Intellectual property rights (IPR)
- Law enforcement and loss of control
- Legal compliance
- Licensing
- Location of data
- Law and jurisdiction
- Monitoring by the cloud provider
- Modifications to the contract
- Ownership of data
- Publicity
- Renewal
- Service-level agreements (SLAs)
- Subcontracting
- Suspension of end-user accounts
- Suspension and termination of the service
- Unauthorized or inappropriate use
- Warranties

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Questions to Ask Before Signing a Cloud Computing Contract

Cloud customers should have a detailed overview about the following concerns before entering into a contract with a CSP.

hade01.ir

- Liability of the CSP for damages to and interruptions in services
- Fulfilment of service-level agreements (SLAs) as mentioned in the contract
- Data availability for the cloud customers
- Physical location of the stored data
- Avoiding vendor lock-in and exit if required
- Maintaining data for legal compliance
- Consequences after the contracts are terminated
- Maintaining intellectual property rights (IPR)
- Consequences, rules, and regulations concerning service termination

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Non-Negotiable Contracts

A clickwrap is a non-negotiable user contract presented as an on-screen license agreement accepted by clicking the acceptance button in the agreement window. The end-user license agreement is part of the initial screens of a typical installation process, which continues only after the user clicks the "I Agree" or "I Accept" button. If this step is not completed or performed, then the installation process is canceled.

- Medium and small CSPs offer services through non-negotiable clickwrap contracts.
- Customers simply need to click the "I agree" button to accept terms and receive services.
- Clickwrap contracts are often vendor-friendly and limit the provider's liability.
- Select such vendors only through proper inquiry with other customers and a full review of the agreement terms.
- Some clickwrap service agreements are negotiable as per customization requirements with higher service fees.

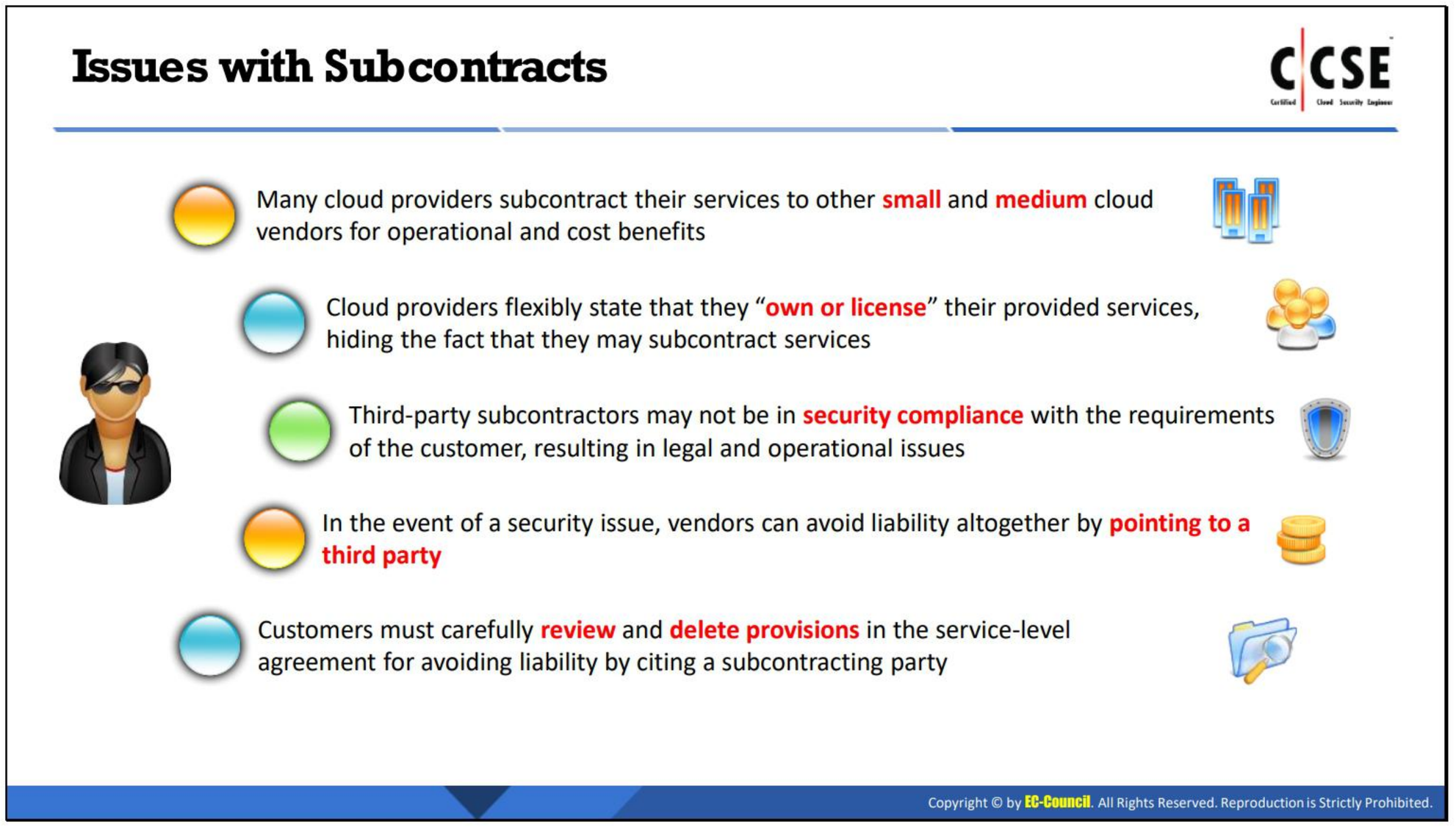
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 11.6: Clickwrap Agreement

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

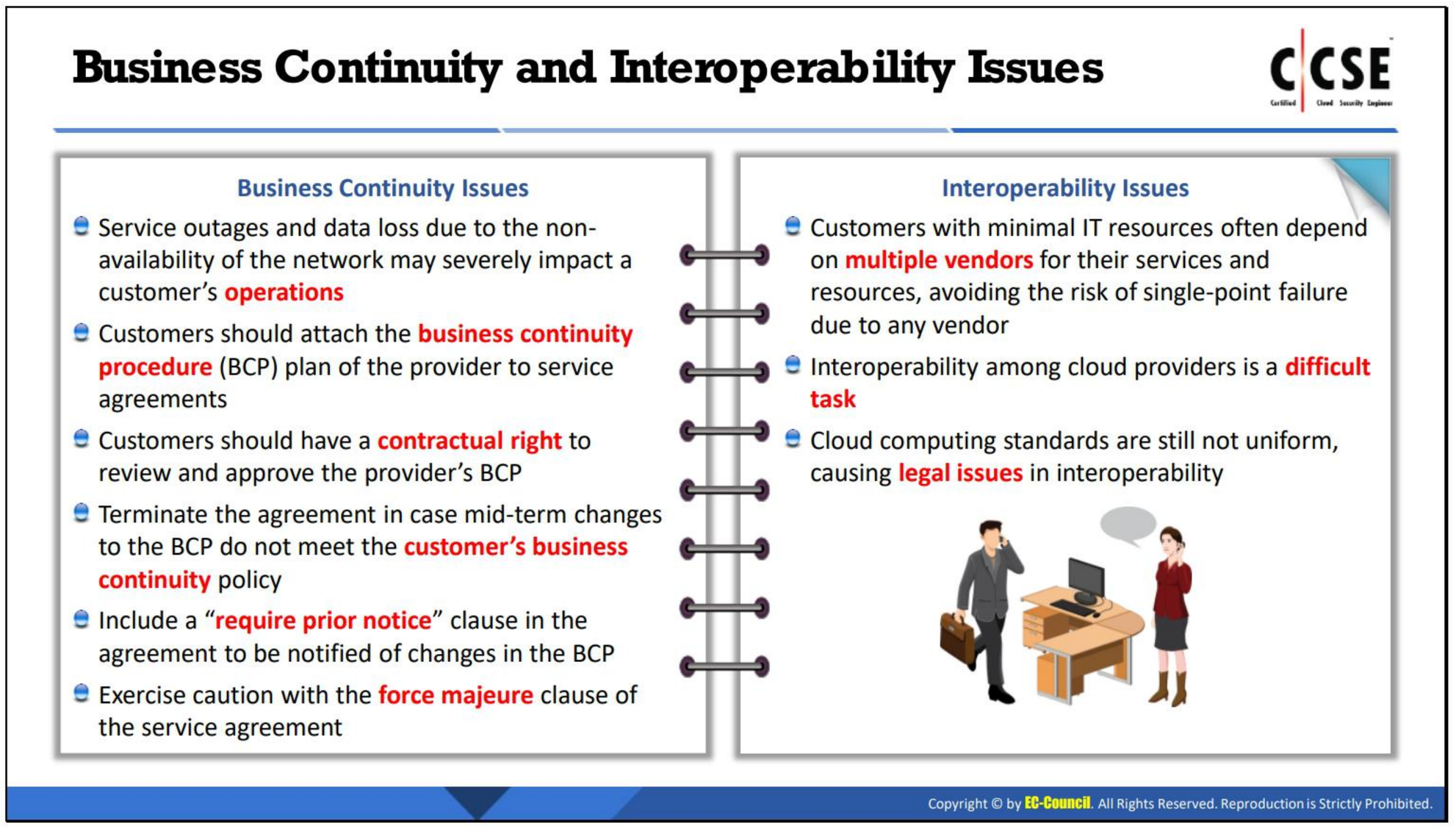


Issues with Subcontracts

A CSP may subcontract parts of the services to a third-party provider, which may be unknown to the client. If some cloud services are outsourced by the CSP, the customer should ensure that third-party service providers fall within the purview of the initial contract. The following are some of the issues associated with subcontracts.

- Many CSP subcontract their services to other small and medium cloud vendors for operational and cost benefits.
- CSPs flexibly state that they "own or license" the provided services, hiding the fact that they may subcontract services.
- Third-party subcontractors may not be in security compliance with the requirements of the customer, resulting in legal and operational issues.
- In case of a security event, the vendor can avoid liability altogether by pointing towards the third-party provider.
- Customers must carefully review and delete provisions in the service agreement for avoiding liability by citing a subcontracting party.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Business Continuity and Interoperability Issues

Business Continuity Issues

Operational issues in cloud services can hamper business continuity and bring an organization to the verge of legal conflicts with the service provider. Awareness and implementation of customer-friendly clauses can prevent forthcoming business continuity issues. The following are the points to consider in agreements regarding business continuity.

- Exercise caution with the force majeure clause of the service agreement.
- Include a "require prior notice" clause in the agreement to be informed of changes in the business continuity procedure (BCP).
- Terminate the agreement in case BCP mid-term changes do not meet the customer's business continuity policy.
- The customer should have a contractual right to review and approve the provider's BCP.
- Service outages and data loss due to the non-availability of the network may severely impact a customer's operations.
- Customers should attach the provider's BCP plan to service agreements.

Example Clause: Business Continuity Issues

Source: *http://www.rackspace.com*

FORCE MAJEURE. Neither of us will be in violation of the Agreement if the failure to perform the obligation is due to an event beyond our control, such as significant failure of a part of the power grid, significant failure of the Internet, natural disaster, war, riot, insurrection, epidemic, strikes

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

or other organized labor action, terrorism, or other events of a magnitude or type for which precautions are not generally taken in the industry.

Interoperability Issues

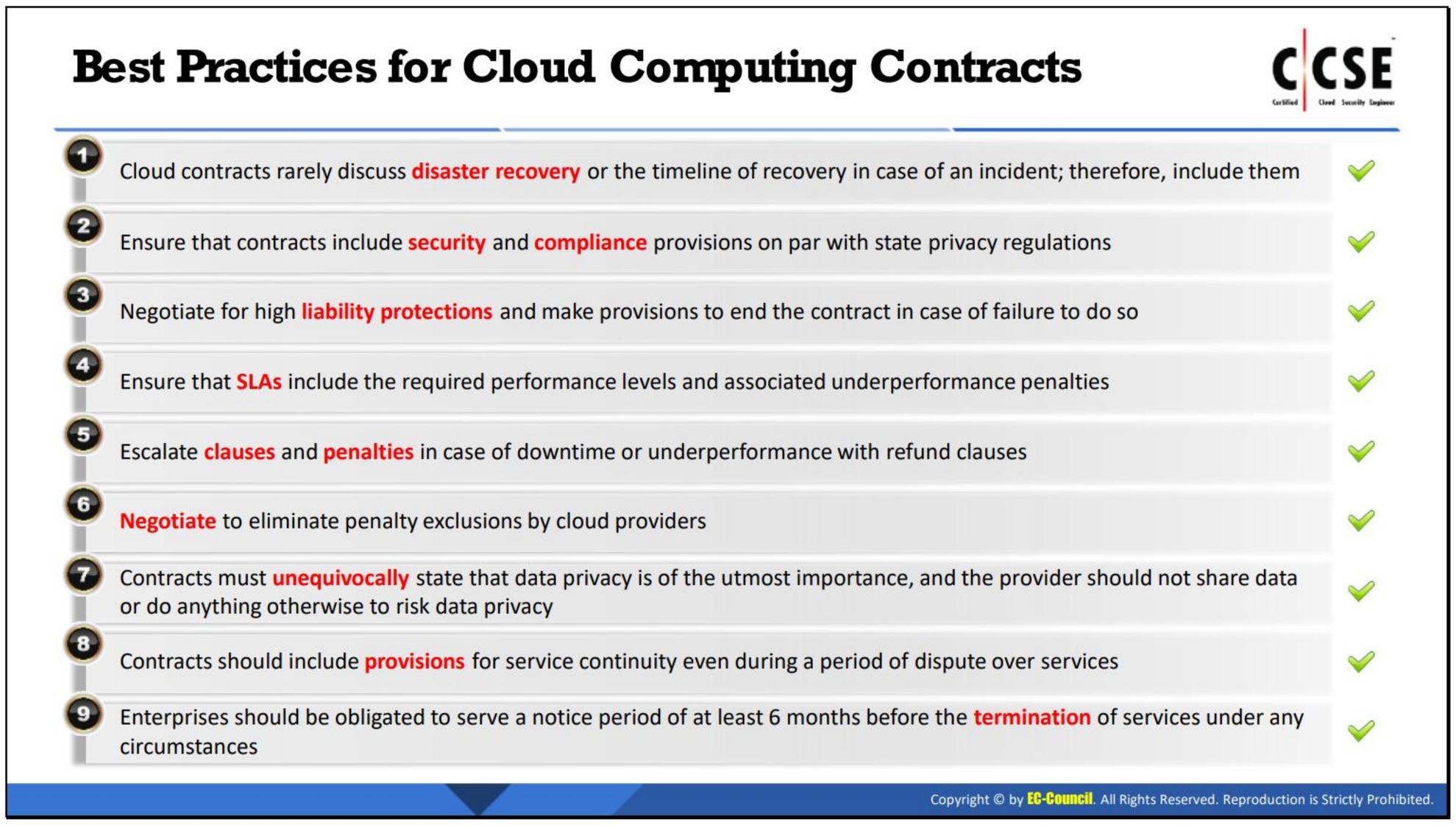
Interoperability between clouds and the portability of applications from one cloud to another are important requirements in cloud computing services. Customers should have the freedom to switch over from one service provider to another as per their needs and business requirements. Cloud customers should ensure that cloud contracts do not push them into legal obstacles while going through such a process.

Interoperability issues include the following.

- Customers with minimal IT resources often depend on multiple vendors for their services and resources, avoiding the risk of single-point failure due to any vendor.
- Interoperability among cloud providers is a difficult task.
- Cloud computing standards are still not uniform, causing legal issues in interoperability.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



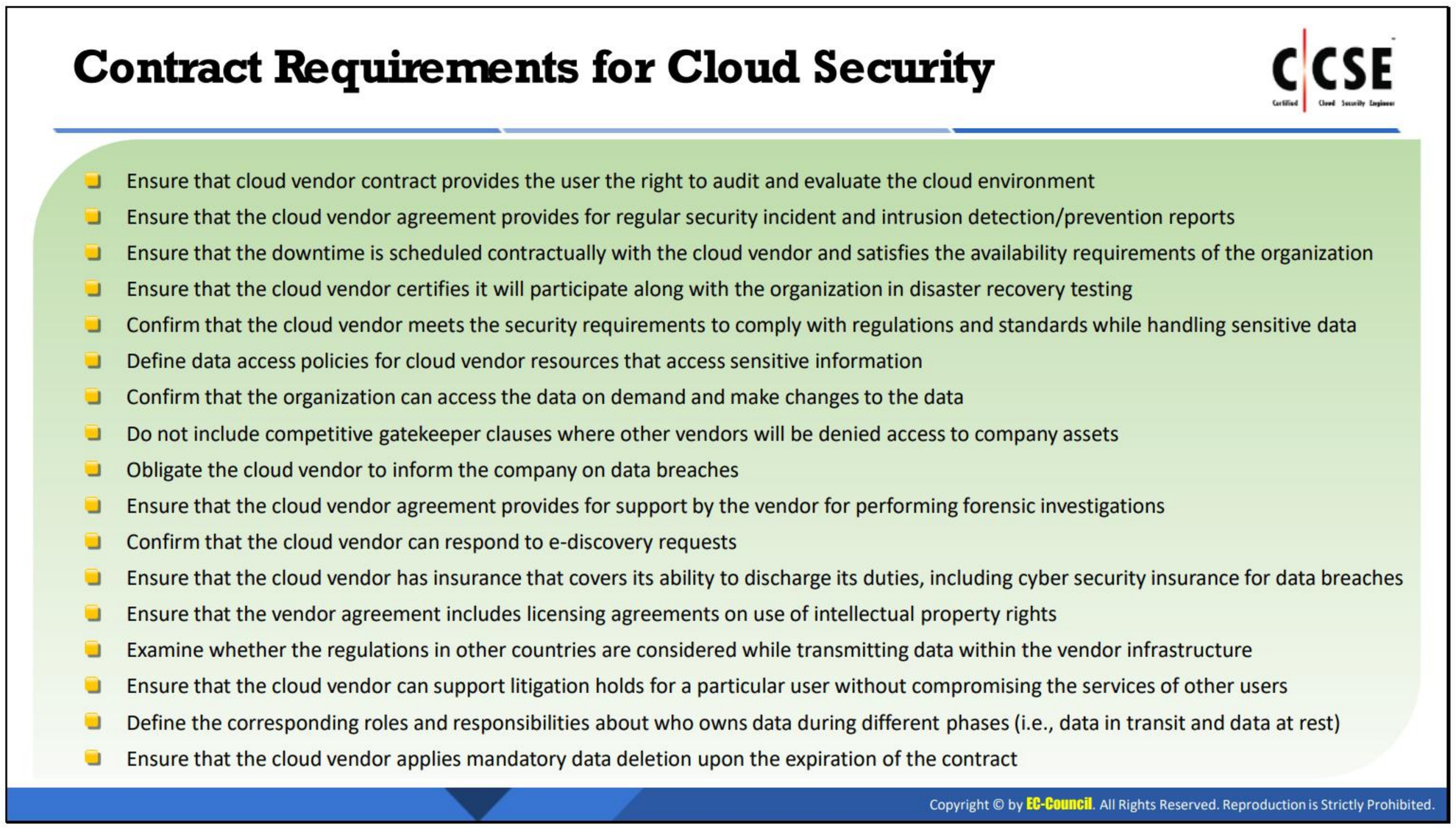
Best Practices for Cloud Computing Contracts

Cloud computing contracts should be drafted in accordance with mutual trust, understandability, and clarity in contract clauses between a CSP and cloud clients.

The following are some guidelines for drafting effective cloud computing contracts.

- Cloud contracts rarely discuss disaster recovery (DR) or the timeline of recovery in case of an incident; therefore, include them.
- Ensure that contracts include security and compliance provisions on par with state privacy regulations.
- Negotiate for high liability protections and make provisions to end the contract in case of failure to do so.
- Ensure that SLAs include the required performance levels and associated underperformance penalties.
- Escalate clauses and penalties in case of downtime or underperformance with refund clauses.
- Negotiate to eliminate penalty exclusions for cloud providers.
- Contracts must unequivocally state that data privacy is of utmost importance, and the provider should not share data or do anything otherwise to risk data privacy.
- Contracts should include provisions for service continuity even during a period of dispute over services.
- Enterprises should be obligated to serve a notice period of at least six months before the termination of services under any circumstances.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Contract Requirements for Cloud Security

The following are the security requirements to be considered by an organization while entering into a contract with a cloud vendor.

hade01.ir

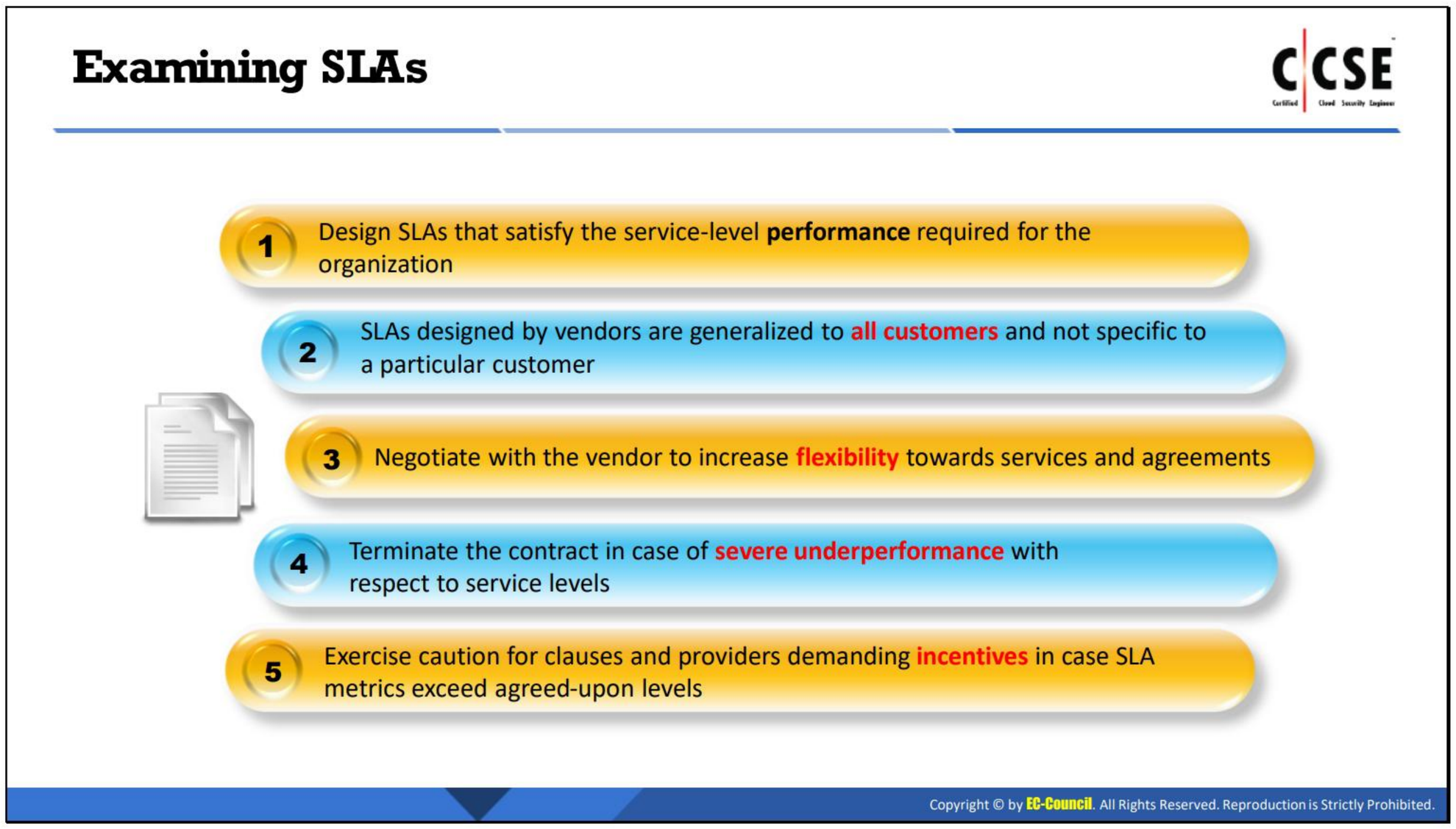
- Ensure that the cloud vendor contract provides the user the right to audit and evaluate the cloud environment.
- Ensure that the cloud vendor agreement provides for regular security incident and intrusion detection/prevention reports.
- Ensure that the downtime is scheduled contractually with the cloud vendor and satisfies the organization's availability requirements.
- Include provisions for terminating the entire agreement if the uptime fails over a particular time period.
- Ensure that the cloud vendor certifies it will participate along with the organization in disaster recovery (DR) testing.
- Confirm that the cloud vendor meets the security requirements to comply with regulations and standards while handling sensitive data.
- Define data access policies for cloud vendor resources that access sensitive information.
- Restrict the cloud vendor from sharing sensitive data with unauthorized parties.
- Confirm that the organization can access the data on demand and make changes to the data.
- Obfuscate the symbols, code, and data of software to make it impossible to reverse engineer it without compromising on the application's performance.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not include competitive gatekeeper clauses where other vendors will be denied access to company assets.
- Obligate the cloud vendor to inform the company on data breaches.
- Ensure that the cloud vendor agreement provides for support by the vendor for performing forensic investigations.
- Confirm that the cloud vendor can respond to e-discovery requests.
- Ensure that the cloud vendor has insurance covering its ability to discharge its duties, including cybersecurity insurance for data breaches.
- Ensure that the vendor agreement includes licensing agreements on the use of intellectual property rights (IPR).
- Examine whether the regulations in other countries are considered while transmitting data within the vendor infrastructure.
- Ensure that the cloud vendor can support litigation holds for a particular user without compromising the services of other users.
- Define the corresponding roles and responsibilities about who owns data during different phases (i.e., data in transit and data at rest).
- Ensure that the cloud vendor applies mandatory data deletion upon the expiration of the contract.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining SLAs

Service-level agreements (SLA) are the metrics through which client-expected performance levels are measured at all times by the CSP. Therefore, customers should design SLAs that mandate their required service level performance. SLAs designed by vendors are generalized to all customers but not specific to a particular customer. Negotiate with the vendor to improve flexibility in services and agreements by customizing SLAs. Terminate the contract for severe underperformance in terms of service levels. Exercise caution with regard to clauses and providers demanding incentives if SLA metrics exceed agreed-upon levels.

Example Clause: SLA

Source: *http://www.windowsazure.com*

Service Levels

Monthly Connectivity Uptime Service Level Definitions

- "Maximum Connectivity Minutes" is the total accumulated minutes during a billing month for all Internet-facing roles with two or more instances deployed in different Update Domains. Maximum Connectivity Minutes is measured from when the Tenant has been deployed and its associated roles have been started resultant from action initiated by Customer to the time Customer has initiated an action that would result in stopping or deleting the Tenant.
- "Connectivity Downtime" is the total accumulated minutes that deployed Internet facing roles that have not been stopped by action from Customer have no external connectivity during a five minute period, as measured and aggregated in five-minute intervals.

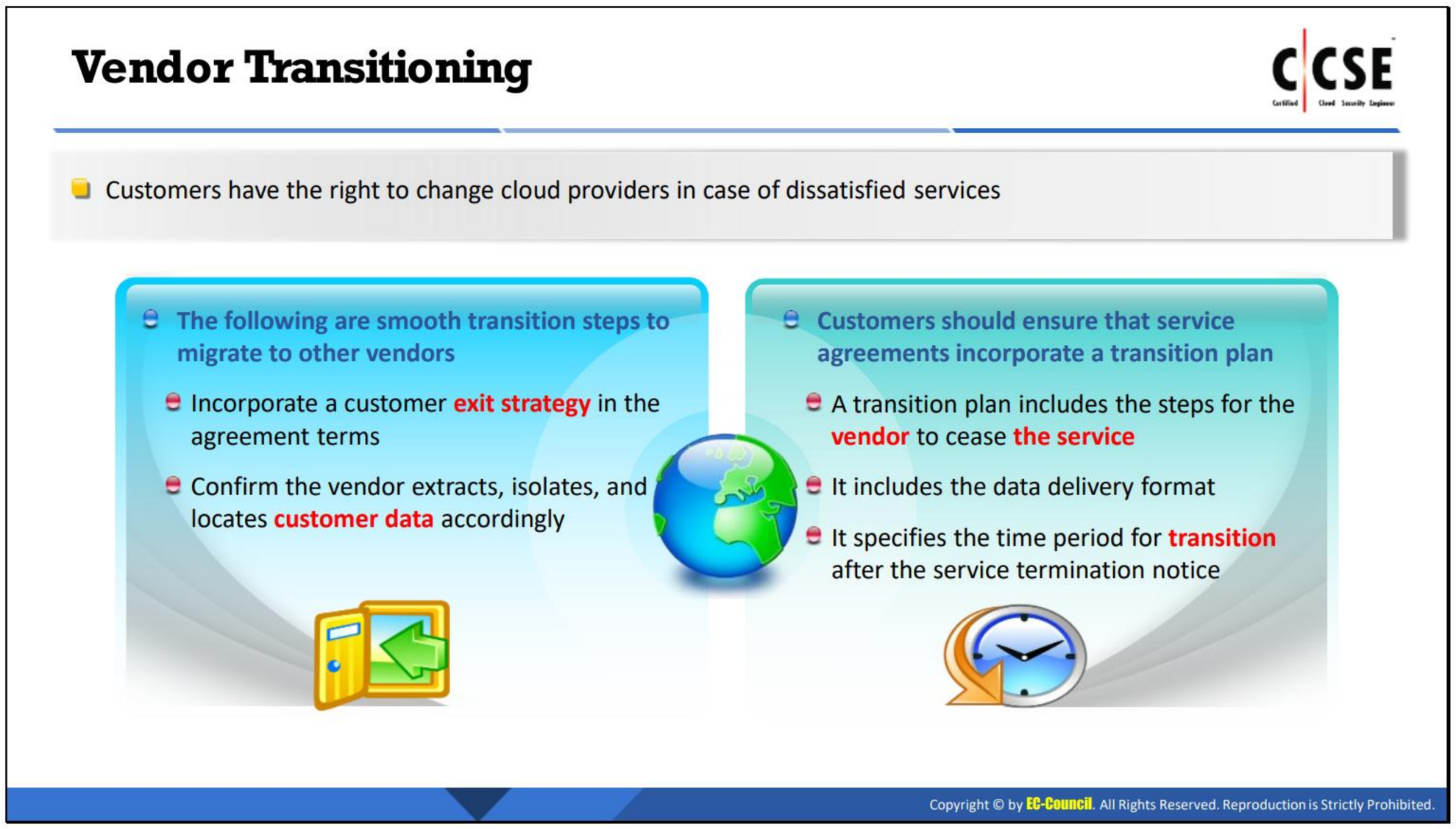
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- "Monthly Connectivity Uptime Percentage" for a specific Customer is the total number of Maximum Connectivity Minutes less Connectivity Downtime divided by Maximum Connectivity Minutes for a billing month for a given subscription of Windows Azure. Monthly Connectivity Uptime Percentage is reflected by the following formula:

  Monthly Connectivity Uptime Percentage = (Maximum Connectivity Minutes – Connectivity Downtime)/(Maximum Connectivity Minutes)

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vendor Transitioning

Cloud customers can switch over to different CSPs based on their current needs. Customers have the right to change CSPs in case of any dissatisfaction with the services. Vendor transitioning can occur in situations where the existing CSP does not meet the requirements specified in the SLA or the CSP is exiting the business.

The following are smooth transition steps to consider when migrating to a different vendor.

- Incorporate a customer exit strategy in the terms of the agreement.
- Ensure that minimal service disruption occurs to the cloud service customer (CSC) while performing the transition.
- Confirm that the CSP incorporates a business continuity strategy while performing the transition.
- Ensure that the CSP wipes the data completely after the exit process is complete.
- Ensure that the CSP leverages standard data formats to perform portability.
- Confirm that the vendor extracts, isolates, and locates customer data accordingly.
- Prioritize the application to be migrated first by determining the return on investment (ROI).

Customers should ensure that service agreements incorporate a transition plan.

- The transition plan includes the strategy steps for the vendor to cease the service.
- It includes the data delivery format.
- It specifies the time period of transition after the service termination notice.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#06: Understand Standards, Policies, and Auditing in AWS

An organization adopting Amazon Web Services (AWS) cloud should be aware of the necessary controls implemented to manage security, regularly audit AWS usage, and meet compliance requirements in the AWS cloud ecosystem. This section explains AWS compliance programs to understand the necessary controls in place, demonstrates how AWS Audit Manager can be used to perform audits in AWS, including security audits with the AWS checklist.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AWS Compliance Program

- The AWS Compliance Program helps organizations understand the necessary controls implemented by AWS for managing security and compliance in the cloud

Area	Standard
Global	Cloud Security Alliance (CSA) controls, PSI DCC Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 3
US Government	CJIS, DoD SRG, FedRAMP, FERPA, FIPS, FISMA, GxP, HIPAA, HITRUST CSF, ITAR, MPAA, NIST, PIPEDA, SEC Rule 17a-4(f), VPAT/Section 508
Asia pacific	FinTech (Japan), FISC (Japan), IRAP (Australia), K-ISMS (Korea), ISMAP (Japan), Medical Information Guidelines (Japan), MTCS Tier 3 (Singapore), NISC (Japan), OSPAR (Singapore)
Europe, Middle East and Africa	HDS (France), C5 (Germany), CISPE (Europe), Cyber Essential Plus (UK), ENS High government standard (Spain), FINMA ISAE 3000 Type 2 report, G-Cloud government standards (UK), TISAX automotive industry standard

Source: https://aws.amazon.com

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

AWS Compliance Program

The AWS Compliance Program helps organizations understand the necessary controls implemented by AWS for managing security and compliance in the cloud. Third-party or independent auditors assess its certificates or attestations. Compliance laws and regulations are compiled and configured by AWS customers to create an IT environment and policy as per their requirement.

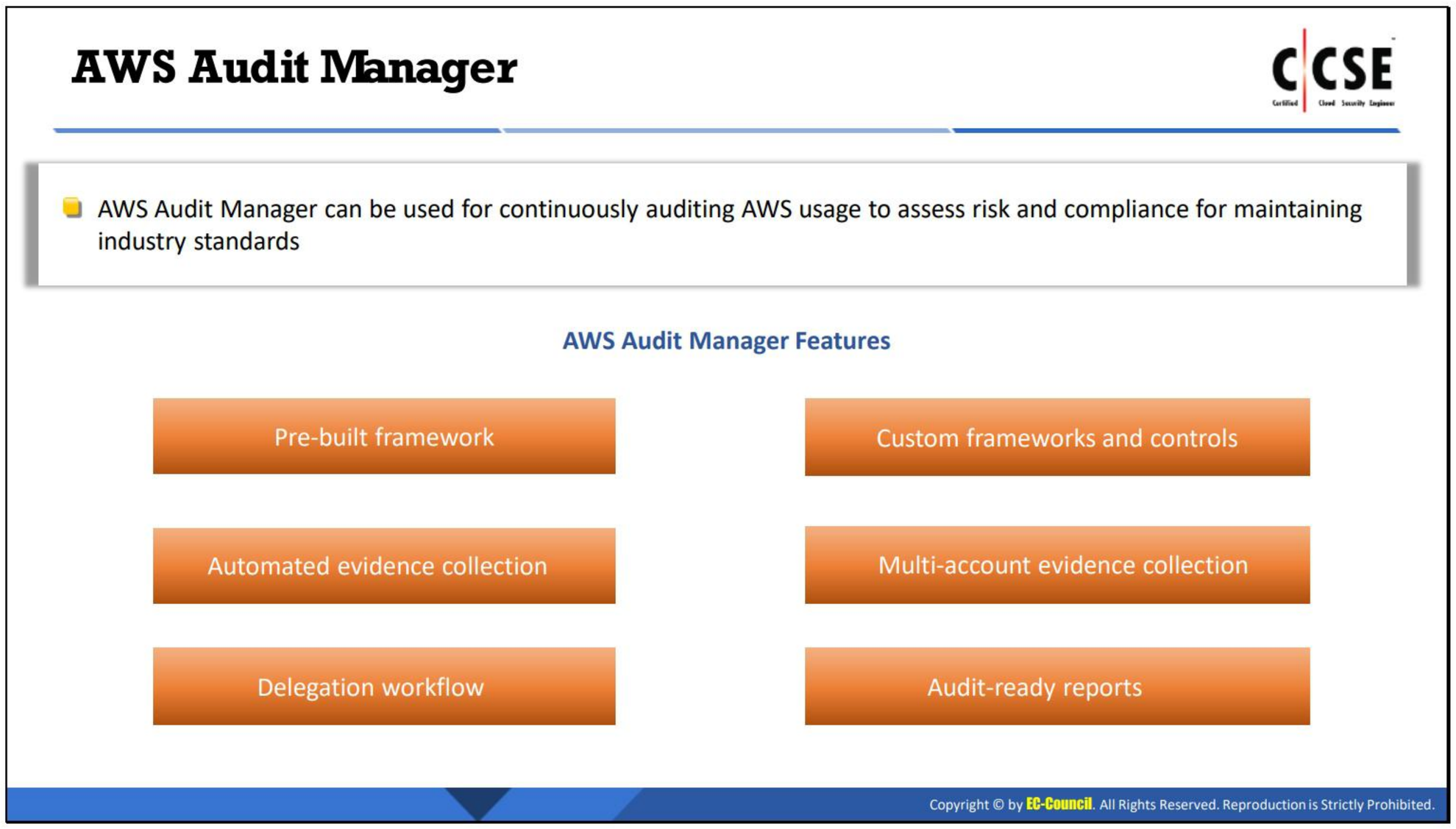
AWS compliance alignments and frameworks comprise compliance requirements for specific purposes, such as a specific industry or function.

***Source**: https://aws.amazon.com/*

Area	Standard
Global	Cloud Security Alliance (CSA) controls, PSI DCC Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 3
America	CJIS, DoD SRG, FedRAMP, FERPA, FIPS, FISMA, GxP, HIPAA, HITRUST CSF, ITAR, MPAA, NIST, PIPEDA, SEC Rule 17a-4(f), VPAT/Section 508
Asia Pacific	FinTech (Japan), FISC (Japan), IRAP (Australia), K-ISMS (Korea), ISMAP (Japan), Medical Information Guidelines (Japan), MTCS Tier 3 (Singapore), NISC (Japan), OSPAR (Singapore)
Europe, Middle East, and Africa	HDS (France), C5 (Germany), CISPE (Europe), Cyber Essential Plus (UK), ENS High government standard (Spain), FINMA ISAE 3000 Type 2 report, G-Cloud government standards (UK), TISAX automotive industry standard

Table 11.2: AWS Compliance Programs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS Audit Manager

AWS Audit Manager can be used for continuously auditing AWS usage to assess risk and compliance for maintaining industry standards. Evidence is collected automatically, enabling the audit to be scaled as per business growth and maintaining control over operations. It manages the stakeholders review and creates audit without many efforts.

Features

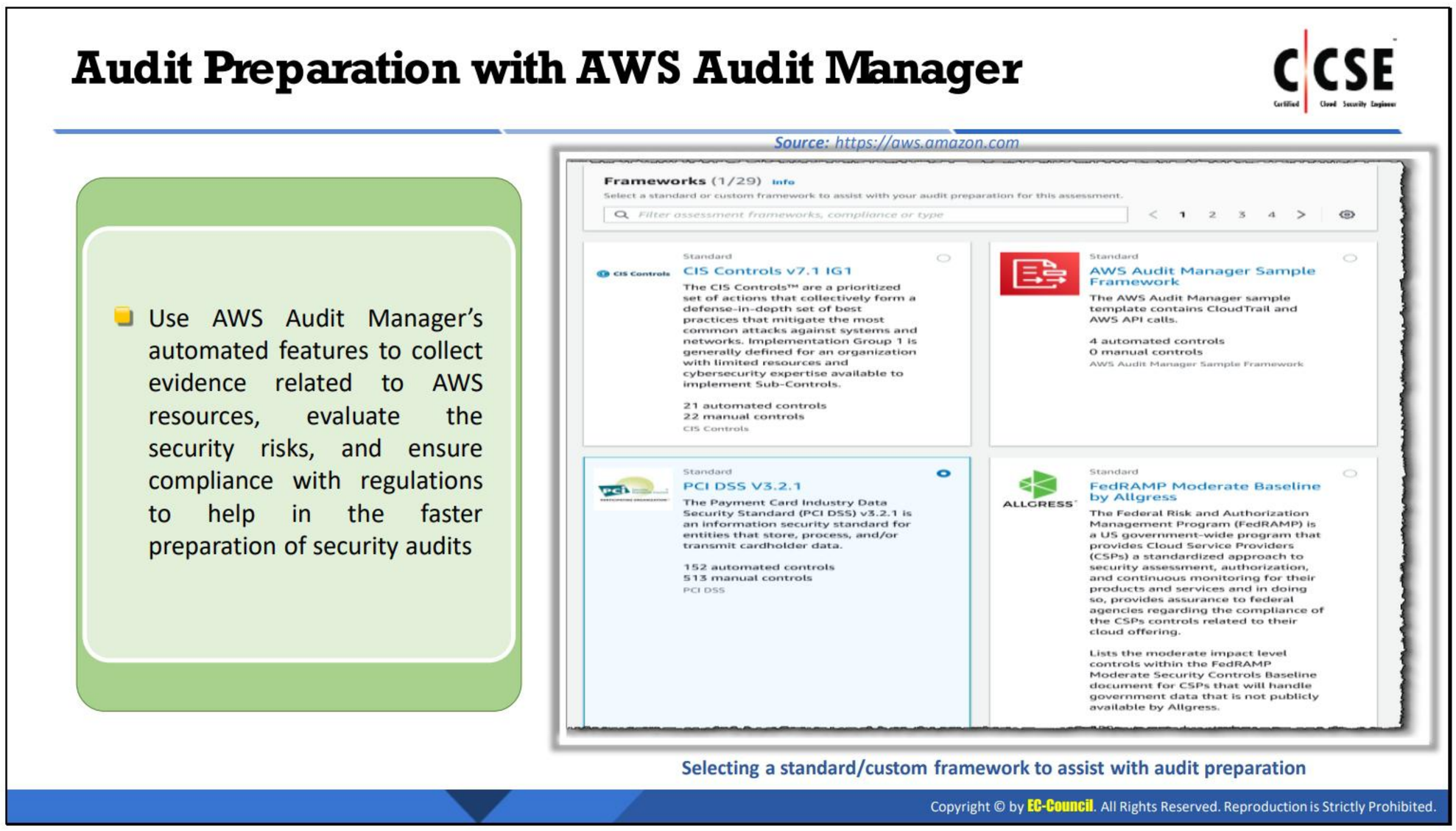
- **Prebuilt framework:** AWS Audit Manager has many pre-built compliance frameworks developed by professionals, which help maintain industry standards and regulatory compliance at a large scale.
- **Custom frameworks and controls:** With custom control and AWS management control, organizations can build their framework according to their business requirements. Custom control helps collect data sources as per the business requirement, which increases control on compliance and auditing.
- **Automated evidence collection:** Once the framework is launched, AWS Audit Manager automatically collects the data and metadata for the scope. These data help in evidence collection for demonstrating compliance with security, change management, business continuity, and software licensing requirements.
- **Multi-account evidence collection:** AWS Audit Manager allows data collection from multiple accounts through integration with AWS organizations.
- **Delegation workflow:** The delegation feature provides access to a support team that specializes in network infrastructure, identity management, software licensing, and personal policies for reviewing evidence and updating the status.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Audit-ready reports:** AWS Audit Manager collects and organizes evidence as per the requirement of the selected framework. You and your team can review, comment, update and upload the evidence and create an auditor assignment.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Audit Preparation with AWS Audit Manager

In the process of meeting the compliance requirements in the cloud, an audit of the infrastructure with conventional practices can cause disruptions and decrease productivity. In AWS, the Audit Manager service has automated features to collect evidence related to AWS resources to evaluate security risks and ensure compliance with regulations, enabling the faster preparation of security audits. Audit Manager has inbuilt features to control the compliance standards of cloud resources, and it converts the gathered evidence into an assessment report, which can be filtered and searched. AWS Audit Manager provides options to add extra evidence into an assessment report, which helps audit teams review and verify the report from a single location.

The following are the steps to prepare audits using AWS Audit Manager.

***Source**: https://aws.amazon.com/*

- Navigate to the home page of AWS Audit Manager in the console.
- Click on **Launch AWS Audit Manager**.
- Click on **Create Assessment**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enter the **Assessment Name**, **Assessment Description** (optional), and **the Amazon S3 bucket** to which the audit reports are to be stored.

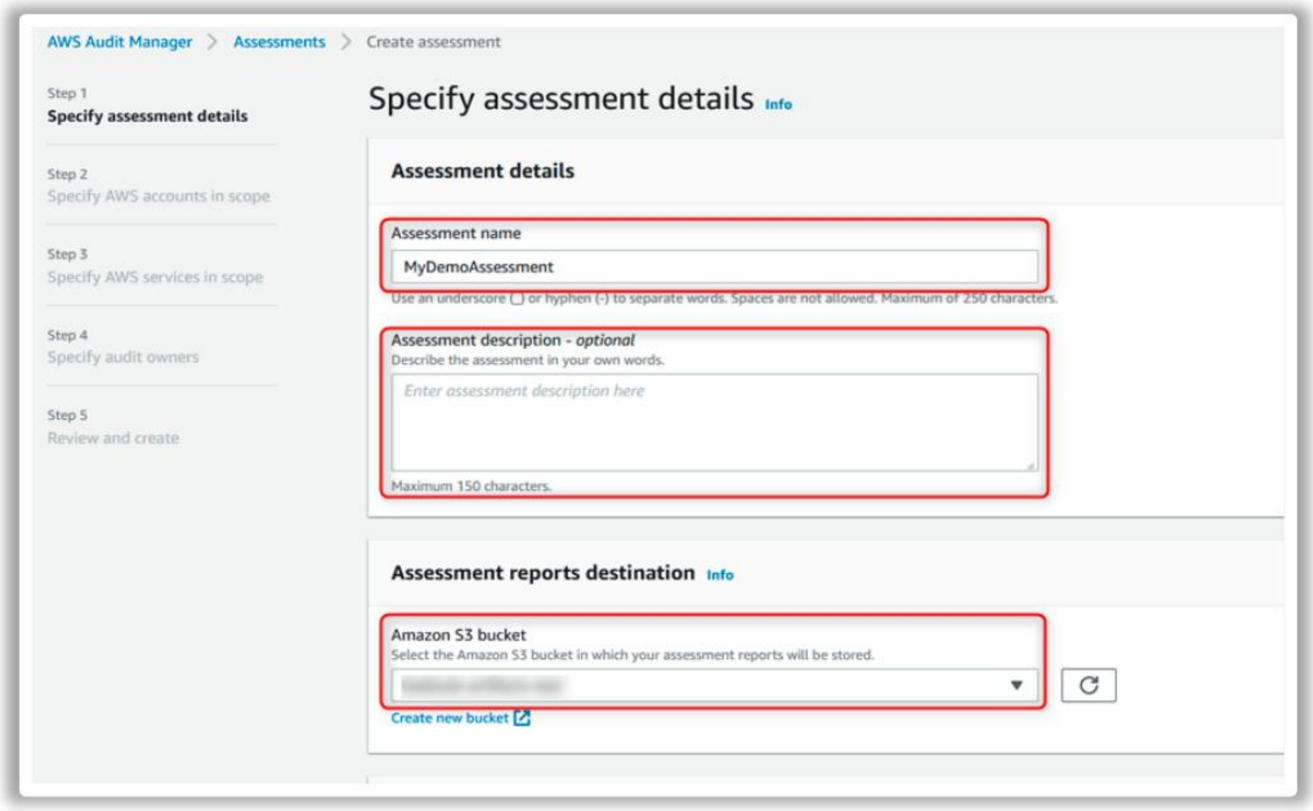


Figure 11.7: AWS Audit Manager

- Select the **Framework** for the assessment.

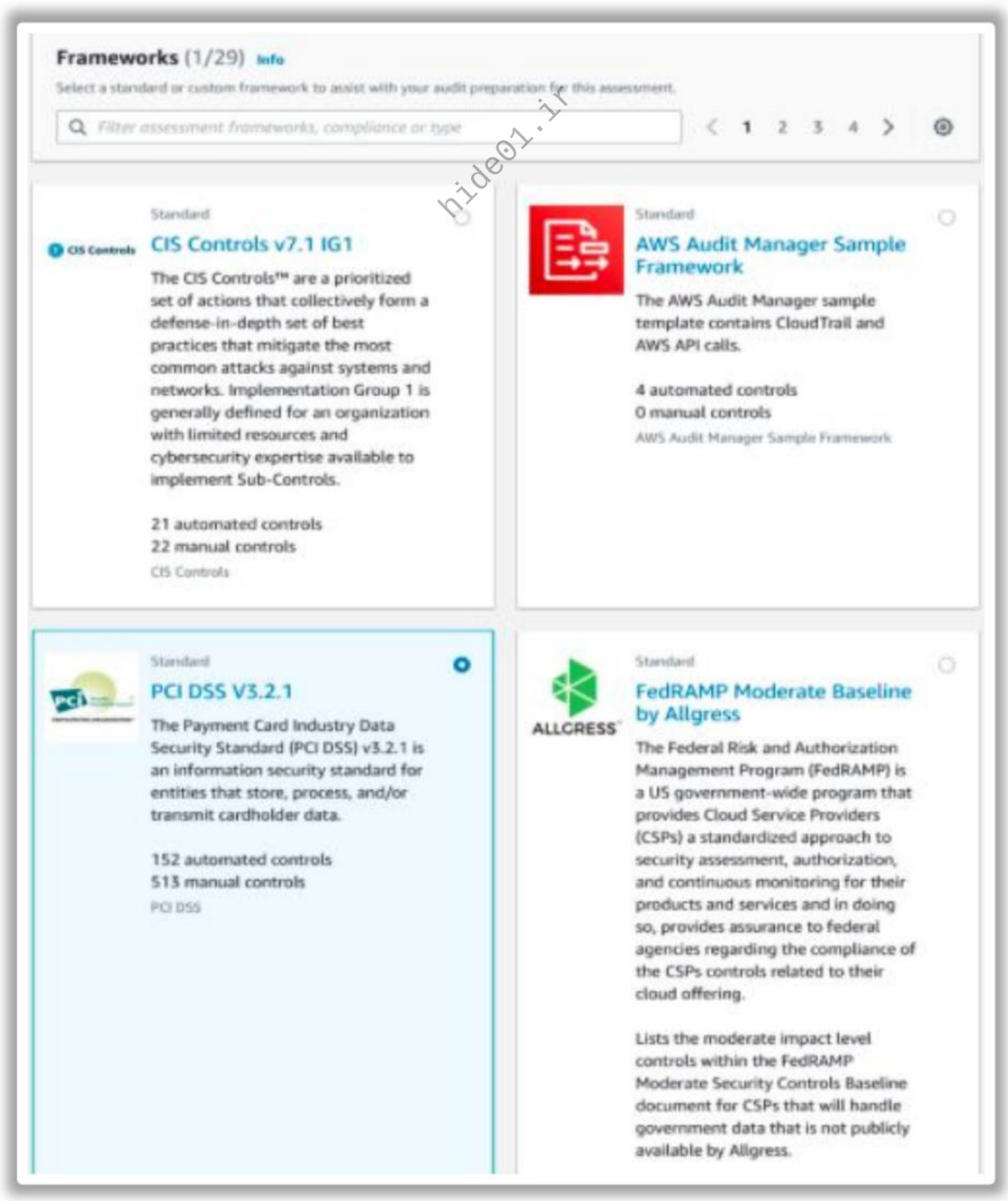


Figure 11.8: Selecting Framework for Assessment

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **Next** and select the AWS accounts to be included in the assessment.
- Click on **Next**, which opens the window to select the AWS services to be included in the collection of evidence.
- Select the services to be included and click on **Next.**

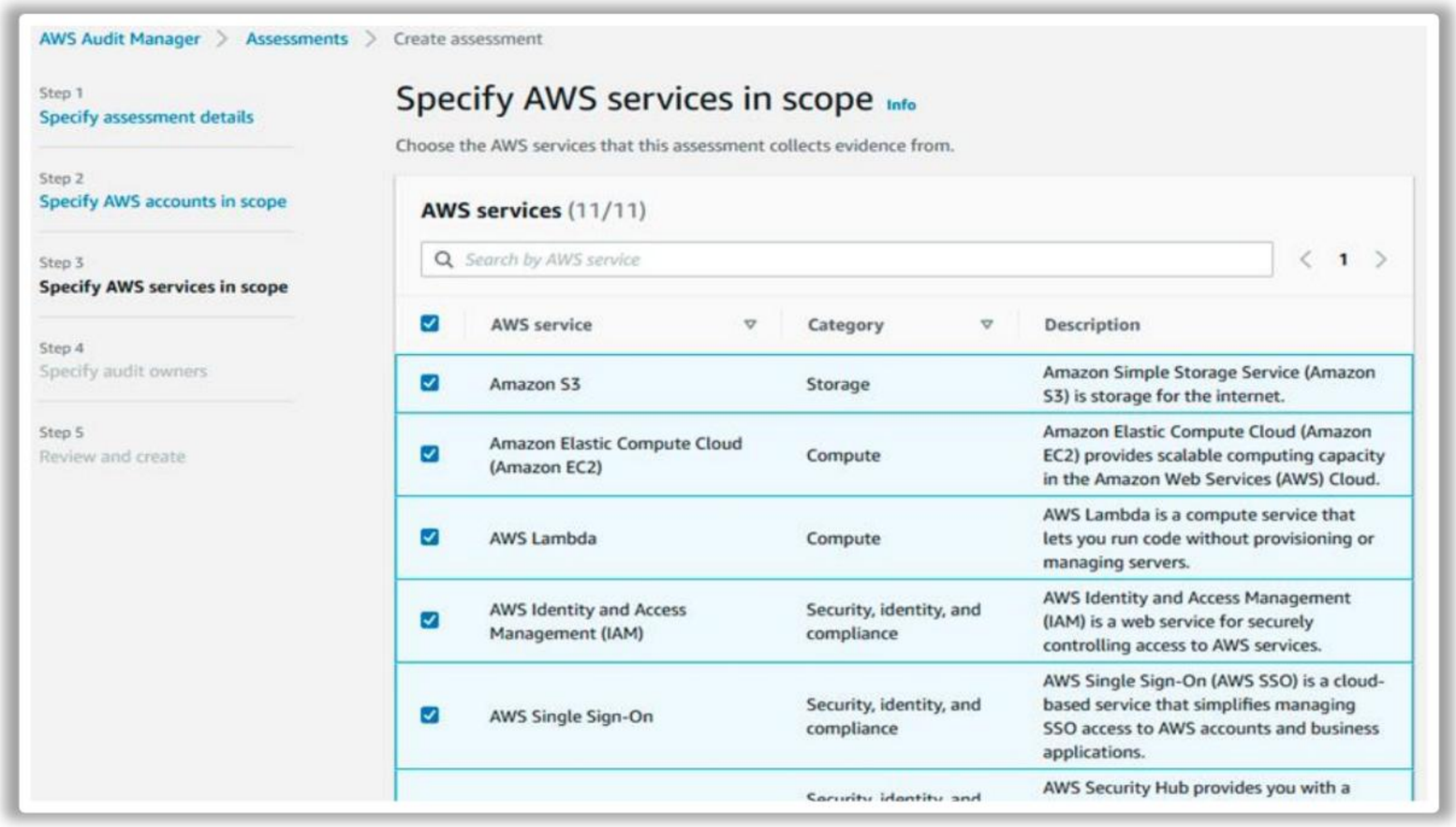


Figure 11.9: AWS Audit Manager

- Select the owners to grant permissions for managing the assessment.
- Click on **Next.**
- In the **Review and Create Page** that appears, click on **Create Assessment.**
- After the assessment is created, navigate to the **Assessments** list and click on the assessment name to view the summary of the evidence collected.

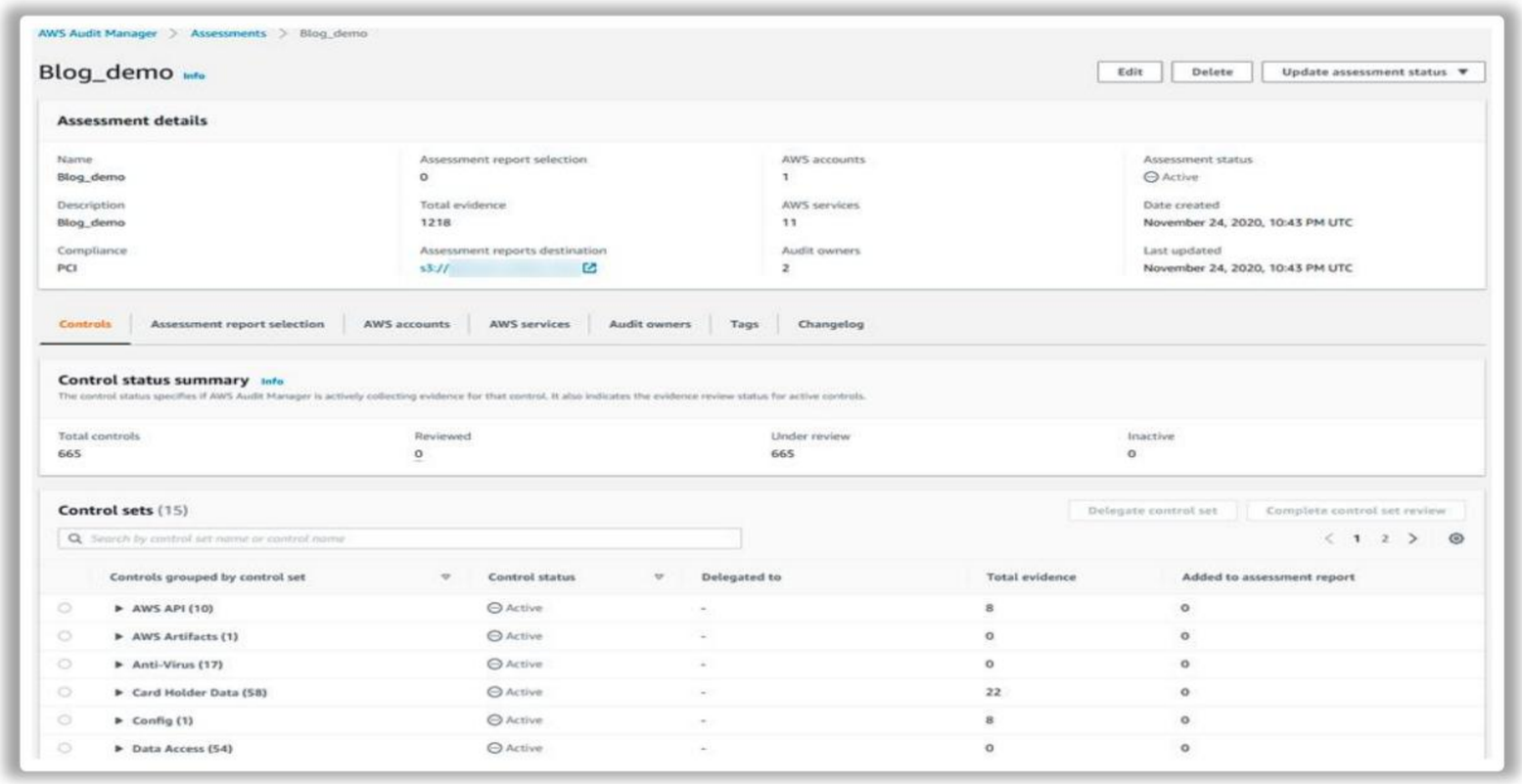


Figure 11.10: Assessment Details

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS Security Auditing Checklist

AWS Security Checklist is intended for customers and their auditors to analyze the security controls of AWS to meet standards such as AICPA, NIST, ISO, and PCI-DSS.

AWS Security Checklist auditing is important to:

- Evaluate the capability of AWS cloud services to meet security compliance requirements
- Ensure that deployments to be performed in the future meet security compliance requirements
- Assess the current use of AWS resources and evaluate the security best practices
- Develop AWS usage policies

Checklist Categories for AWS Audit

- **Pre-Audit Procedures**

  Pre-audit procedures help check whether an organization is prepared for an audit. Pre-audit includes the following procedures.

  - Understand the use of AWS within the organization.
  - Define AWS audit objectives.
  - Define the AWS boundaries to be considered for review.
  - Identify potential risks.
  - Review risks and risk documentation.
  - Include AWS service elements into risk assessment procedures.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Governance**

  The checklist for governance checks whether the organization is aware of the AWS services and resources being used. Governance also checks whether the risk management program of AWS is considered in the use of AWS. The governance checklist includes the following procedures.

  - Identify the assets.
  - Access the security policies of the organization.
  - Evaluate the organization's risk profile.
  - Modify the audit plan.

- **Asset Configuration and Management**

  The checklist for asset configuration and management check whether the organization manages the security vulnerabilities to protect the stability, security, and integrity of assets. The checklist for asset configuration and management includes the following procedures.

  - Obtain the asset inventory.
  - Validate patches for software and system components.
  - Validate configuration management.
  - Validate privileged access.

hide01.ir

- **Logical Access Control**

  The checklist for logical access control checks whether the organization is aware of how users and permissions are configured in AWS. Logical access control also checks whether the organization manages user credentials securely. The checklist for logical access control includes the following procedures.

  - Validate AWS account management.
  - Validate multi-factor authentication (MFA).
  - Evaluate identity and access management (IAM) user accounts.
  - Evaluate group permissions.
  - Evaluate the organization's system user accounts.
  - Examine the access credentials for application and system processes.
  - Validate IAM roles.
  - Perform access control testing.
  - Document the permission management of AWS resources.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Data Encryption**

  The checklist for data encryption checks whether the organization is aware of where the data are stored. Data encryption also checks whether organizational data are protected. The checklist for data encryption includes the following procedures.

  - Recognize data assets and requirements.
  - Verify the encryption of data at rest.
  - Verify the encryption of data in transit.

- **Network Configuration and Management**

  The checklist for network configuration and management checks whether the organization is aware of the network architecture of AWS resources. The checklist for network configuration and management includes the following procedures.

  - Verify traffic to Elastic Compute Cloud (EC2) instances.
  - Verify traffic to virtual private cloud (VPC) networks.
  - Evaluate additional network controls.

- **Security Logging and Monitoring**

  The checklist for security logging and monitoring checks whether the systems deployed on AWS are logged and monitored. The checklist for security logging and monitoring includes the following procedures.

  - Evaluate logging requirements.
  - Evaluate user access logging.
  - Validate change management logging.
  - Review log protection.
  - Validate monitoring mechanisms and procedures.

- **Security Incident Response**

  The checklist for security incident response checks whether the incident management plan of the organization includes AWS resources. The checklist for security incident response includes the following procedures.

  - Evaluate the current incident management process.
  - Evaluate the incident management plan.
  - Assess the communication of the incident management plan.

- **Disaster Recovery (DR)**

  The DR checklist evaluates whether the DR plan of the organization includes AWS resources. The DR checklist procedures include the following.

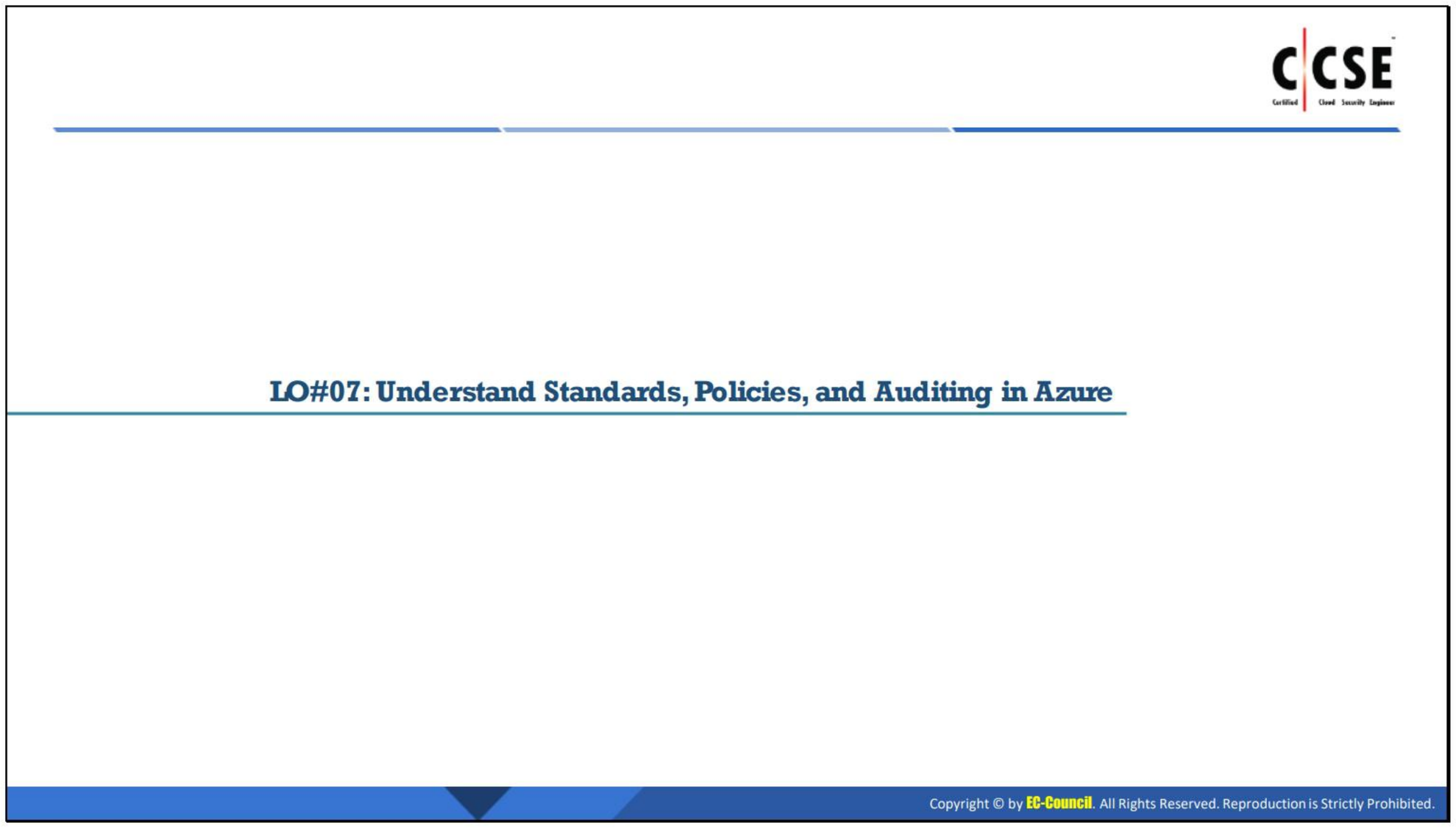
  - Analyze the current DR plan of the organization.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Validate the incident management plan.
- Validate the communication of the incident management plan.
- Evaluate the use of AWS capabilities.
- Analyze DR testing.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#07: Understand Standards, Policies, and Auditing in Azure

An organization using Microsoft Azure should be well-acquainted with the standards and policies of Azure and should know how to perform auditing in Azure to achieve governance, evaluate the compliance status of Azure resources, and fulfill compliance requirements. This section explains Azure compliance offerings, how to create a policy assignment to identify virtual machines (VMs) that do not use managed disks, how to set up auditing for Azure SQL Database, and recommendations to audit Azure services.

hidoo1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Azure Compliance Offerings

Segment		Regulatory Standards
Global		Azure Policy Regulatory Compliance (preview), CIS benchmark, CSA STAR attestation, CSA STAR certification, CSA STAR self-assessment, SOC 1, SOC 2, SOC 3
US Government		CJIS, CNSSI 1253, DFARS, DoD IL2, DoD IL4, DoD IL5, DoD IL6, DoE 10 CFR Part 810, EAR, FedRAMP, FERPA , FIPS 140-2, IRS 1075, ITAR, NIST 800-171, NIST 800-53, NIST CSF, Section 508 VPATs
Industry Specific	Financial Services	23 NYCRR Part 500 (US), AFM and DNB (Netherlands), AMF and ACPR (France), APRA (Australia), CFTC 1.31 (US), EBA (EU), FCA and PRA (UK), FFIEC (US), FINMA (Switzerland), FINRA 4511 (US), FISC (Japan), FSA (Denmark), GLBA (US), KNF (Poland), MAS and ABS (Singapore), NBB and FSMA (Belgium), OSFI (Canada), OSPAR (Singapore), PCI 3DS, PCI DSS, RBI and IRDAI (India), SEC 17a-4 (US), SEC Regulation SCI (US), SOX (US), TruSight
	Healthcare and Life Sciences	ASIP HDS (France), GxP (FDA 21 CFR Part 11), HIPAA (US), HITRUST, MARS-E (US) NEN 7510 (Netherlands)
	Automotive, Energy, Media, and Telecommunications	CDSA, DPP (UK), FACT (UK), MPA, GSMA, NERC (US), TISAX
Region/Country	Americas	PDPA (Argentina), Canadian privacy laws, US CCPA
	Asia Pacific	Australia IRAP, China GB 18030, China DJCP (MLPS), China TCS, India MeitY, Japan CS Gold Mark, Japan My Number Act, Korea K-ISMS, New Zealand ISPC, Singapore MTCS
	Europe, the Middle East, and Africa	EU EN 301 549, ENISA IAF, EU GDPR, EU Model Clauses, Germany C5, Netherlands BIR 2012, Spain ENS High, UAE DESC, UK Cyber Essentials Plus, UK G-Cloud, UK PASF

Source: https://www.microsoft.com

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

Azure Compliance Offerings

Azure has the most significant security compliance features in terms of the number of offerings and customer-facing services. Azure compliance offerings are based on certifications, attestation, validation, third-party audits, etc. and are grouped into four segments.

***Source**: https://www.microsoft.com*

hiu01.ir

Segment		Regulatory Standards
Global		Azure Policy Regulatory Compliance (preview), CIS benchmark, CSA STAR attestation, CSA STAR certification, CSA STAR self-assessment, SOC 1, SOC 2, SOC 3
US Government		CJIS, CNSSI 1253, DFARS, DoD IL2, DoD IL4, DoD IL5, DoD IL6, DoE 10 CFR Part 810, EAR, FedRAMP, FERPA , FIPS 140-2, IRS 1075, ITAR, NIST 800-171 ,NIST 800-53 , NIST CSF, Section 508 VPATs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Industry Specific	Financial Services	23 NYCRR Part 500 (US), AFM and DNB (Netherlands), AMF and ACPR (France), APRA (Australia), CFTC 1.31 (US), EBA (EU), FCA and PRA (UK), FFIEC (US), FINMA (Switzerland), FINRA 4511 (US), FISC (Japan), FSA (Denmark), GLBA (US), KNF (Poland), MAS and ABS (Singapore), NBB and FSMA (Belgium), OSFI (Canada), OSPAR (Singapore), PCI 3DS, PCI DSS, RBI and IRDAI (India), SEC 17a-4 (US), SEC Regulation SCI (US), SOX (US), TruSight
	Healthcare and Life Sciences	ASIP HDS (France), GxP (FDA 21 CFR Part 11), HIPAA (US), HITRUST, MARS-E (US), NEN 7510 (Netherlands)
	Automotive, Energy, Media, and Telecommunications	CDSA, DPP (UK), FACT (UK), MPA, GSMA, NERC (US), TISAX
Region/Country	Americas	PDPA (Argentina), Canadian privacy laws, US CCPA
	Asia Pacific	Australia IRAP, China GB 18030, China DJCP (MLPS), China TCS, India MeitY, Japan CS Gold Mark, Japan My Number Act, Korea K-ISMS, New Zealand ISPC, Singapore MTCS
	Europe, the Middle East, and Africa	EU EN 301 549, ENISA IAF, EU GDPR, EU Model Clauses, Germany C5, Netherlands BIR 2012, Spain ENS High, UAE DESC, UK Cyber Essentials Plus, UK G-Cloud, UK PASF

hide01.ir

Table 11.3: Azure Compliance Offerings

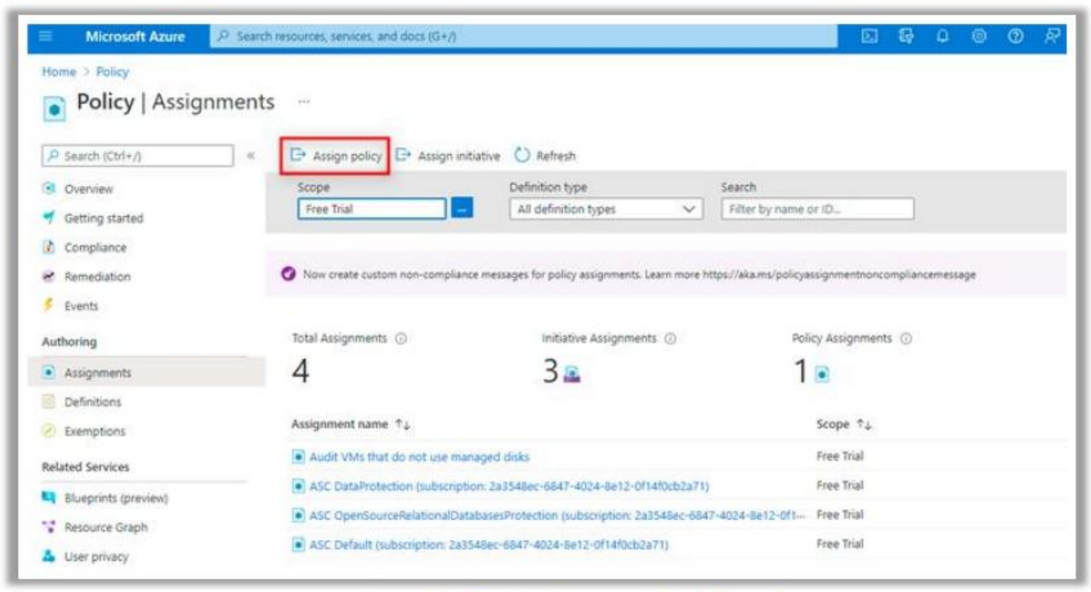
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Azure Policy

- Azure Policy helps enforce the policies on deployed resources to achieve resource governance and evaluate the resource compliance status

Features

- **Enforcement and compliance:** Azure Policy ensures compliance by turning on built-in policies or custom policies for resources
- **Apply policies at scale:** Azure Policy has functionalities for applying multiple policies and can be implemented in a management group or subscription
- **Remediation:** Azure Policy can perform real-time remediation



Azure Policy Assignment Dashboard

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

Azure Policy

Azure Policy helps enforce the policies on deployed resources to achieve resource governance and evaluate the resource compliance status. Azure Policy ensures compliance through the full remediation of the current resources and by performing automatic remediation for new resources.

hidoo1.ir

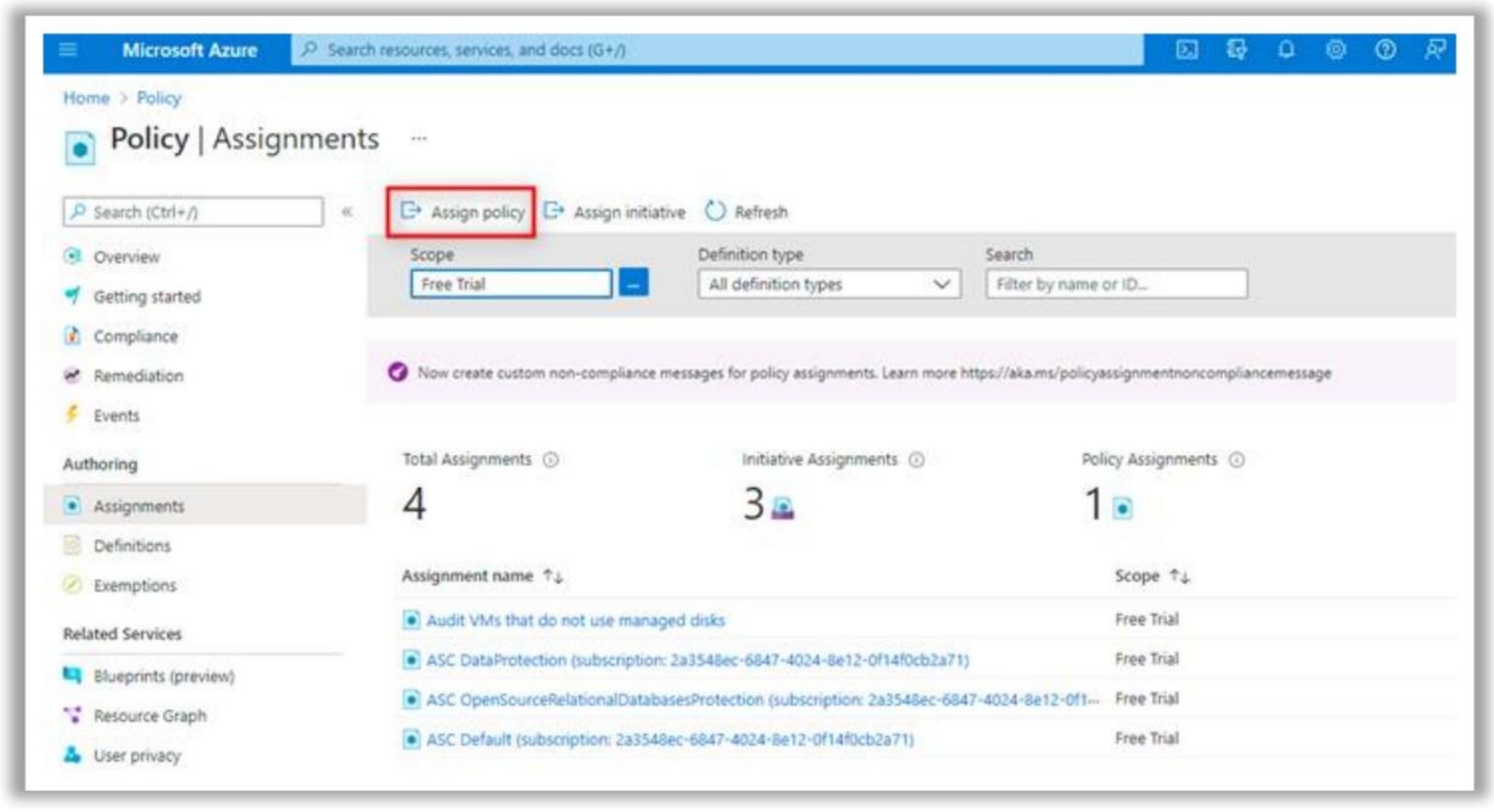


Figure 11.11: Policy - Assignments

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features

Azure Policy has the following features.

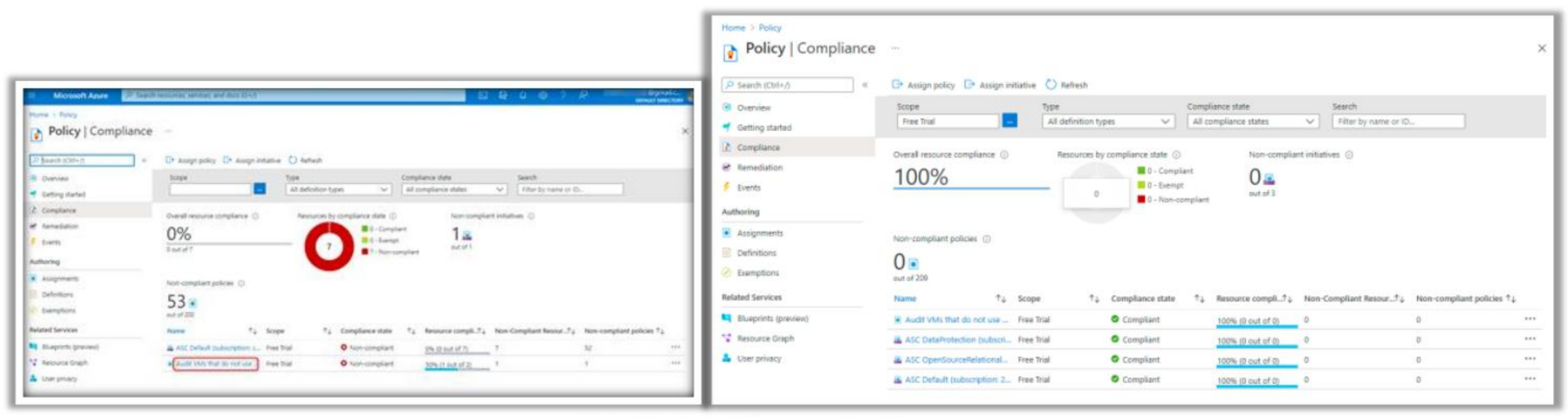
- **Enforcement and compliance:** Azure Policy ensures compliance by turning on built-in policies or custom policies for resources. The policies are evaluated and enforced in real time. Azure Policy also performs periodic compliance evaluations.
- **Apply policies at scale:** Azure Policy has functionalities for applying multiple policies and can be implemented in a management group or subscription.
- **Remediation:** Azure Policy can perform real-time remediation.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Creating Policy Assignment to Identify Non-Compliant Resources

- In the Azure Policy service, policy assignments can be created to identify resources that are non-compliant with a particular organizational policy



Identification of Non-compliant Resources

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

Creating Policy Assignment to Identify Non-Compliant Resources

In the Azure Policy service, policy assignments are used to define the policies assigned to the respective resources. Policy assignments can determine the values of parameters for particular resources at the assigned time. The policy assignments contain a display name, description, metadata, enforcement mode, excluded scopes, parameters, policy definition, and non-compliance messages. A policy assignment can be created for a particular task, which helps identify non-compliant resources.

The following are the steps to create a policy assignment to identify virtual machines (VMs) that do not use managed disks.

Source: *https://www.microsoft.com/*

- **Step 1: Creating a Policy Assignment**
  - Navigate to Azure Portal.
  - Select **All Services** and search for **Policy**.

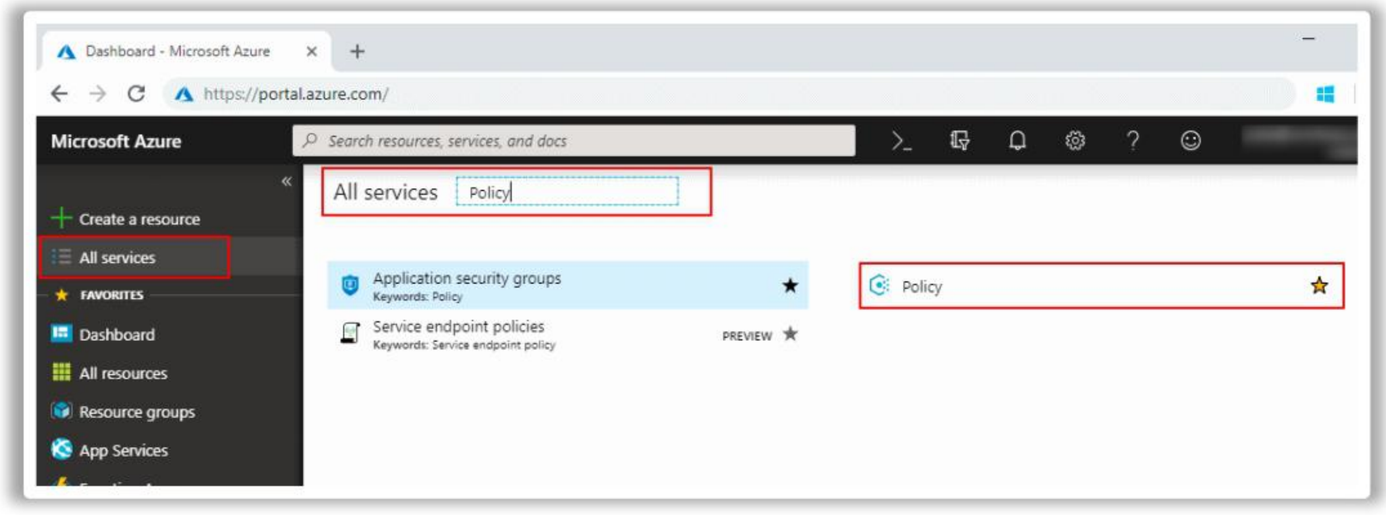


Figure 11.12: Creating a Policy Assignment

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the Azure Policy page that appears, click on Assignments on the left side.

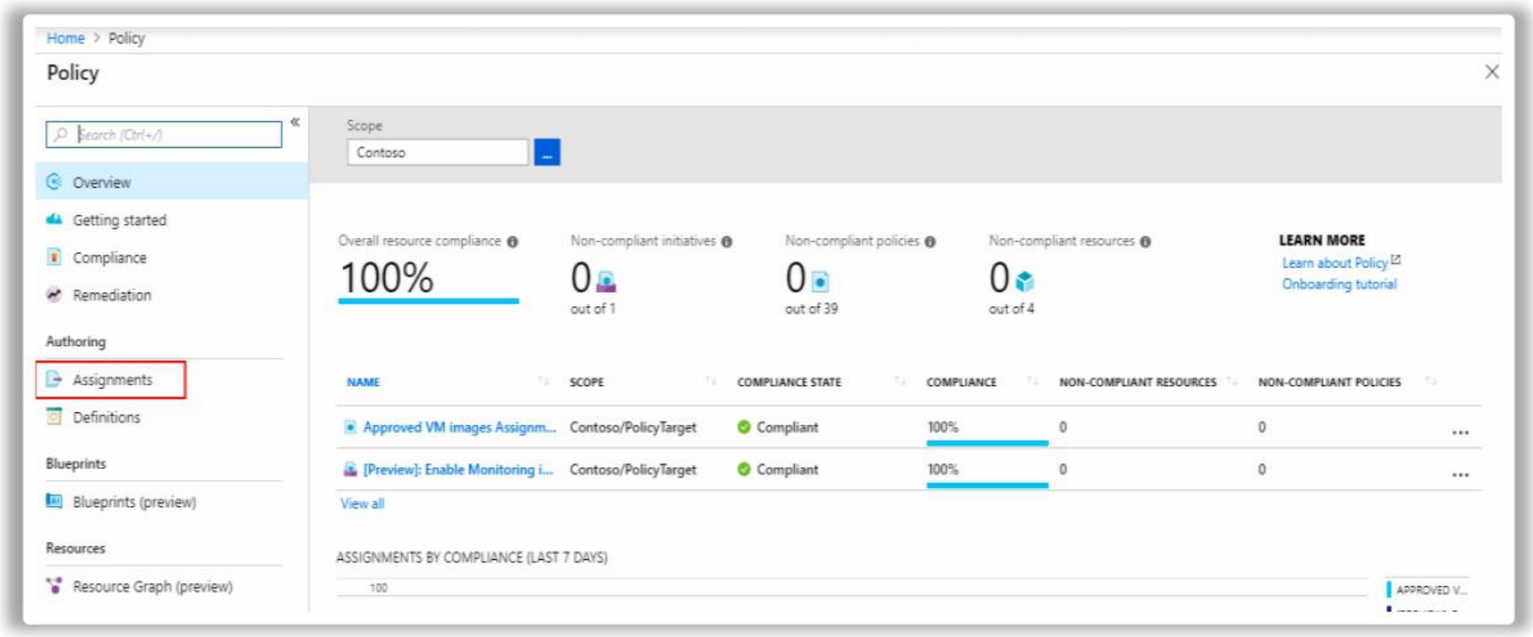


Figure 11.13: Selecting Assignments in Policy Window

- From the Policy Assignments page that appears, click on Assign Policy.

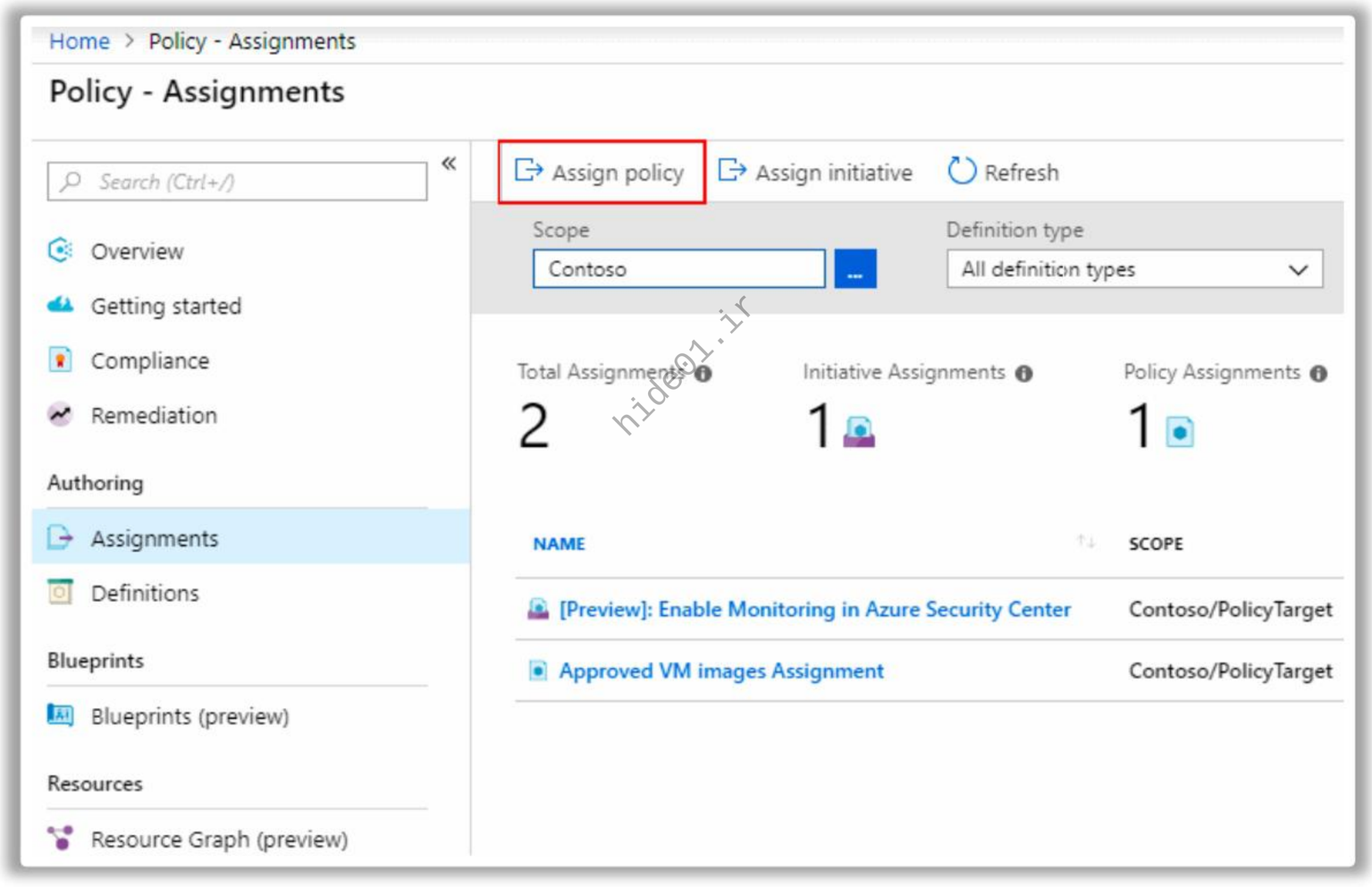


Figure 11.14: Selecting Assign Policy

- Click on the ellipsis under **Scope** and select a subscription or management group in the **Assign Policy** page that appears.
- Leave the **Exclusions** blank.
- Click on the ellipsis under Policy Definition and search for the policy definitions to be configured. Here, select the definition Audit VMs that do not use managed disks.
- Click on the Select button.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

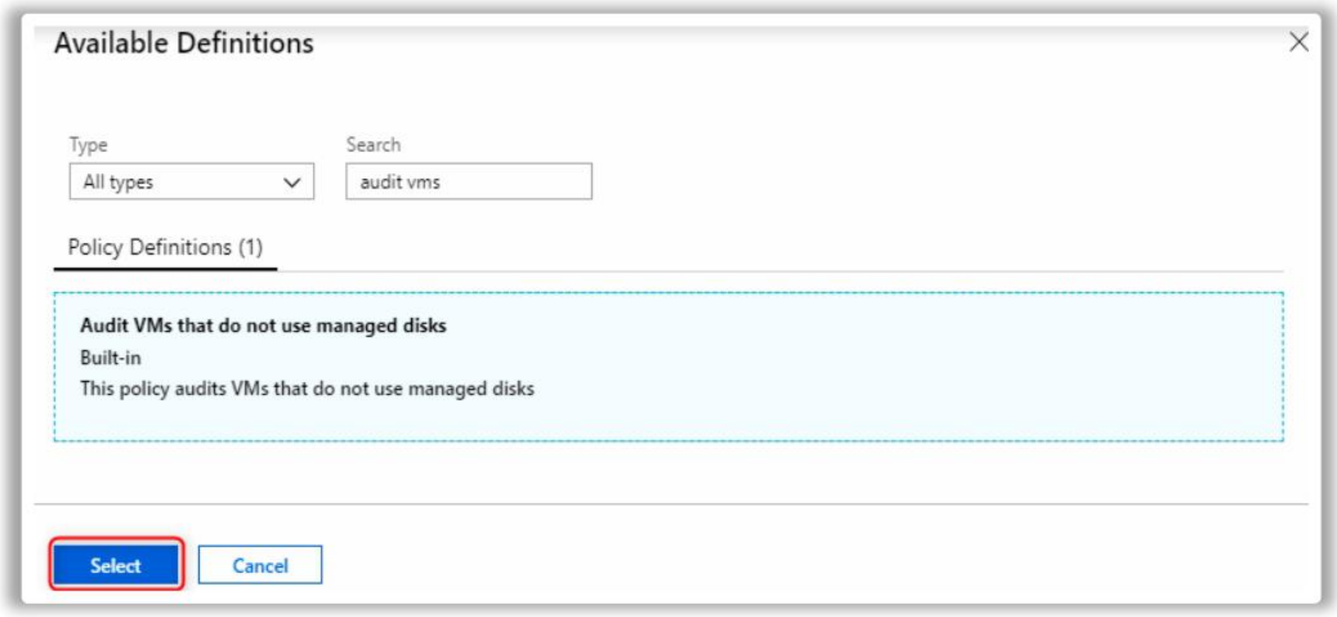


Figure 11.15: Selecting Available Definitions

- **Assignment name** gets filled with the selected policy name, and **Assigned by** gets filled with who is logged in.
- To move to the next page, click on Next at the bottom or Parameters at the bottom.
- In this tab, the policy definition parameters get included, if parameters were included in the **Basics** tab.
- Uncheck **Create a Managed Identity**.
- To navigate to the next page, either click on **Next** at the bottom or **Non-Compliance messages** at the top.
- In this page, a **Non-Compliance message** can be configured. Here, set the message as *Virtual machines should use a managed disk.*
- Navigate to the next page by clicking on **Next** at the bottom or **Review + Create** at the top.
- Click on **Create** at the bottom.

- **Step 2: Identification of the Non-compliant Resources**
  - Click on **All Services** and navigate to the **Policy** page.
  - Click on **Compliance** on the left and find the created policy assignment.

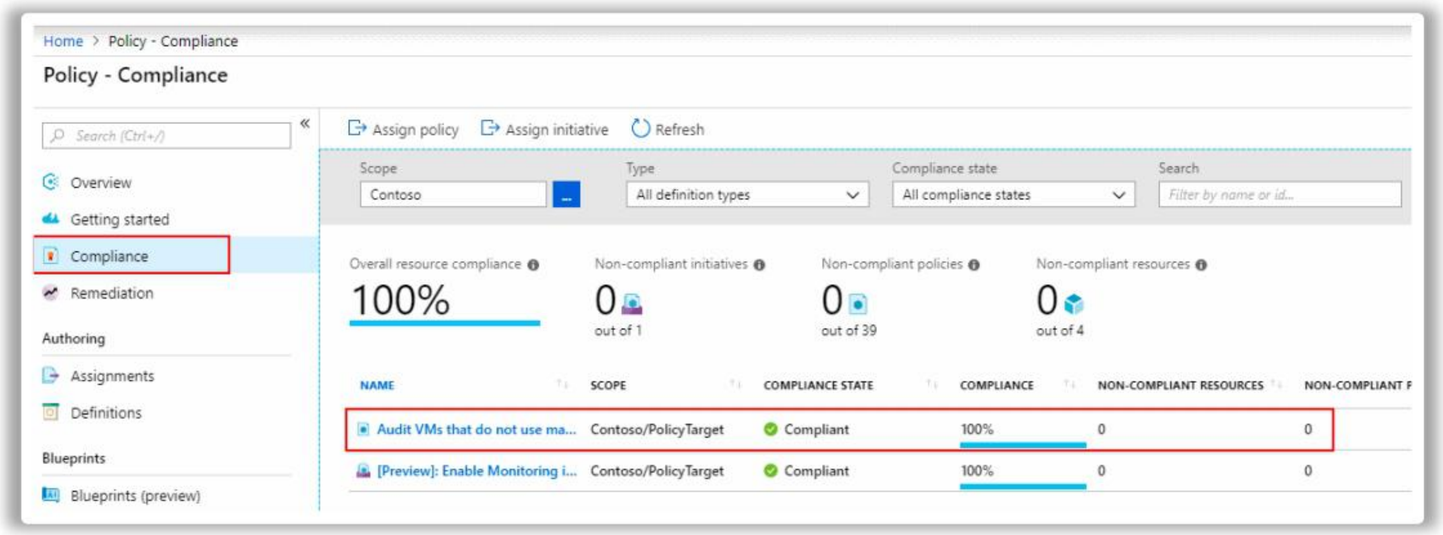
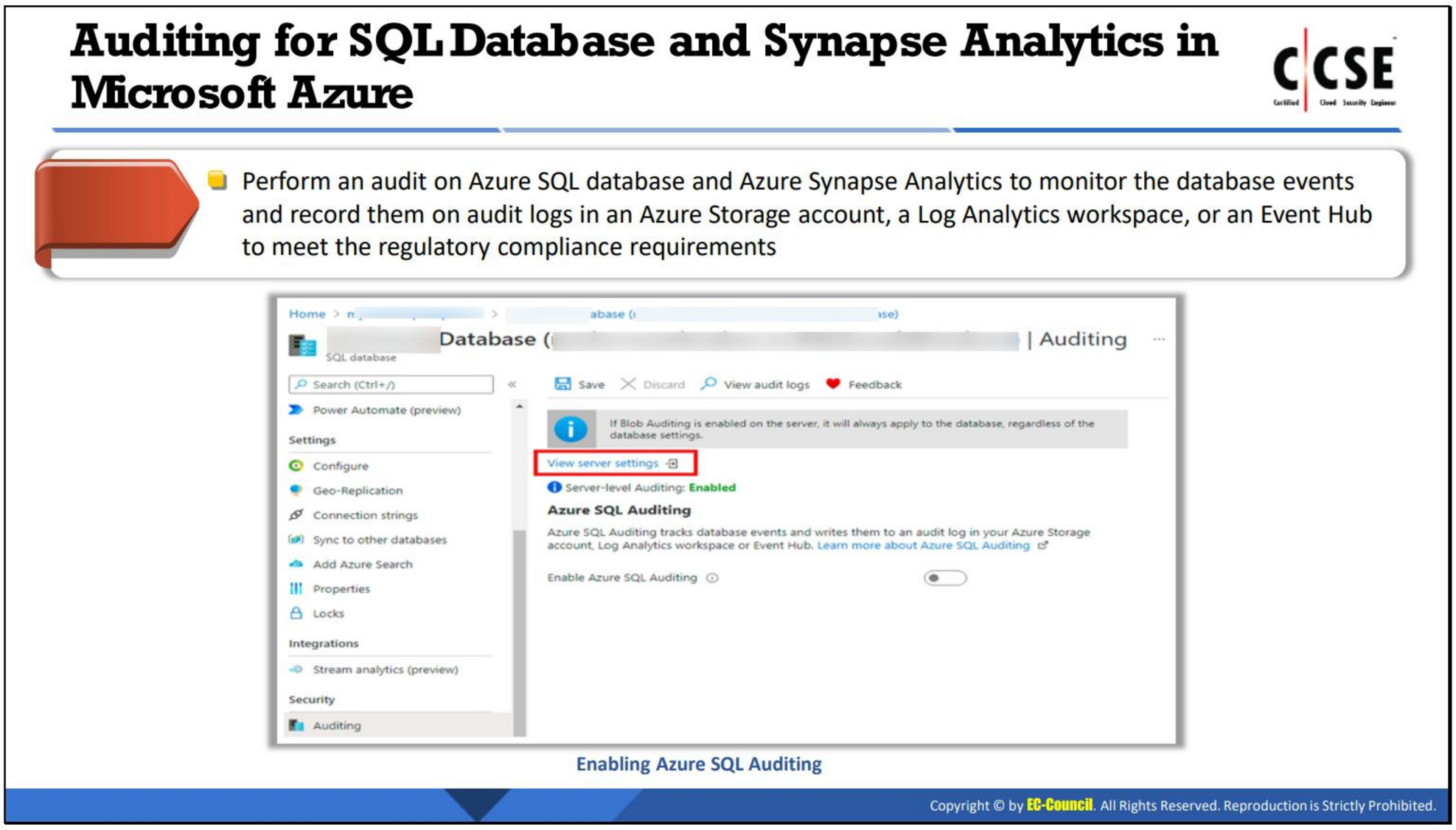


Figure 11.16: Finding the Created Policy Assignment in Policy-Compliance Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enabling Azure SQL Auditing

Auditing for SQL Database and Synapse Analytics in Microsoft Azure

Perform an audit on Azure SQL Database and Azure Synapse Analytics to monitor the database events and record them on audit logs in an Azure Storage account, a Log Analytics workspace, or an Event Hub.

The following are the steps to set up auditing for Azure SQL Database and Azure Synapse Analytics.

Note: While auditing Azure SQL Database and Azure Synapse Analytics, only 4000 characters are stored in the audit record. Excess data beyond the first 4000 characters get truncated and will not be audited.

Source: *https://www.microsoft.com/*

- Navigate to Azure portal.
- In the **SQL Server** pane, click on **Auditing** under security.
- Click on **View Server Settings** to configure the auditing policy.
- Toggle **ON** Azure SQL auditing if auditing is to be performed at the database level.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

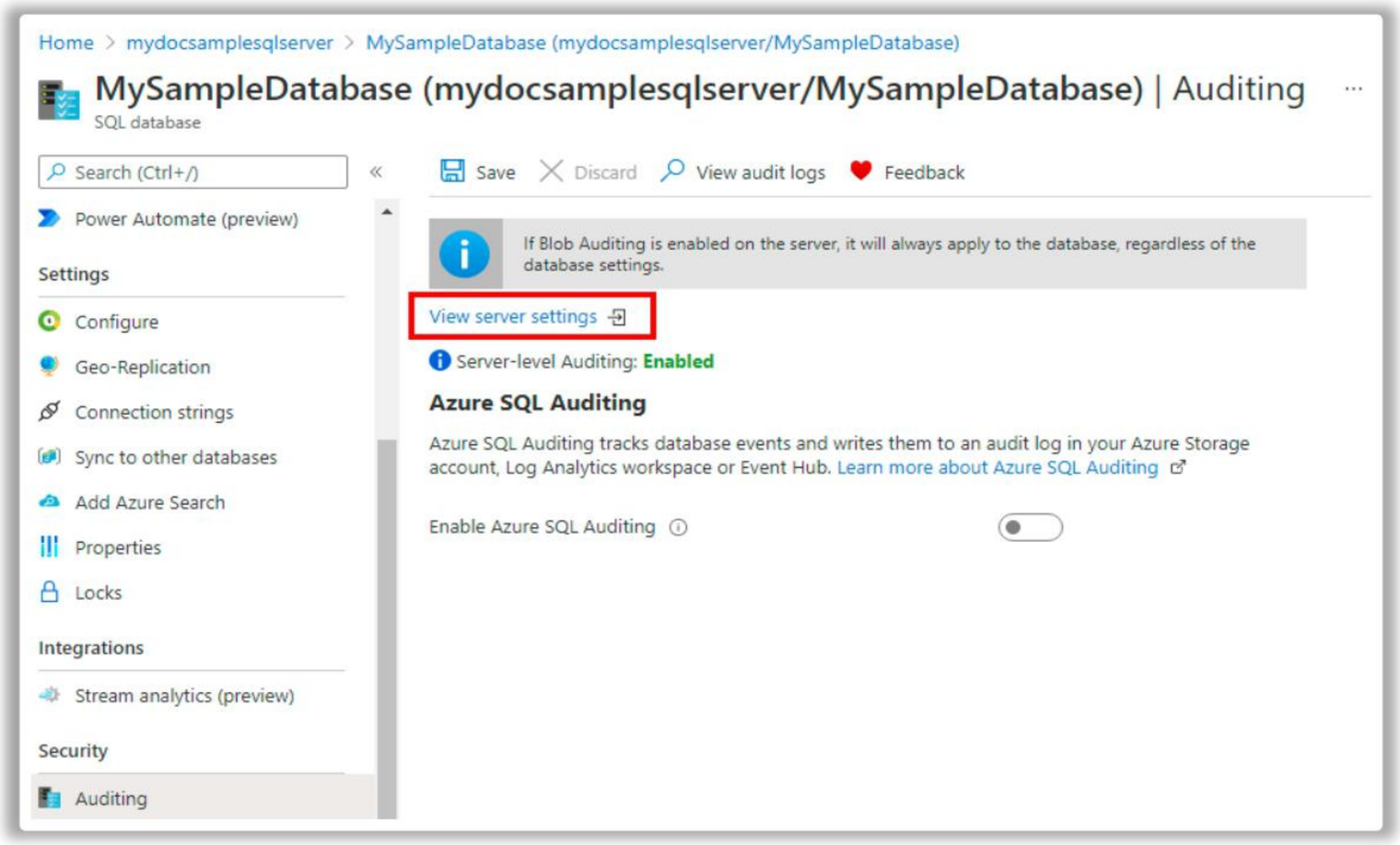


Figure 11.17: Configuring the Auditing Policy

- The Azure audit logs can be configured to be written to an Azure Storage account, Log Analytics, or an Event Hub.

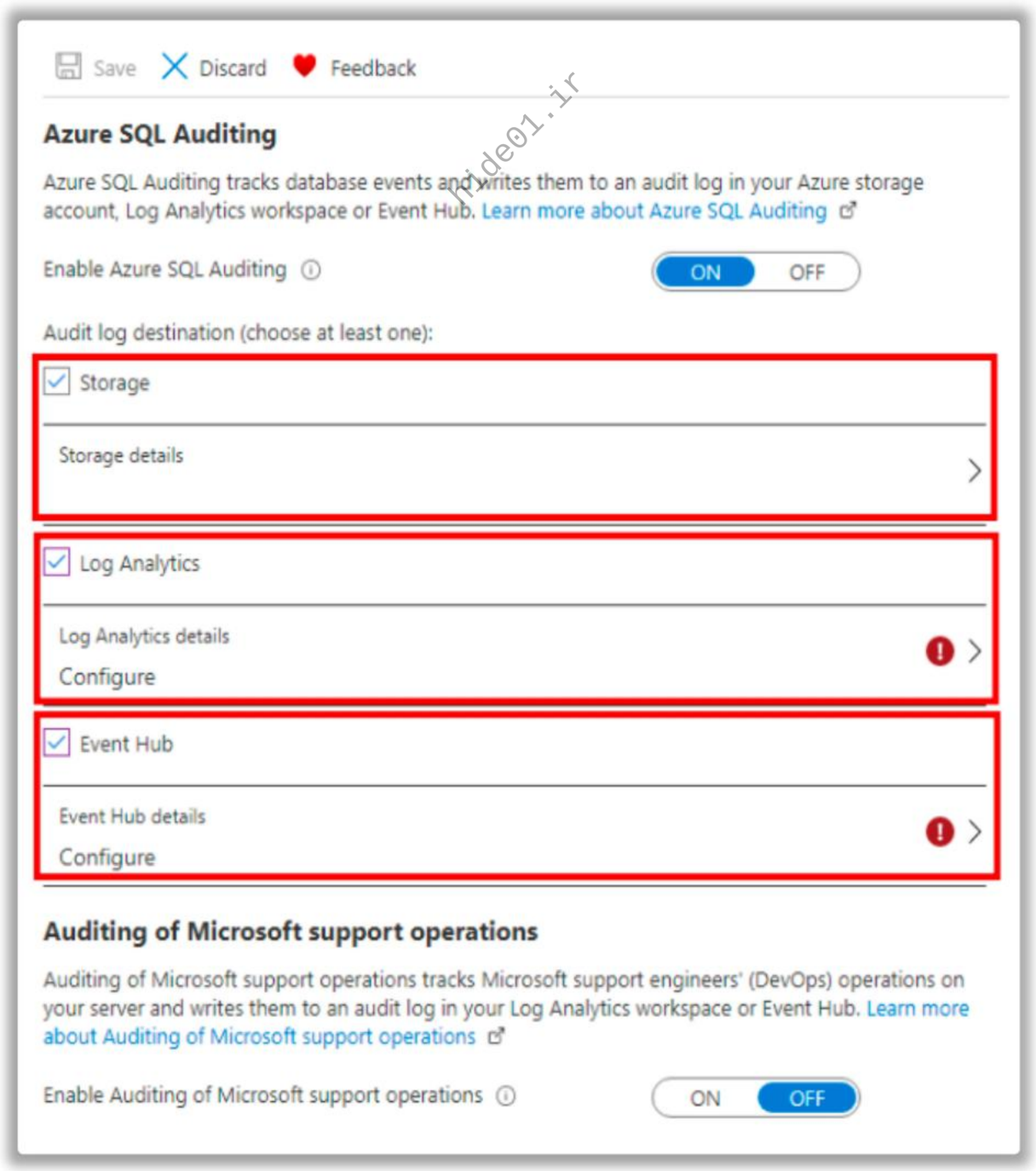


Figure 11.18: Azure SQL Auditing

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Auditing of Microsoft Support Operations**
  - Navigate to **Auditing** in the **Azure SQL Server** window.
  - Toggle **ON** the **Auditing of Microsoft Support Operations** option.

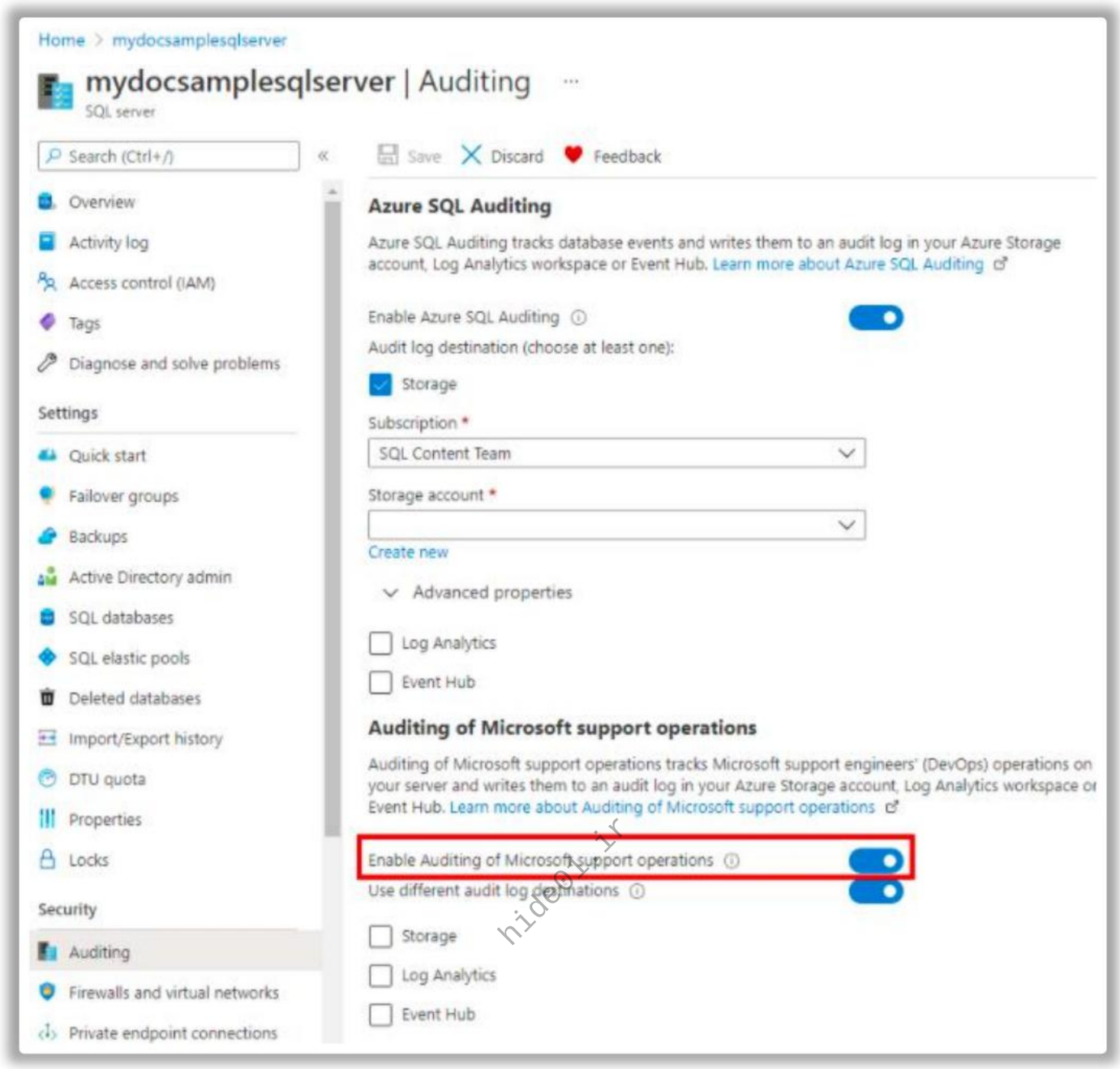


Figure 11.19: Auditing of Microsoft Support Operations

- **Configuring the Writing of Audit Logs to Storage**
  - Navigate to **Auditing** in the **Azure SQL Server** window.
  - Mark the checkbox near **Storage.**
  - Select the Azure Storage account to which logs are to be saved.
  - Open Advanced Properties.
  - Select the **Retention (Days)** by moving the slider.
  - Click Save.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

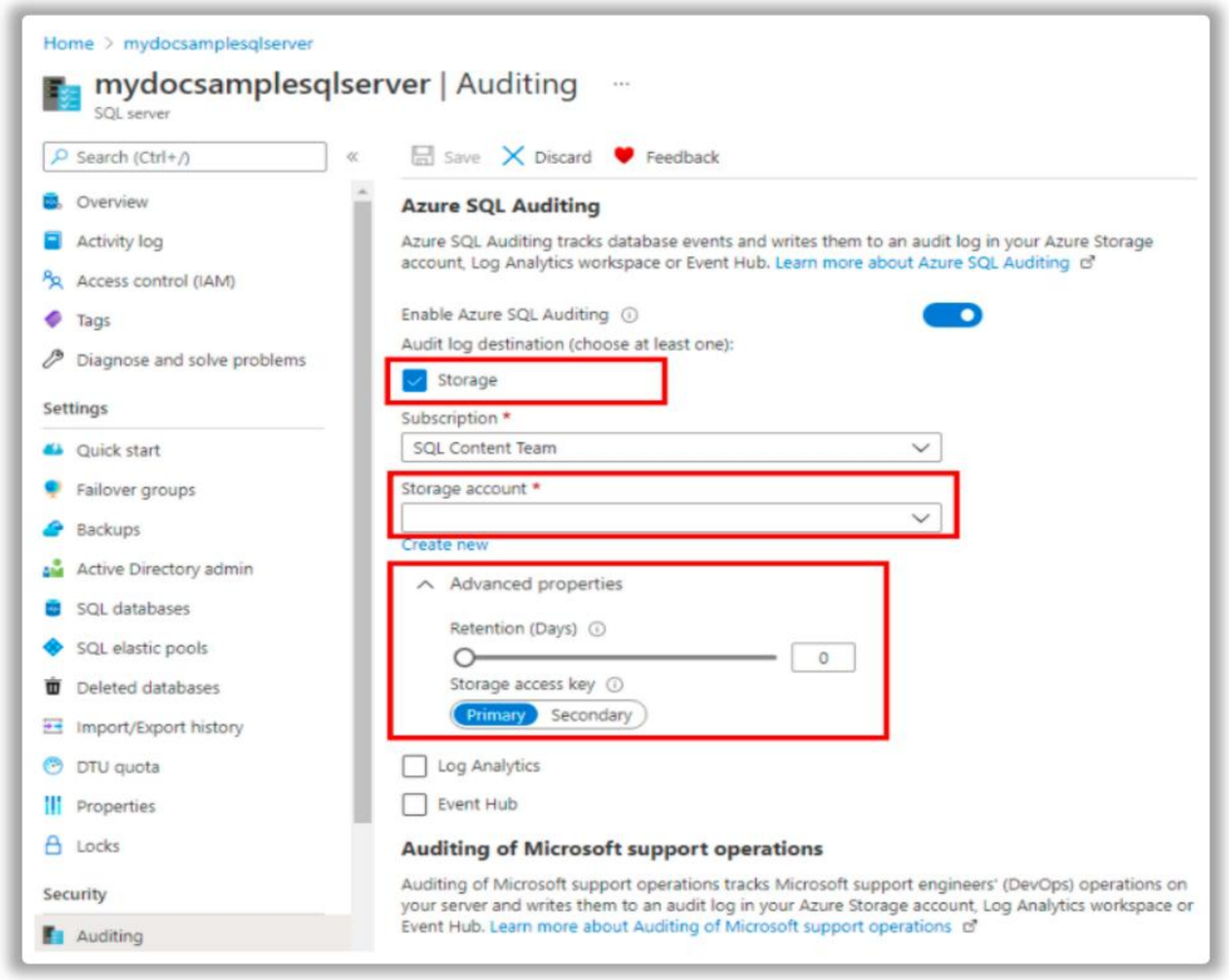


Figure 11.20: Configuring the Writing of Audit Logs to Storage

- **Configuring the Writing of Audit Logs to Log Analytics**
  - Navigate to **Auditing** under **Security** in the **Azure SQL Server** window.
  - Mark the Checkbox near **Log Analytics**.
  - Open **Log Analytics** details.
  - Select the Log Analytics workspace to which logs are to be written.
  - Click **OK**.

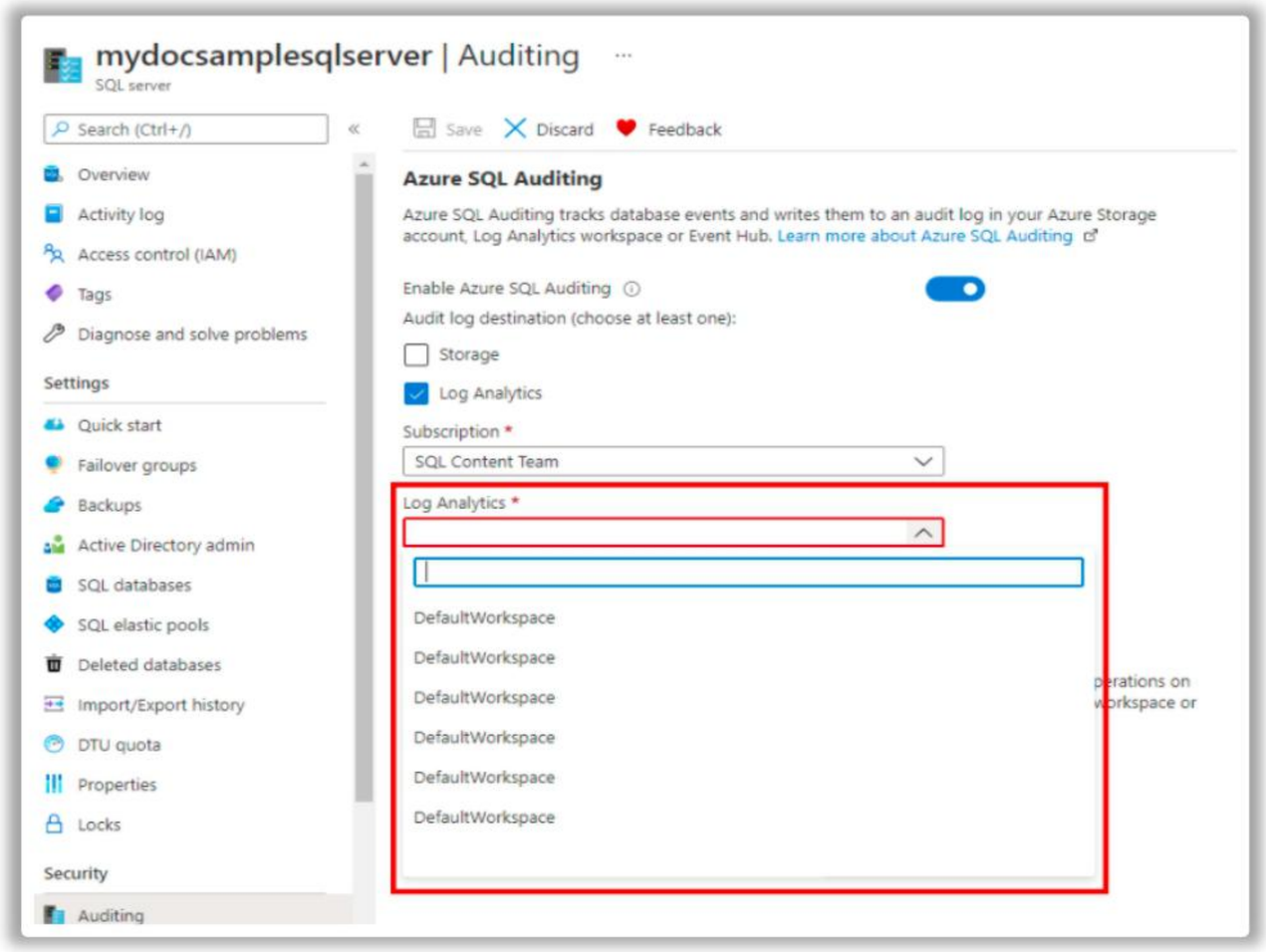


Figure 11.21: Configuring the Writing of Audit Logs to Log Analytics

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Configuring the Writing of Audit Logs to Event Hub**
  - Navigate to Auditing under Security in the Azure SQL Server window.
  - Mark the checkbox near **Event Hub**.
  - Select the Event Hub to which logs are to be written.
  - Click **Save**.

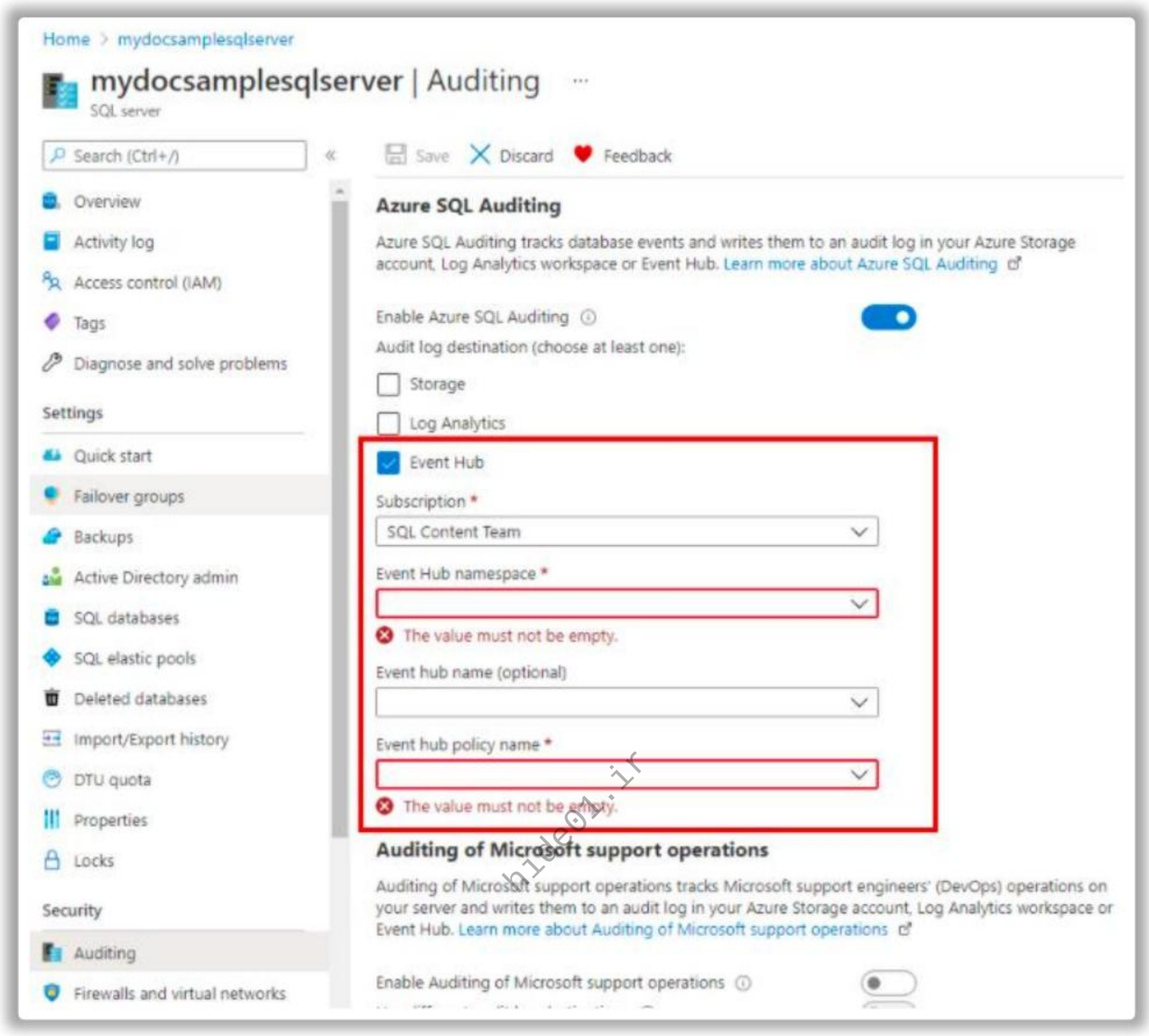


Figure 11.22: Configuring the Writing of Audit Logs to Event Hub

- **Analyzing Audit Logs and Reports**
  - Navigate to Azure Portal.
  - Open the database in which logs are to be audited.
  - Click on **View Audit Logs.**

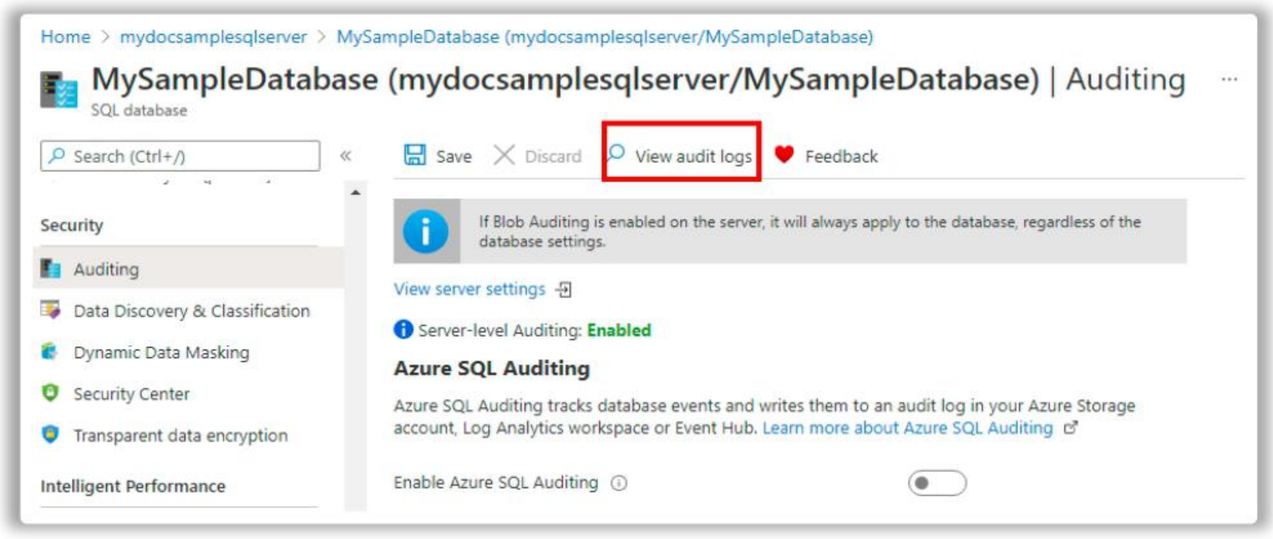


Figure 11.23: Viewing Audit Logs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on Log Analytics in the Audit Records page to view the logs in a Log Analytics workspace.

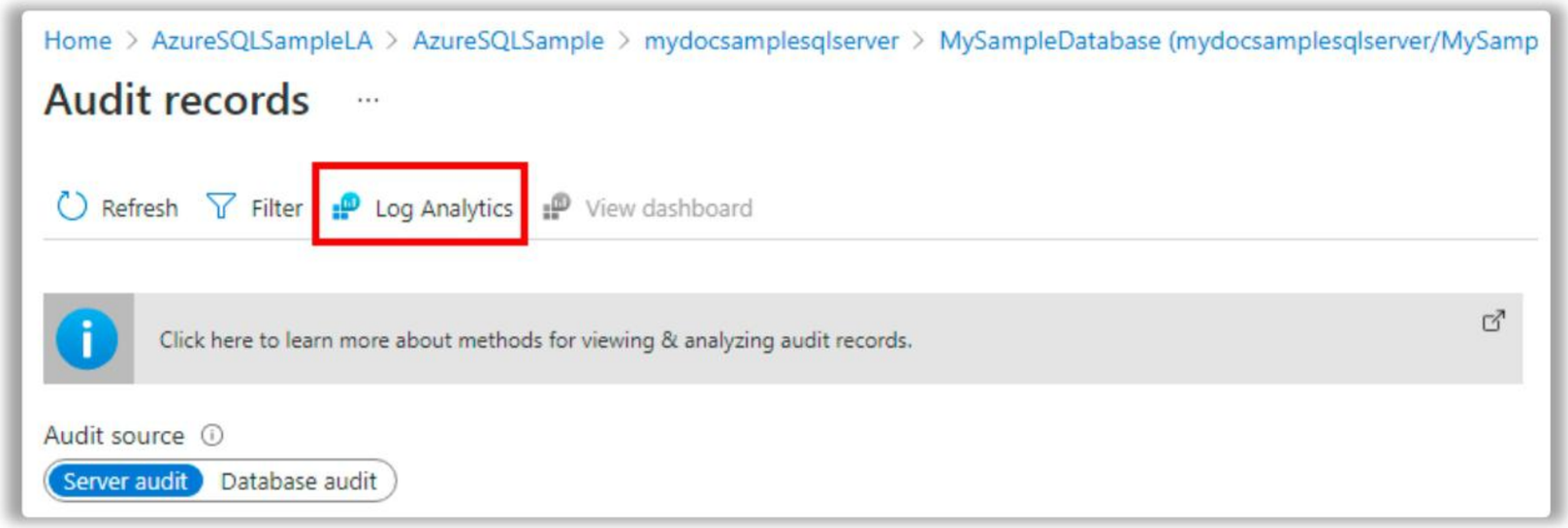


Figure 11.24: Viewing the Logs in a Log Analytics Workspace

- Click on View Dashboard on the top portion in the Audit Records page to gain insights into sensitive data.

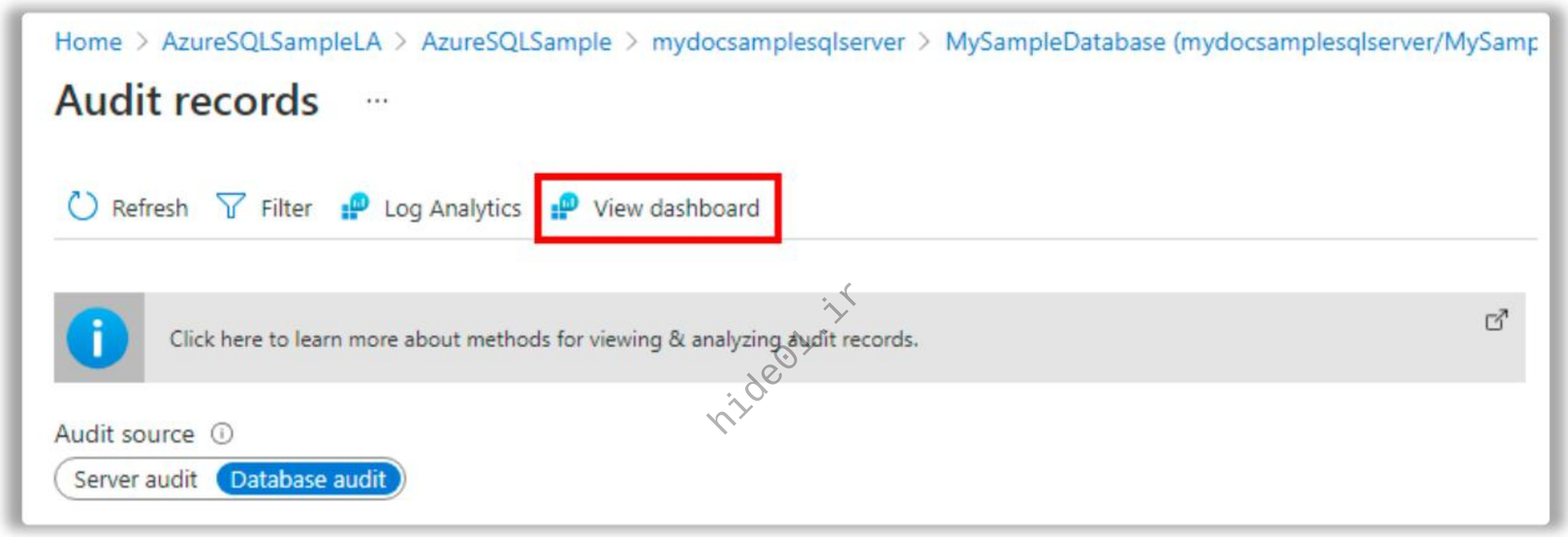


Figure 11.25: Selecting View Dashboard tab

- Customize the time range to obtain filtered results.

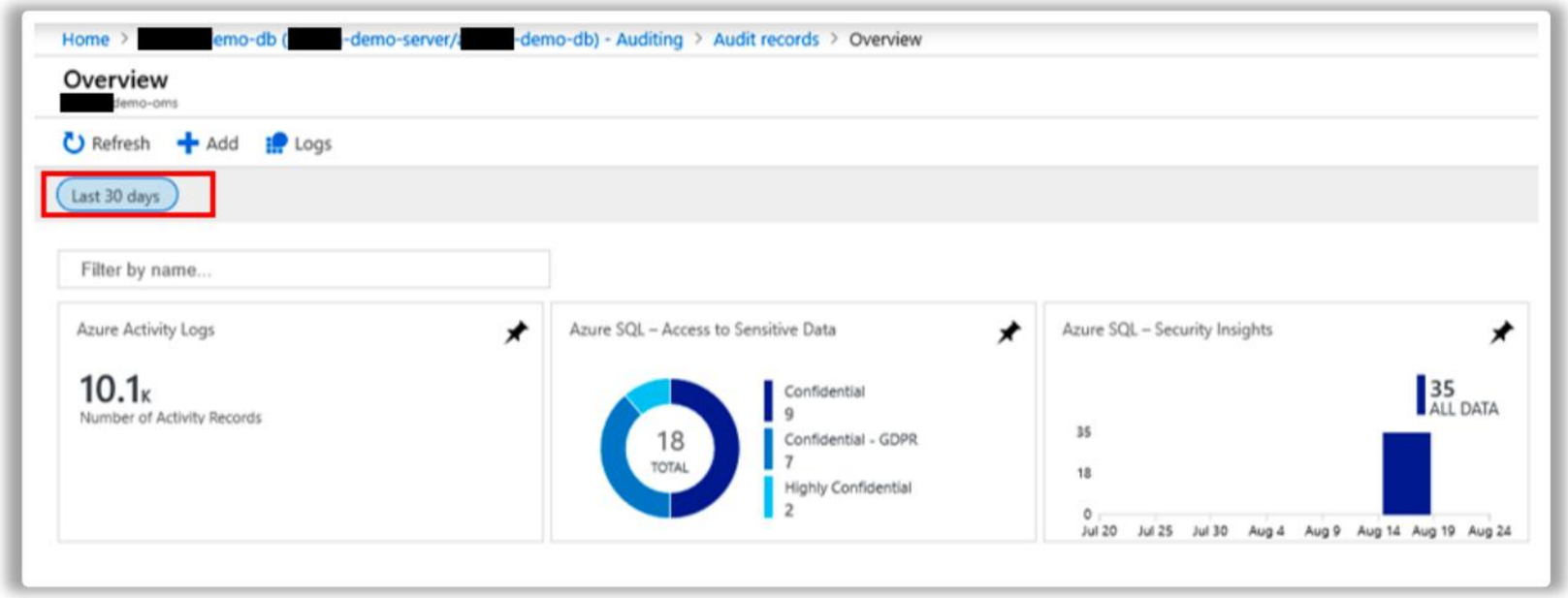


Figure 11.26: Customizing Time Range

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

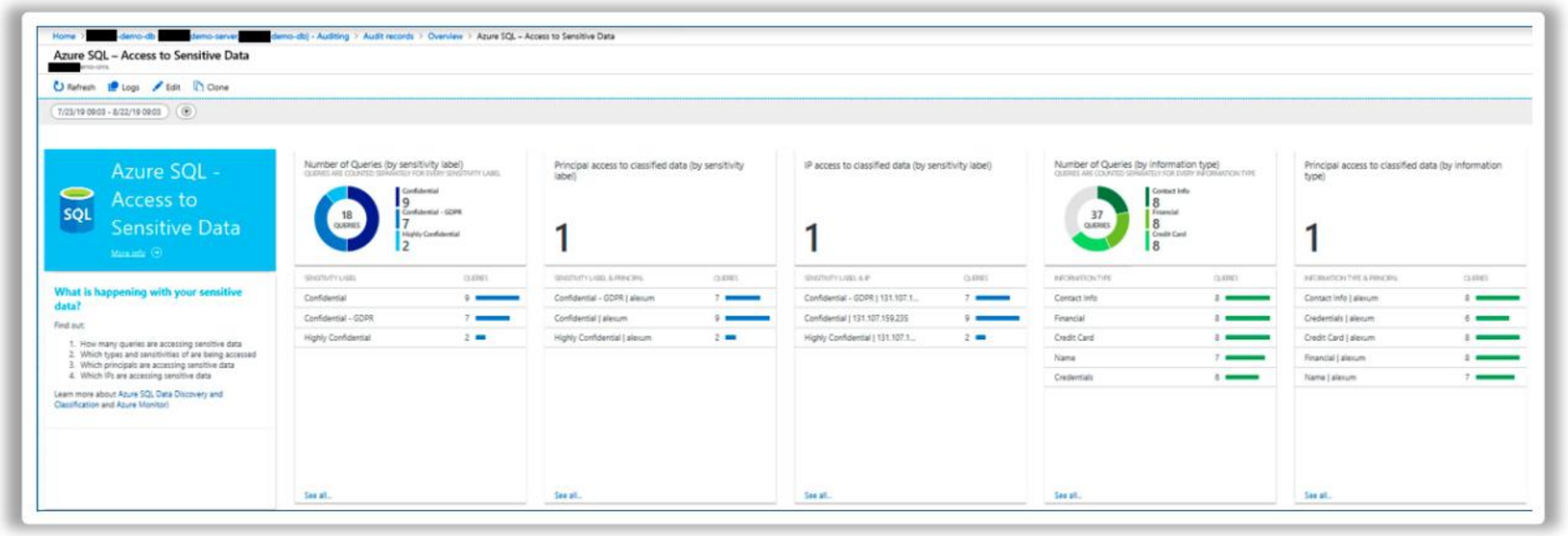


Figure 11.27: Filtered Results

- **Viewing the Logs Written to Azure Storage Account**
  - Navigate to Azure Portal.
  - Open the database and click on **View Audit Logs.**

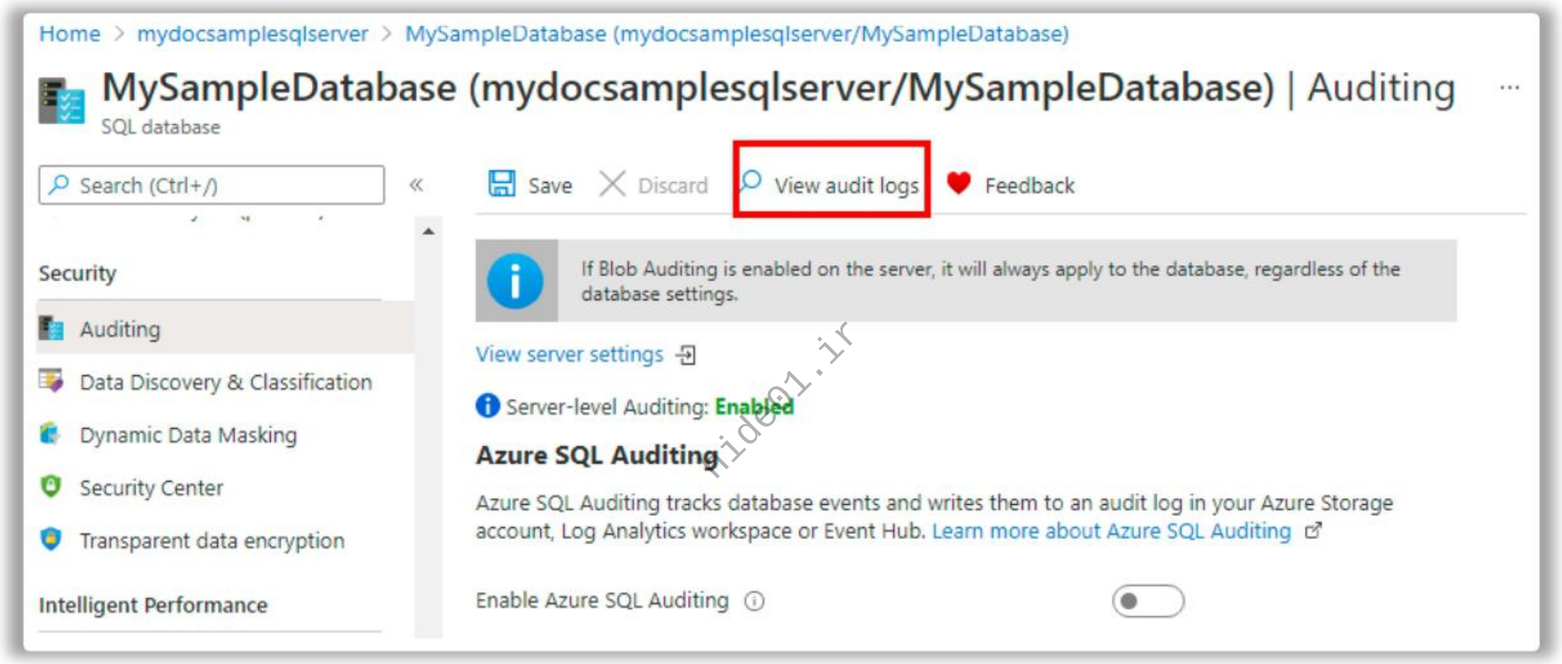


Figure 11.28: Viewing the Logs Written to Azure Storage Account

  - Click on **Filter** at the top of the **Audit Records** window to view the logs by date.
  - Toggle **Audit Source** to switch between the server audit policy and database audit policy.

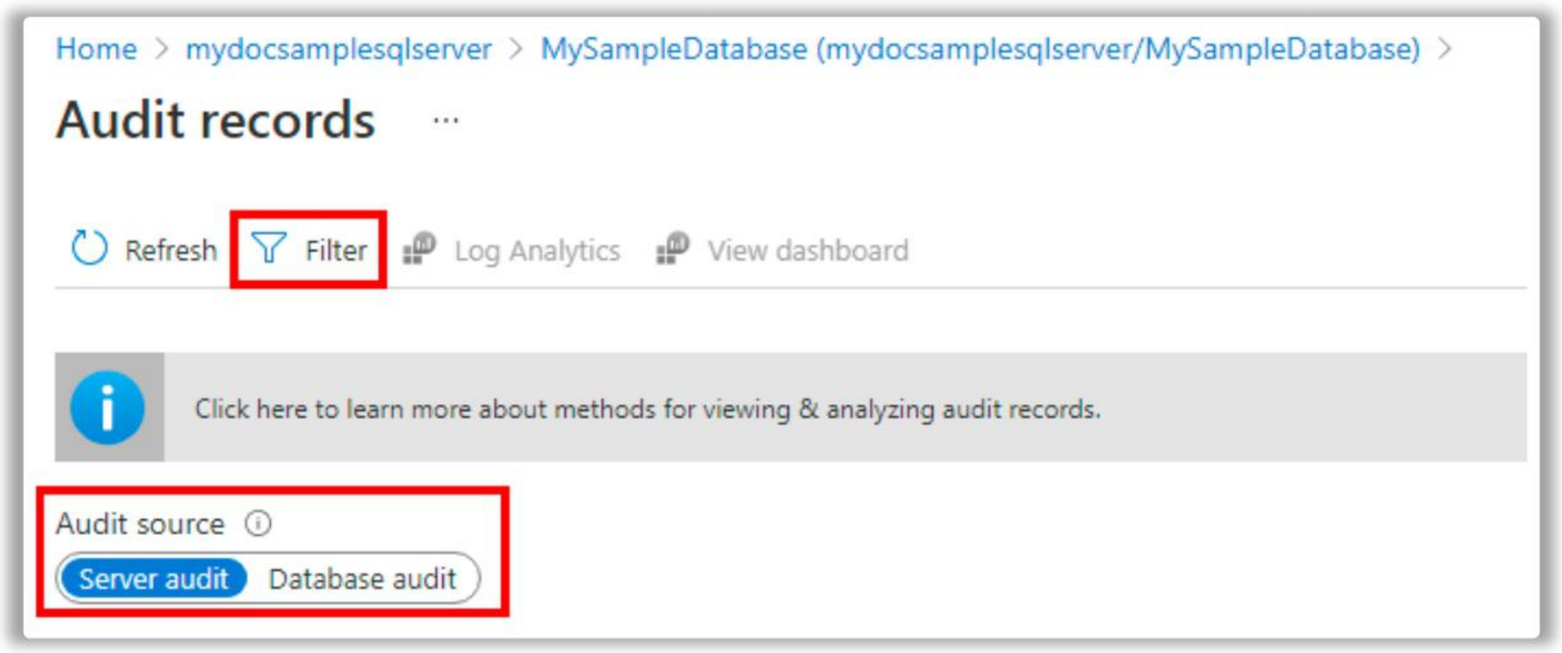


Figure 11.29: Filtering Audit records

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Viewing the Audit Log Data in Tabular Format Using SQL Server Management Studio**
  - Click on **File > Open > Merge Audit Files** in **SQL Server Management Studio**.

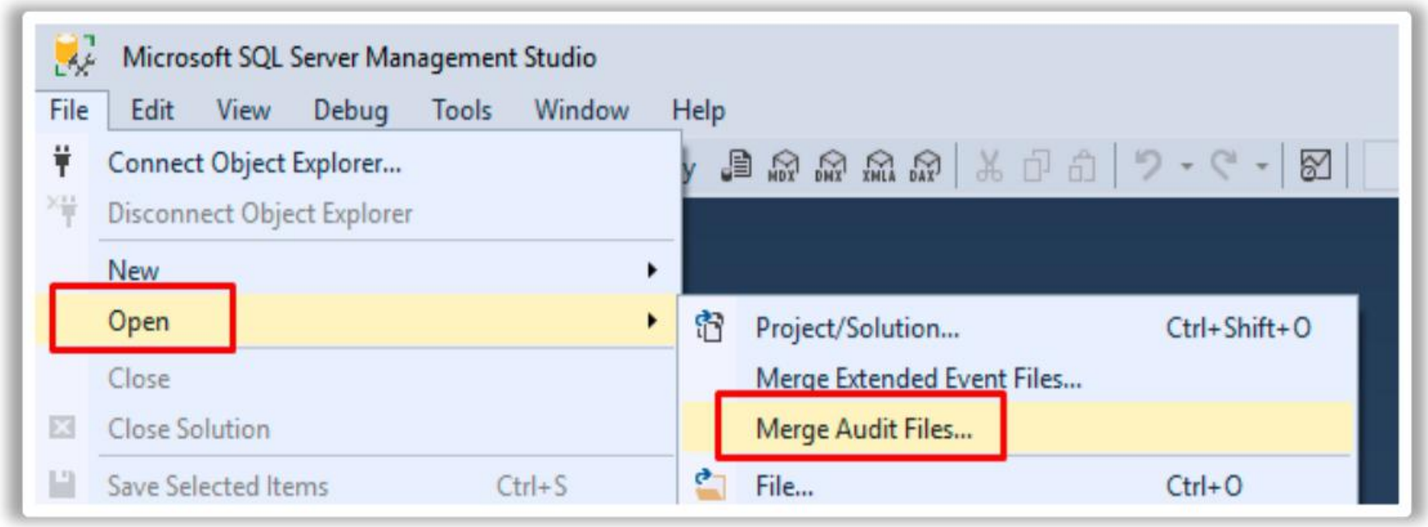


Figure 11.30: Microsoft SQL Server Management Studio

  - Select any of the **Add** options in the **Add Audit Files** window that appears.
  - Provide Azure storage details and an account key.
  - Click **OK** after all files are added.
  - Analyze the merged file in **SQL Server Management Studio** and export it to a table.

- **Regeneration of Storage Keys**
  - Navigate to Auditing under Security in the Azure SQL Server window.
  - Click on **Advanced Properties** under **Storage.**
  - Toggle Storage Access Key to Secondary.
  - Click on Save at the top.

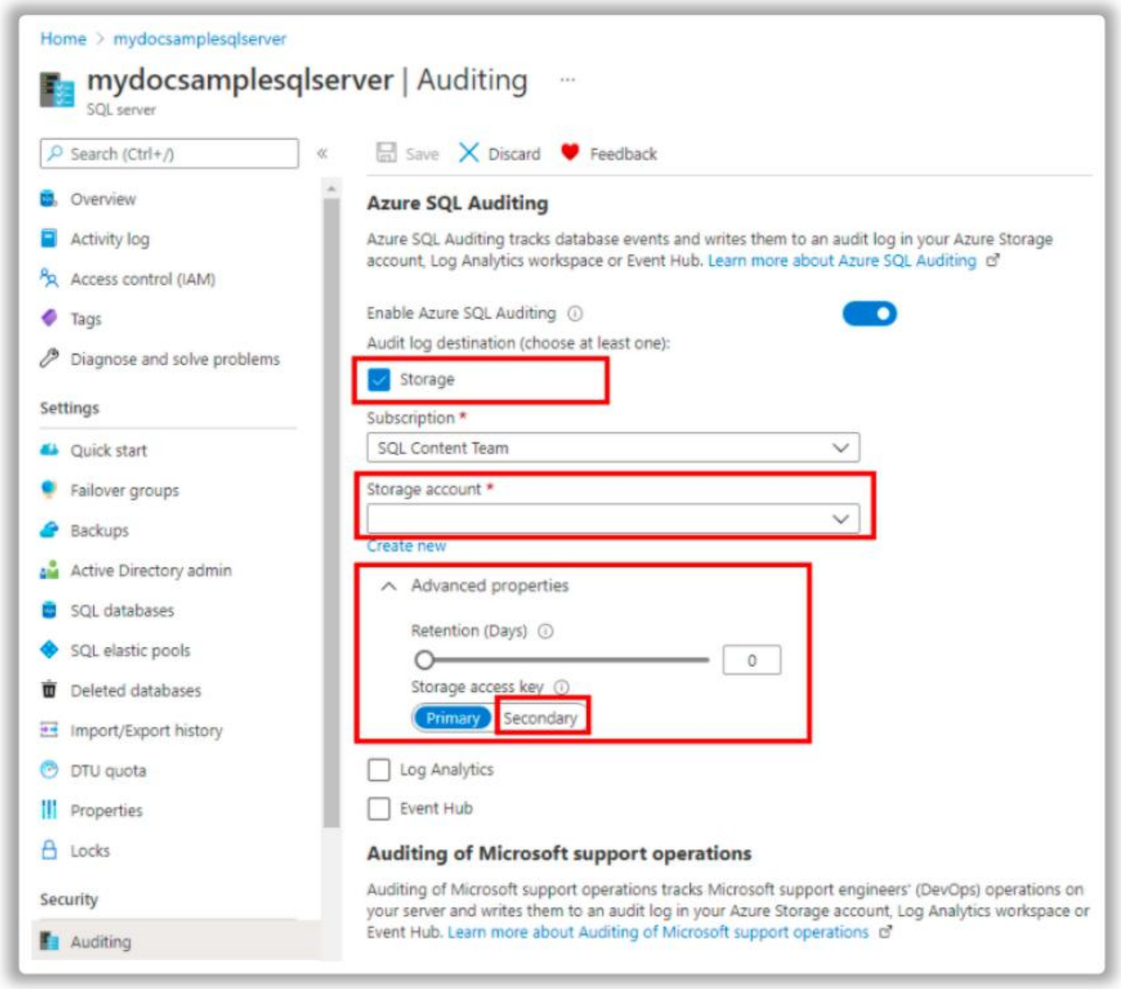


Figure 11.31: Storage Key Regeneration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the Storage Configuration page, click on the button next to key 1.

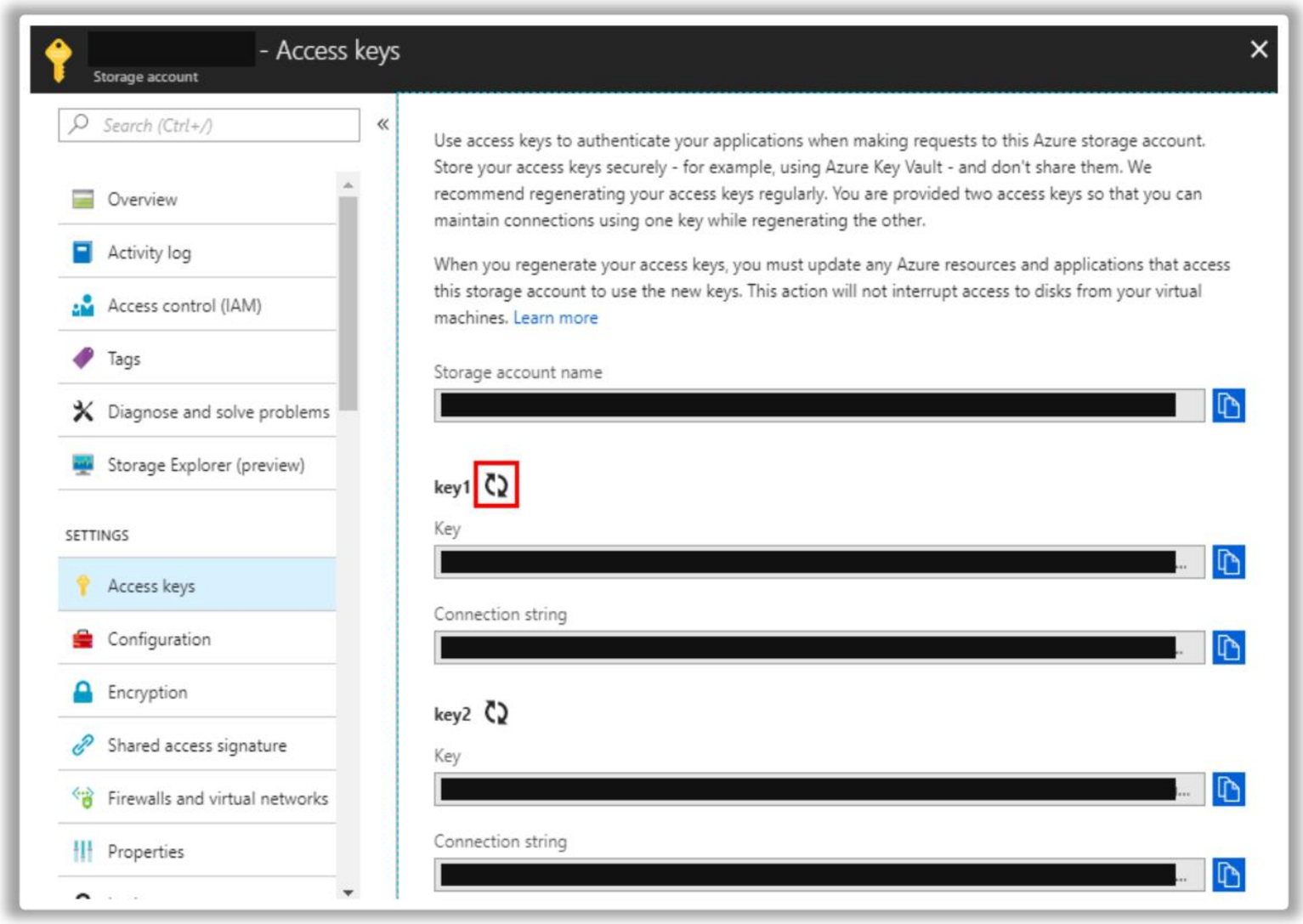
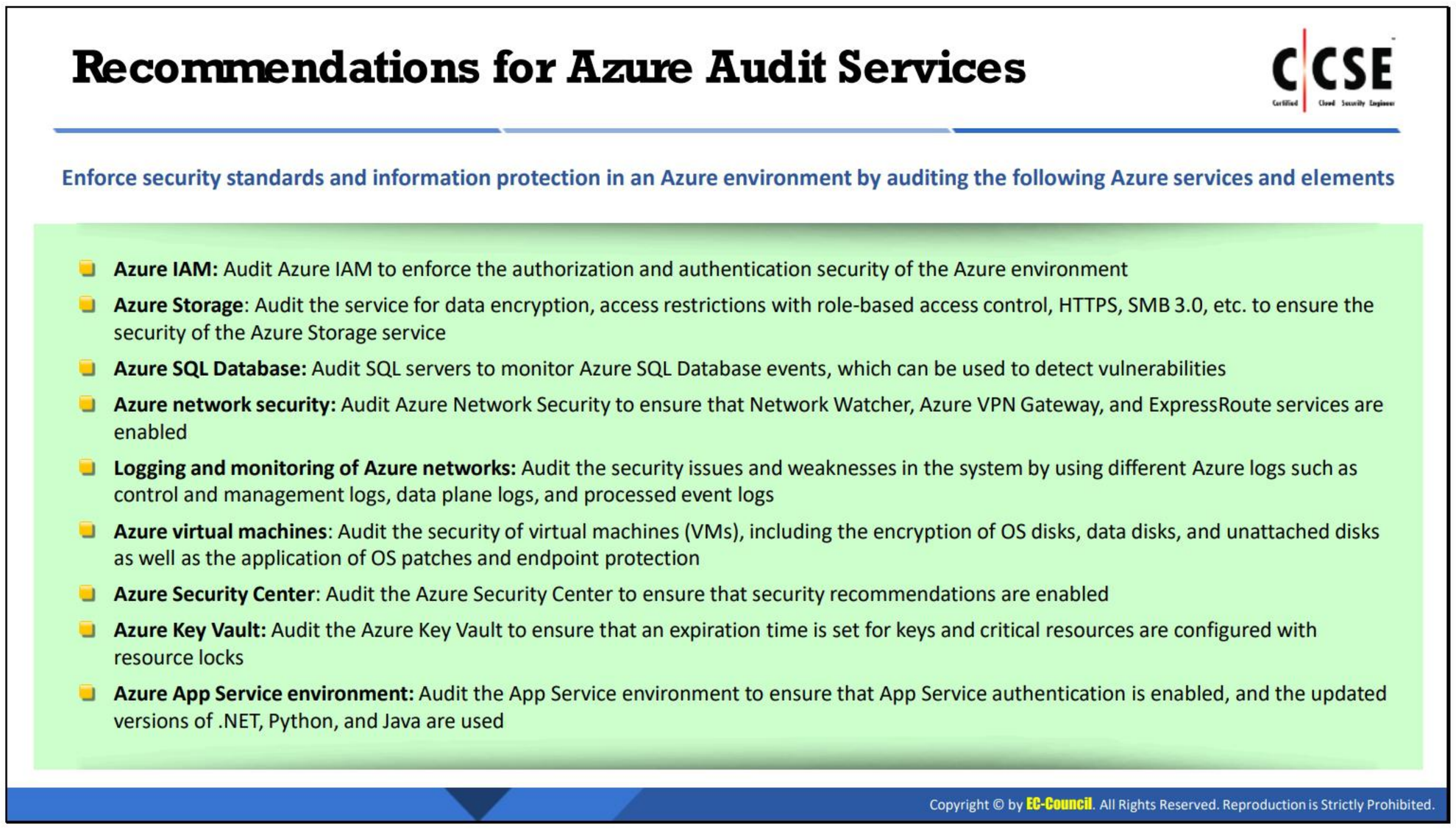


Figure 11.32: Storage Configuration Page

- Navigate to the **Auditing Configuration** page.
- Toggle the **Storage Access Key** to **Primary**.
- Click **OK**.
- Click on **Save.**
- Navigate to the **Storage Configuration** page.
- Click on the button next to **key 2**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recommendations for Azure Audit Services

Conduct an audit of the following Azure services to ensure the overall security of the Azure environment.

hade01.ir

- **Azure IAM**: Audit Azure IAM to enforce the authorization and authentication security of the Azure environment
- **Azure Storage**: Audit the service for data encryption, access restrictions with role-based access control, HTTPS, SMB 3.0, etc. to ensure the security of the Azure Storage service
- **Azure SQL Database**: Audit SQL servers to monitor Azure SQL Database events, which can be used to detect vulnerabilities
- **Azure Network Security**: Audit Azure Network Security to ensure that Network Watcher, Azure VPN Gateway, and ExpressRoute services are enabled
- **Logging and Monitoring of Azure Networks**: Audit the security issues and weaknesses in the system by using different Azure logs such as control and management logs, data plane logs, and processed event logs
- **Azure Virtual Machines**: Audit the security of virtual machines (VMs), including the encryption of OS disks, data disks, and unattached disks as well as the application of OS patches and endpoint protection
- **Azure Security Center**: Audit the Azure Security Center to ensure that security recommendations are enabled
- **Azure Key Vault**: Audit the Azure Key Vault to ensure that an expiration time is set for keys and critical resources are configured with resource locks

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Azure App Service Environment**: Audit the App Service environment to ensure that App Service authentication is enabled, and the updated versions of .NET, Python, and Java are used

Following are the Recommendations for Auditing Azure Services

- **Azure IAM**
  - Enable multi-factor authentication (MFA) for all users with privileged and non-privileged roles.
  - Do not create custom subscription owner roles in the Azure environment.
  - Do not create guest users unless necessary.
  - Prohibit users from auto-filling MFA passwords.
  - Alert users if passwords are reset.
  - Deny the creation of custom owner roles with subscription ownership.
  - Deny access to Azure Active Directory Portal for non-administrators.
  - Assign administrators to create security groups and self-service groups.
  - Disable self-service group management.
- **Azure Storage**
  - Encrypt the data in transit by allowing only HTTPS connections to access Azure Storage.
  - Disable anonymous access to Azure Blob containers.
  - Disable default network access rules.
  - Implement the circular shifting of keys.
  - Enable logging for successful and failed access requests to Azure Storage.
- **Azure SQL Database**
  - Enable all types of threat detection on SQL servers.
  - Allow security alerts to be received by admins and co-admins.
  - Encrypt the data at rest.
  - Enable SSL connections.
- **Azure Network Security**
  - Block direct RDP and SSH access from the Internet to network security groups.
  - Block access from 0.0.0.0 (any IP) for Azure SQL databases.
  - Configure Network Watcher to find issues with a private network.
  - Enable Azure VPN Gateway to establish a secure connection.

hidedl.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use ExpressRoute for creating private connections between data centers.

- **Logging and Monitoring of Azure Networks**
  - Monitor the three different types of Azure logs.
    - Control and management logs
    - Data plane logs
    - Processed event logs
  - Configure a log profile and perform the following steps.
    - Export activity logs.
    - Export all activities from the control and management plane.
    - Deny public access to the storage account container.
  - Create activity log alerts for the following events.
    - Creation of policy assignments
    - Create, update, and delete events of the following:
      - Network security group
      - Network security group rules
      - SQL server firewall rules

hide01.ir

- **Azure Virtual Machines**
  - Prevent unauthorized access by encrypting OS disks and data disks.
  - Secure sensitive information by encrypting unattached disks.
  - Apply the latest patches and endpoint protection for all VMs.

- **Azure Security Center**
  - Evaluate the overall security posture of Azure Security Center using the feature "Quickly assess your security posture with Secure Center."
  - Allow the automatic provisioning of the monitoring environment.
  - Enable the following recommendations:
    - System update
    - OS vulnerability recommendations
    - Endpoint protection
    - Disk encryption
    - Storage encryption
    - SQL auditing

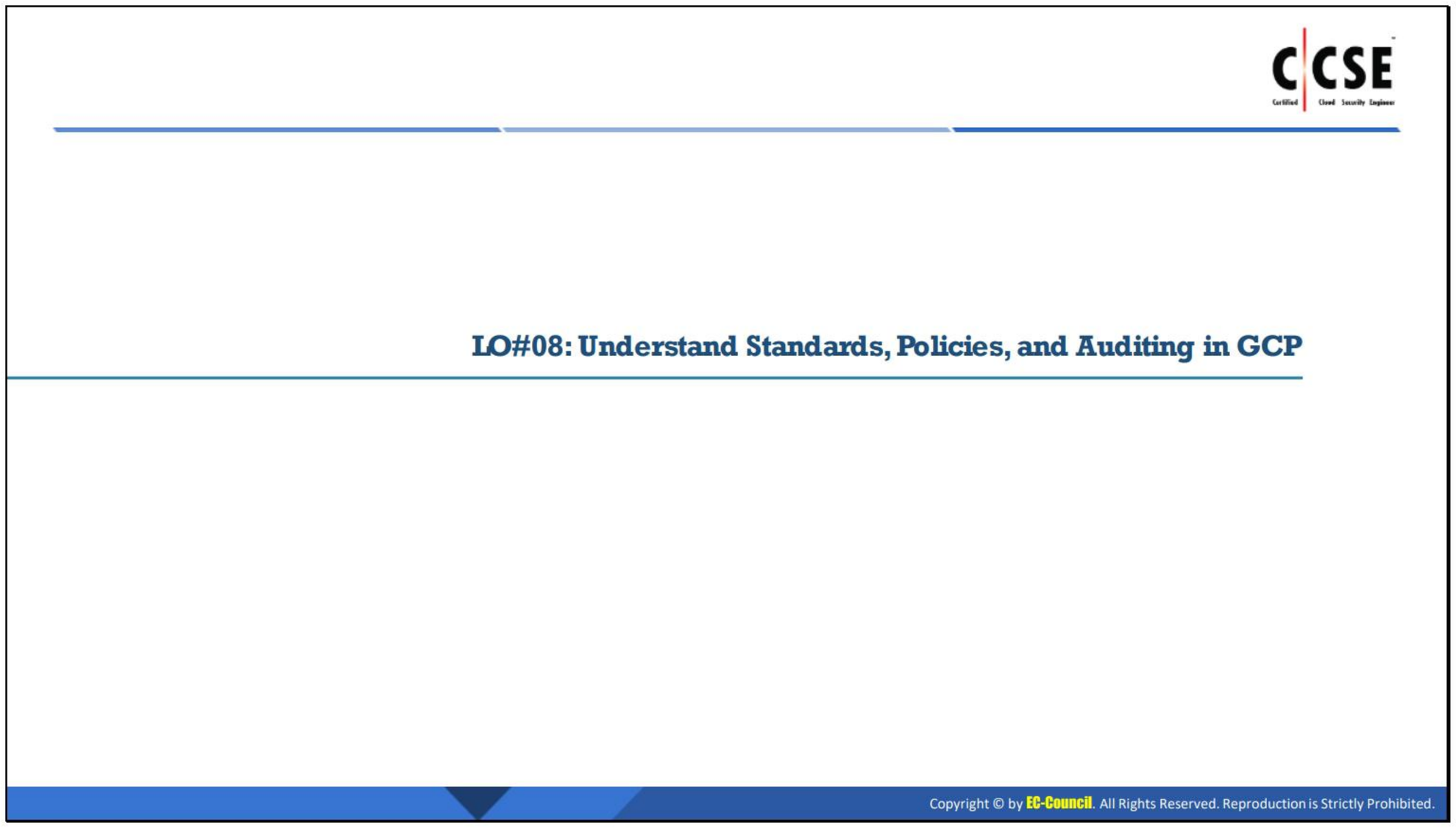
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

        - SQL encryption
    - Provide an email and a contact number to be informed of security events.

- **Azure App Service Environment**
    - Enable App Service authentication.
    - Configure HTTPS traffic for web applications.
    - Ensure that the web applications have the latest Transport Layer Security (TLS) encryption standards.
    - Use updated versions of .NET Framework, Java, and Python for web-application development.

hide01.ir

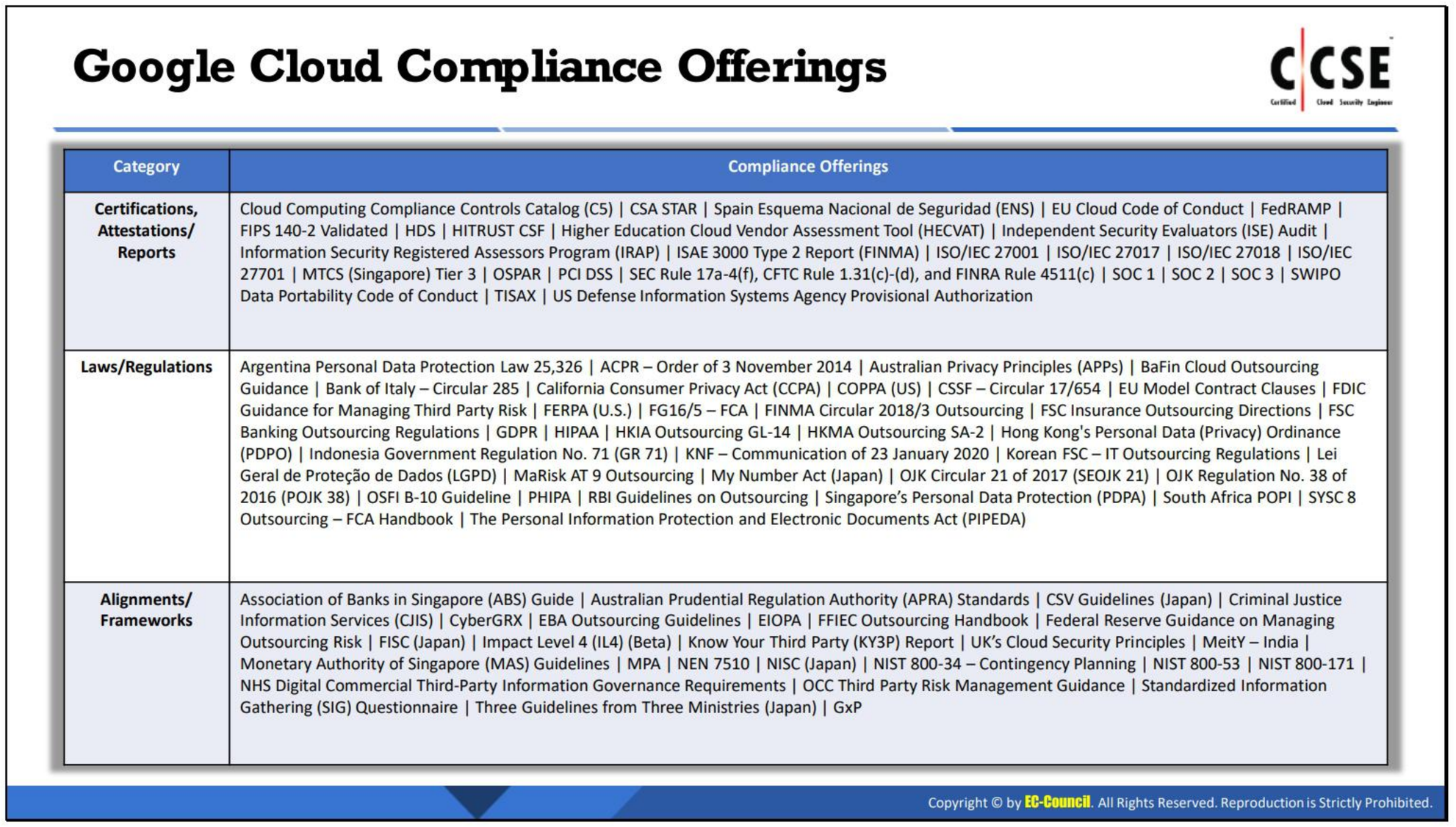
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#08: Understand Standards, Policies, and Auditing in GCP

An organization adopting Google Cloud Platform (GCP) should be well-versed with the standards and policies as well as auditing processes in GCP to meet compliance requirements. This section explains Google Cloud compliance offerings, GCP Audit Logs, how to conduct audits in Google with Cloud Audit Logs, and the best practices to be followed for Cloud Audit Logs, which will help an organization maintain compliance in the Google Cloud environment.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Google Cloud Compliance Offerings

Google Cloud is compliant with the data, privacy, and network policies of different countries. Using the compliance offerings of GCP, the user can ensure that they meet the policy and regulatory requirements required for their business. GCP services undergo the regular verification of security and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance.

GCP Compliance Offerings

***Source**: https://cloud.google.com/*

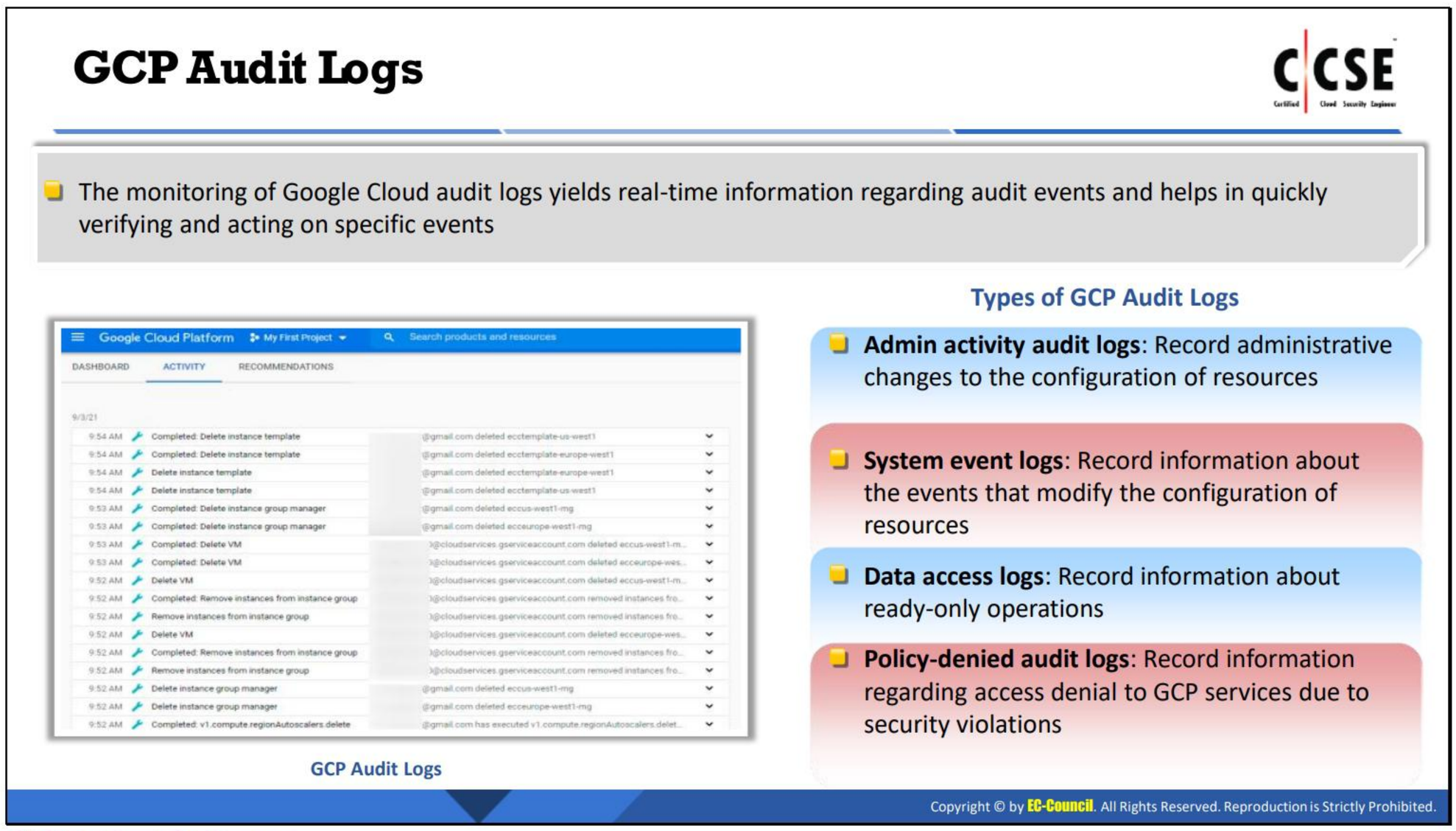
Category	Compliance Offerings
Certifications, Attestations/Reports	Cloud Computing Compliance Controls Catalog (C5) | CSA STAR | Spain Esquema Nacional de Seguridad (ENS) | EU Cloud Code of Conduct | FedRAMP | FIPS 140-2 Validated | HDS | HITRUST CSF | Higher Education Cloud Vendor Assessment Tool (HECVAT) | Independent Security Evaluators (ISE) Audit | Information Security Registered Assessors Program (IRAP) | ISAE 3000 Type 2 Report (FINMA) | ISO/IEC 27001 | ISO/IEC 27017 | ISO/IEC 27018 | ISO/IEC 27701 | MTCS (Singapore) Tier 3 | OSPAR | PCI DSS | SEC Rule 17a-4(f), CFTC Rule 1.31(c)-(d), and FINRA Rule 4511(c) | SOC 1 | SOC 2 | SOC 3 | SWIPO Data Portability Code of

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Conduct | TISAX | US Defense Information Systems Agency Provisional Authorization
Laws/Regulations	Argentina Personal Data Protection Law 25,326 | ACPR – Order of 3 November 2014 | Australian Privacy Principles (APPs) | BaFin Cloud Outsourcing Guidance | Bank of Italy – Circular 285 | California Consumer Privacy Act (CCPA) | COPPA (US) | CSSF – Circular 17/654 | EU Model Contract Clauses | FDIC Guidance for Managing Third Party Risk | FERPA (U.S.) | FG16/5 – FCA | FINMA Circular 2018/3 Outsourcing | FSC Insurance Outsourcing Directions | FSC Banking Outsourcing Regulations | GDPR | HIPAA | HKIA Outsourcing GL-14 | HKMA Outsourcing SA-2 | Hong Kong's Personal Data (Privacy) Ordinance (PDPO) | Indonesia Government Regulation No. 71 (GR 71) | KNF – Communication of 23 January 2020 | Korean FSC – IT Outsourcing Regulations | Lei Geral de Proteção de Dados (LGPD) | MaRisk AT 9 Outsourcing | My Number Act (Japan) | OJK Circular 21 of 2017 (SEOJK 21) | OJK Regulation No. 38 of 2016 (POJK 38) | OSFI B-10 Guideline | PHIPA | RBI Guidelines on Outsourcing | Singapore's Personal Data Protection (PDPA) | South Africa POPI | SYSC 8 Outsourcing – FCA Handbook | The Personal Information Protection and Electronic Documents Act (PIPEDA)
Alignments/ Frameworks	Association of Banks in Singapore (ABS) Guide | Australian Prudential Regulation Authority (APRA) Standards | CSV Guidelines (Japan) | Criminal Justice Information Services (CJIS) | CyberGRX | EBA Outsourcing Guidelines | EIOPA | FFIEC Outsourcing Handbook | Federal Reserve Guidance on Managing Outsourcing Risk | FISC (Japan) | Impact Level 4 (IL4) (Beta) | Know Your Third Party (KY3P) Report | UK's Cloud Security Principles | MeitY – India | Monetary Authority of Singapore (MAS) Guidelines | MPA | NEN 7510 | NISC (Japan) | NIST 800-34 – Contingency Planning | NIST 800-53 | NIST 800-171 | NHS Digital Commercial Third-Party Information Governance Requirements | OCC Third Party Risk Management Guidance | Standardized Information Gathering (SIG) Questionnaire | Three Guidelines from Three Ministries (Japan) | GxP

Table 11.4: GCP Compliance Offerings

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GCP Audit Logs

GCP audit logs can be used to maintain audit trails of all GCP activities, which help the security, auditing, and compliance teams. All the administrative activities can be stored on a continuously available and highly secure audit trail, which cannot be disabled.

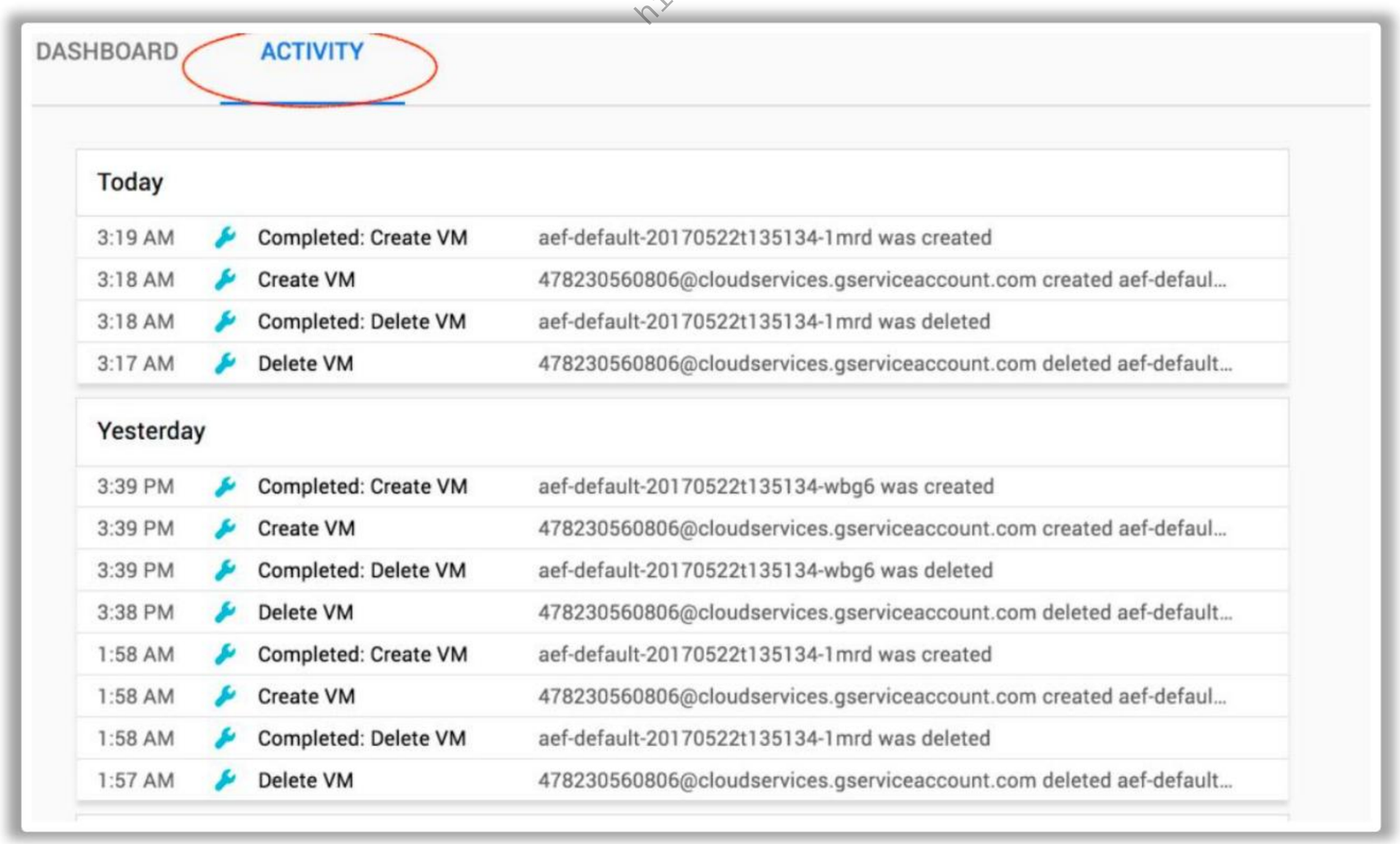


Figure 11.33: GCP Audit Logs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the types of audit logs recorded by GCP projects.

- **Admin Activity Audit Logs**

  Admin activity audit logs are enabled by default, and they record administrative changes to the configuration of resources. Cloud audit logs have a retention period of 400 days, and the following audit logs related to admin activity are recorded in GCP:

  - Creating, updating, and patching resources
  - Configuration or change of tags, labels, metadata, and permissions
  - Configuration or change of resource properties
  - Events that modify the configuration and metadata of resources

- **System Event Logs**

  System event logs contain information about the events that modify the configuration of resources, and they are enabled by default. The retention period for system event logs is 400 days. System event logs record the following:

  - Maintenance operations
  - Instance reset
  - Automatic restart
  - Instance pre-emption
  - Serial port connection/disconnection

hade01.ir

- **Data Access Logs**

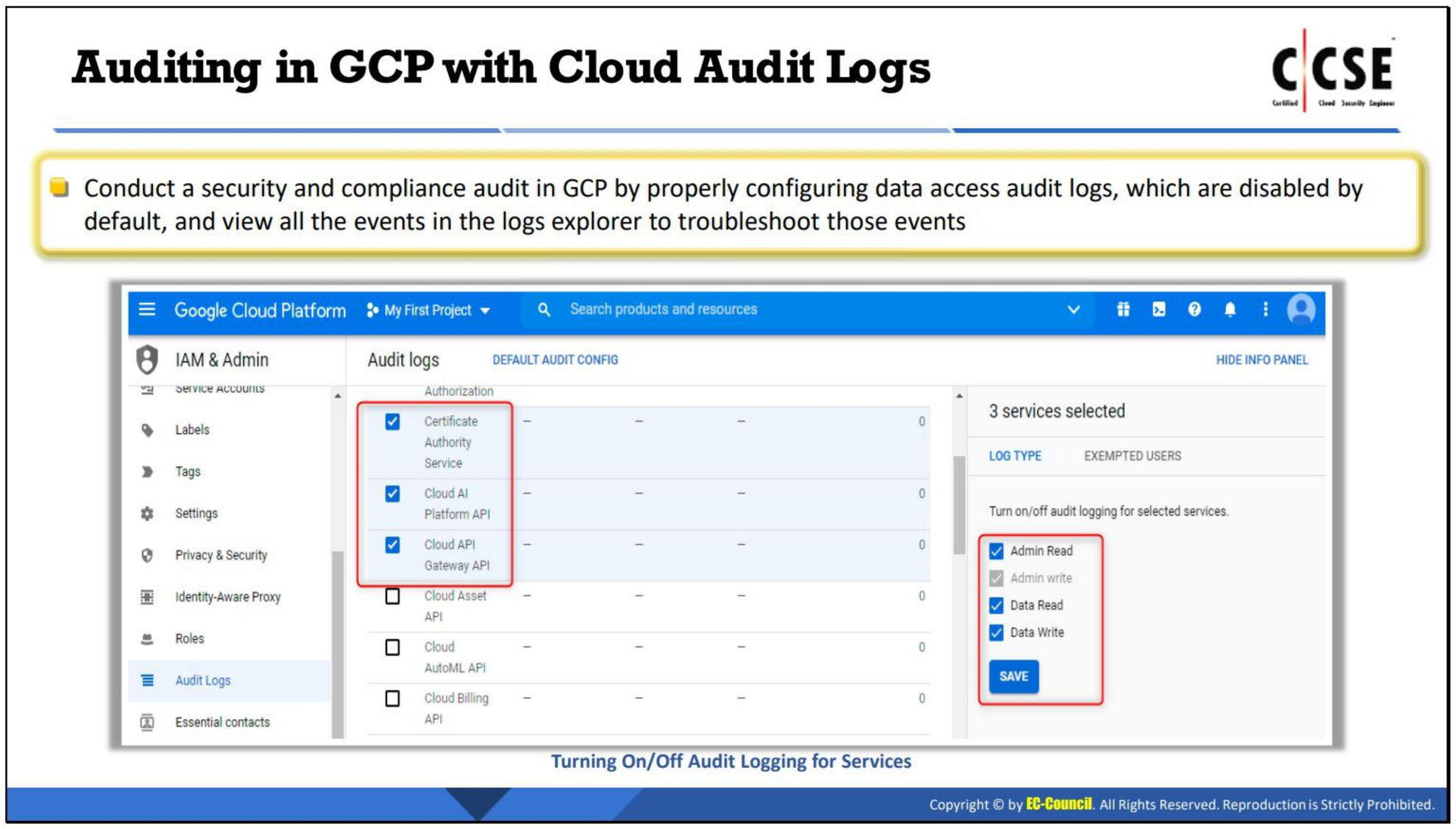
  Data access audit logs are disabled by default, and they record information about ready-only operations. The retention period for cloud data access logs is 30 days, and there are three types of such access logs.

  - **Admin read**: Records logs regarding service or configuration metadata
  - **Data read**: Records logs regarding the reads of data within a service
  - **Data write: Records logs regarding the writes of data to a service**

- **Policy-denied Audit logs**

  Policy-denied audit logs record information regarding the denial of access to GCP services due to security violations; they are enabled by default.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Auditing in GCP with Cloud Audit Logs

Cloud audit logs, which collect admin access logs, data access audit logs, system event audit logs, and policy-denied audit logs, should be configured properly to gain insights into security events and perform actions on them. Admin access audit logs, system event audit logs, and policy-denied audit logs are enabled by default and cannot be configured or disabled. Data access audit logs need to be enabled explicitly.

The following are the steps to conduct audits with cloud audit logs

- **Step 1: Enable Data Access Audit Logs**
  - Navigate to **IAM & Admin** and select **Audit Logs** in the console.

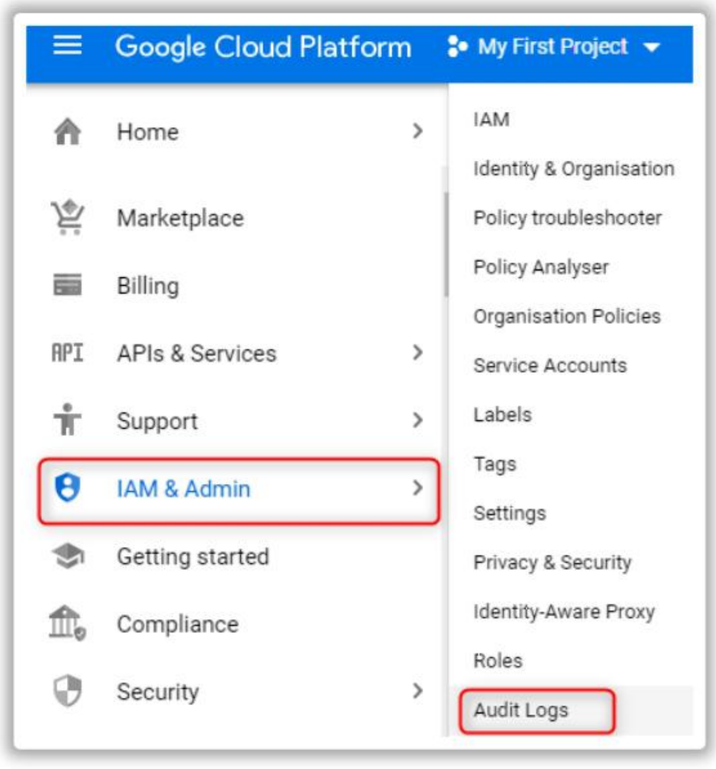


Figure 11.34: Selecting Audit Logs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the existing GCP project at the top of the Audit Logs page.

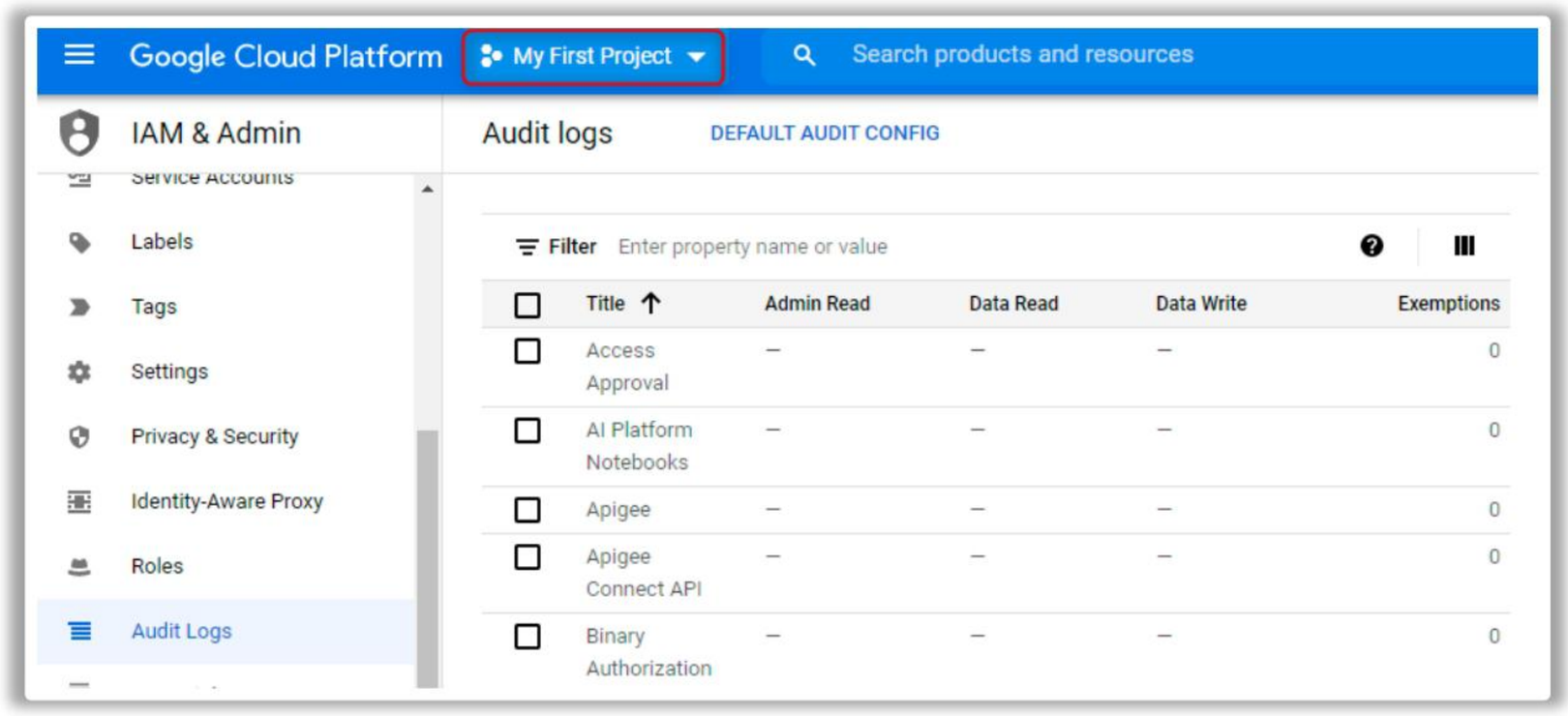


Figure 11.35: Selecting the Existing GCP Project

- In the table of Audit Logs page, select the Google Cloud services for logging data access audit logs.
- Under Log Type tab on the right, enable the different types of data access audit logs.
- Click **Save.**

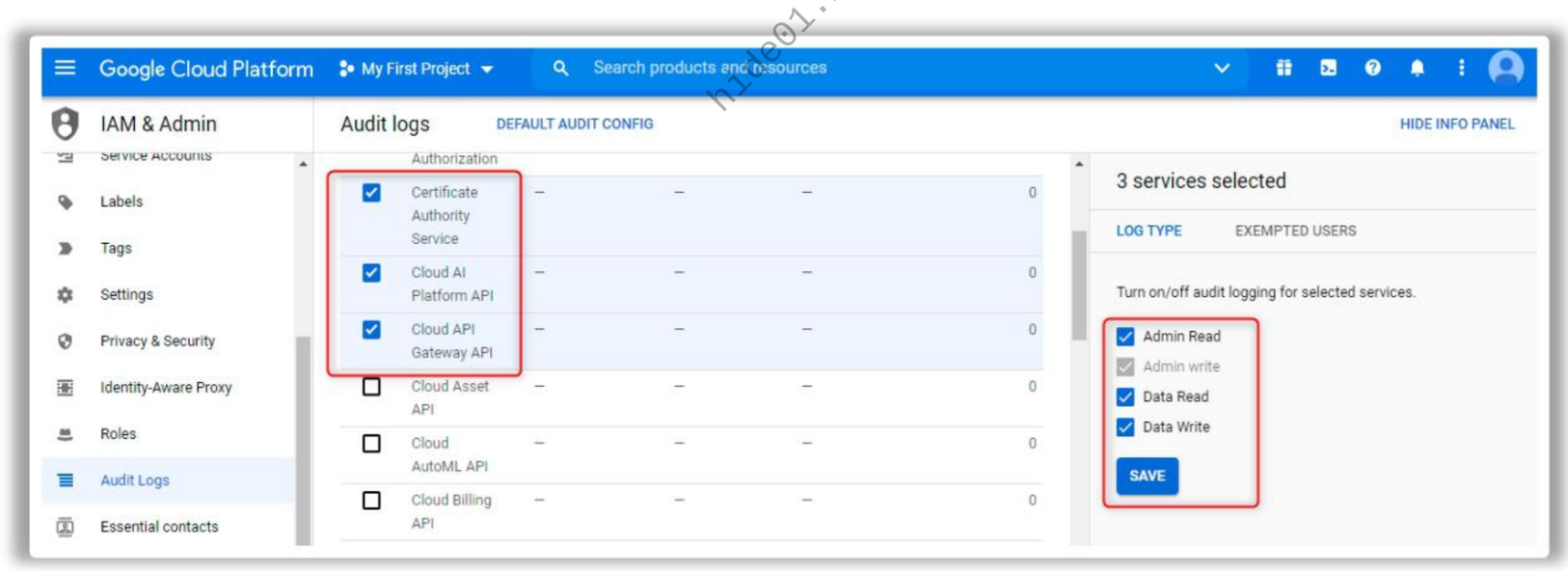


Figure 11.36: Audit Logs Window

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2: Viewing Audit Logs for Conducting Audits**
  - Navigate to Logging and click on Logs Explorer in the console.

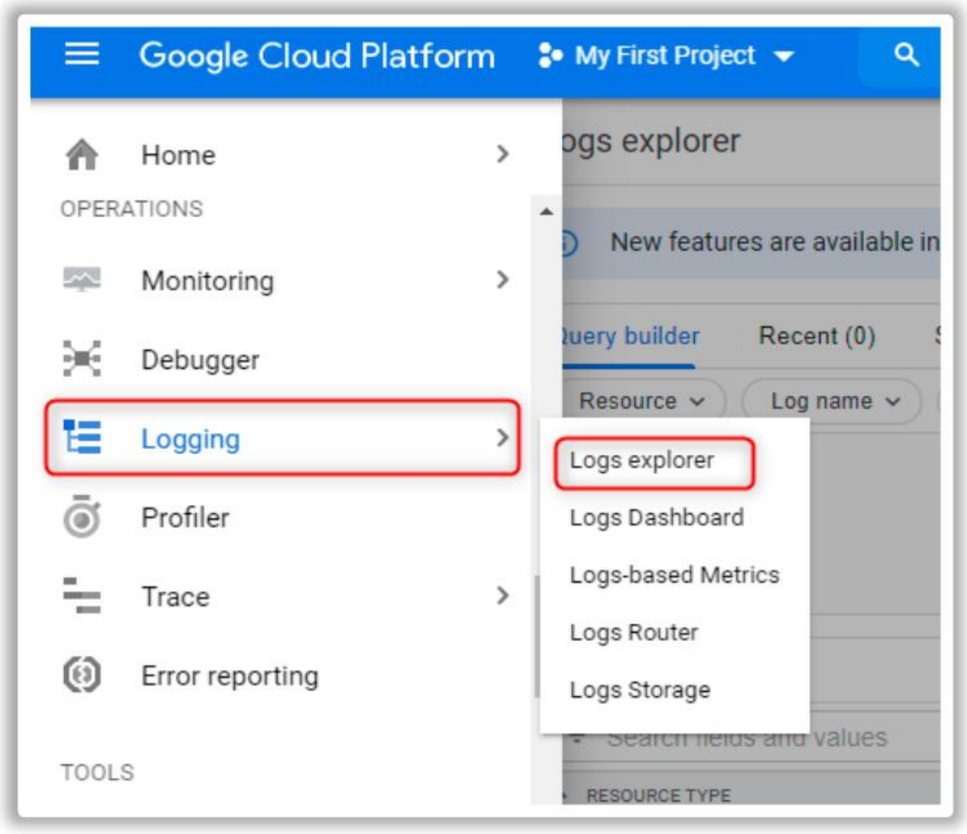


Figure 11.37: Selecting Log Explorer

  - Select the cloud project for which audit logs are to be viewed on the **Logs Explorer** page.

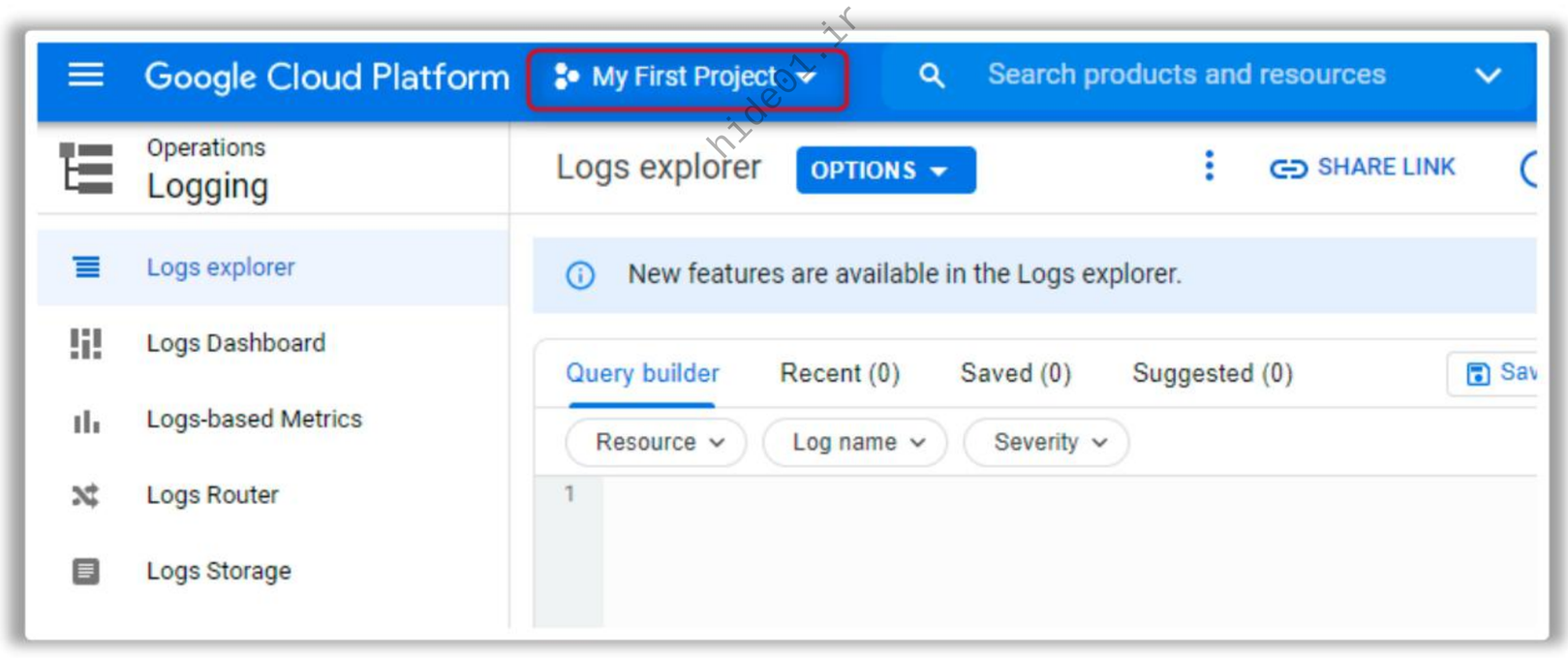


Figure 11.38: Viewing Audit Logs in Log Explorer Window

  - Under the Query Builder tab, do the following.
    - Under **Resource**, select the GCP resource type for which audit logs are to be viewed.
    - Under **Log Name**, select the type of audit log.
      - Select **activity** for viewing admin activity audit logs.
      - Select **data_access** for viewing data access audit logs.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select **system_event** for viewing system event audit logs.
- Select **policy** for viewing policy-denied audit logs.

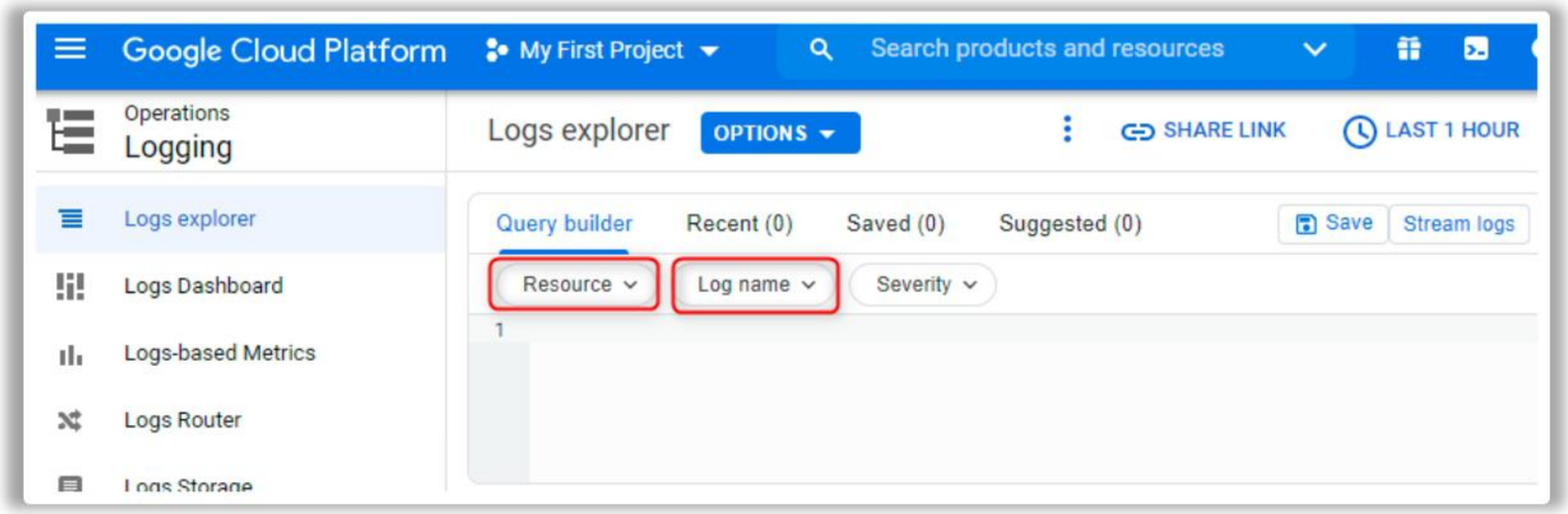
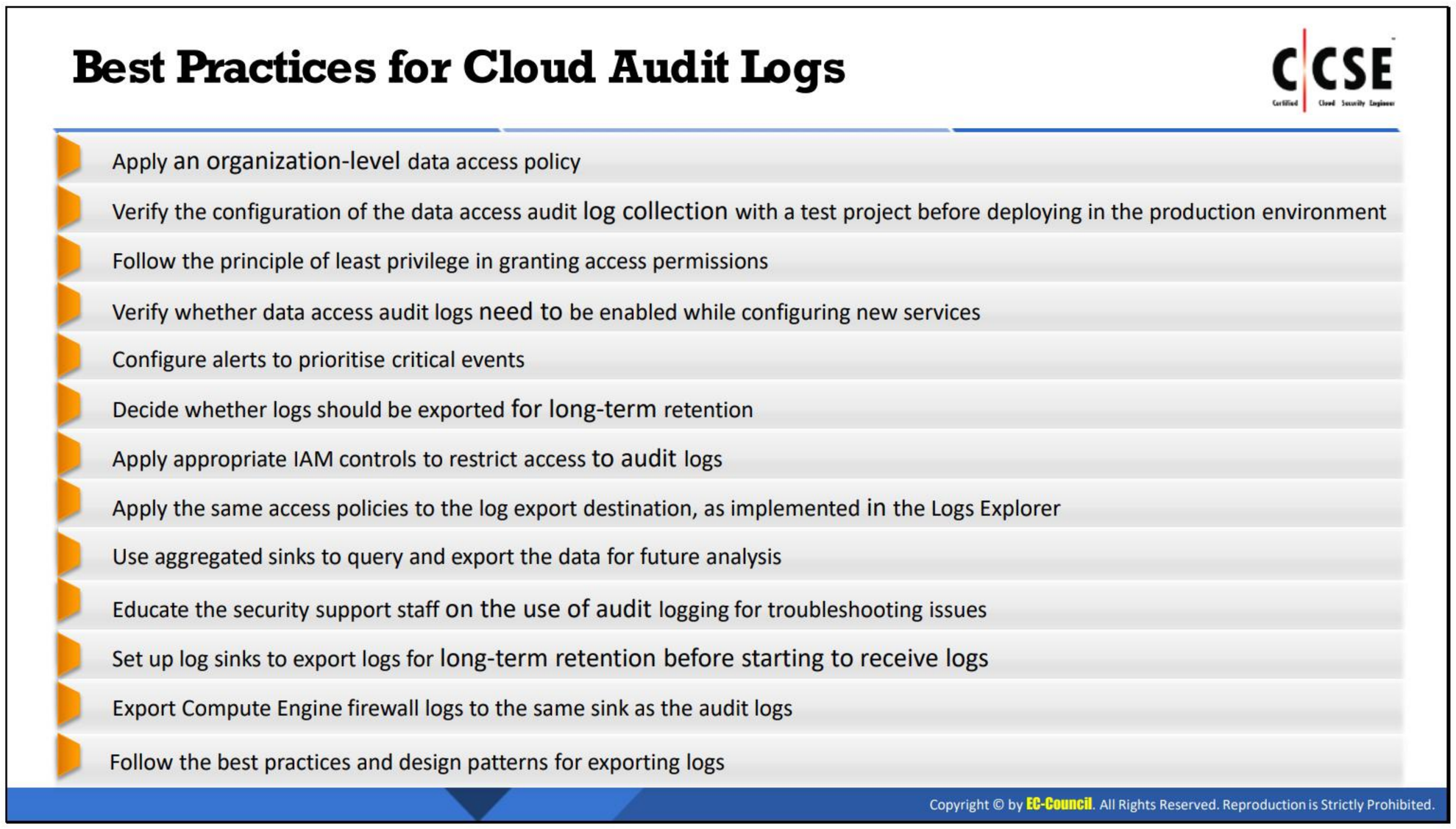


Figure 11.39: Query Builder Tab in Log Explorer Window

hide01.ir

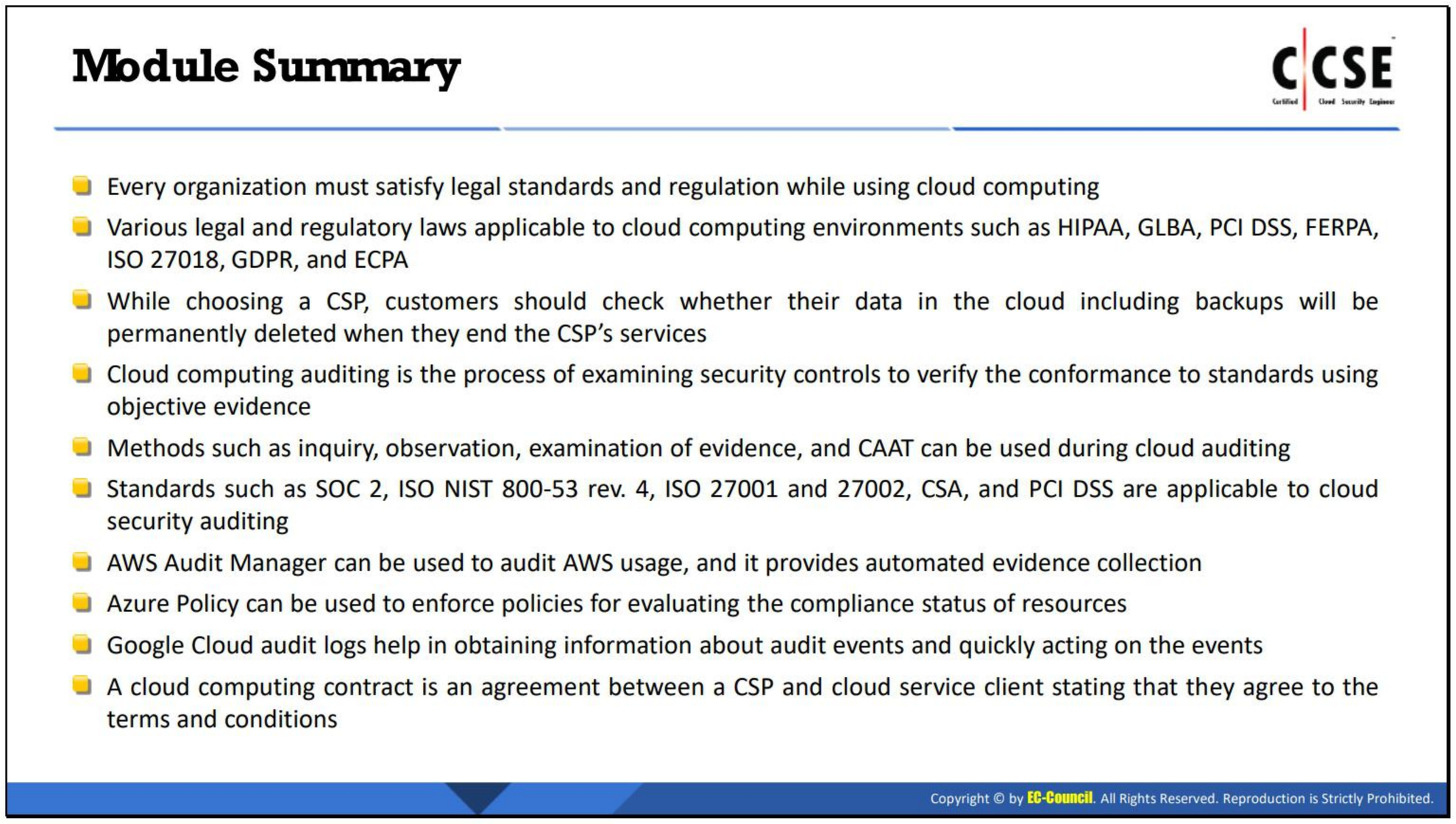
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for Cloud Audit Logs

- Apply an organization-level data access policy.
- Verify the configuration of the data access audit log collection with a test project before deploying in the production environment.
- Follow the principle of least privilege in granting access permissions.
- Verify whether data access audit logs need to be enabled while configuring new services.
- Configure alerts to prioritize critical events.
- Decide whether logs should be exported for long-term retention.
- Apply appropriate IAM controls to restrict access to audit logs.
- Apply the same access policies to the log export destination, as implemented in the Logs Explorer.
- Use aggregated sinks to query and export the data for future analysis.
- Educate the security support staff on the use of audit logging for troubleshooting issues.
- Set up log sinks to export logs for long-term retention before starting to receive logs.
- Export Compute Engine firewall logs to the same sink as the audit logs.
- Follow the best practices and design patterns for exporting logs.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed various aspects related to policies, standards, and legal issues in the cloud. It covered various cloud security standards, cloud standard organizations, cloud computing audits, and internal audits. The module also discussed standards, auditing processes, and tools in Azure, GCP, and AWS. By the end of this module, cloud security engineers would be well-versed with the laws impacting cloud computing and the various standards and policies that could be useful for their organization's cloud ecosystem. Furthermore, the information in this module can help in preventing any legal issues related to the cloud, adhering to the cloud computing standards and policies, and securing the organization's cloud environment.

The following are the highlights of this module.

- Every organization must satisfy legal standards and regulations while using cloud computing.
- Various legal and regulatory laws are applicable to cloud computing environments such as HIPAA, GLBA, PCI DSS, FERPA, ISO 27018, GDPR, and ECPA.
- While choosing a CSP, customers should check whether their data in the cloud including backups will be permanently deleted when they end the CSP's services.
- Cloud computing auditing is the process of examining security controls to verify the conformance to standards using objective evidence.
- Methods such as inquiry, observation, examination of evidence, and CAAT can be used during cloud auditing.
- Standards such as SOC 2, ISO NIST 800-53 rev. 4, ISO 27001 and 27002, CSA, and PCI DSS are applicable to cloud security auditing.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- AWS Audit Manager can be used to audit AWS usage, and it provides automated evidence collection.
- Azure Policy can be used to enforce policies for evaluating the compliance status of resources.
- Google Cloud audit logs help in obtaining information about audit events and quickly acting on the events.
- A cloud computing contract is an agreement between a CSP and cloud service client stating that they agree to the terms and conditions.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.