EC-Council

CCSE™

Certified Cloud Security Engineer

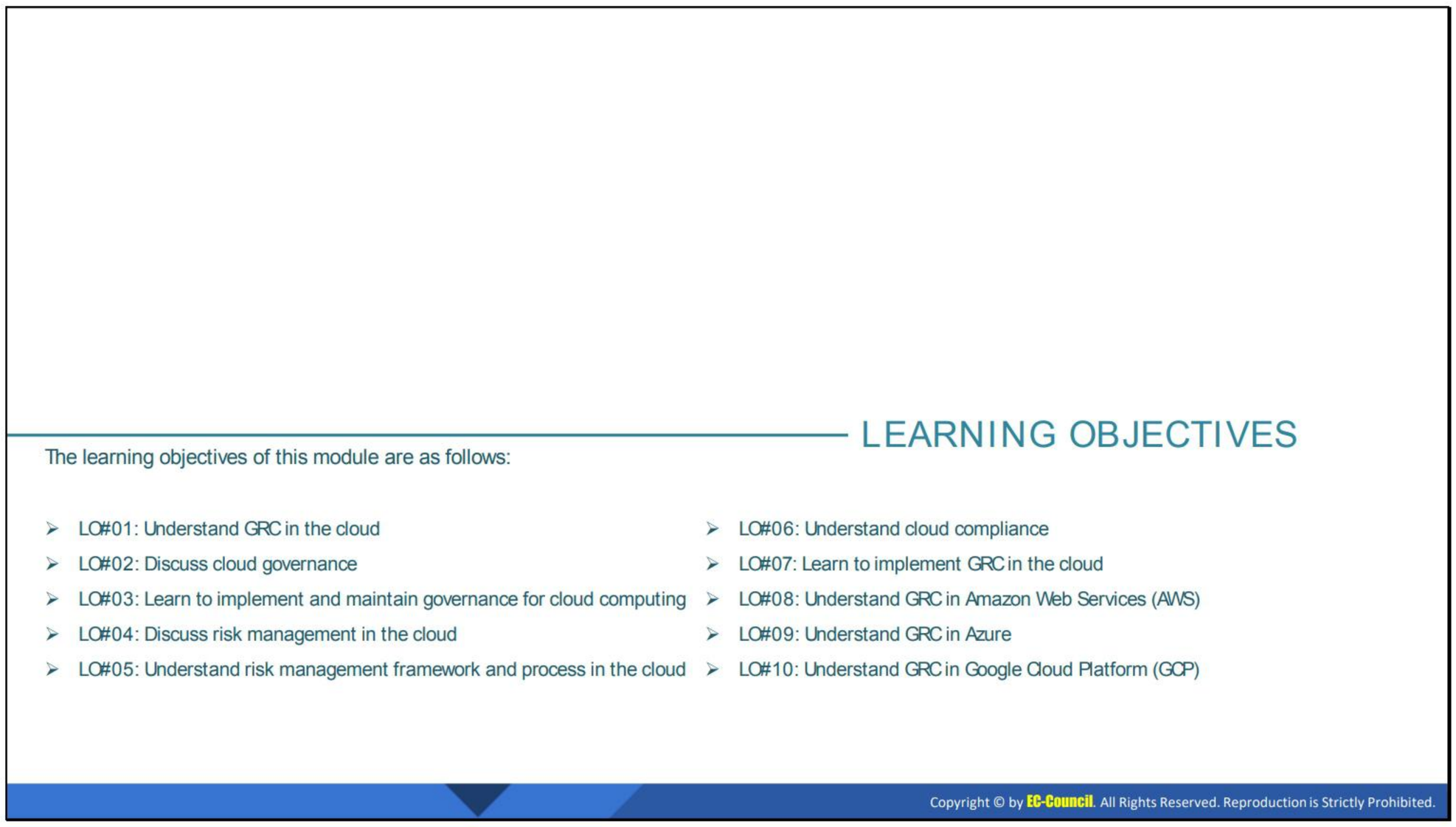


Governance, Risk management, and Compliance in Cloud

Module 10

This page is intentionally left blank.

hide01.ir

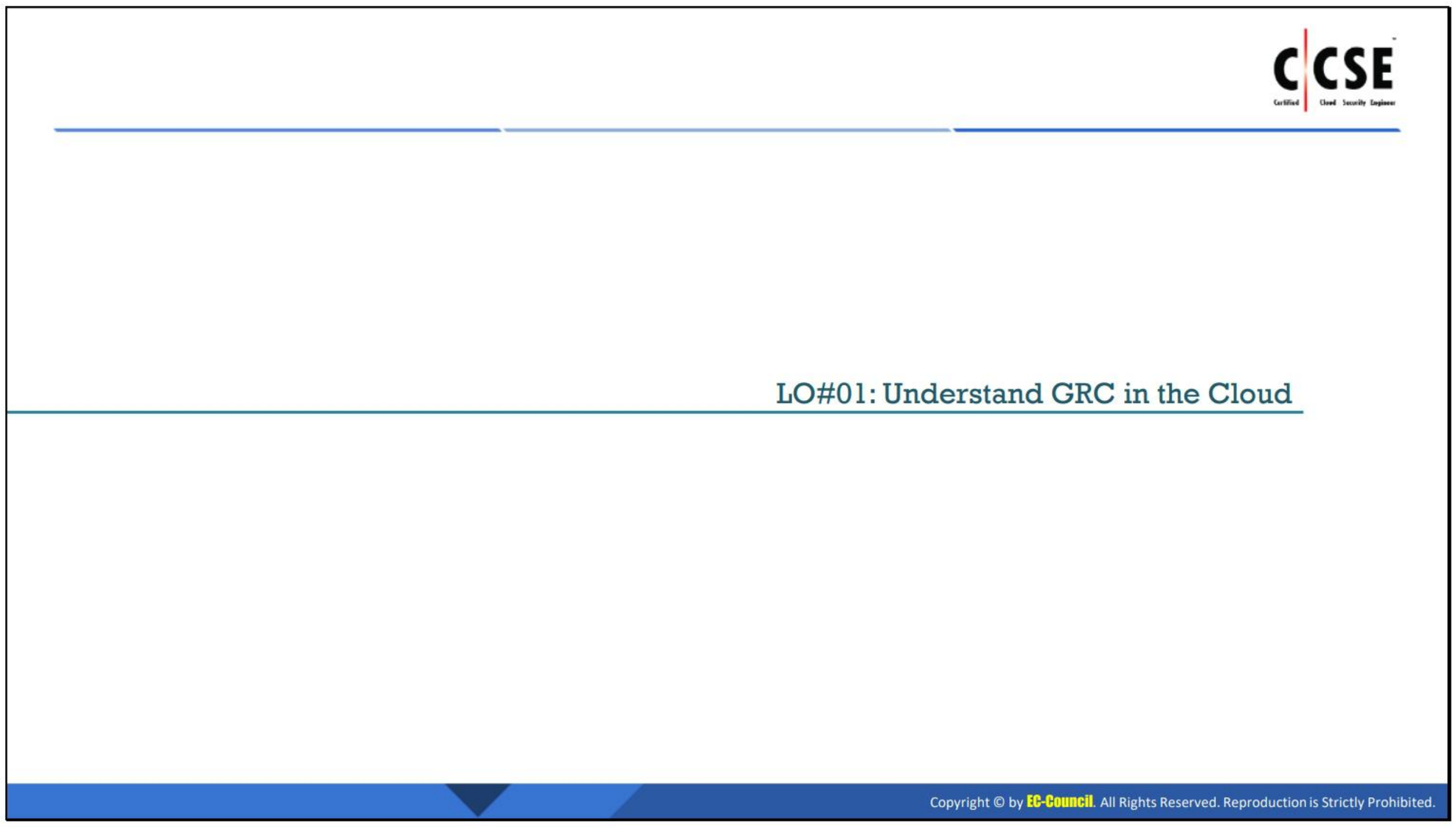


Learning Objectives

This module explains the importance of governance, risk, and compliance in the cloud to minimize the risks, improve the governance, and enhance the compliance of an organization. The module discusses various components of cloud governance, risk management, and cloud compliance, along with compilance and governance features and management tools provided by major cloud service providers (CSPs). The learning objectives of this module are as follows:

- Understand governance, risk management, and compliance (GRC) in the cloud
- Introduction to cloud governance
- Implementing and maintaining governance for cloud computing
- Risk management in the cloud
- Risk management framework and process in the cloud
- Understand cloud compliance
- Implementation of GRC in the cloud
- GRC in AWS
- GRC in Azure
- GRC in Google

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

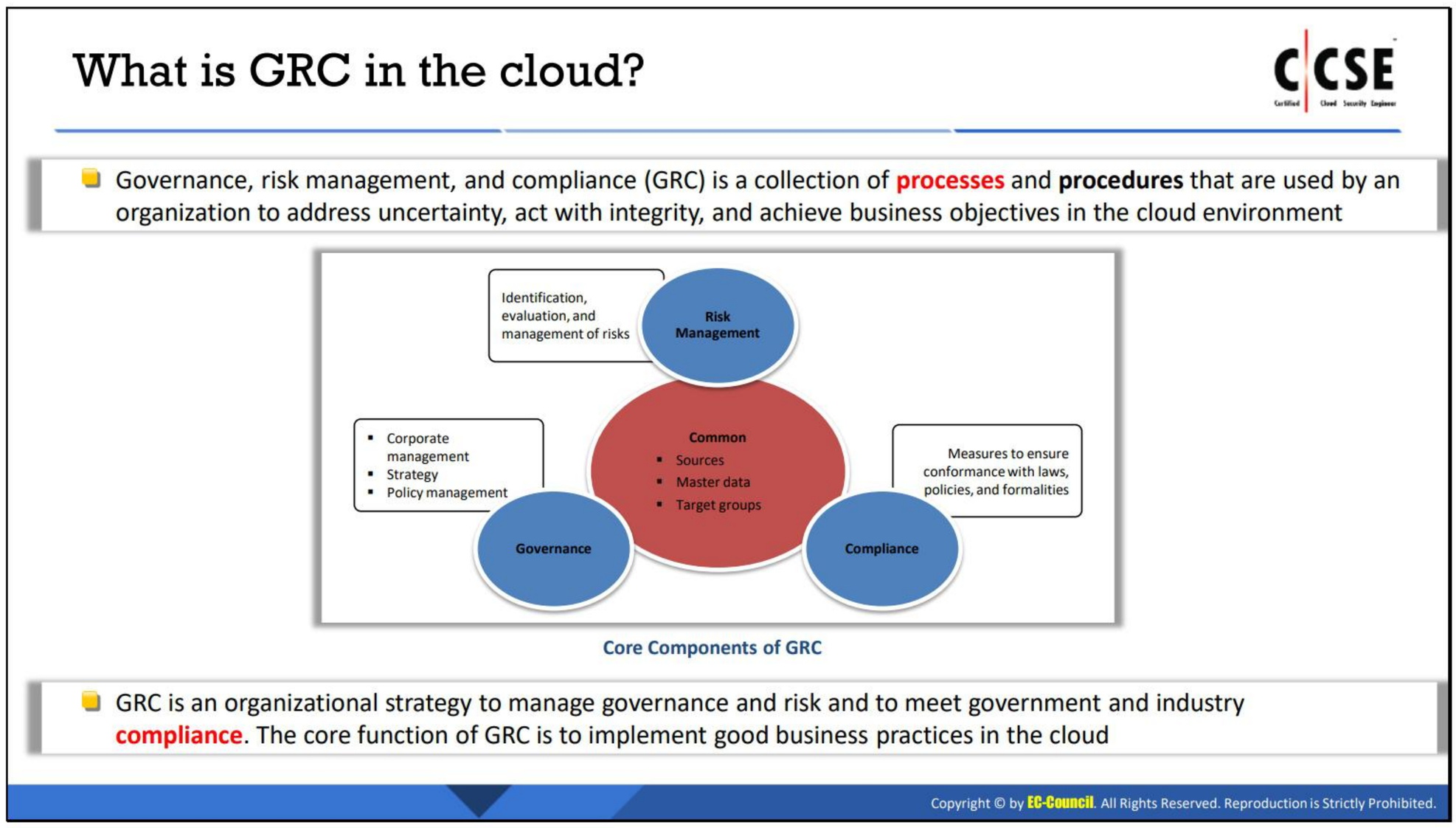


LO#01: Understand GRC in Cloud

The objective of this section is to understand the importance of governance, risk management, and compliance (GRC) to an organization. It highlights the usage of GRC tools, along with the benefits and recommendations of GRC in the cloud.

hidoo1.ir

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



What is GRC in the Cloud?

Governance, risk, and compliance (GRC) is a collection of processes and procedures that are used by an organization to address uncertainty, act with integrity, and achieve business objectives in the cloud environment. It is an organizational strategy to manage governance and risk and to ensure government and industry compliance. The core function of GRC is to implement good business practices in the cloud. With increase in the risks associated with the cloud, the demandfor GRC has grown from different perspectives. GRC spans various disciplines such as enterprise risk management, internal auditing, and compliance. With GRC, an organization can successfully manage security and IT risks, minimize costs, and fulfill compliance requirements. GRC also helps an organization in enhancing its performance and decision-making capabilities in a cloud environment.

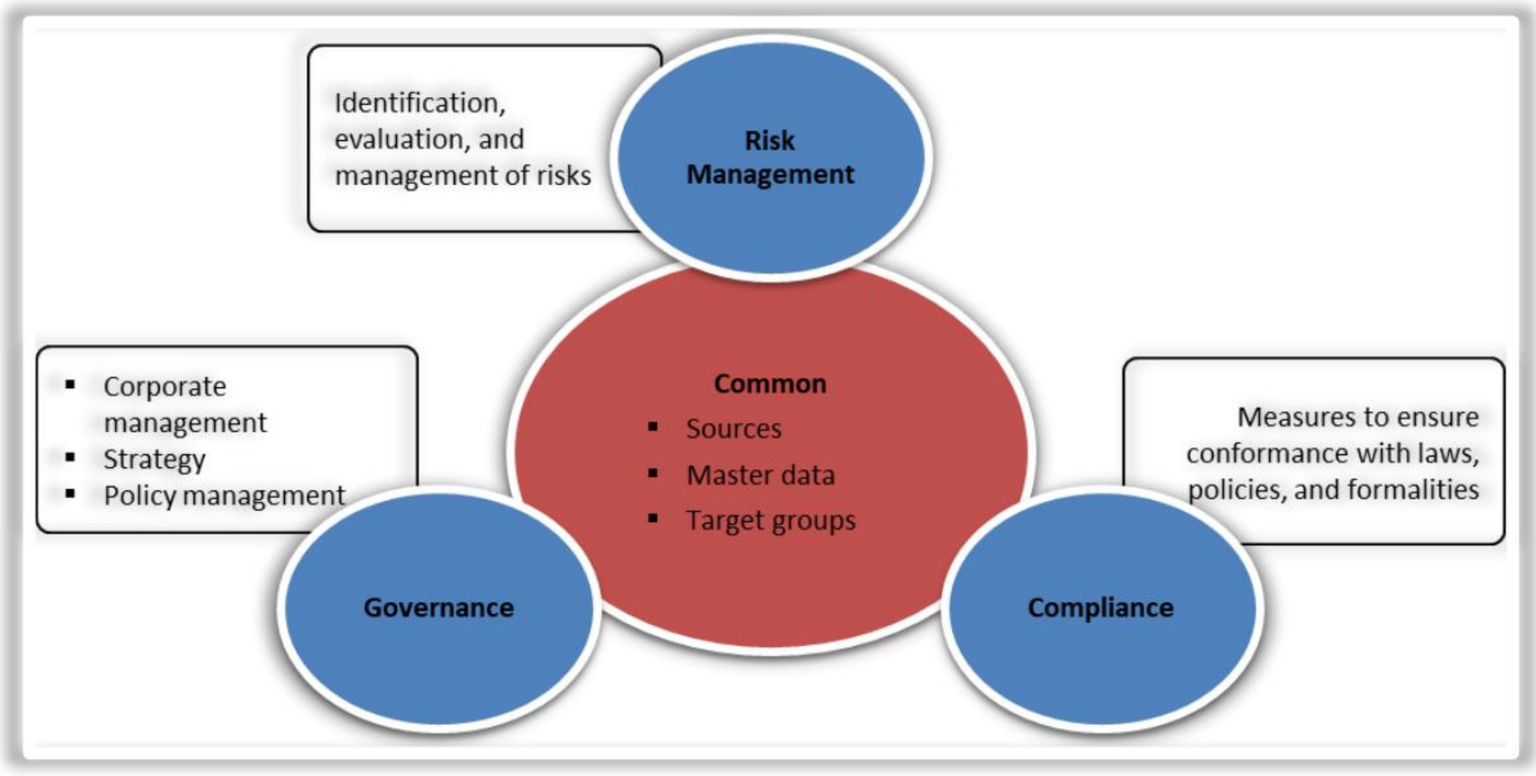


Figure 10.1: Core Components of GRC

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

The core components of GRC in the cloud are as follows.

Governance: Governance is defined as a collection of processes, rules, and policies used to ensure that corporate activities support business objectives. It consists of resource management, ethics, management controls, and accountability. It also ensures that the upper management can direct and control the activities occurring in the cloud environment at various levels of the organization as well as the business needs to support customer requirements and achieve the business objectives. Efficient governance can realize an environment in which employees feel empowered and the resources and behaviors are properly regulated and coordinated. An important goal of GRC is to bring balance to the interests of corporate stakeholders such as upper management, employees, investors, and suppliers. With efficient governance, the organization can achieve control on its cloud infrastructure and facilities such as data centers and manage applications at the portfolio level.

Risk Management: Risk management is the process of identifying, assessing, and responding to risks by implementing activities that control how the organization manages the potential risk. Risk management is prominent throughout the security lifecycle in the cloud. It is a continuous process of increasing complexity. Risk management requires anticipating risks and creating a plan to overcome the risk when it occurs. The type of risks varies among organizations, but all organizations working in cloud environments must prepare a risk management plan. Risk management helps in saving time, money, and effort.

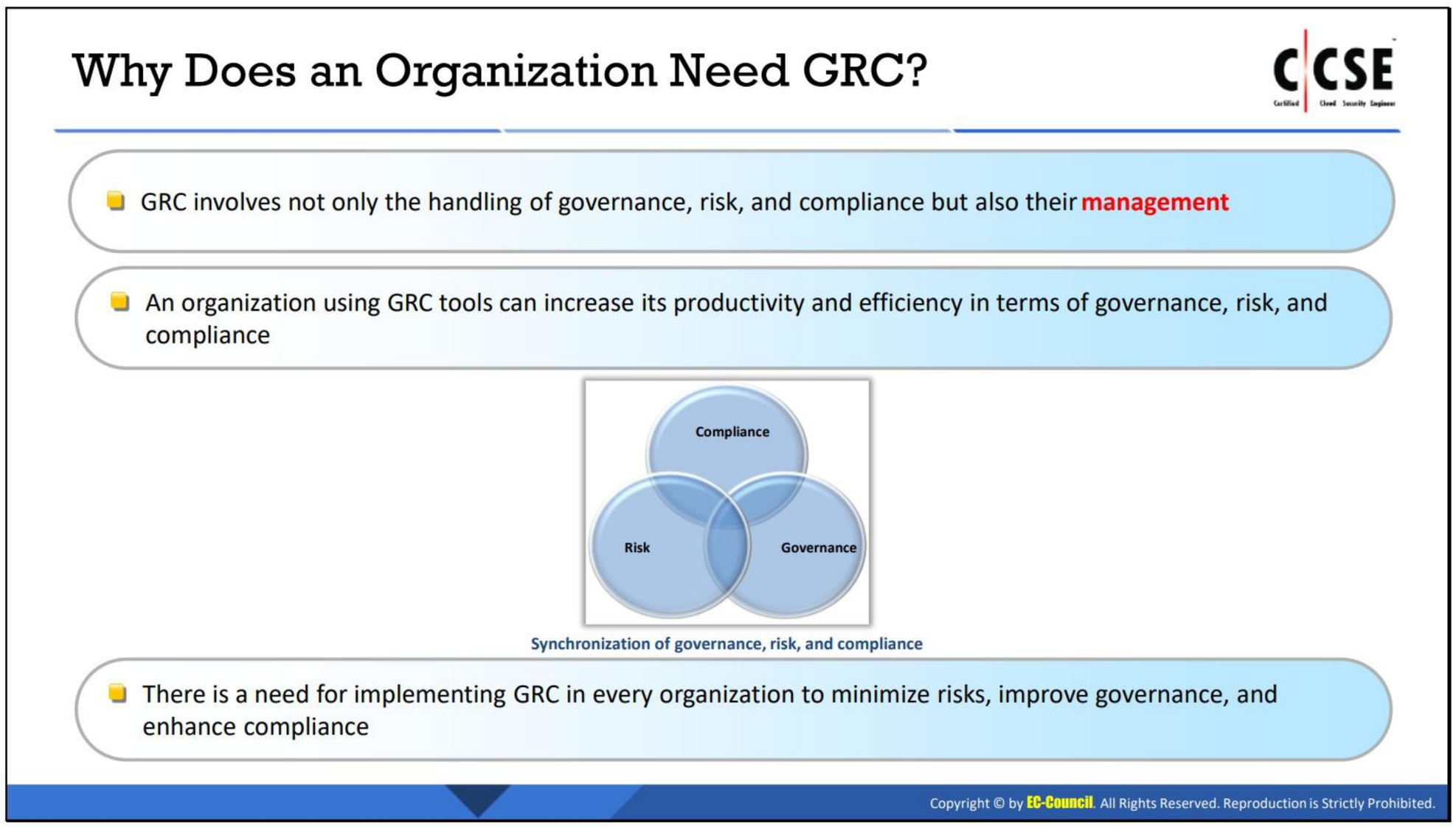
Risk management provides a structured approach to identifying risks. A clear idea of all risks allows an organization to analyze, prioritize, and take appropriate actions to reduce losses in the cloud. Furthermore, it allows an organization to focus on potential risk impact areas, addresses risks according to their severity level, improves the risk handling process, allows security officers to act effectively in adverse situations, enables the effective use of resources, minimizes the effect of risk on the organization's revenue, and identifies suitable controls for security.

Compliance: Compliance is defined as the adherence to standards, policies, rules, and laws framed by industrial or government agencies. If the organization or cloud service provider (CSP) fails to achieve compliance in the cloud, then the organization may face penalties, fines, or lawsuits.

Regulatory compliance addresses regulations, standards, and external laws that apply to a company. Internal or corporate compliance covers regulations, internal controls, and rules framed by a specific organization. Internal compliance management should be integrated with external compliance requirements.

For creating a robust compliance program in the cloud, the organization should identify the areas in the cloud environment that pose a high risk, following which the organization must develop, implement, and communicate to its employees the policies addressing those high-risk areas.

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



Why Does an Organization Need GRC?

GRC represents governance, risk, and compliance, which are very important factors for any organization. GRC includes not only the handling of these three factors but also their management. The goals of the three factors are the same. When organizations started using various technologies for on-premises as well as cloud management, they discovered that governance, risk, and compliance frequently intersect with each other. For example, an issue related to governance may create problems in risk and compliance. Therefore, if an organization desires to improve risk management and compliance, then it should improve the governance as well.



Figure 10.2: Synchronization of Governance, Risk, and Complaince

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

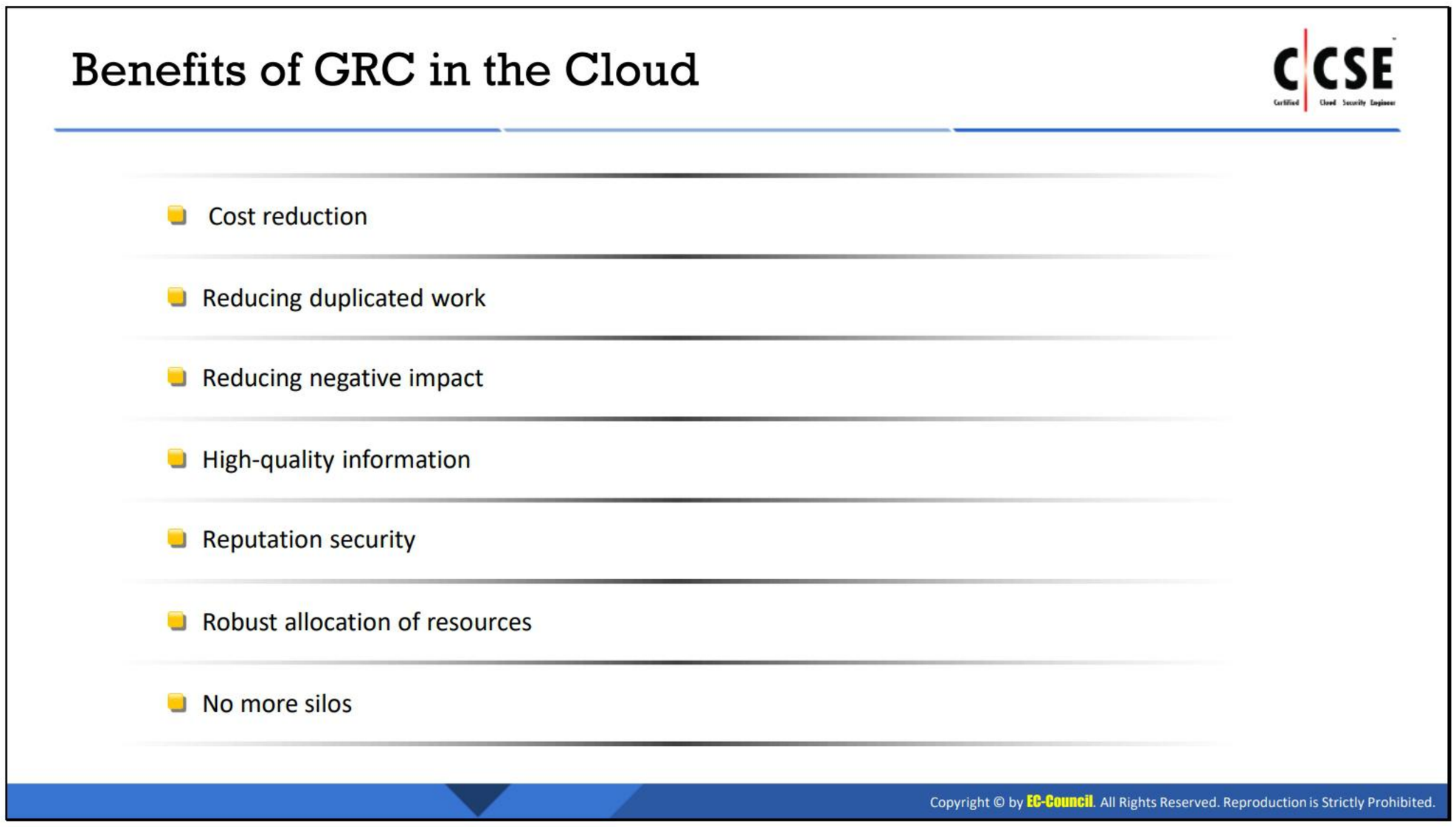
Governance, risk, and compliance are based on the same factors and have the same goals; therefore, it is essential to synchronize all three.

GRC requires technology that allows governance, risk, and compliance to communicate with each other. In other words, the application that manages governance, the one that manages risk, and the one that manages compliance should communicate with each other. If an organization manages governance, risk, and compliance using GRC technology, then that organization can easily remove redundant tasks and processes, which helps in cost reduction. New GRC solutions have incorporated automation and artificial intelligence, which helps in automating the process. With such solutions, tasks that conventionally take hours to complete can be completed within a short time owing to the availability of data and information on one system. Because of the automation of monitoring, unusual activities are detected easily, and notifications are sent automatically. An organization that uses GRC tools can increase its productivity and efficiency in terms of governance, risk, and compliance.

Previously, governance, risk, and compliance were managed manually. In such a scenario, for the higher management to view the status of all the issues in the organization, they must ask the employees to make a report. With a GRC tool, the management gains visibility in GRC and can instantly view all the issues related to the organization. In addition, reporting is quite easy with GRC. Previously, it took hours to generate reports, but with a GRC solution, reports are automatically generated within minutes because all the information and data required to prepare a report are present in the system. GRC allows the management of an organization to become fully aware of ongoing issues. It enables the management to view the risks, governance, and compliance issues prevailing in the organization. They can not only view the issues but can also track the actions initiated on various issues. Furthermore, the management can easily view the issues that are resolved and those that require their direct input. Therefore, there is a need for implementing GRC in every organization to minimize risks, improve governance, and enhance compliance.

hide01.ir

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



Benefits of GRC in the Cloud

GRC in the cloud provides clarity to the existing processes and helps in the smooth running of these processes. The key benefits of using GRC in the cloud environment are as follows.

- **Cost Reduction**: Owing to the growth of threats and regulatory requirements in the cloud, an organization needs to spend a large amount of money, fees, and penalties when it fails to monitor and tackle threats and to meet all the regulatory requirements. Using GRC technology, an organization can cut all these expenses and enhance efficiency by handling various threats and regulatory requirements from a single dashboard.
- **Reducing Duplicated Work:** Duplicating a similar process across the business is considered an ineffective way of operating. By using GRC technology, an organization can implement less duplicated work across the business, thereby freeing up teams and allowing them to focus on important tasks.
- **Reducing Negative Impact**: If an organization has numerous procedures that cannot work logically, then it will waste staff time across the business and decrease productivity. Including these procedures in the GRC strategy can reduce bureaucracy and paperwork, which reduces the negative impact and boosts staff morale, thereby increasing productivity.
- **High-quality Information:** A reliable, consistent, and centralized approach to GRC would help in collecting quality information quickly. This information can be used by an organization to make quick strategic decisions with confidence.
- **Reputation Security**: Governance, risk management, and compliance are important components that can safeguard the reputation of an organization and prevent penalties

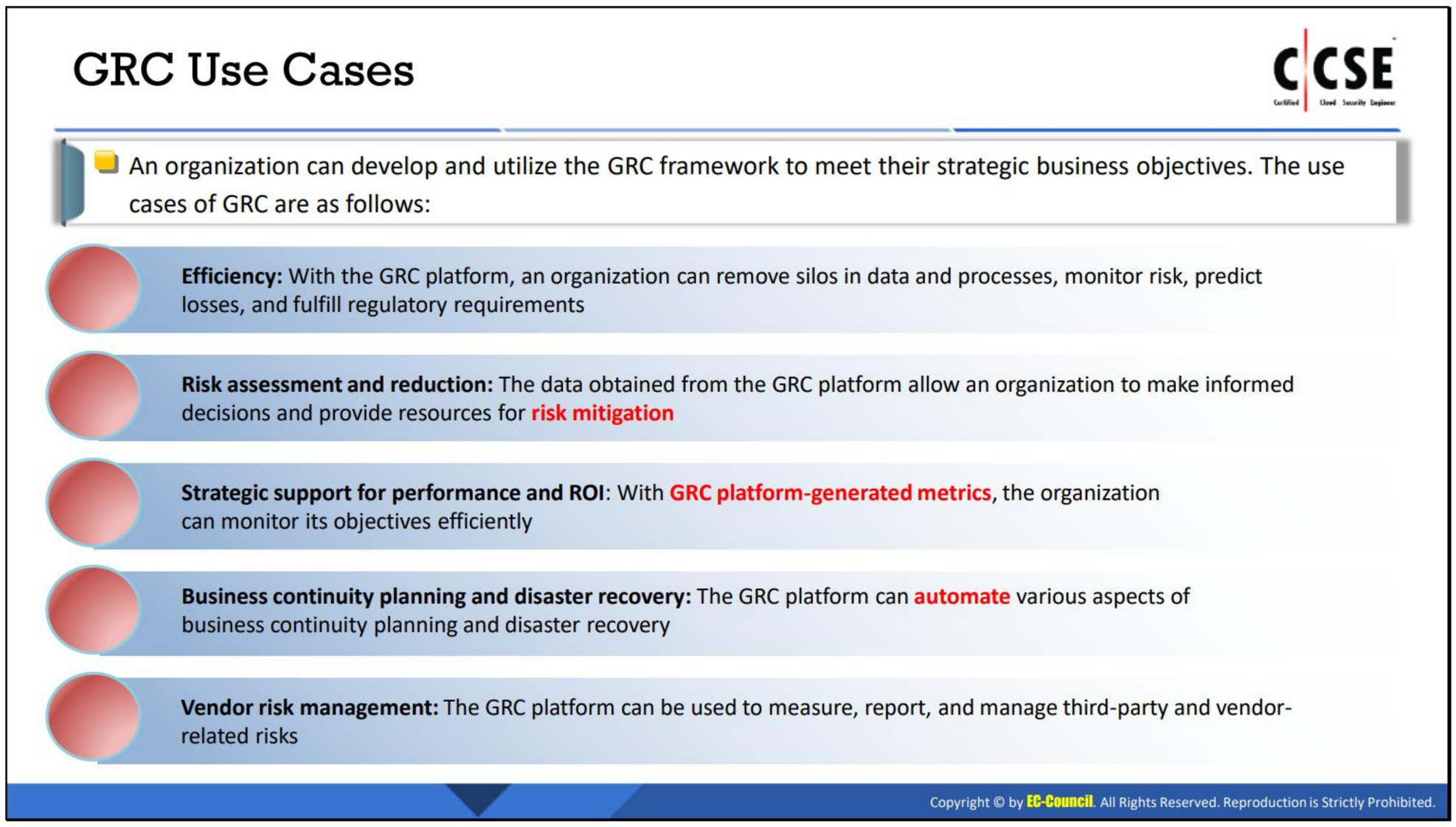
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and lawsuits. Therefore, managing these components efficiently using GRC technology can be an efficient method of reputation security.

- **Robust Allocation of Resources**: Obtaining quality information quickly and attaining a thorough understanding of areas with duplicated work across the business are useful for an organization to allocate resources efficiently and take the business in the appropriate direction.
- **No More Silos**: A large enterprise has various issues with staff working in silos, as the information does not flow in or out productively. Although GRC technology does not completely remove these issues, it reduces the impact of these issues on important areas.

hide01.ir

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



GRC Use Cases

An organization can use the GRC framework for setting up policies and practices to reduce compliance risk. An information technology and security GRC solution aims to leverage information on infrastructure, data, cloud applications, etc. The GRC program of an organization can enhance performance, minimize risks, and increase efficiency and return on investment (ROI). The organization develops and utilizes the GRC framework to meet its strategic business objectives. The following are the use cases of GRC.

Efficiency: When business activities such as risk assessment, internal audits, and compliance management are performed manually, they consume a large amount of time and resources. With the GRC platform, an organization can remove silos in data and processes, monitor risk, predict losses, and fulfill regulatory requirements. It helps the organization in managing financial and artificial intelligence (AI) drive models and helps in improving IT controls and compliance.

Risk Assessment and Reduction: GRC allows an organization to manage risk assessment and reduction. The data obtained from the GRC platform allows an organization to make informed decisions and provide resources for risk mitigation.

Regulation audits such as the Sarbanes-Oxley Act are considered milestones through which GRC operates, and the department should maintain and safeguard sensitive data such as financial reports, invoices, and HR records to prepare themselves for this audit.

An efficient GRC program will be useful for organizations that have already experienced risk events, compliance issues, governance failure, etc. Additionally, an organization lacking trust in their compliance or external and internal financial risk reporting can enforce a GRC model for

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

fixing and monitoring redundant control sets and useless frameworks to prevent repeatable risk issues.

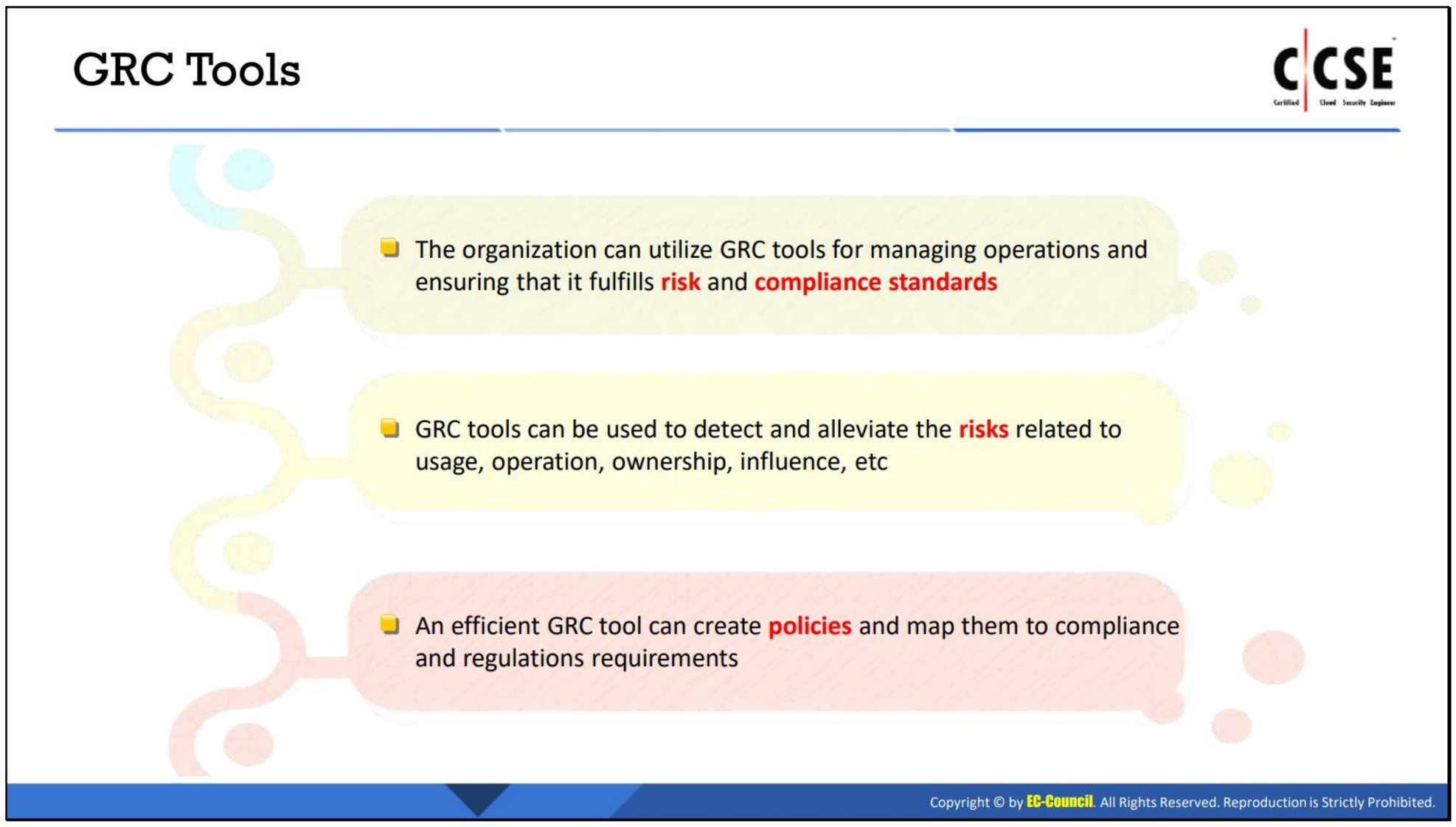
Strategic Support for Performance and ROI: Occasionally, organizations find it difficult to determine success, tackle conflicts of interest, and allocate resources because of the increased cost of addressing the risks. With the metrics generated by the GRC platform, an organization can monitor its objectives efficiently. Using the GRC platform, the organization can enhance its performance and increase the ROI.

Business continuity Planning and Disaster Recovery: As the GRC platform is an extension of service management and governance, risk, and compliance, it can automate various aspects of business continuity planning and disaster recovery.

Vendor Risk Management: The security assessment of a third party that has access to an organization's application and data is a challenging and tedious task. The GRC platform can be used to measure, report, and manage third-party and vendor-related risks.

hide01.ir

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



GRC Tools

An organization can utilize GRC tools for managing operations and ensuring that the organization fulfills risk and compliance standards. GRC tools can be used to detect and alleviate the risks related to usage, operation, ownership, influence, etc. GRC tools should incorporate IT governance, operational risk, internal auditing, policy, and compliance.

The common features found in GRC tools are as follows.

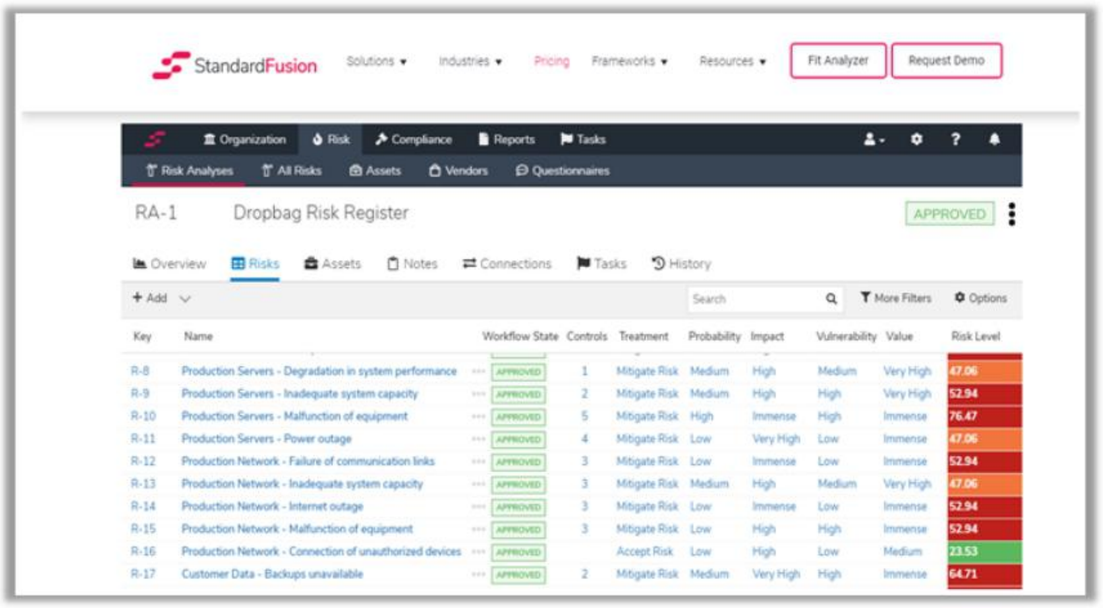
- The content and document management feature of GRC helps an organization in creating, tracking, and storing digitalized content.
- The risk data management and analytics feature of GRC helps in predicting, quantifying, measuring, and mitigating risks.
- The work management feature of GRC allows an organization to execute, monitor, and establish workflows related to GRC.
- The audit management feature of GRC helps an organization simplify the processes to conduct internal audits and manage data.
- The dashboard feature of GRC provides a central interface where key performance indicators (KPIs) associated with the business process can be monitored.

An efficient GRC tool can create policies and map them to compliance and regulatory requirements. Such a tool can help in determining whether controls are properly deployed, appropriately implementing functions, and effectively assessing and mitigating risks.

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

GRC Tool: StandardFusion

- StandardFusion GRC tool has many features such as risk identification, risk assessment, risk treatment, policy management, tracking and monitoring, and vendor assessment



StandardFusion

Source: https://www.standardfusion.com

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

GRC Tool: StandardFusion

Source: https://www.standardfusion.com

StandardFusion is one of the most popular cloud-based GRC platforms and makes compliance and security simple and approachable. It helps organizations manage operational risk, follow best practices, and comply with standards quickly and easily.

The key features of the StandardFusion GRC tool are as follows.

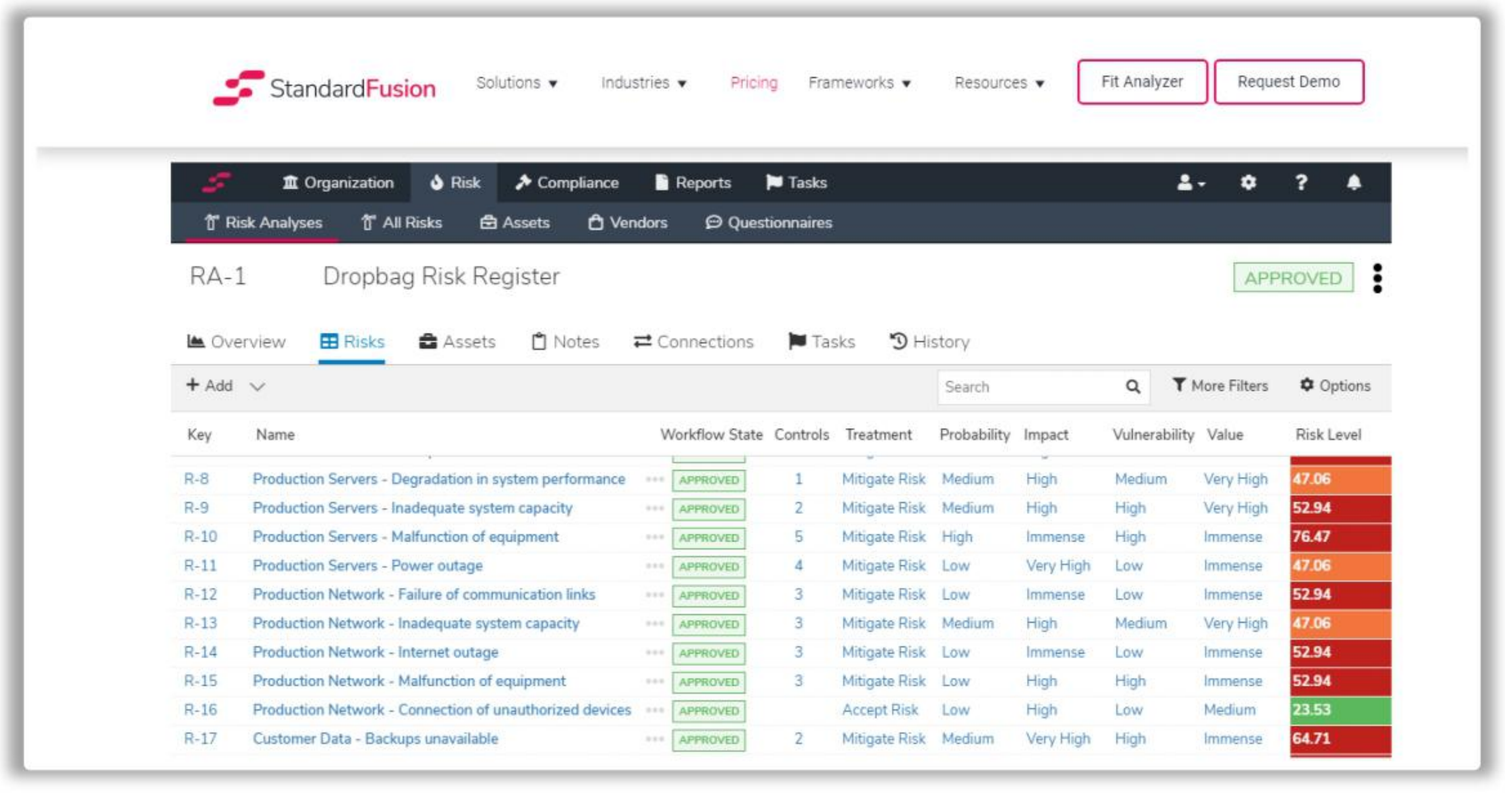


Figure 10.3: StandardFusion

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

Risk Identification: StandardFusion GRC software enables the user to track not only the risk but also the associated assets.

Risk Assessment: Once risks are identified, the user can assess them using one of many included qualitative and quantitative risk methodologies; alternatively, the user can define custom calculations. Standardfusion is not only simple but also flexible; users can employ one of the built-in risk methodologies or upload their own.

Risk Treatment: Risks can be connected to mitigating controls to show how the organization treats its threats. Viewing the risks on a heat map or in a report helps in obtaining a holistic view of the risks.

Distributed Effort: The tasks associated with managing compliance programs can be shared with the entire organization. A culture of compliance can be created by company-wide task delegation management.

Policy Management: Users can manage the development, approval, mapping, and distribution of policies organization-wide. Further, they can create powerful connections between policies, requirements, controls, and risks. Moreover, users can manage approval states and implement recurring review tasks on important policies.

Tracking and Monitoring: The user is provided complete visibility into every aspect of the organization's compliance program, ensuring that they are the first to know when straying from conformity. Reports and dashboards allow the user to understand focus areas at all times.

ride01.ir

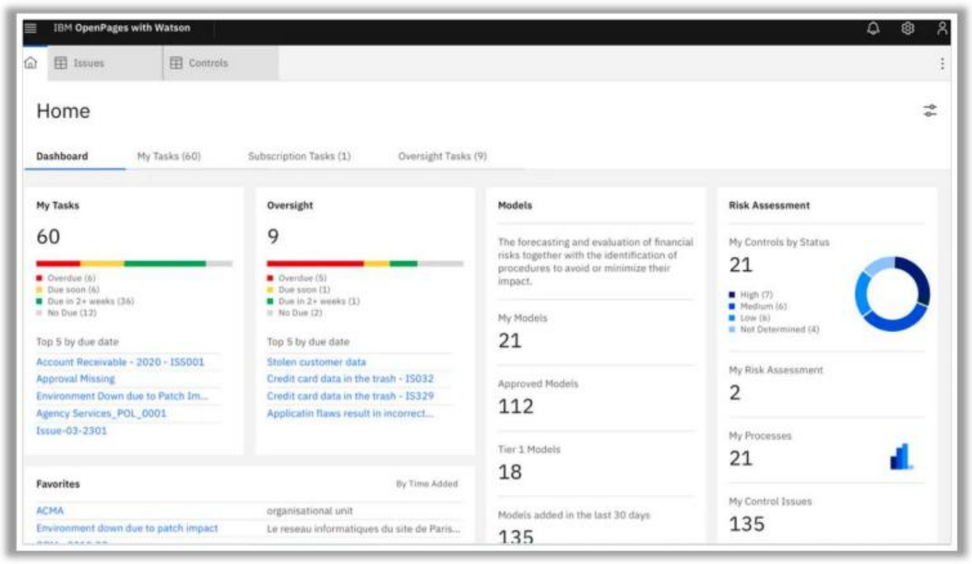
Conduct Audits With Confidence: StandardFusion allows performing internal and external audits with direct access to recorded evidence and audit remediation status. Users can reduce duplication and perform audits on the controls and requirements in place.

Vendor Assessment: Users can easily send invitations to vendors, third-parties, and employees to complete security questionnaires and provide supporting documentation and evidence. Furthermore, users can simplify workflows and reduce risk by using StandardFusion to manage questionnaires.

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

GRC Tool: IBM OpenPages with Watson

- IBM OpenPages with Watson is an **AI-driven**, highly scalable governance, risk management, and compliance (GRC) solution that runs on any cloud
- It centralizes siloed **risk management functions** within a single environment designed to help in identifying, managing, monitoring, and reporting on risk and regulatory compliance



IBM OpenPages with Watson

Source: https://www.ibm.com

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

GRC Tool: IBM OpenPages with Watson

Source: https://www.ibm.com

IBM OpenPages with Watson is an AI-driven, highly scalable governance, risk, and compliance (GRC) solution that runs on any cloud. It enables the centralization of siloed risk management functions within a single environment designed to help identify, manage, monitor, and report on risk and regulatory compliance, especially in today's changing business landscape.

IBM OpenPages with Watson transforms the way risk and compliance professionals work. By providing core services and functional components on a scalable platform that spans operational risk, regulatory compliance, IT governance, internal audit, and financial controls management, IBM OpenPages with Watson delivers a holistic view of risk and regulatory responsibilities across the enterprise. It delivers on the clear and present need in the marketplace for an integrated end-to-end solution that enables organizations to connect internal GRC policies and practices to the external regulatory environment.

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

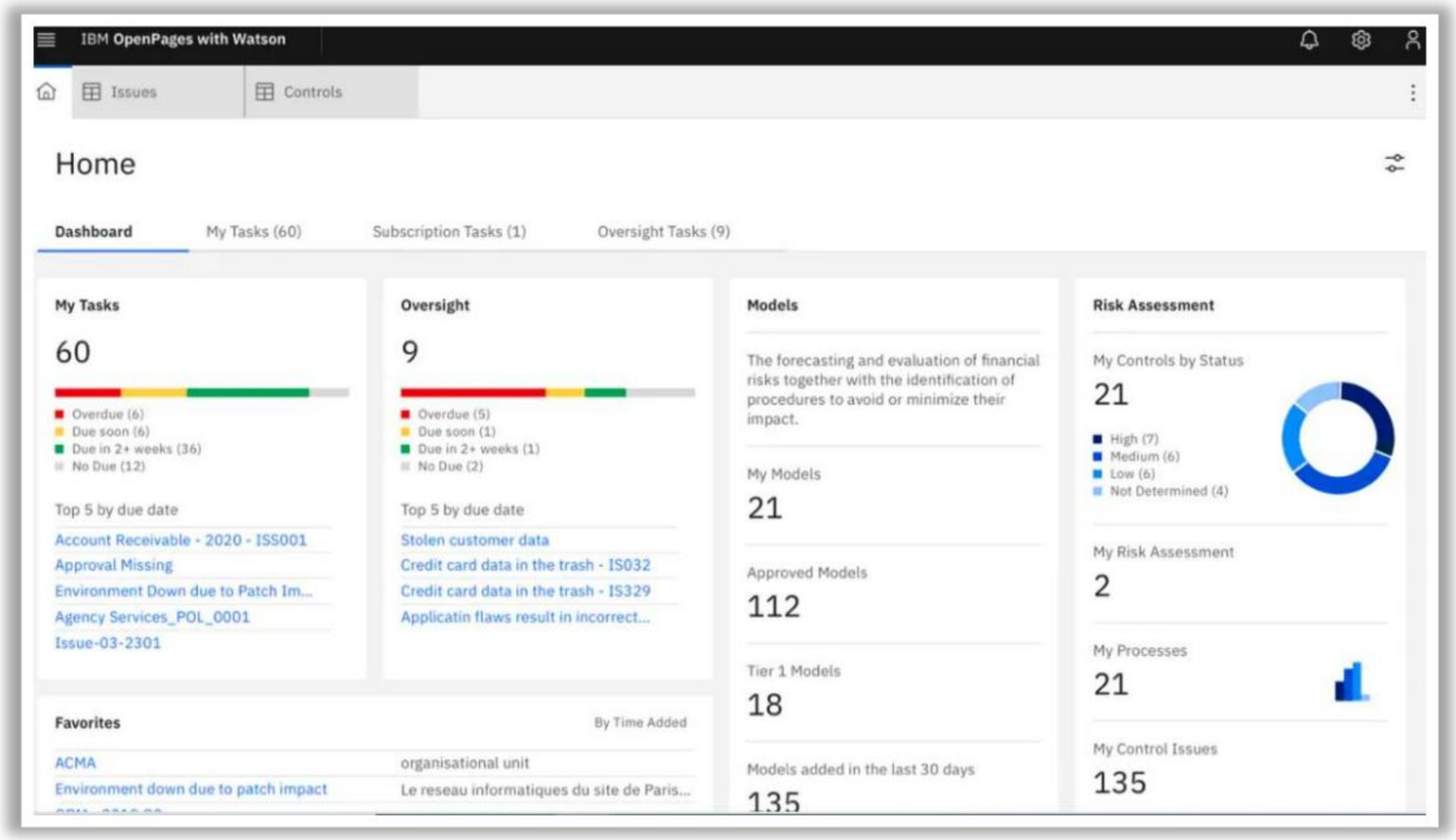


Figure 10.4: IBM OpenPages with Watson

IBM OpenPages with Watson offers unprecedented flexibility to use on any cloud or on-premises environment or as part of the IBM Cloud Pak for Data platform through one universal entitlement that supports unique use cases and hybrid environments. IBM OpenPages with Watson offers businesses the capability to deploy nine targeted product domains to meet specific risk and compliance challenges. Users can choose the product domains they need within a single integrated environment.

IBM OpenPages with Watson redefines governance risk and compliance with AI and advanced analytics. IBM OpenPages with Watson features the market's only cognitive-driven GRC portfolio that helps organizations meet their most challenging risk and compliance requirements. This platform provides core services and functional components that span operational risk, policy and compliance, financial controls management, IT governance, and internal audit.

IBM OpenPages with Watson improves data quality, as users can choose one or more relevant classifications based on the knowledge of experts, rather than their training. It brings together all key stakeholders that often work independently on siloed data. OpenPages Model Risk Governance combines a flexible data model with document management, powerful workflow capabilities, and business intelligence. It helps ensure a greater level of engagement and transparency in the model risk management and governance processes.

IBM OpenPages with Watson reduces the complexity and cumbersome nature of complying with numerous industries, ethics, privacy, and government regulatory mandates. OpenPages Policy Management automates ongoing test, review, approval, and remediation processes. It also helps identify similarities between regulations to reduce the redundancy and duplication of effort.

IBM OpenPages with Watson automates the process of identifying, measuring, monitoring, analyzing, and managing operational risk. OpenPages Operational Risk Management enables

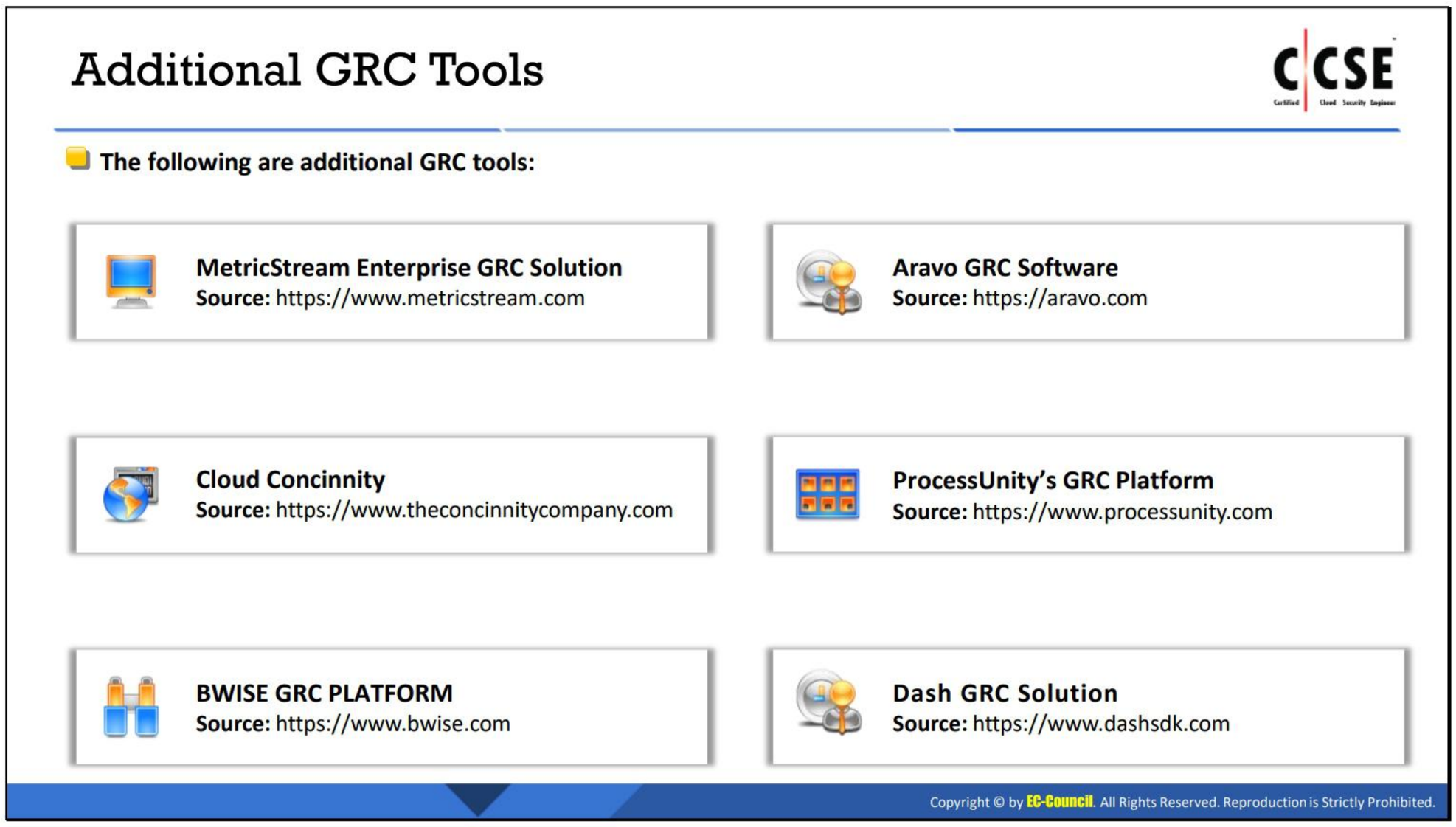
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

businesses to integrate all risk data—risk and control assessments, internal and external loss events, key risk indicators, and issue/action plan management—within a single environment.

IBM OpenPages with Watson provides internal auditors with a cross-departmental view into organizational GRC. It helps organizations efficiently plan, execute, report on, and review their audit universe. Further, it allows users to compare the best practice control environment to the one that has been documented and perform gap analyses to identify vulnerabilities and/or improvement opportunities.

hide01.ir

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



Additional GRC Tools

MetricStream Enterprise GRC Solution

Source: https://www.metricstream.com

guide01.ir

MetricStream Enterprise GRC Solution is built on the M7 Integrated Risk Platform, which is intelligent by design, and cuts across organizational silos, enabling a holistic and collaborative approach to GRC. Risk and compliance data from across the enterprise and third-party vendors can be effectively rolled up and transformed into actionable business intelligence to support risk-aware decision-making. With support for mobile, real-time reporting, advanced risk analytics, and regulatory notifications, the solution is comprehensively designed to meet the GRC needs of today's complex, global enterprises and their extended ecosystem.

Cloud Concinnity

Source: https://www.theconcinnitycompany.com

Cloud Concinnity is GRC Software custom-built for the board and the c-suite to transform mission-critical management and governance, risk management, and compliance processes. It simplifies mission-critical elements; provides centralization with a single, secure hub in the cloud; and automates processes for efficiency.

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

BWISE GRC PLATFORM

Source: https://www.bwise.com

BWise provides a leading enterprise governance, risk management, and compliance (GRC) platform that enables organizations to be in control of their key financial and reputational risks, including the risk of non-compliance. The platform offers role-based solutions for internal audits, risk management, compliance management, information security, etc.

Aravo GRC Software

Source: https://aravo.com

Aravo is a cloud-based GRC platform that delivers the industry's most powerful set of capabilities designed to help companies manage third-party risk at scale.

The Aravo GRC platform allows clients to map a broad range of capabilities to their governance framework and policies and to integrate with internal business systems and third-party risk content providers. Content management, a relational data model, workflow management, reporting, visualization, and a dynamic dashboard are some of the features of this tool

ProcessUnity's GRC Platform

Source: https://www.processunity.com

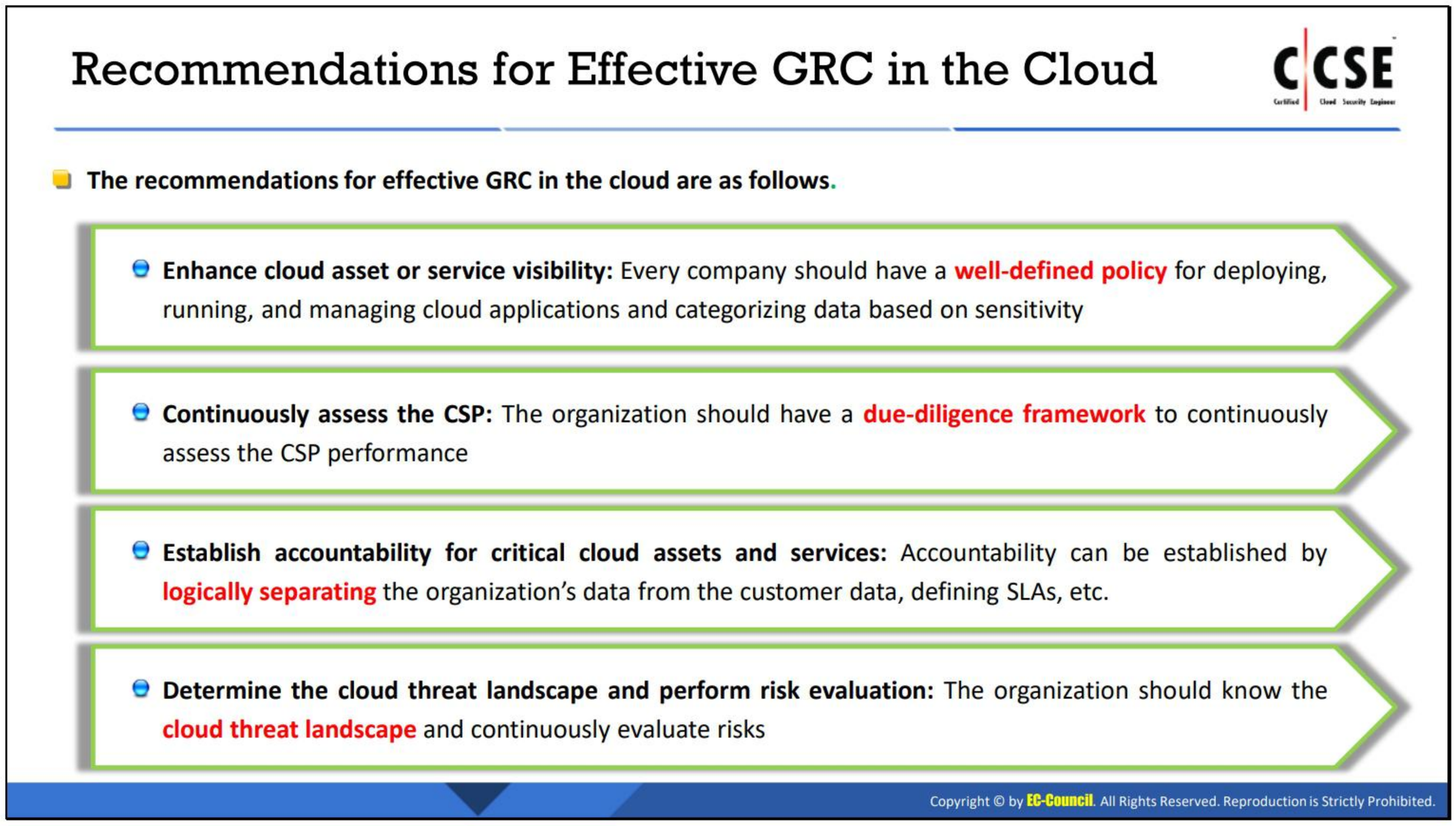
ProcessUnity applications are delivered on ProcesUnity's software-as-a-service GRC management platform. Its flexible, easy-to-use technology creates a common user experience and seamless application and data integration across all of its GRC solutions through a shared enterprise architecture, security model, user interface, data source, application integration service, etc.

Dash GRC Solution

Source: https://www.dashsdk.com

The Dash ComplyOps streamlines regulatory compliance and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) governance, risk, and compliance in the public cloud. The Dash solution enables organizations to set administrative policies that connect directly to compliance alerts in their infrastructure. Dash Continuous Compliance Monitoring proactively scans the environment for security and compliance issues. Dash makes it easy for security teams to instantly gain insight into their state of compliance.

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



Recommendations for Effective GRC in the Cloud

The adoption of cloud technology has been increasing at a rapid pace. To maximally draw benefits from cloud deployments and reduce risks, an organization should enforce a cohesive approach for governance, risk management, and compliance (GRC). A GRC framework automates risks, security, and compliance workflows, allows stakeholder visibility and reporting, etc. The recommendations below can ensure an appropriate GRC framework for cloud operations and assets.

Enhance Cloud Asset or Service Visibility: Cloud security professionals should have a complete understanding of the scope of cloud services in use within their organization. Information technology and infrastructure managers should have full information regarding the processes running on the cloud deployments, assets, ownership, etc. Every company should have a well-defined policy for deploying, running, and managing cloud applications and categorizing data based on sensitivity to ensure that appropriate controls are in place for managing the data.

Continuously Assess the Cloud Service Provider (CSP): Every organization has thought of losing control of an application deployed in a cloud environment. An organization should choose a CSP that can validate controls such as physical data security, network security, and standard audit framework. At the time of selecting a CSP, the organization should look into various key issues such as business continuity and data recovery, access privileges, data segregation, and regulatory compliance. The organization should have a due-diligence framework to continuously assess the CSP performance.

Establish Accountability for Critical Cloud Assets and Services: Every organization should realize the importance of governance in the cloud environment. Organizations should document the cloud services, cloud policies, cloud services, business process, business objectives, etc. Furthermore, organizations should have full clarity on the assigned processes

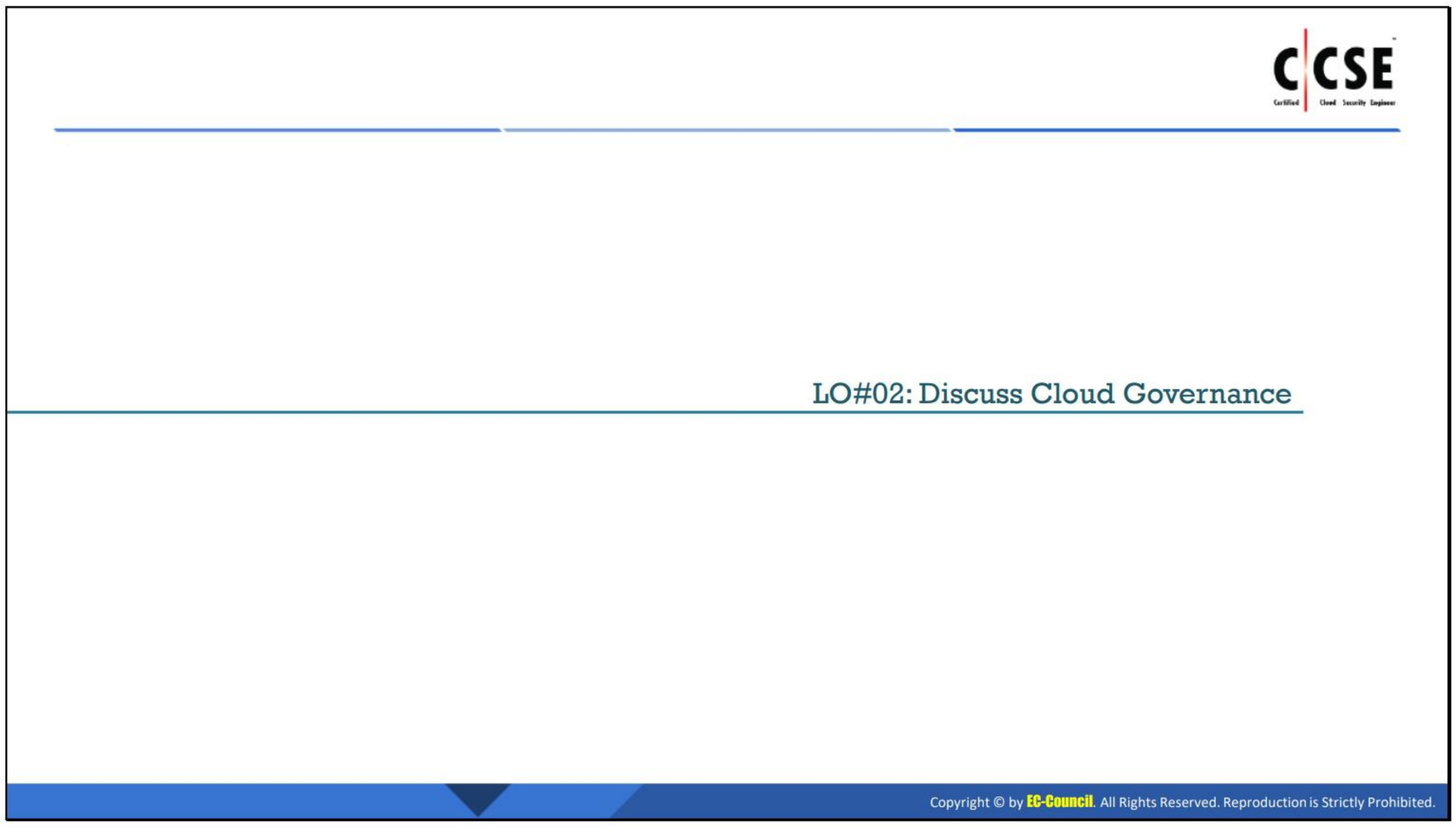
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and policies. It is important to establish accountability because the data related to customers are interconnected to the CSP. Accountability can be established by logically separating the organizational data from customer data or user data, defining service-level agreements (SLAs), categorizing the consumed services, etc.

Determine the Cloud Threat Landscape and Perform Risk Evaluation: There are risks associated with the cloud environment, and an organization should know the cloud threat landscape and continuously evaluate risks. After evaluating the risks, the organization should mitigate those risks to safeguard itself and associated parties from exposure. Owing to the evolving and changing nature of threats, every organization should keep itself alert and updated with the latest technology.

hide01.ir

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

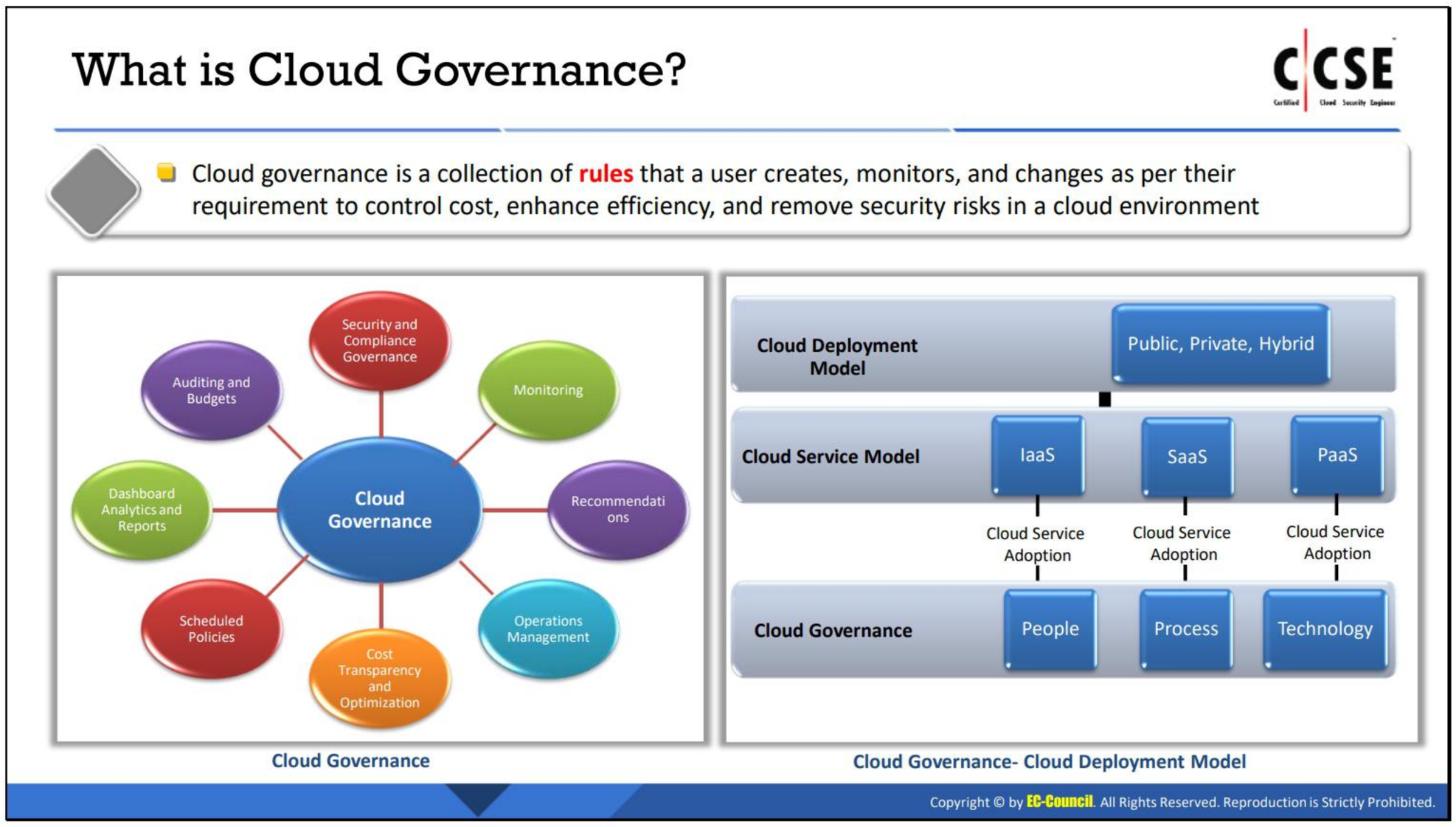


LO#02: Discuss Cloud Governance

To minimize risk exposure in the cloud, a cloud security engineer should learn how to implement strict policies to secure data and integrate privacy controls in the cloud. The objective of this section is to introduce cloud governance and its challenges and processes.

hidoo1.ir

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



What is Cloud Governance?

An organization running a business in a cloud environment must follow certain rules, which are related to personal privacy and data security. However, these rules vary depending on the industry. Furthermore, these rules are not significantly different from the rules implemented when operating on-premises IT infrastructure; the only difference is in the landscape.

An organization running a business in IT infrastructure will be well-acquainted with the capital costs and monthly operational costs. The organization will also have complete knowledge about the departments running approved software, applications, and programs.

In the cloud, various departments have their own systems and deploy their own assets. They need not concern themselves with the capital cost, but the operational costs may exceed set thresholds if no proper controls are in place. Moreover, the programs, applications, and software deployed by one department cannot communicate with those of another department.

The absence of controls creates problems with cost and efficiency and also raises security issues. Even if cloud services are secure, deployed assets with weak access controls or configurations can allow easy access to attackers.

To eliminate the concerns with cost and efficiency, an organization should create a collection of rules. The rules of cloud governance consist of the budgets allocated to each department; cloud security–related policies; guidelines about which applications, programs, and software the departments can use, etc. These rules are flexible, but there should be an approval process to prevent excessive flexibility. Furthermore, compliance with the rules must be monitored. Monitoring can be performed using various cloud management software. An organization operating in a hybrid cloud environment or multi-cloud environment is recommended to use third-party tools that provide complete visibility of its business processes. When starting to

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

monitor compliance with the rules, the organization may find areas that can be fine-tuned to adjust cost and efficiency.

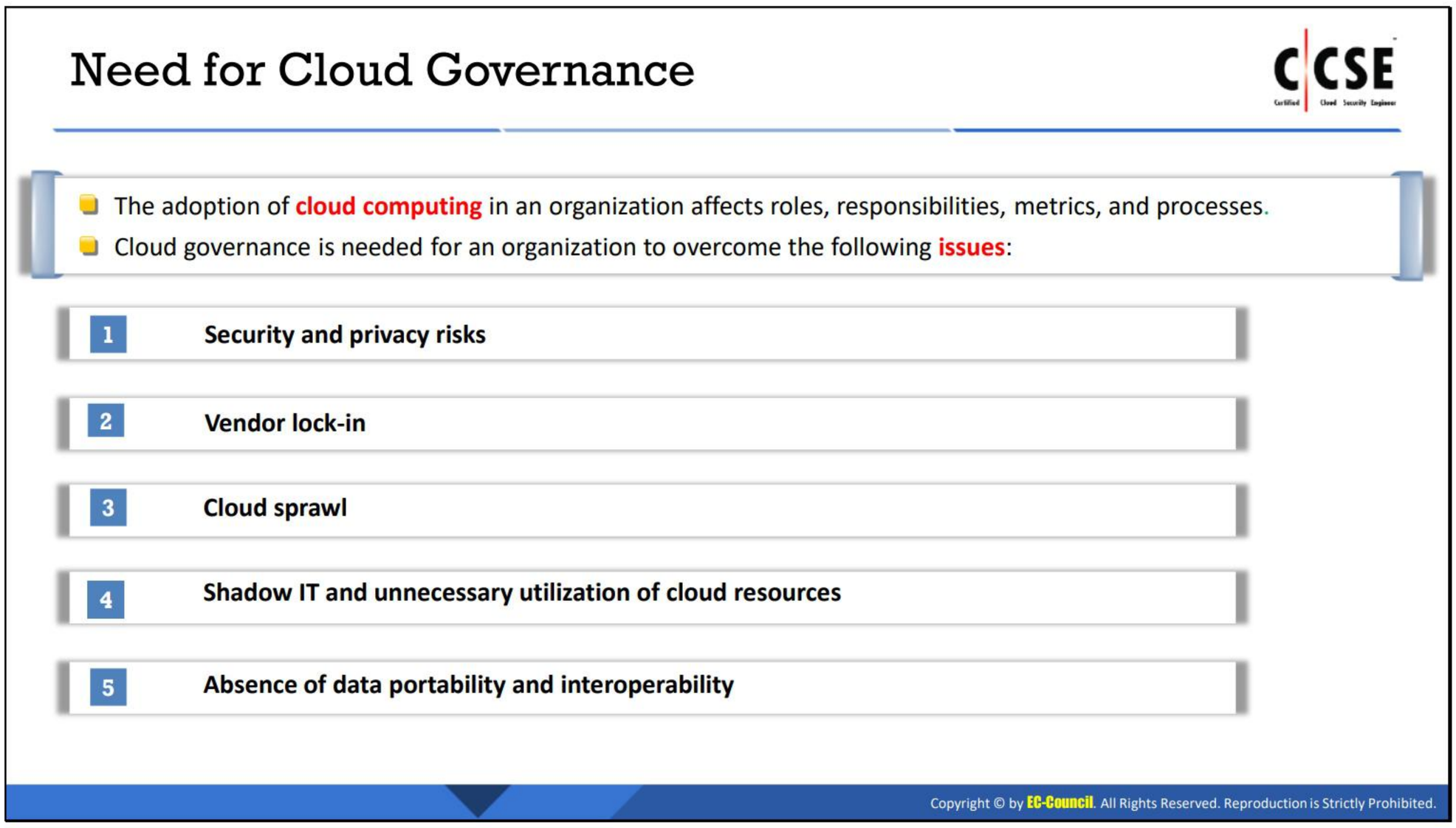


Figure 10.5: Cloud Governance

hide01.ir

Cloud governance is a collection of rules that a user creates, monitors, and changes as per their requirement to control cost, enhance efficiency, and remove security risks in a cloud environment. It is a collection of agreed-upon policies and standards based on risk assessment and an agreed-upon framework including auditing, reporting procedures, and implementation of policies and standards.

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



Need for Cloud Governance

The adoption of cloud computing in an organization affects roles, responsibilities, metrics, and processes. Cloud governance is needed for an organization to overcome the following issues.

Security and Privacy Risks: Security and privacy risks can arise from the unauthorized installation or download of software, access to restricted sites, and storage of illegal data. Cloud governance covers various cloud security components such as access controls, encryption, application access rules, and security groups, which safeguard an organization against security and privacy risks.

Vendor Lock-in: The majority of cloud service providers (CSPs) or vendors opt for vendor lock-in, which is a clause that makes the client organization dependent on the service provider for products and services. The organization can avoid this dependency by making suitable changes to service-level agreements (SLAs). This increases the organization's freedom and minimizes its dependency on a single vendor.

Cloud Sprawl: Cloud sprawl occurs when staff of different departments utilize different programs from a third party by obtaining approvals without incorporating the IT department of the organization. If cloud sprawl is not detected or restricted, it can cause inefficient, redundant, fragmented, and unmanaged cloud programs in the cloud environment and create unnecessary problems.

Shadow IT and Unnecessary Utilization of Cloud Resources: Shadow IT and the unwarranted usage of cloud resources occur when employees belonging to various departments of an organization fail to implement the rules and regulations framed by the IT department of the organization. This can lead to fragmented control and breaches across the organization and affect the efficiency of cloud services.

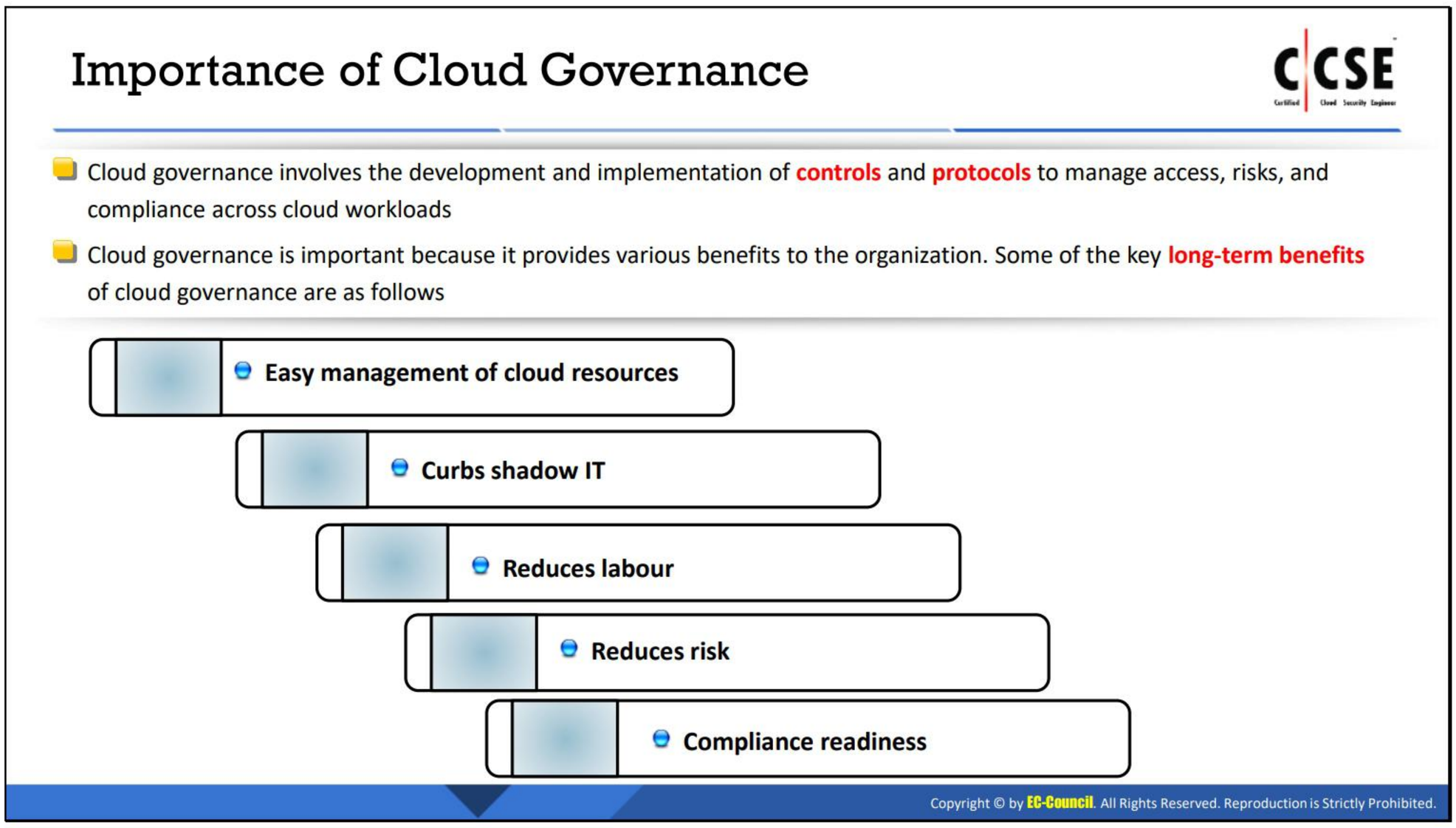
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Absence of Data Portability and Interoperability: This issue occurs when the built-in features of the data center fail to connect well with the software and products outside the organization. This can lead to module incompatibility and insufficiency in the system.

In addition to overcoming the above-mentioned issues, cloud governance is needed to tackle common problems such as the misalignment of enterprise objectives, regular policy exception reviews, stalled projects, compliance failures or regulatory penalties, cost overruns, and partial risk assessments.

hide01.ir

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



Importance of Cloud Governance

Every business that operates in the cloud must handle risks such as attacks from hackers and should implement a plan to address technical issues that cause the temporary failure of systems. Cloud governance is helpful for such issues.

Cloud governance involves the development and implementation of controls and protocols to manage access, risks, and compliance across cloud workloads. Although moving from on-premises to cloud storage offers various advantages, it adds an additional layer of complexity. With the cloud, more people in the organization have the chance to impact the cloud architecture. Therefore, it is important to implement efficient and comprehensive cloud governance.

Although developing and implementing cloud governance takes time and effort, cloud governance offers proportionate benefits. Proper implementation of cloud governance offers long-term benefits such as the following.

- **Easy Management of Cloud Resources:** Cloud service providers (CSPs) commonly ask their customers to move their multi-tenant workloads in single cloud account to different accounts. It is recommended to use different accounts to manage different cloud workloads of the customers. This helps deliver proper access controls and improves cost efficiency. Moreover, using the best practices of cloud governance limits security and financial risks in the event of an issue. A proper and effective governance strategy helps organize the accounts that the organization needs. It also provides visibility of the cloud activities and trends.
- **Curbs Shadow IT:** When the organization is unaware of the systems in use and the locations of data storage, costs and risks increase. Employees use shadow IT when a

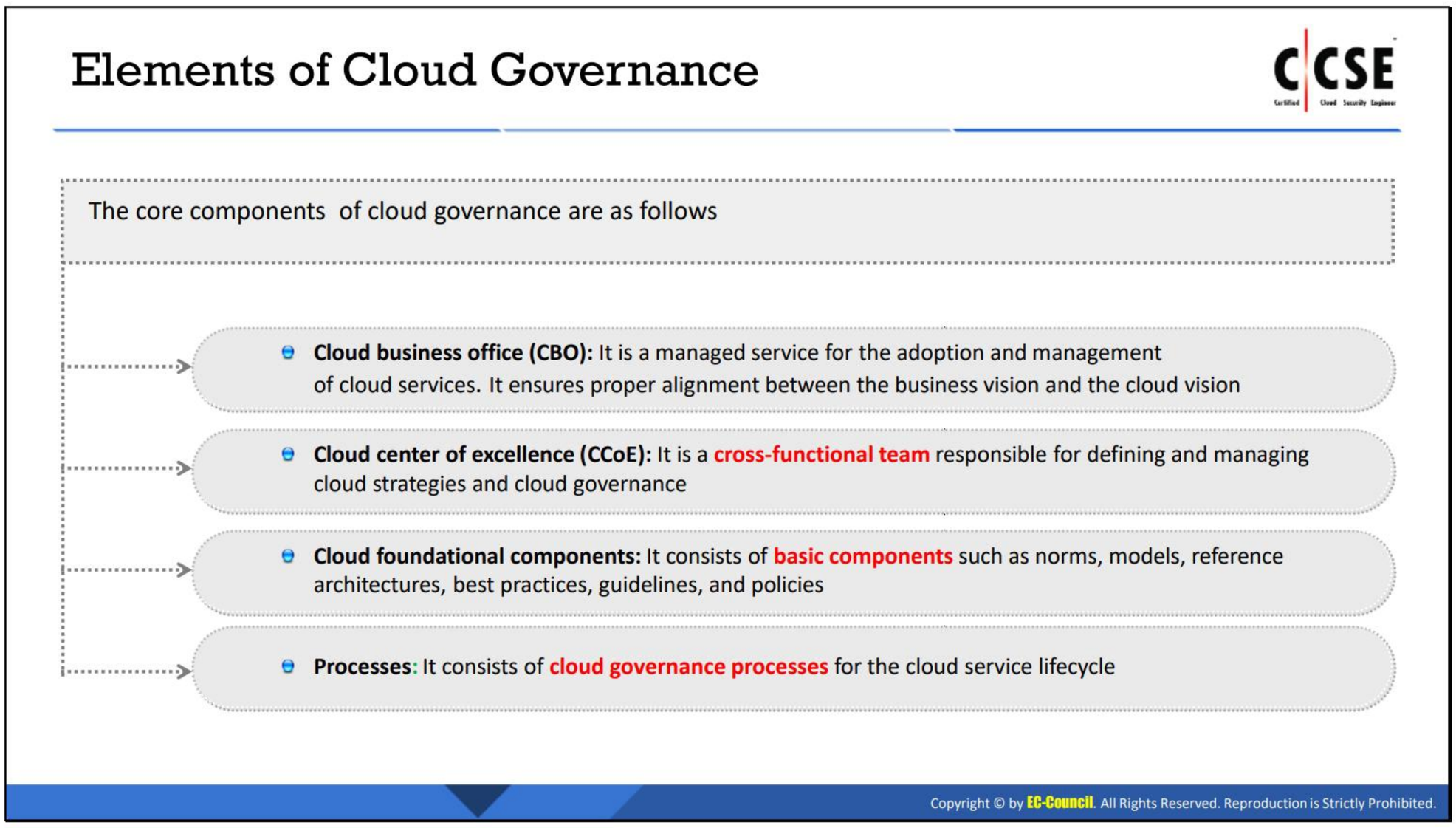
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

delay exists in gaining access to resources. Cloud governance helps develop a framework to easily make requests and access resources. Consequently, team members can gain access to allowed resources within budget constraints.

- **Reduces Labor:** Instead of using spreadsheets or a manual process to track accounts, guardrails can be implemented at an appropriate point in the organizational hierarchy. This controls the budget, access, and policies for a specific project. Moreover, full cloud governance enforces actions that eliminate the need for responding to alerts. By following cloud governance, non-compliant activities can be prevented. Cloud governance also saves time and effort.
- **Reduces Risk:** Although moving data to the cloud is more convenient than moving data to on-premises facilities, it also involves risks such as data breaches and unauthorized access to the data. A cloud governance solution helps in identifying the vulnerabilities in the system and in implementing plans to handle the risks. It also establishes metrics to estimate the impact of security measures.
- **Compliance Readiness:** In any industry, an organization must pass regular audits and compliance assessments. Irrespective of the requirements, cloud governance streamlines compliance preparation and makes it easier to achieve compliance. Developing cloud governance with compliance requirements helps enforce compliance standards in the processes and architecture. Users will have an archive of the system's history and status, which can be used for documenting compliance.

hide01.ir

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



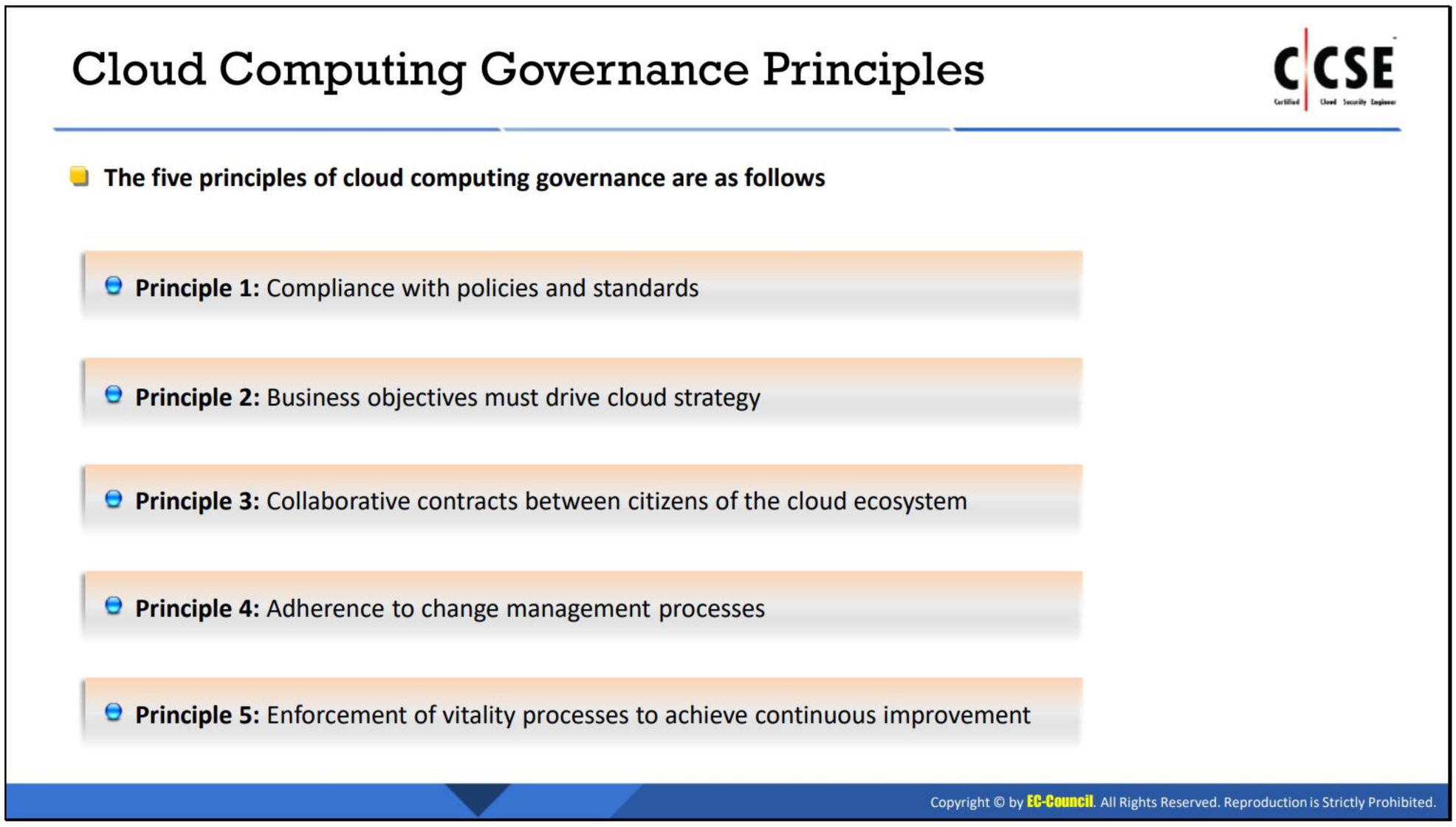
Elements of Cloud Governance

Cloud governance consists of the following key components.

- **Cloud Business Office (CBO):** CBO ensures alignment between the cloud vision and business vision. It also ensures that the governance is implemented across the organization. CBO is also responsible for managing demands, optimizing costs, and prioritization.
- **Cloud Center of Excellence (CCoE):** CCoE is a cross-functional team that is responsible for defining and managing cloud strategies and cloud governance to handle migration to the cloud and operations in the organization.
- **Basic Components:** Cloud governance also includes basic components such as norms, models, reference architectures, best practices, guidelines, and policies.
- **Processes:** Cloud governance includes the processes necessary for the cloud service lifecycle.

h3le0_ir

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



Cloud Computing Governance Principles

Cloud governance helps secure applications and data. For effective governance, compliance with rules and policies must be monitored. The following are the five principles of cloud computing governance.

hide01.ir

Principle 1: Compliance with Policies and Standards

For effective governance, cloud security standards and policies should be based on the standards prevalent in the industry. Compliance with the standards and policies ensures a consistent approach to responding and mitigating security risks faced by the organization. Furthermore, complying with the standards and policies helps in ensuring defined principles across the organization. Open standards in the cloud support interoperability, which is essential for the cloud. However, before achieving compliance to existing standards in the industry, region, and government, organizations should ensure that those standards apply to them.

Best Practices for Compliance with Policies and Standards

- Establish cloud security at the early stage of the cloud lifecycle.
- Ensure that all stakeholders comply with laws, regulations, and external policies.
- Specify all architectural layers.
- Include a common reference architecture across all cloud environments for effective communication.
- Comply with the laws and regulations regarding the collection and management of data.

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

Principle 2: Business Objectives Must Drive Cloud Strategy

Cloud strategy should be considered an important factor in the business. Cloud governance must be based on business objectives such as the "business of the business" and "business of IT" of the organization. A cloud strategy document must be created so that the various teams in the business can coordinate to align with the adoption of cloud services. Cloud services have capabilities to empower the business and IT objectives of the organization. The business and IT stakeholders must be included at the beginning of the decision-making process of adopting the cloud strategy.

Recommendations for Identifying Business Objectives

- Recognize the benefits to the organization in adopting the cloud services.
- Identify the services to be availed from a CSP and the services to be deployed on premises.
- Decide how the organization can provide consistent policies and governance across the cloud environment.
- Decide on the protections required for reducing attacks on and threats to the resources.

Principle 3: Collaborative Contracts Between Citizens of the Cloud Ecosystem

Peaceful interaction between the different stakeholders in a cloud environment can be ensured by including a clear set of rules and policies. Signing a contract provides well-defined roles and responsibilities, authority, and accountability to different stakeholders because the cloud system includes stakeholders internal and external to the organization. Furthermore, service-level agreements (SLAs) should mention the recovery time objectives (RTOs) and recovery point objectives (RPOs) of the organization. SLAs should also include the mean time to recovery (MTTR) and mean time to failure (MTTF). Other best practices are as follows.

- Specify the governing rules in a memorandum of understanding (MoU) or an SLA.
- Ensure that a proper mechanism exists for the resolution of disputes.

Principle 4: Adherence to Change Management Processes

Cloud systems consist of a vast number of inter-related equipment. A change in any of the components can have adverse effects on others. Therefore, changes occurring in the cloud infrastructure must be enforced across all resources in the cloud in a standardized manner. A change management process can thus improve quality control and service. The absence of a well-defined change management process can negatively impact the interoperability feature of the cloud system, causing service disruptions from unplanned change activities. The following are recommendations for a change management system.

- Include change management procedures in the initial deployment as well as during ongoing maintenance activities.
- Include a federated change management process to coordinate change management between stakeholders.

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

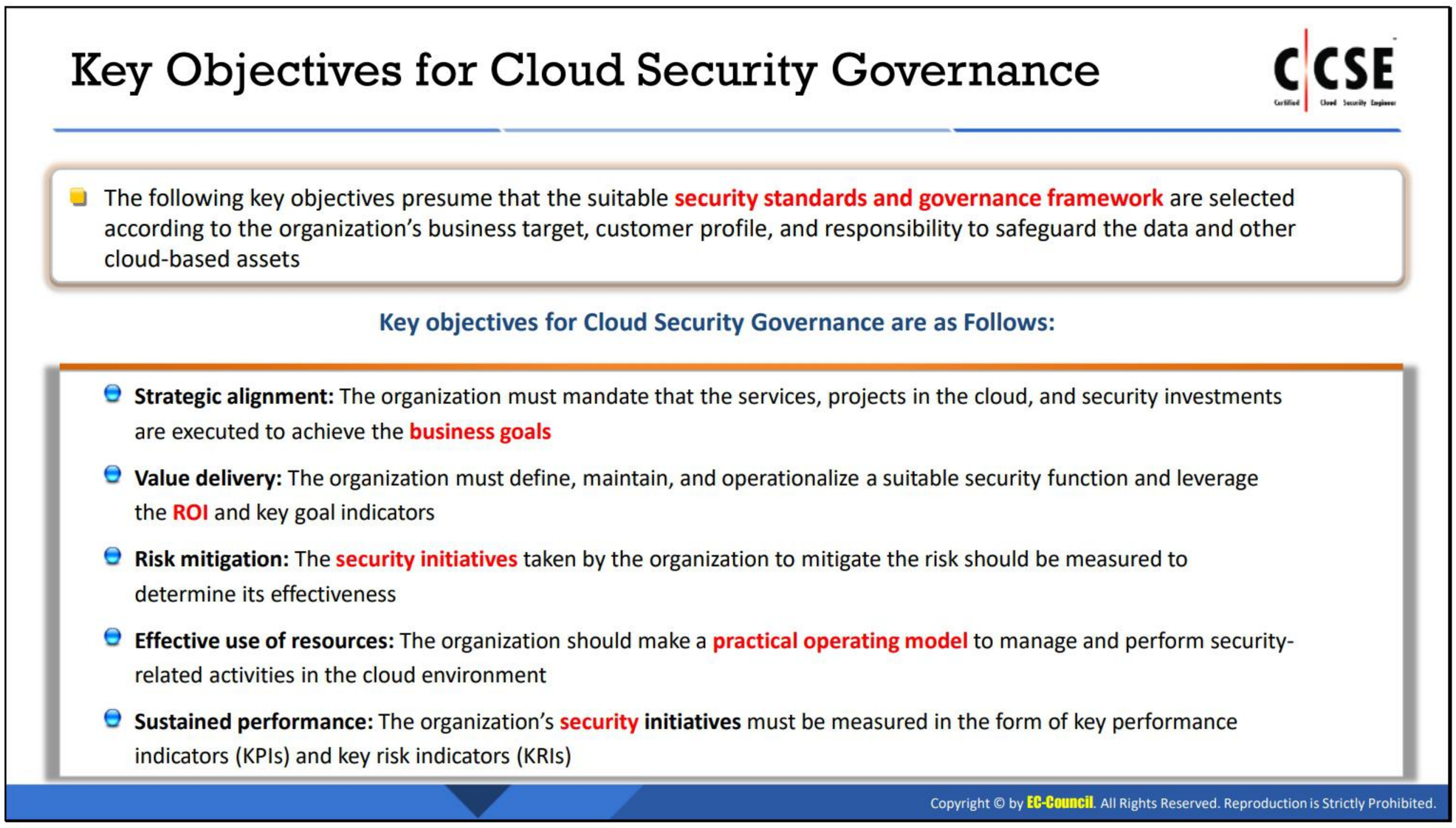
Principle 5: Enforcement of Vitality Processes to Achieve Continuous Improvement

Organizations undergo continuous improvements owing to changes in demand and innovative business objectives. The cloud computing governance process must include options for monitoring events that cause continuous improvements and must adapt to these changes. The continuous improvement process is most effective when the areas being governed are adjusted to changes. Other recommendations for achieving continuous improvement are as follows.

- Implement proactive and reactive measures for improvements.
- Ensure the implementation of appropriate infrastructure to monitor the cloud governance process.

hide01.ir

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



Key Objectives for Cloud Security Governance

To build a cloud security governance model for an organization, the security governance analyst needs strategic-level security management; governance frameworks such as Control Objectives for Information and Related Technologies (COBIT); suitable security standards; and frameworks such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and CSA (Canadian Standards Association) standards. The security governance analyst should visualize the entire governance structure and inherent components as well as perform designing and implementation. The minimum standards of security controls can be achieved by utilizing suitable security standards and frameworks. The customer and regulatory compliance requirements should be met wherever necessary. The governance framework delivers referential guidance as well as best practices to create a cloud governance model of security.

The following key objectives presume that the security standards and governance frameworks are selected based on the organization's business target, customer profile, and responsibility to safeguard data and other cloud-based assets. The key objectives for cloud security governance are as follows.

Strategic Alignment: The organization must mandate that the services, projects in the cloud, and security investments meet business goals for indicators such as operational performance and market competitiveness.

Value Delivery: The organization must define, maintain, and operationalize a suitable security function and leverage the return on investment (ROI) and key goal indicators.

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

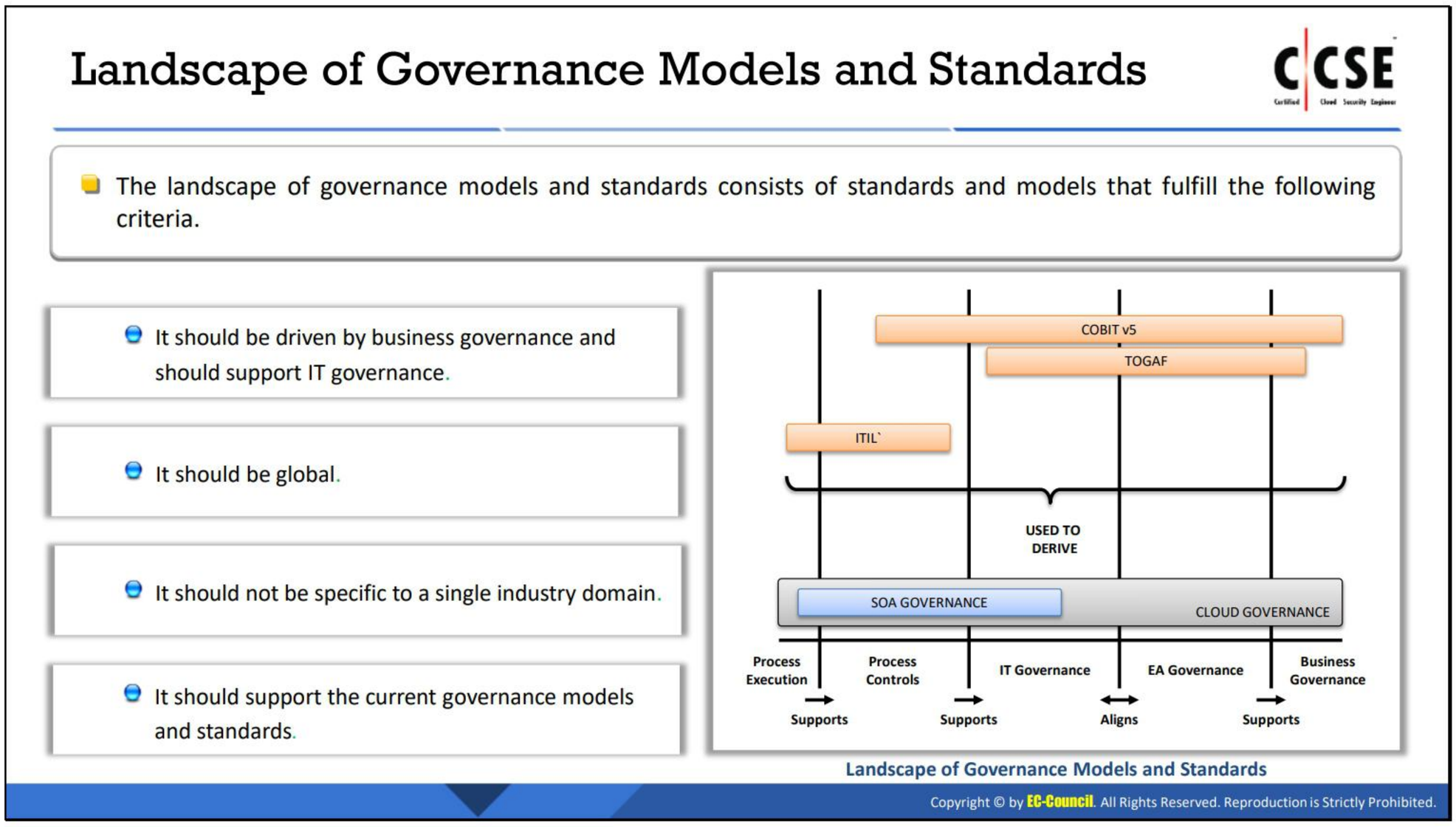
Risk Mitigation: The security initiatives taken by the organization to mitigate risk should be measured to determine their effectiveness. The results obtained from the security initiatives must indicate a reduction in risk over time.

Effective Use of Resources: The organization should create a practical operating model to manage and perform security-related activities in the cloud environment including the utilization of appropriate tools to enhance efficiency.

Sustained Performance: The organization's security initiatives must be measured in the form of key performance indicators (KPIs) and key risk indicators (KRIs), and these indicators must result in the target key goal indicators (KGIs).

hide01.ir

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



Landscape of Governance Models and Standards

The landscape of governance models and standards comprises the standards and models that satisfy the below criteria.

hide01.ir

- Driven by business governance
- Supports IT governance
- Global
- Not specific to a single industry domain
- Supports the current governance models and standards

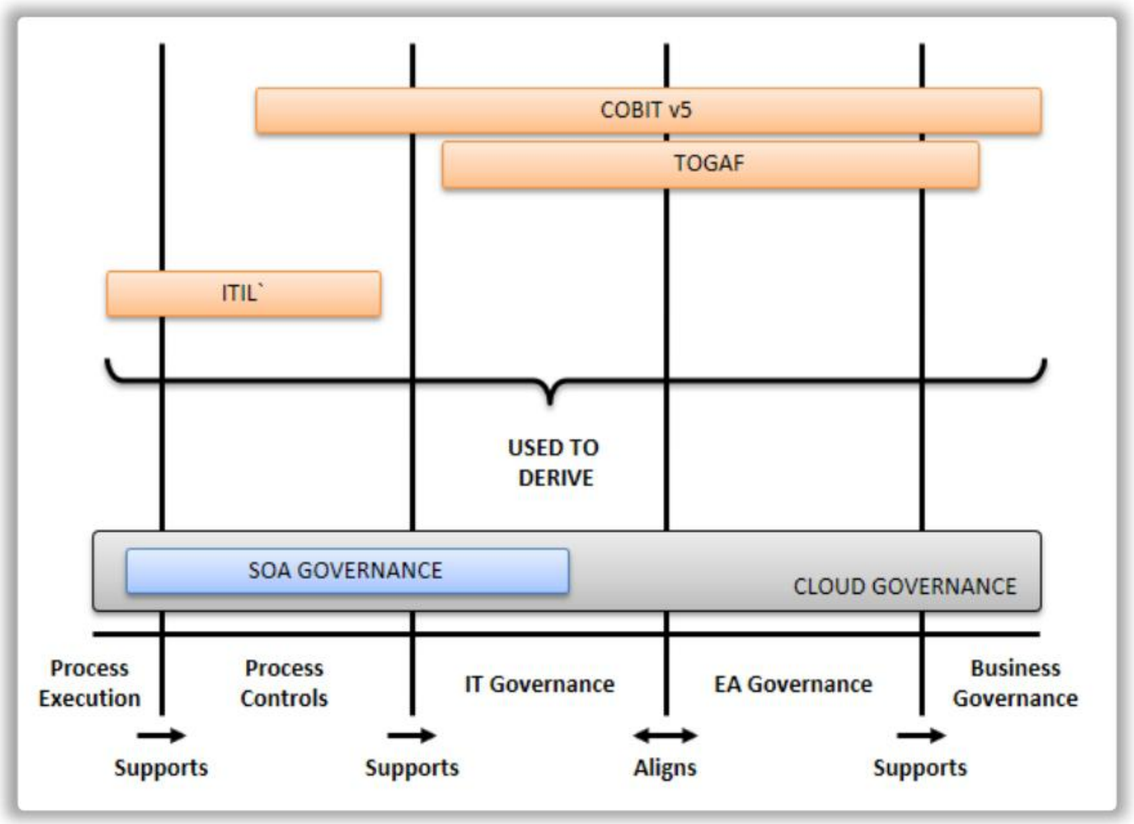


Figure 10.6: Landscape of Governance Models and Standards

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

The above diagram describes the relations among different frameworks in the landscape of governance models and standards. In the diagram, the domains of strategic importance are vertically split from left to right. Each domain is related to the next domain. IT governance and EA governance are aligned with each other, and both are included in the technology governance domain.

The framework of cloud computing governance is a subset of business governance, which also includes enterprise architecture (EA) and IT governance. However, it has some necessary characteristics distinct from the characteristics of other governance types. IT and EA governance enables business governance, which refers to the overall governance of the business.

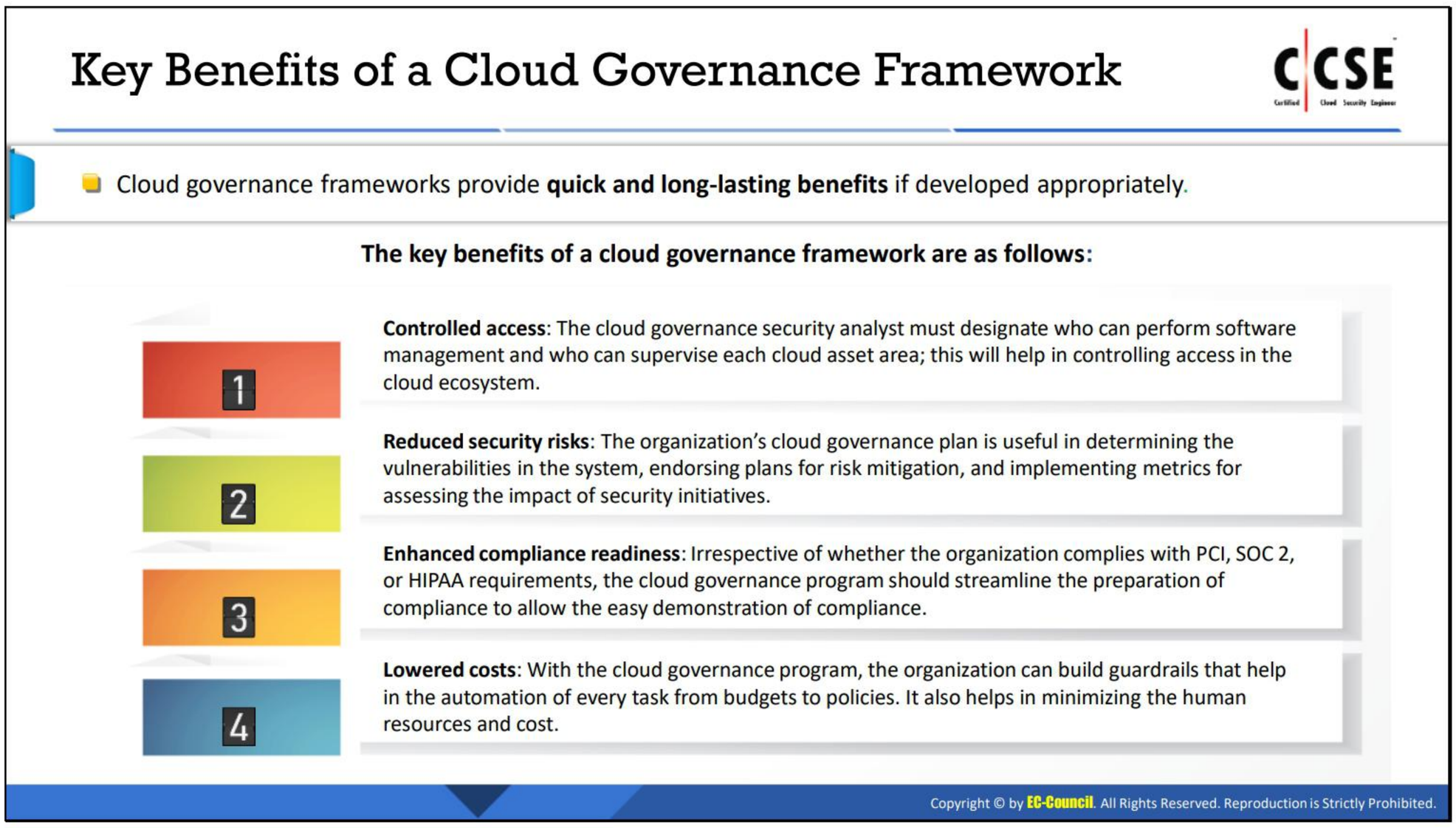
IT governance (COBIT) directs the creation of business value by optimizing IT benefits, risk, resources, and value delivery. A particular aspect of IT governance that concerns the risk, resources, and benefits of cloud computing is included in the cloud computing governance framework.

EA governance or The Open Group Architecture Framework (TOGAF), along with IT governance, is an important management process for efficient IT governance. Particular aspects of EA governance are covered in the cloud computing governance framework and are considered important.

Service governance is addressed by ITIL v3, which includes the service strategy, IT services, design, and operation of the business. Cloud computing governance features are covered in the cloud computing governance framework for design, operation, and business and IT service strategy.

The cloud computing governance framework is built on the foundation of the service-oriented architecture (SOA) governance framework. For robust cloud computing governance, IT, EA, service management, and SOA governance are necessary.

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



Key Benefits of a Cloud Governance Framework

Designing and enforcing a robust cloud governance framework take a large amount of time and effort. An appropriately developed cloud governance framework provides quick and long-term benefits. The key benefits of the cloud governance framework are as follows.

hidan91.ir

Controlled Access

The cloud governance security analyst must decide who performs software management and who supervises each cloud asset area; this helps in controlling access in the cloud ecosystem. Controlling access to critical cloud assets is important, as it improves the reliability of cloud processes.

Reduced Security Risks

When an organization wants to move its data to the cloud, it must enforce security measures that can safeguard the data. Compared to on-premises storage and hosting of the data, cloud storage and hosting are much easier, but the risk of data breaches and unauthorized access is higher in the cloud environment. The organization's cloud governance plan is useful in determining the vulnerabilities in the system, endorsing plans for risk mitigation, and implementing metrics for assessing the impact of security initiatives.

Enhanced Compliance Readiness

Every organization must clear audit and compliance assessments. Irrespective of whether the organization complies with Payment Card Industry (PCI), System and Organization Controls 2 (SOC 2), or HIPAA requirements, the cloud governance program should streamline the preparation of compliance and allow the easy demonstration of the compliance.

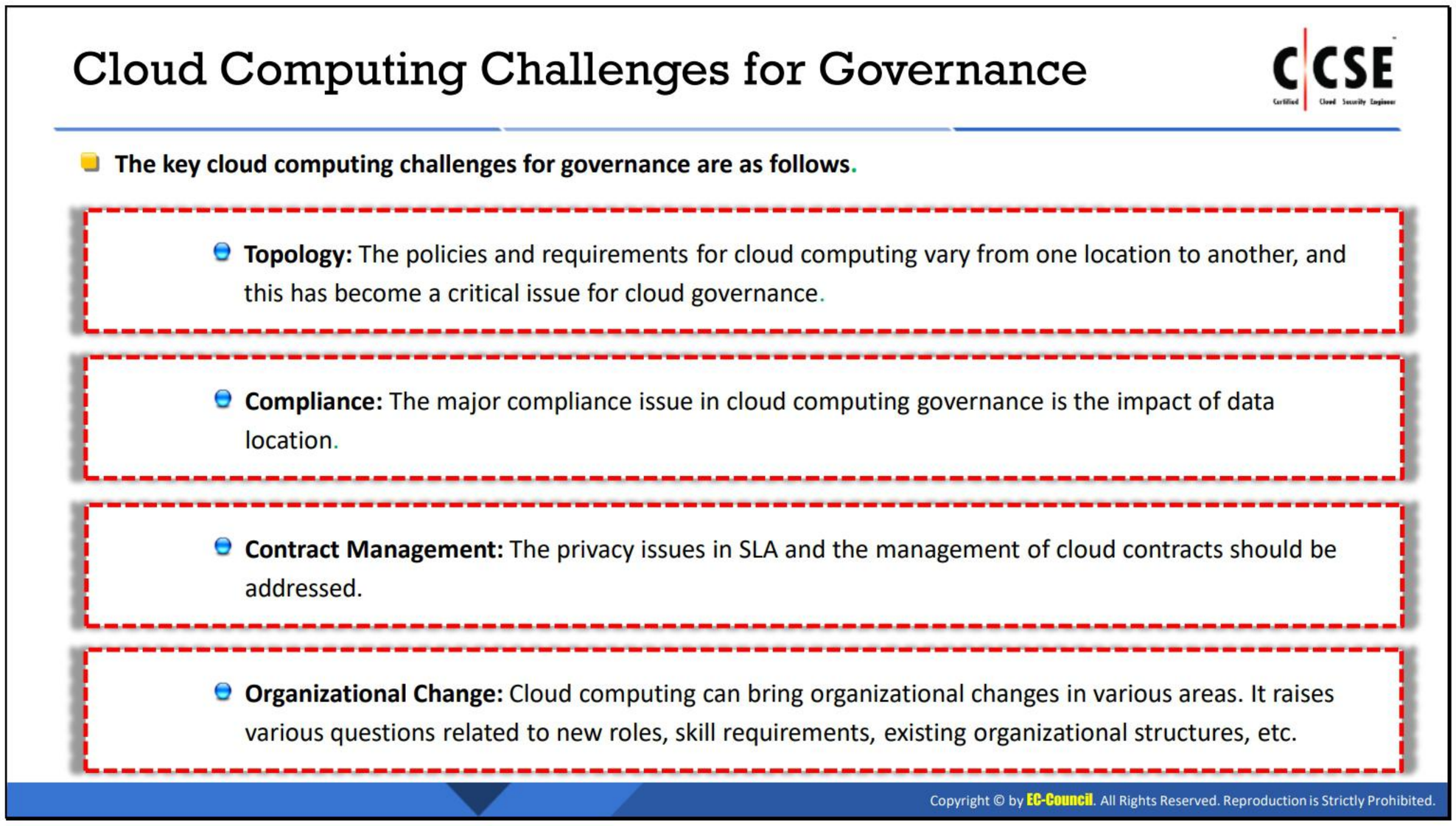
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lowered Costs

With cloud governance, the workflow can be shifted from manual to automated. That is, the organization toned not rely on time-consuming manual processes. With a cloud governance program, the organization can build guardrails that help in automating tasks ranging from budgets to policies. It also helps in minimizing human resources and cost.

hide01.ir

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



Cloud Computing Challenges for Governance

Cloud computing provides a secure environment to the organization for meeting their computing needs and business objectives. In the cloud computing environment, the cloud consumer is considered the principal, and the cloud service provider (CSP) is considered an agent. A mechanism should be implemented for reducing the risks and cost when operational controls are outsourced from the principal to the agent. This change of responsibilities can pose challenges, which can be resolved through governance. Initially, the interests of the principal and agent might differ, but they should be balanced to reach the goals of minimizing cost, providing robust security, establishing multi-tenancy, etc.

The key challenges to cloud computing are as follows.

Topology: Cloud computing comprehensively changes isolated dedicated IT scenarios to scenarios that involve the cooperation and collaboration of various services that are provided by different external or internal CSPs. This has created IT and business topologies that are distributed across many domains and delineated by boundaries such as geographical, architectural, governmental, and corporate boundaries. Consequently, the governance of the cloud environment is also distributed.

This distribution needs the implementation of a proactive approach to understand, delegate, and govern the concerning authority, accountability, and responsibility. Occasionally, the cloud consumer does not know the location of the server used for storing and processing data and applications. Irrespective of whether the data is at rest or in motion, the physical location and transition between locations affect the organization's capability to meet its policies and requirements, which are, in turn, affected by governmental regulations and statutes.

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

As these policies and requirements vary from one location to another, this has become a critical issue in cloud governance. Apart from the physical location issues, data protection issues also arise from multi-tenancy. Securely storing the data and allowing permission only to authorized users require the placement of appropriate controls. This is challenging because the data are stored in the CSP's infrastructure, which is not under the direct control of the data-owning organization.

Therefore, a cloud governance framework that can integrate and interlock the organization policies and standards with the CSP is important to verify, establish, and maintain end-to-end security across a distributed cloud environment.

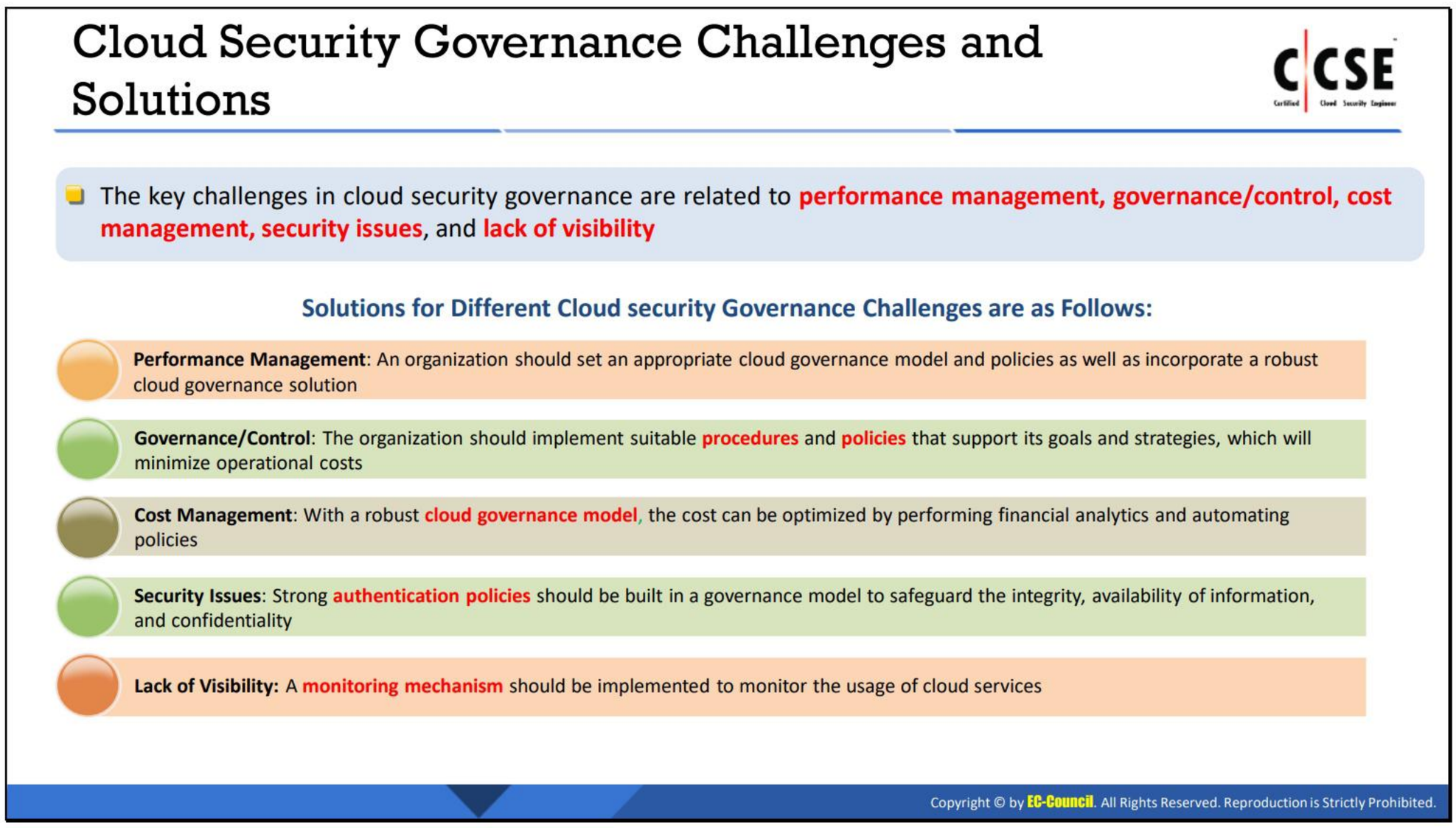
Compliance: The major compliance issue in cloud computing is the impact of data location. The use of an in-house data center allows an organization to have complete knowledge about the location of data and the appropriate controls that safeguard the data in compliance with regulations. In contrast, the data in the cloud are redundantly placed at various geographical locations. In such a situation, detailed information regarding the data of the organization is not available, or the cloud service provider (CSP) does not disclose the information. These conditions increase the uncertainty and raise various questions such as whether sufficient controls are safeguarding the organization's data and whether legal and regulatory requirements are appropriately met. Although security certifications and external audits can mitigate these issues to a certain extent, these are not satisfactory. In case of a violation, heavy fines and penalties will be levied on the organization. Therefore, cloud computing governance must set up appropriate monitoring procedures and processes for auditing and verifying compliance.

hide01.ir

Contract Management: Cloud services have both functional and non-functional characteristics, and the service-level agreements (SLAs) between cloud consumers and CSPs should address them. Security and privacy are considered non-functional requirements for cloud-based solutions. It is recommended to address the privacy issues in SLAs and cloud contracts. The staff of an organization, who is responsible for controlling access and security to personally identifiable information (PII), should ensure that the CSP adheres to the agreed security and privacy policies. Cloud computing governance ensures that CSPs maintain compliance with their policies as mentioned in the SLAs, including security and privacy policies.

Organizational Change: Cloud computing can cause organizational changes in various areas. It raises various questions related to new roles, skill requirements, existing organization structures, etc. This impact is alleviated through governance, which ensures that all the decisions related to the organization are taken within a suitable framework, considering the core principles and communicating the changes in a timely manner.

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



Cloud Security Governance Challenges and Solutions

The challenges to cloud security governance are as follows.

Performance Management: When an organization utilizes a cloud service, the CSP is responsible for providing services and scaling up performance. If the CSP shuts down, then all the customer services, including cloud governance services, also shut down. To prevent such a situation, an organization should set an appropriate cloud governance model and policies as well as incorporate a robust cloud governance solution.

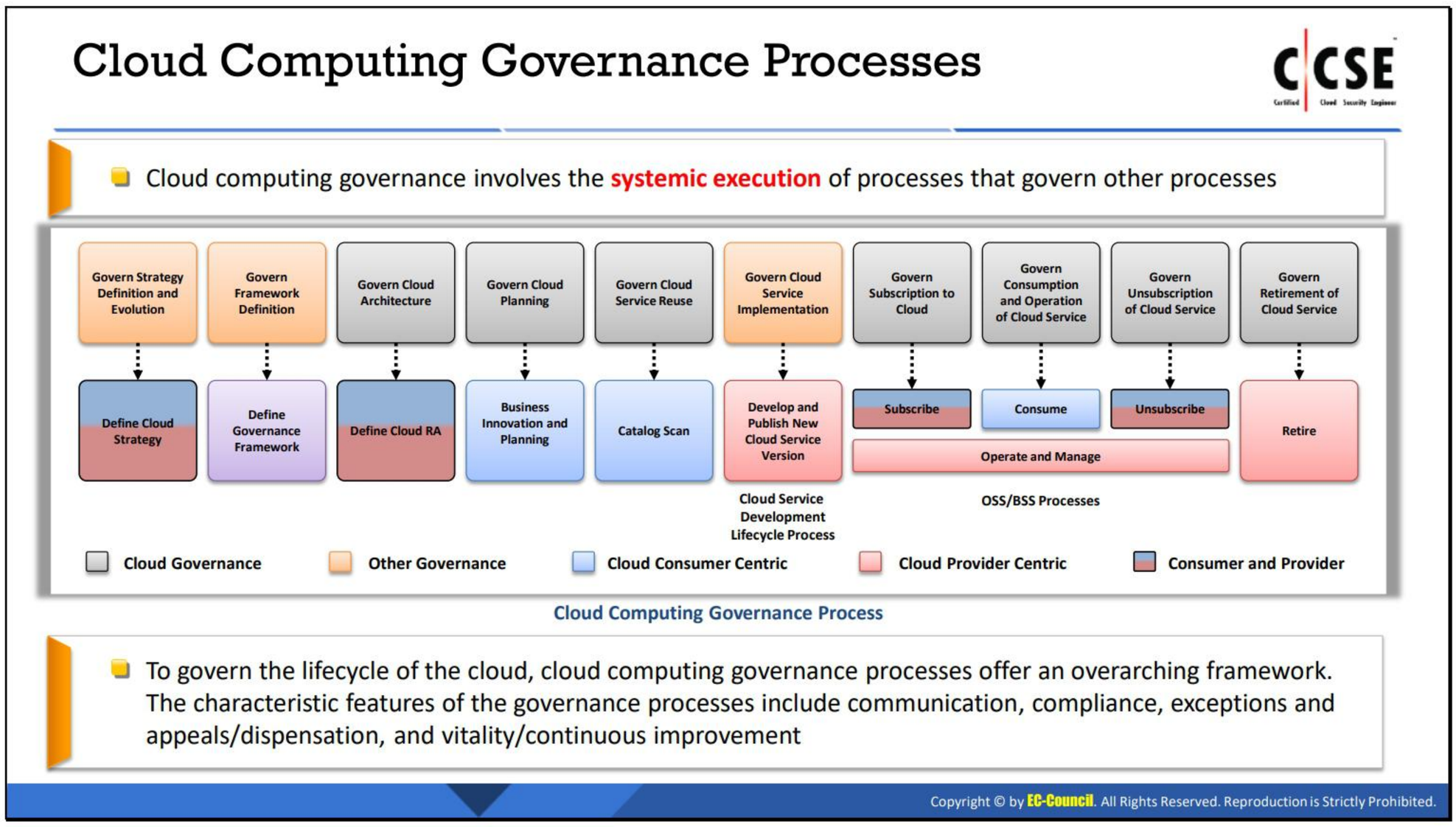
Governance/control: The organization should implement suitable procedures and policies that support its goals and strategies. This not only minimizes operational costs but also helps in growing the business.

Cost Management: As cloud-based services are cost-effective, the companies that are embracing these services have been profiting. Cloud-based policies are meticulously designed to ensure high profits to the customers. In a robust cloud governance model, the cost can be optimized by performing financial analytics and automating policies or incorporating the management reporting practice.

Security Issues: Data security is an important concern in cloud computing. Data security issues can be prevented by implementing the best practices, strict rules, and policies for cloud governance. Strong authentication policies should be built in a governance model to safeguard the integrity, availability of information, and confidentiality.

Lack of Visibility: A monitoring mechanism should be implemented to monitor the usage of cloud services. This will help cloud customers in viewing the current charges, and a notification will be sent to a customer if they exceed the limit.

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



Cloud Computing Governance Processes

Cloud computing governance involves the systemic execution of processes that govern other processes. Cloud initiatives have a lifecycle, and all cloud initiatives should be continuously governed through an overarching governance framework. There is no start or end to cloud computing governance; rather, it is enforced across the lifecycles of all the cloud initiatives in the cloud ecosystem.

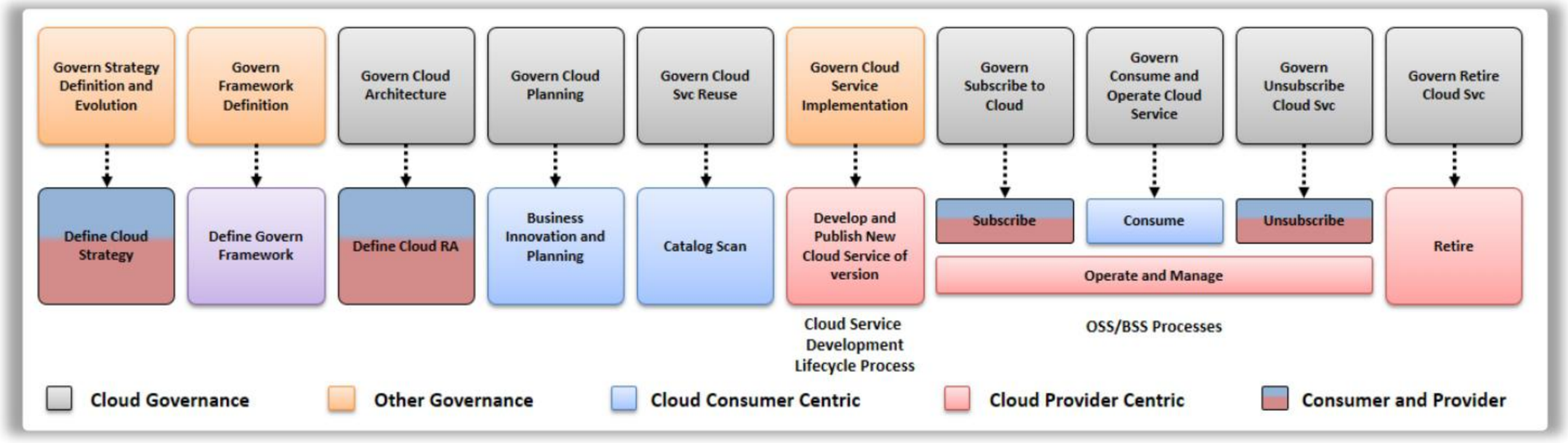


Figure 10.7: Cloud Computing Governance Process

The lifecycle of cloud initiatives should be governed using the overarching framework provided by the cloud computing governance processes. The features of the governance processes are as follows.

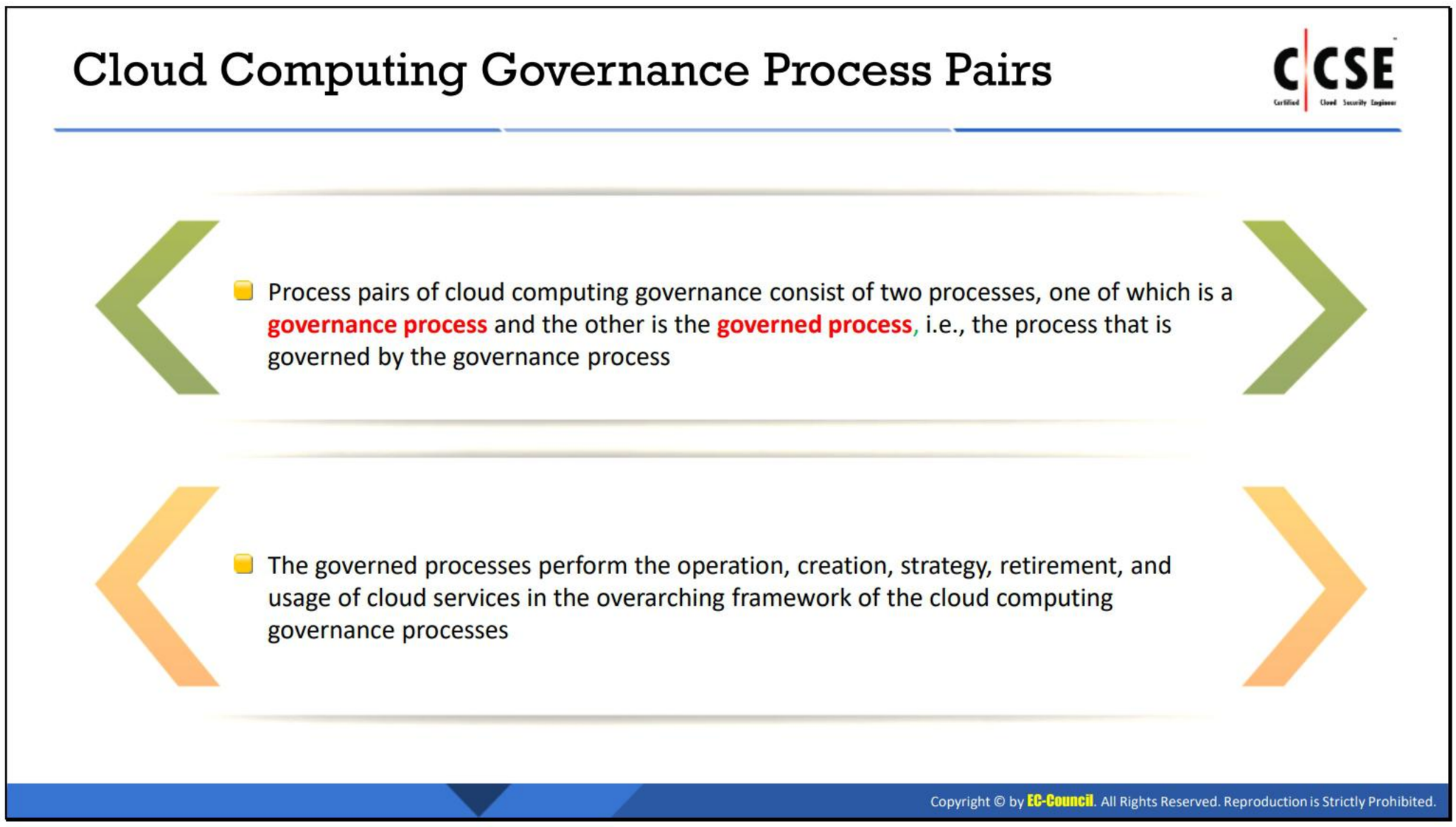
- **Communication**: Ensure that all staff members know their responsibility and the correct ways to fullfil their responsibilities.
- **Compliance**: Ensure that all staff members abide by the standards, policies, guidelines, best practices, and principles.

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

- **Exceptions and Appeals/dispensation**: Allow edge-of-the-bell-curve requirements for special treatment and quick consideration.
- **Vitality/continuous Improvement**: Ensure that services do not fail and perform continuous improvement.

hide01.ir

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



Cloud Computing Governance Process Pairs

It is important to have a clear understanding that governance processes are not equivalent to governed processes. The cloud computing governance process has an overarching framework. The governed process includes the operation, creation, strategy, retirement, and usage of cloud services.

Cloud computing governance process pairs comprise two types of processes: governance processes and governed proceses (processes governed by governance process). The following table describes cloud governance process pairs.

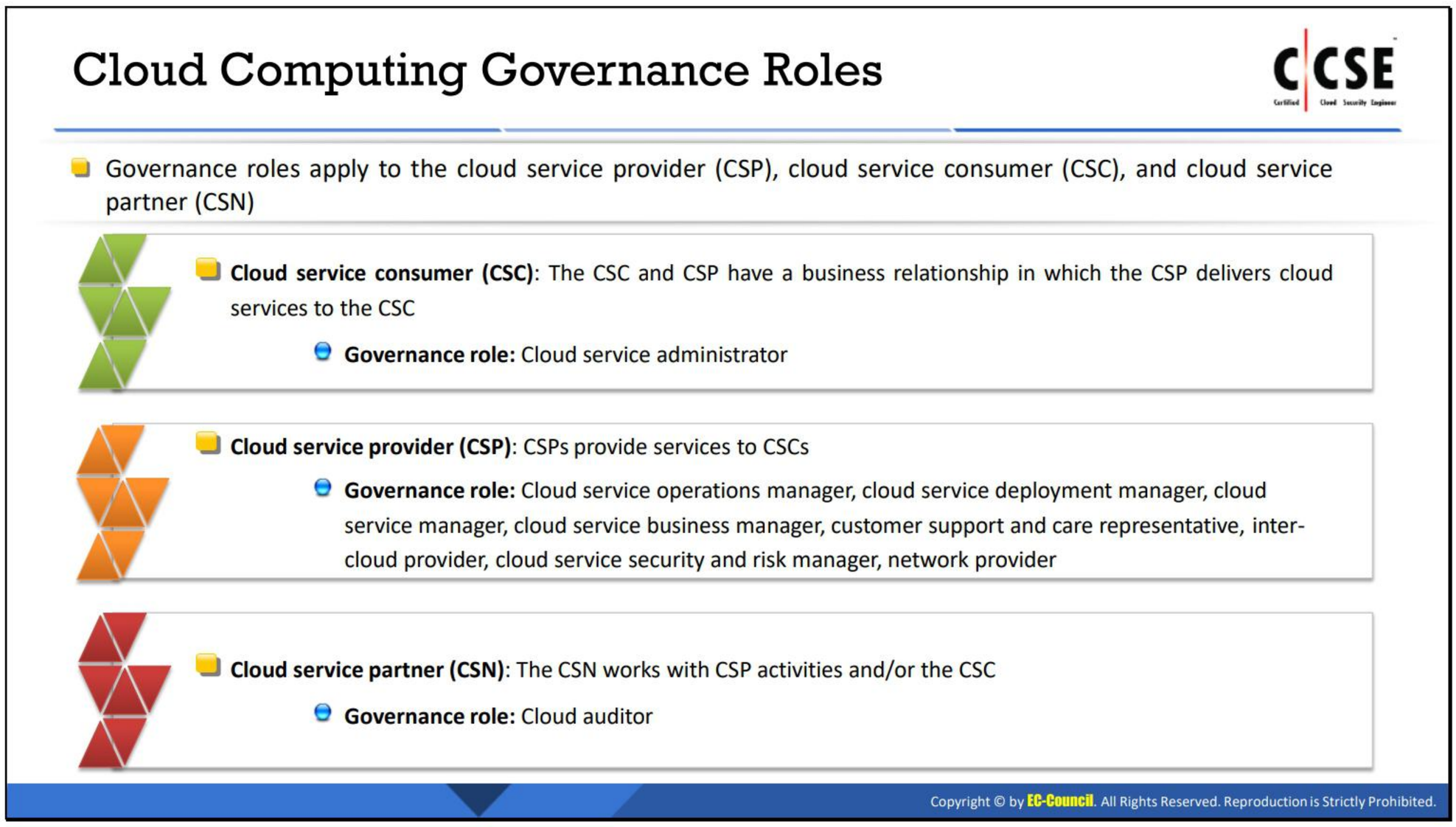
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Process Pair	Description
Planning	For cloud transformation, the planning process makes a business case. The cloud computing governance process that is applied on this process ensures that the planned business initiatives select suitable cloud services and strengthen the cloud transformation strategy.
Reference Architecture	For cloud transformation, the reference architecture process defines the reference architecture. The cloud computing governance process ensures that the reference architecture is consistent and as per industry standards.
Subscribe	This process ensures that the CSP services satisfy the customer requirements. It helps in the execution of a service contract with an appropriate funding model.
Service Reuse	This process can enhance the proper service utilization in cloud, prevent redundant services, and ensure the presence of proper services in the service catalog.
Unsubscribe	This process ensures that cloud service discontinuation is in line with the contract.
Consume	This process summarizes how the customer ensures that the service works as expected. It includes recording appropriate measurements about the service behavior and then performing analysis to determine SLA exceptions and actions that should be initiated to resolve the exceptions.
Operate	This process helps in incident monitoring. Suitable measurements are performed, which will help the customer as well as CSP to initiate appropriate action.
Retire	This process identifies outdated services, notifies the stakeholders, and takes the decision to retire service. It takes suitable mitigation measures to reduce the impact of the retired service on the customer base.

Table 10.1: Cloud Governance Process Pairs

h1de01.ir

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



Cloud Computing Governance Roles

Governance roles apply to the cloud service provider (CSP), cloud service consumer (CSC), and the cloud service partner.

hide01.ir

Cloud Service Consumer (CSC): The CSC and CSP have a business relationship in which the CSP delivers cloud services to the CSC. The CSC also has a business relationship with the cloud service partner for various reasons. Important activities performed by the CSC include the selection, monitoring, implementation of reporting, and ensuring the security of the cloud services. CSC ensures IT/business alignment and the interoperability of the service provider.

Governance Role: Cloud service administrator

Governed Role: Cloud service user, cloud service business manager, cloud service integrator

Cloud Service Provider (CSP): CSPs provide services to CSCs. The role and sub-roles of the CSP are aimed at delivering cloud computing activities that are required to deliver a cloud service.

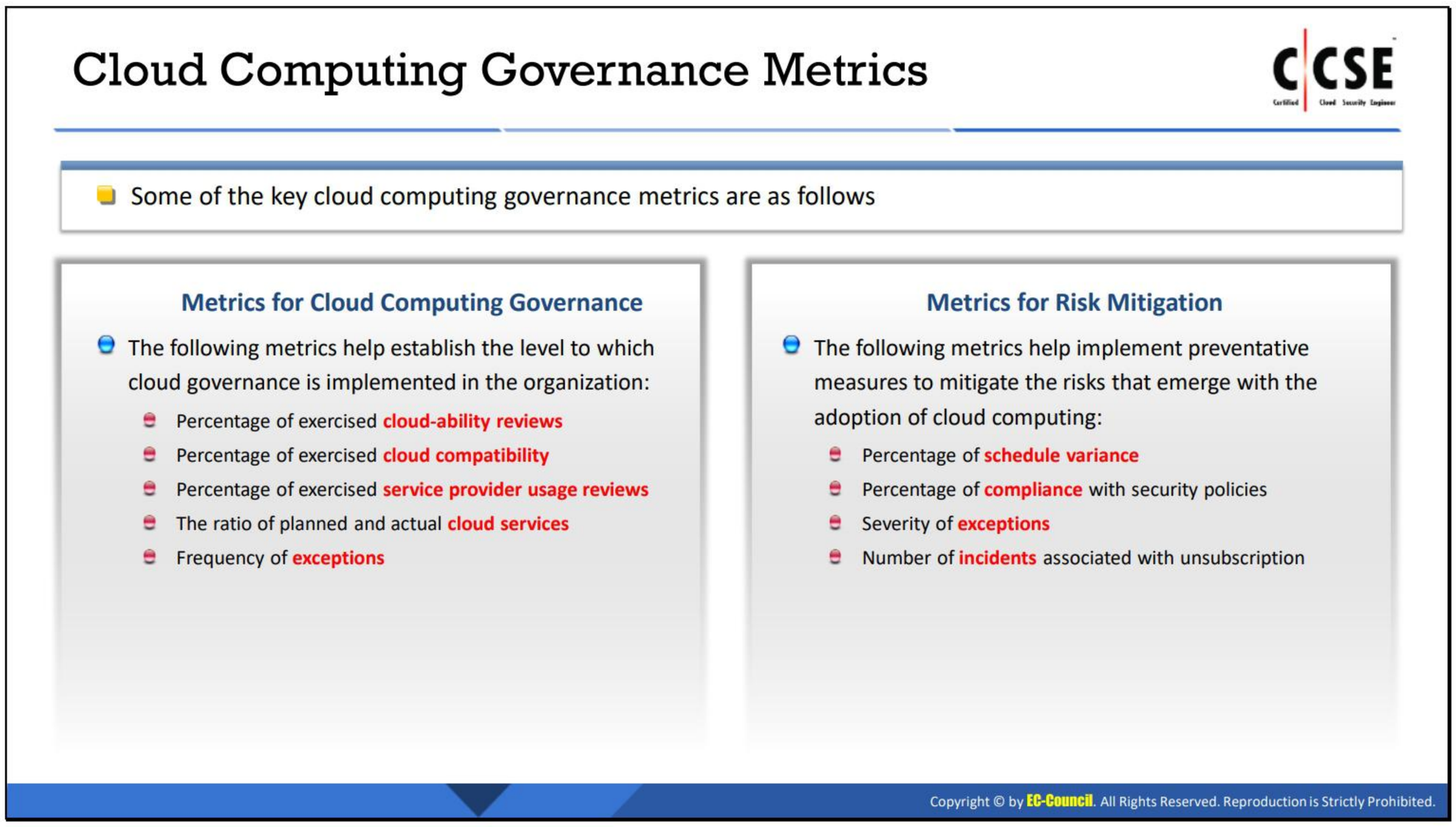
Governance Role: Cloud service operations manager, cloud service deployment manager, cloud service manager, cloud service business manager, customer support and care representative, inter-cloud provider, cloud service security and risk manager, network provider

Cloud Service Partner: The cloud service partner works with CSP activities and/or the CSC. The cloud service partner creates, designs, maintains, and enhances service components, in addition to ensuring adherence to audit and security controls.

Governance Role: Cloud auditor

Governed Role: Cloud service broker, cloud service developer

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



Cloud Computing Governance Metrics

Cloud computing governance metrics can be tracked across different process pairs. The metrics are tracked to determine the level of cloud adoption, level of cloud computing governance, operational efficiency, etc. The cloud computing governance metrics are as follows.

hidd01.ir

Metrics for Cloud Adoption

The cloud computing adoption level in an organization is determined by tracking the following metrics.

- Percentage of existing projects not included in cloud transformation
- Percentage of cloud services subscribed to by the organization
- Average number of subscribers for a cloud service
- Percentage of consumption patterns (IaaS, PaaS, and SaaS)
- Rate of change in the number of subscribers

Metric for Cloud Computing Governance

The cloud computing governance adoption level in an organization is determined using the following metrics.

- Percentage of exercised cloud-ability reviews
- Percentage of exercised cloud compatibility
- Percentage of exercised service provider usage reviews
- Ratio of planned and actual cloud services

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

- Frequency of exceptions

Metrics for Operational Efficiency

The operational efficiency parameters for the sustenance of infrastructure and application components are tracked using the following metrics.

- Percentage of reported incidents
- Average time required for deployment
- Average time required for onboarding

Metrics for Cost Reduction

The following metric is used to determine the funding for cloud transformation in an enterprise.

- Percentage of budget allocated for IT

Metrics for Business Value Alignment

The extent to which cloud adoption is aligned with an organization's business objectives is determined using the following metrics.

- Percentage of decrease in the services that are idle
- Percentage of achieved business service–level requirements
- Ratio of the number of subscriptions to the number of non-subscriptions

hide01.ir

Metrics for Service-driven Integration

The level of cloud computing deployment that is built on existing service-based systems is tracked using the following metrics.

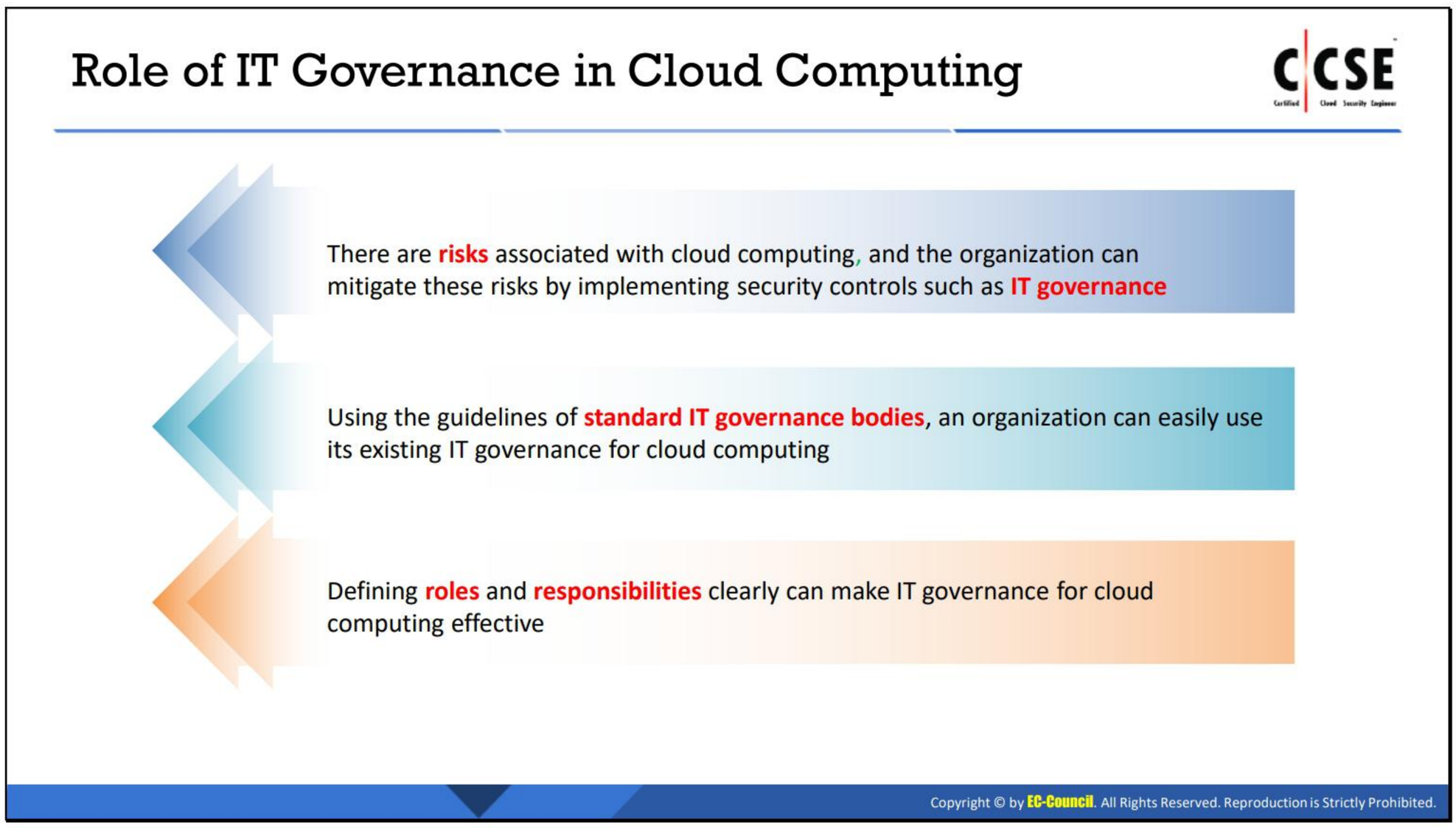
- Percentage of exceptions of the cloud service provider (CSP)/the integrations of the CSP
- Percentage of the enterprise services that are subscribed
- Impact of exceptions on the number of SLAs

Metrics for Risk Mitigation

The following are preventive metrics used to avoid the risks linked with cloud adoption.

- Percentage of compliance with security policies
- Percentage of schedule variance
- Severity of exceptions
- Number of incidents associated with unsubscription

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



Role of IT Governance in Cloud Computing

Cloud computing offers various benefits to an organization, but there are certain potential risks associated with cloud computing, which the organization must address. Security controls such as IT governance should be implemented to mitigate risks and to ensure that cloud computing adds value to the business.

IT delivers business value when the IT operations are aligned with the business, but business–IT alignment is a problem that can be solved through IT governance. Without this alignment, the business cannot deliver what the customers need, and IT cannot achieve what the business needs.

IT governance handles the risks associated with IT projects. It plays an important role in how the organization uses IT. Hence, IT governance is important for cloud computing to achieve business–IT alignment. The main objectives of IT governance are to guide the use of IT to add value to the business and to handle the risks associated with IT.

IT governance is a complex task, for which the Standard IT governance bodies have developed guidelines. Using those guidelines, an organization can easily use its existing IT governance for cloud computing. These guidelines can also be used to handle the risks associated with the adoption of cloud computing.

Using Existing IT Governance for Cloud Computing

Most of the standard bodies recommend using the existing IT governance for cloud computing. Applying the existing IT governance to cloud computing is helpful as the organization is familiar with it. Adding cloud computing to the existing IT governance can be easier than developing a new governance framework.

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

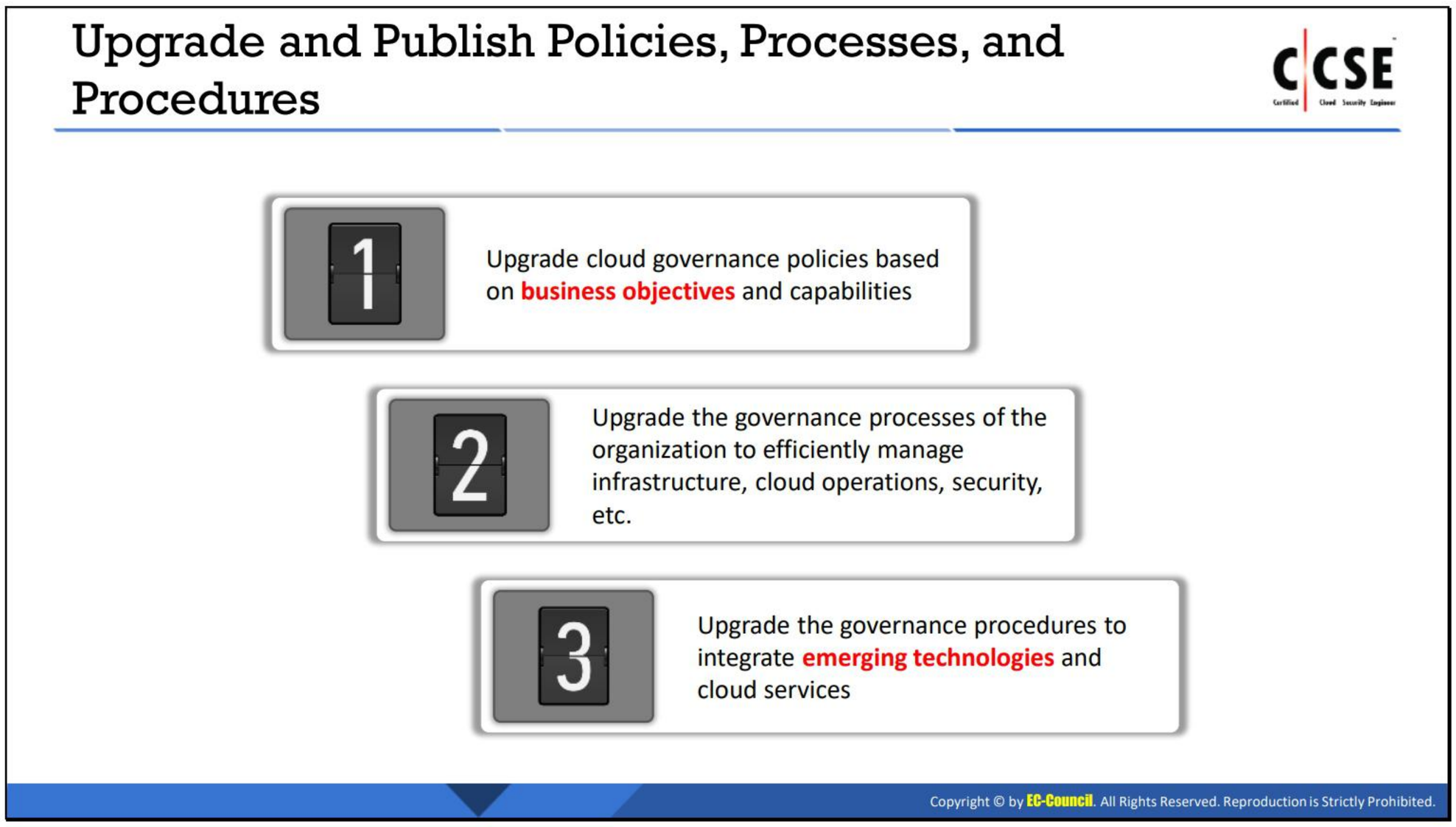
The International Organization for Standardization (ISO) is developing standards for cloud computing, and the Cloud Security Alliance (CSA) already has a reference architecture for a trusted cloud. Both standards provide IT governance for cloud computing.

Every organization must focus on the development of business goals for cloud computing and should assign roles and responsibilities for every level of management. Establishing business goals for cloud computing will align the business value with the adoption of cloud computing. The Information System Audit and Control Association (ISACA) helps an organization set business goals and objectives for cloud computing. ISACA developed an IT governance framework named Control Objectives for Information and Related Technologies (COBIT), which can be applied to cloud computing.

Organizations must also focus on properly defining roles and responsibilities. A clear definition of roles and responsibilities is important for establishing a governance framework. Pre-existing roles and responsibilities used by an organization for on-premises IT infrastructure can be modified to apply to cloud computing. Furthermore, defining proper roles and responsibilities reduces the gap in understanding responsibilities and authorities. The Committee of Sponsoring Organizations (COSO) describes roles and responsibilities for the board of directors, managers, chief executive officers, and internal auditors. COSO also provides a list of considerations for the board of directors and managers while migrating to cloud computing. Hence, defining roles and responsibilities clearly can make IT governance for cloud computing effective.

hide01.ir

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



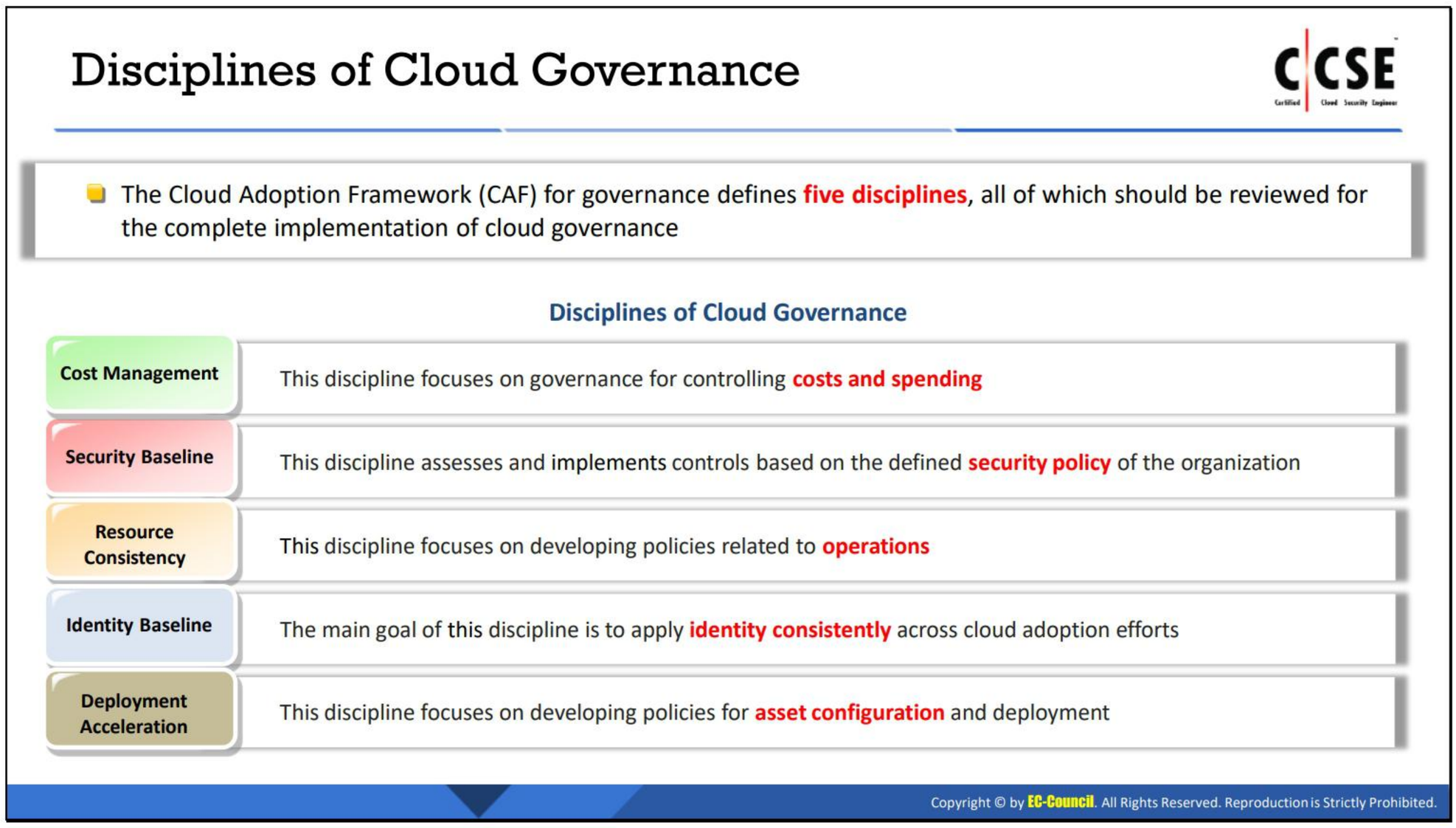
Upgrade and Publish Policies, Processes, and Procedures

Cloud governance includes policies and best practices. The policies are used for cost optimization, resilience, compliance, and security. Governance policies include protocols for regulating things on the cloud. Hence, governance policies should be created and reviewed by managers, business executives, and IT experts. The governance policies must include programming standards, standards for designing infrastructure, and security policies. Cloud governance policies should be upgraded based on business objectives and capabilities.

Governance processes provide a framework for governing the cloud lifecycle. The processes for modern organization and management techniques, namely, DevSecOps and Agile, should be upgraded to specify how to upgrade old technologies. Upgrading governance processes help organizations efficiently manage infrastructure, cloud operations, security, etc.

The procedures should also be upgraded to integrate emerging technologies and cloud services.

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



Disciplines of Cloud Governance

Irrespective of the cloud platform, the Cloud Adoption Framework (CAF) for governance defines five disciplines. All five disciplines should be reviewed for the complete implementation of cloud governance. The five disciplines of cloud governance are as follows.

Cost Management

Cost management is critical for business success and is in high demand. The cost management discipline focuses on governance for controlling costs and spending. Certain cost control policies should be developed to control costs. In this discipline, controls such as tagging, subscriptions, owners, and resource groups are important.

Security Baseline

This discipline concerns the security baseline throughout the cloud environment. The security baseline discipline assesses and implements controls based on the defined security policy of the organization. Once security requirements are defined, the cloud governance policies apply those requirements across the network, asset configuration, and data. This discipline creates a framework for the application team to build and adopt on the cloud.

Resource Consistency

Resources can quickly become out of control. The resource consistency discipline focuses on developing policies related to operations. The lack of a proper approach for deploying and managing resources can accelerate costs and security risks.

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

Identity Baseline

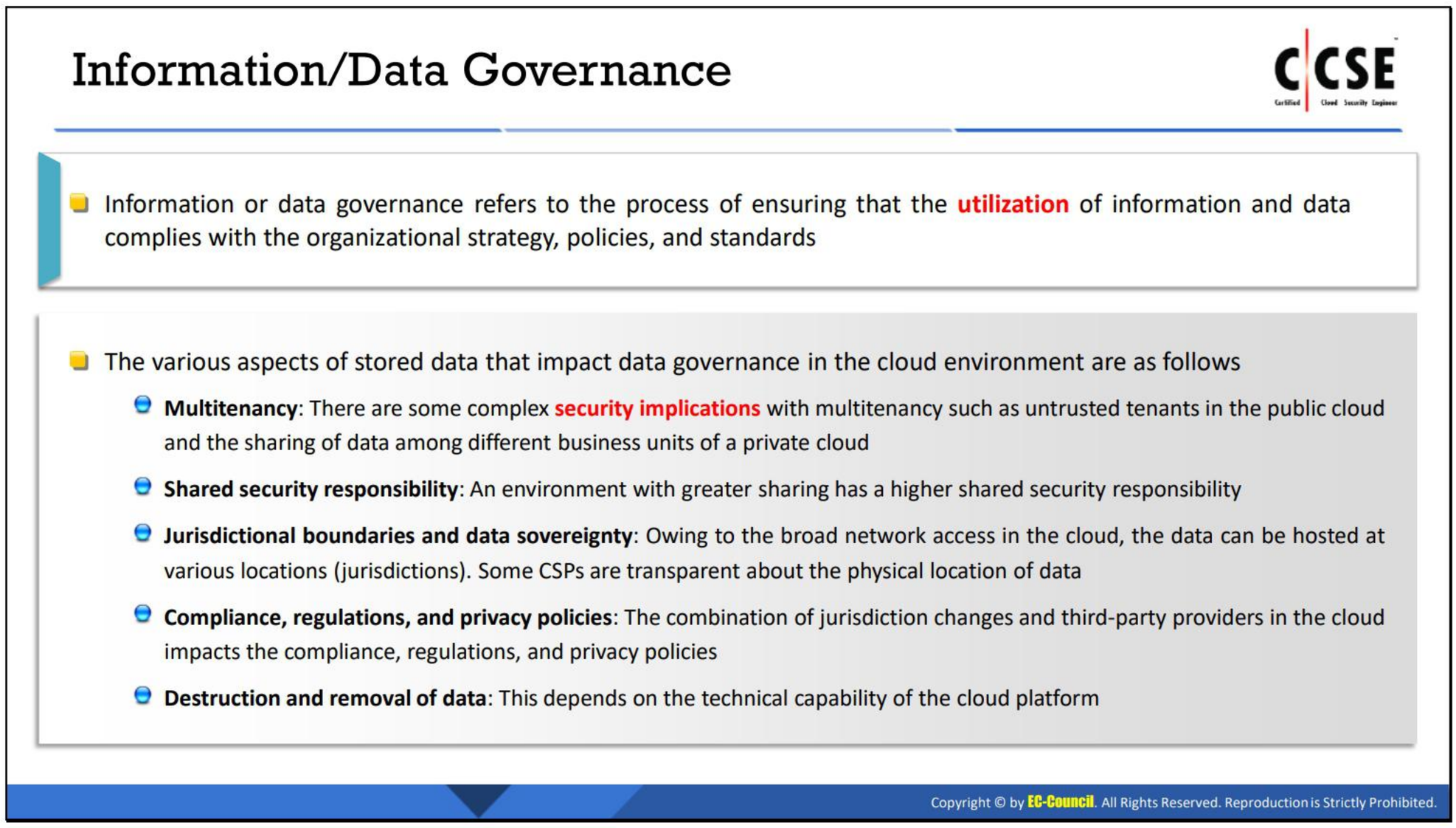
The identity baseline is one of the most popular requests made by cloud customers. It is a primary security parameter in the cloud. The main goal of the identity baseline discipline is to apply identity consistently across cloud adoption efforts.

Deployment Acceleration

This discipline focuses on developing policies for asset configuration and deployment. It reviews DevOps activities and searches for ways to automate processes to achieve consistency and accountability.

hide01.ir

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



Information/Data Governance

Information or data governance refers to the process of ensuring that the utilization of information and data complies with the organization's strategy, policies, and standards. This includes contractual, regulatory, and business objectives. Data governance helps organizations establish rules to manage different types of business data.

The data stored and managed by an organization are always subject to requirements imposed by the organization itself based on its risk tolerance or by others (e.g., regulatory agencies, partners, or customers). Data governance helps the organization handle data as per its requirements and objectives.

The various aspects of the data stored in the cloud environment that have an impact on information or data governance are as follows.

- **Multitenancy**: Multitenancy has some complex security implications. For example, in a public cloud environment, an organization's data are stored in infrastructure that is shared by different, untrusted tenants. Similarly, in a private cloud environment, the data are stored in infrastructure that is shared by various business units (within the same organization) that may have different governance needs.
- **Shared Security Responsibility**: When more parties share an environment, shared security responsibilities increase because data would be owned and managed by multiple teams or organizations. Thus, it is essential to identify the difference between data ownership and data custodianship.
    - **Data Ownership**: It refers to who owns the data. Data ownership depends on the law, contracts, and policies. For example, if an organization stores data of a customer, the data ownership will be either with the customer or the

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

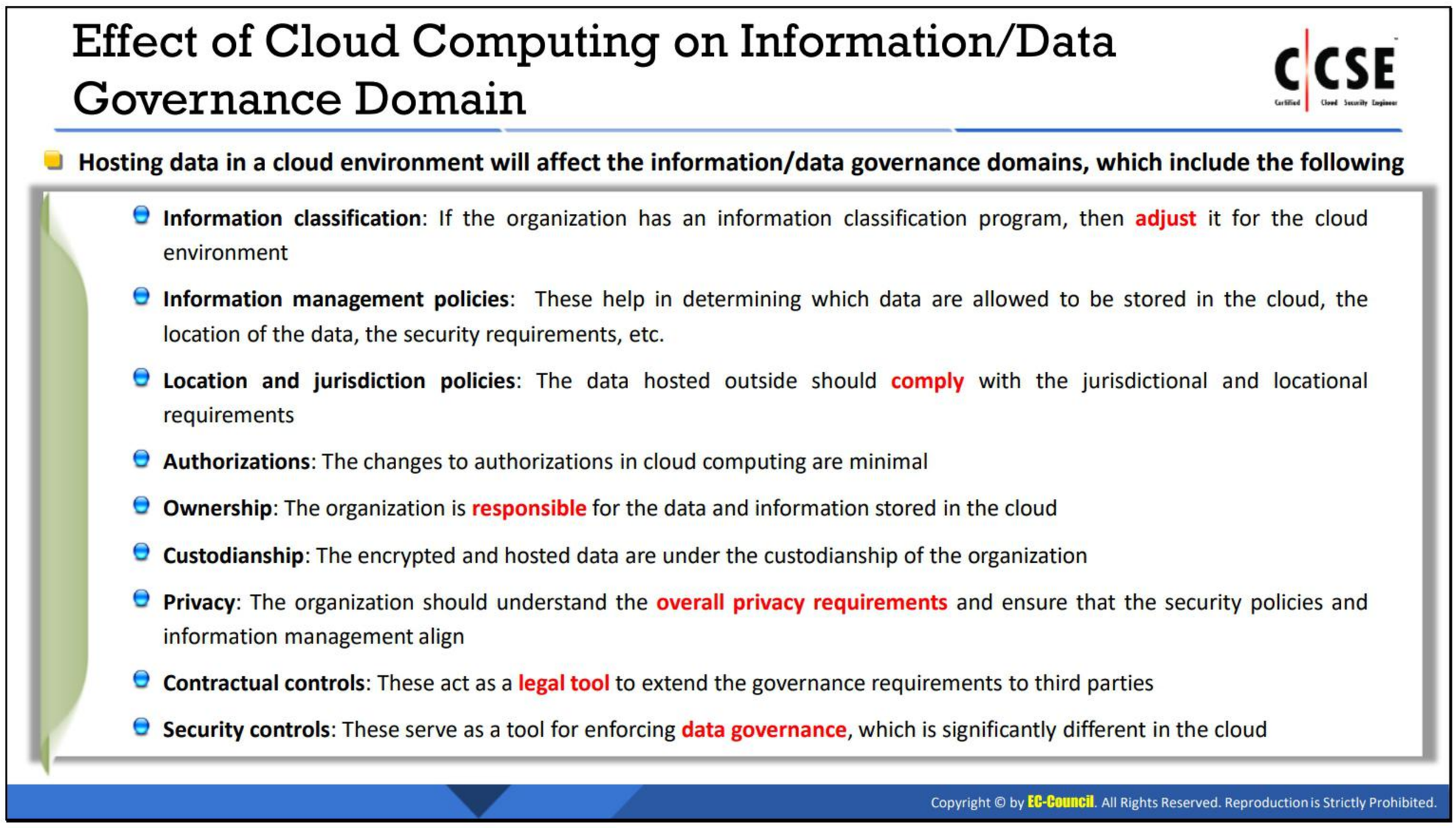
organization, depending on the contract, policies, and laws. Similarly, data hosted in a public cloud environment are owned by the customer, who stores the data as per the contract signed with the provider.

- **Data Custodianship**: It refers to who manages the data. When a customer's data are handled by an organization, the organization is considered a custodian of the data. Similarly, the data stored in a public cloud environment are owned by the customer, and the cloud provider serves as a custodian of the data. Data owners can select and define rules and regulations for data stored on the cloud, and the provider implements them.

- **Jurisdictional Boundaries and Data Sovereignty**: Owing to the broad network access in the cloud, data can be hosted at various locations (jurisdictions) and migrated anywhere. Some CSPs may not inform their customers about the physical location of their data. However, in other cases, data may be restricted to particular locations using additional controls.
- **Compliance, Regulations, and Privacy Policies**: The combination of jurisdiction changes and third-party providers in the cloud impacts compliance, regulations, and privacy policies. For example, an organization may or may not use/share the data of its customers stored on a cloud platform, depending on the terms of customer agreement.
- **Destruction and Removal of Data**: Data destruction and removal depend on the technical capabilities of the cloud platform. An organization using the cloud must ensure that data destruction and removal occur in accordance with its policies.

hidemi.ir

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



Effect of Cloud Computing on Information/Data Governance Domain

Since cloud environments are shared by multiple tenants simultaneously, it is essential for organizations using cloud services to ensure that their CSPs implement strong data governance practices to prevent valuable data from becoming compromised. Cloud computing requires data governance practices and standards that differ from on-premises data governance standards and practices because of its virtualized and distributed nature.

Hosting data in a cloud environment affects the information/data governance domains in the following ways.

Information Classification: Information classification is often related to compliance and has an impact on cloud destinations and handling requirements. If the organization already has an information classification program, then it can be adjusted for the cloud environment.

Information Management Policies: Information management policies help in determining which data are allowed to be stored in the cloud, the location of the data, the security requirements, etc. These policies are linked to information classification and must cover various SPI tiers because sending data to a software-as-a-service (SaaS) vendor is different from creating an infrastructure-as-a-service (IaaS) app.

Location and Jurisdiction Policies: Cloud computing directly affects location and jurisdiction policies because data hosted in the cloud are stored at different geographical locations. Data hosted outside the organization should comply with jurisdictional and locational requirements. To ensure compliance, organizations must take the help of their legal departments to understand the laws and contracts that can create conflicts while handling regulated data.

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

Authorizations: The changes to authorizations in cloud computing are minimal.

Ownership: The organization is responsible for the data and information stored in the cloud.

Custodianship: If the organization hosts its customers' data in a cloud environment, the cloud provider is the custodian of the data. However, encrypted data hosted on the cloud would still be under the custodianship of the organization (as the customers are the owners of the data).

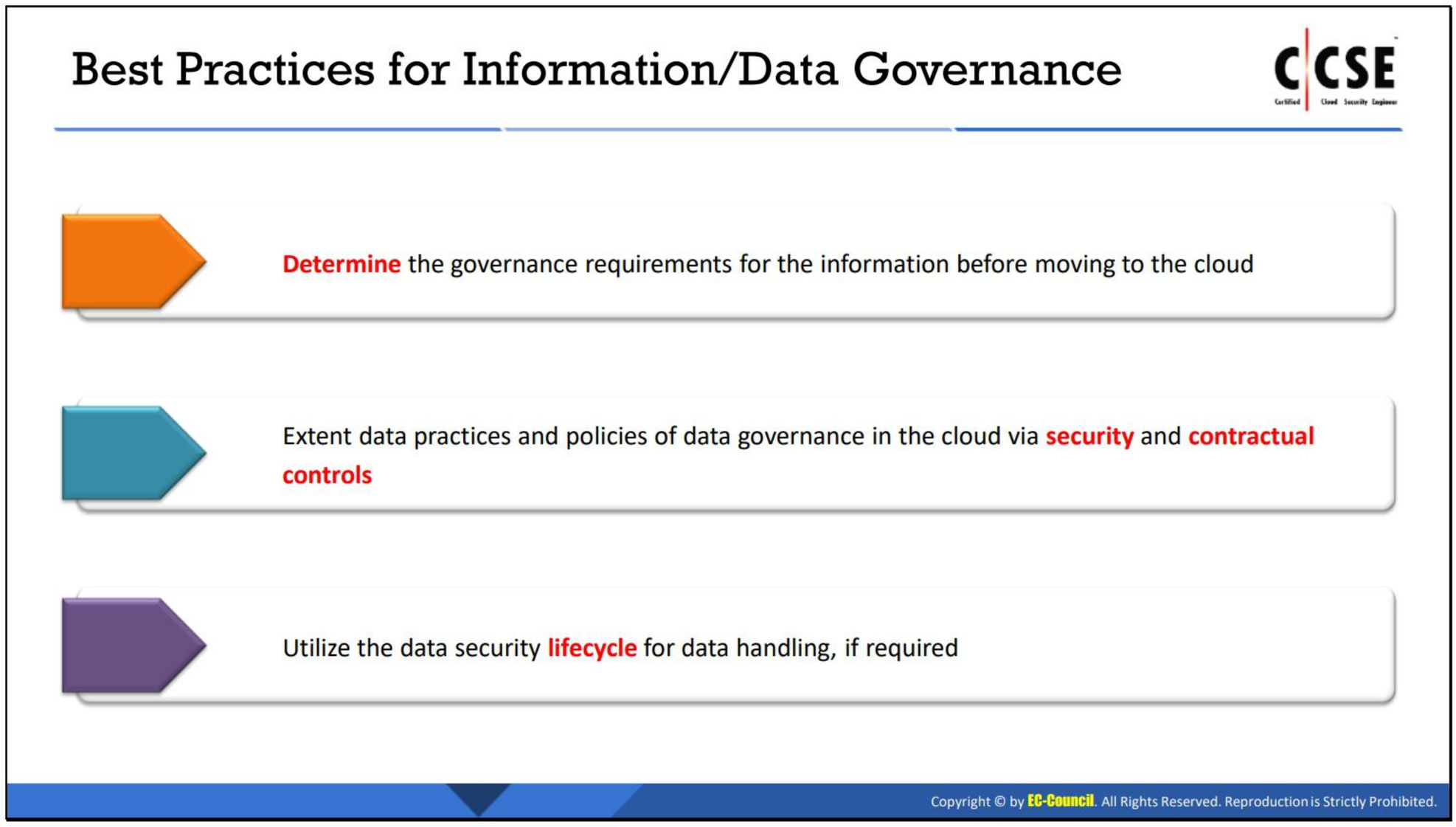
Privacy: Privacy is a combination of contractual obligations, regulatory requirements, and commitments to customers. The organization should understand the overall privacy requirements and ensure that its security policies and information management are aligned.

Contractual Controls: Contractual controls act as a legal tool for the organization to extend the governance requirements to a third party (e.g., a CSP). Contractual controls are different for cloud computing and on-premises environments. Public clouds offer limited access to contract clause negotiations.

Security Controls: These controls serve as an effective tool for enforcing data governance both in cloud and on-premises environments. Security controls deployed in the cloud are different from those used in an on-premises environment. In a cloud environment, the main security controls are access-control lists (ACLs) and security groups.

hide01.ir

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



Best Practices for Information/Data Governance

Organizations must ensure that strong data governance policies and practices are implemented in their cloud environments to secure their data.

hole01.ir

The key best practices for information/data governance include the following.

- **Determine and Update Governance Requirements:** Organizations must have governance requirements for the information they handle, which should be established before moving to the cloud. The governance requirements include contractual obligations, corporate policies, and legal and regulatory requirements. Corporate policies and standards must be updated to enable a third party to handle data.
- **Extend Governance Practices and Policies to the Cloud:** Organizations must extend their policies and practices for information governance to the cloud through contractual and security controls.
- **Model Data Handling and Controls:** If required, organizations must utilize the data security lifecycle for developing data handling and controls.
- **Restructure the Existing Information Architectures:** Organizations must plan and restructure fractured approaches in their current information architectures while migrating to the cloud, instead of lifting and shifting existing information architectures.
- **Align the Cloud Governance Policy to the Business Objectives:** Organizations must consider their business objectives while developing their cloud governance policies. For example, if an organization wishes to be agile, it should not implement a rigid governance policy. Similarly, a heavily regulated bank must implement a tight governance policy.

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

- **Include Strong Access Management:** Organizations must clearly define rules and roles so that they know who has access to what cloud resources and why. Here, strong access management refers to gaining knowledge on who requests access to what and ensuring that only those who actually require access to sensitive data or apps receive it.
- **Consider Compliance and Audit:** As data are hosted in the cloud by third parties, cloud audits, which help organizations ensure that their data hosted in the cloud are secure, have become increasingly popular and necessary. Cloud audits also reduce the risk of information being hacked or accessed by unauthorized users. Organizations must prepare a governance policy that incorporates even the external rules and regulations of regulatory agencies that apply to the data as well as the terms for handling cloud audits.
- **Leverage Automation:** It is recommended that organizations utilize automation in their governance framework to detect policy violations easily. For example, if an organization's employee attempts to deploy an untested app, an automated system can notify the IT team about the action and prevent the employee from continuing the operation.
- **Customize Governance Rules to Match Data:** Organizations must consider what type of data they store, where they store the data, and what measures should be taken to protect the data. Most organizations store both non-confidential and confidential data. They must customize their governance rules to match the data they store and manage. This entails the implementation of rigid governance rules for sensitive data and flexible rules for non-sensitive data.

hide01.ir

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

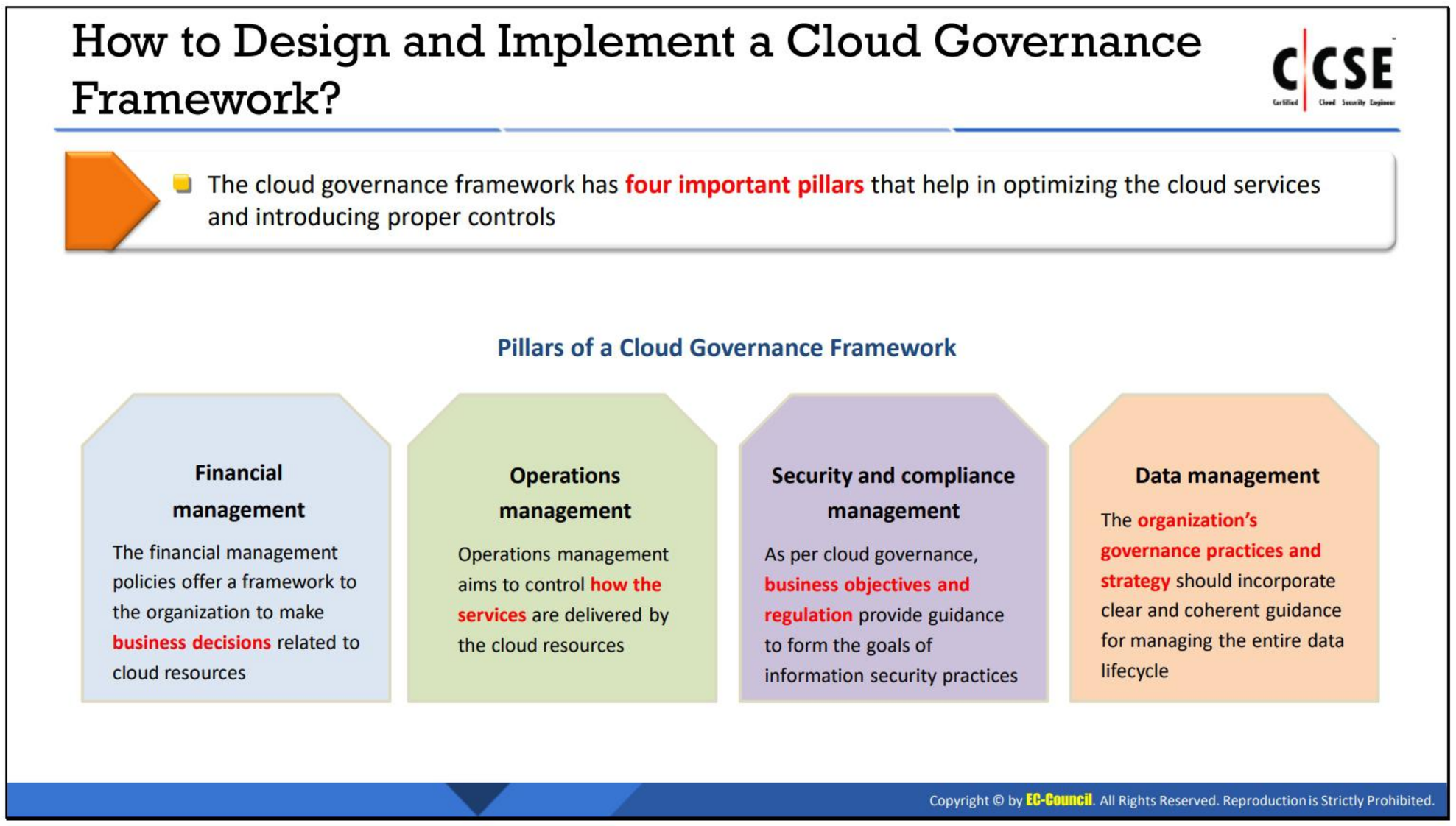


LO#03: Learn to Implement and Maintain Governance for Cloud Computing

This section aims to explain the implementation and maintenance of cloud governance in cloud environments to ensure that governance measures are met. It illustrates how to design and implement a governance framework.

hide01.ir

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



How to Design and Implement a Cloud Governance Framework?

The changing demands of businesses are successfully met through cloud computing, and most organizations are adopting it. Although cloud computing offers various benefits, it involves risks such as loss of control, budget overruns, data leaks, security breaches, and failure to fulfill compliance requirements.

hidd01.ir

With robust cloud computing governance practices, it is possible to mitigate the compliance risk. The cloud governance framework is the application of governance practices to cloud operations.

The cloud governance framework has four important pillars that help in optimizing cloud services and introducing proper controls. These pillars are as follows:

- Financial management
- Operations management
- Security and compliance management
- Data management

Financial Management

An organization can use cloud computing, instead of spending on their own IT infrastructure, to minimize cost and scale up performance. Cloud computing is cost-effective only if the organization is effectively able to control the cloud costs, which need budgets, policies, and reporting.

Financial management policies offer a framework to an organization to make business decisions related to cloud resources. It is very difficult to estimate the cost in a cloud environment,

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

especially when the CSP does not provide complete information about the incurred charges. For example, if an organization wants to determine the cost for storing backup snapshots, it should search across regions, cloud services, and accounts to gather information about all the instances of those backups. Most CSPs offer cost-reporting tools. However, if those tools do not fulfill the organization's requirement, then it should fill the gap using third-party tools. If the organization has exceeded a particular limit such as 50% of their budget for a given month, then an alert will be sent to the organization, providing ample time to adjust the cost.

Operations Management

Operations management aims to control how services are delivered by cloud resources. It includes describing the processes to create new services for which the organization must include clauses in SLAs to allocate resources. Furthermore, the application code needs to be deployed to various environments, especially the production environment. Moreover, the state of services should be monitored to ensure that SLAs are properly met.

An appropriately defined operations policy provides relevant information about providing new applications to customers. The operations management policy also helps in safeguarding the cloud environment against shadow IT operations.

Security and Compliance Management

All the enterprise security measures are observed in cloud governance security measures such as risk assessment, identity and access management (IAM), data encryption and key management, contingency planning, and application security. From the perspective of cloud governance, business objectives and regulation provide guidance to forming the goals of information security practices.

hiteoir

The governance model must be developed on existing framework and governance policies, which include privacy and risk management and cybersecurity. Moreover, the specialized security services provided by public CSPs can be incorporated to alleviate the risks of data leaks and denial of service (DoS) attacks.

Data Management

With the tremendous expansion in the technology to collect, store, and analyze data, the difficulties in effectively managing these data have been increasing. An organization's governance practices and strategy should incorporate clear and coherent guidance for managing the entire data lifecycle.

Data management should start with the classification of data, as different types of data have different levels of importance and require different levels of security. Confidential and sensitive data require more stringent security than public data. By default, all the data at rest and in motion in the cloud environment must be encrypted. Furthermore, the organization should implement other controls to regulate who can access the data, modify the data, etc.

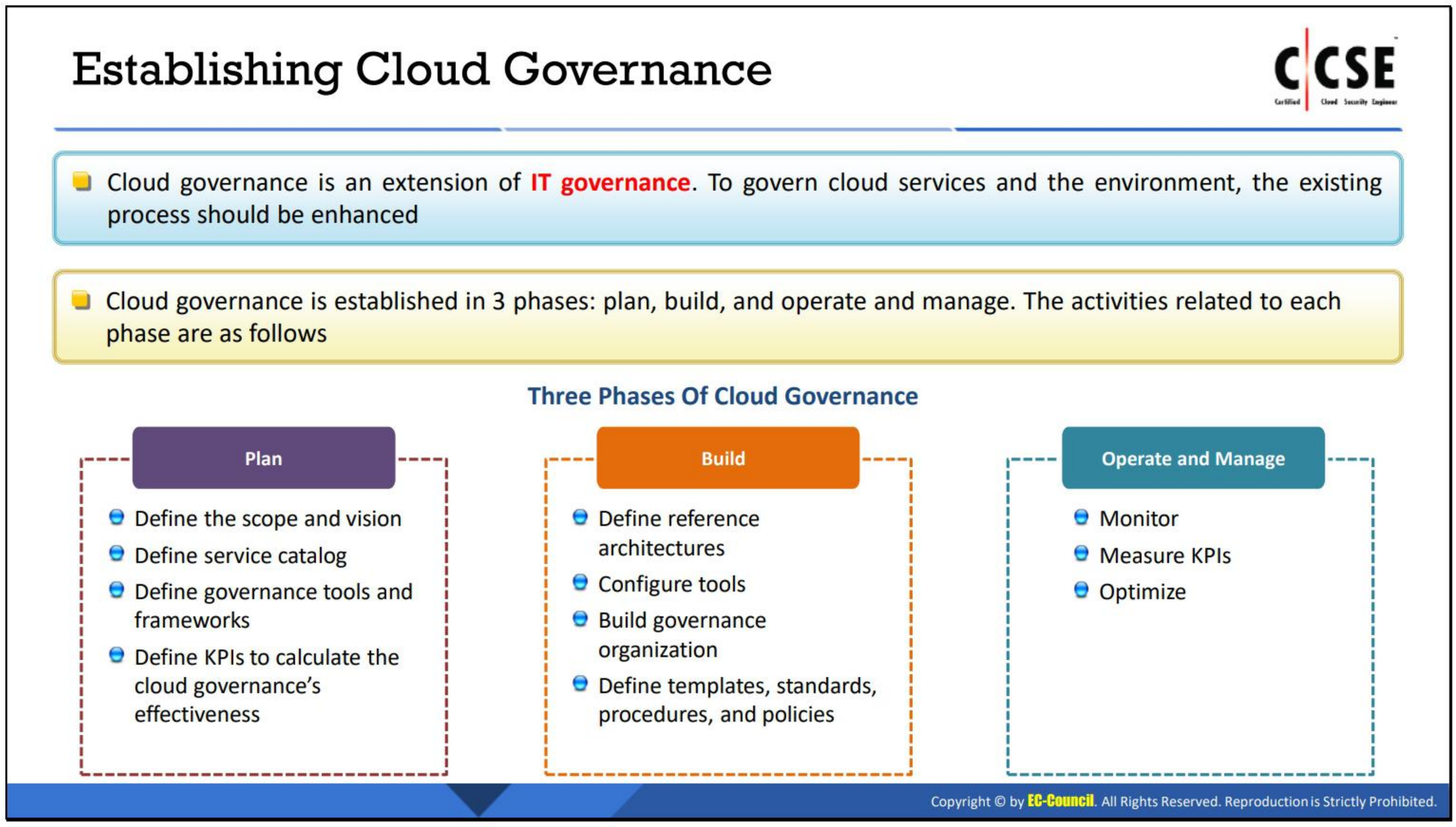
The governance policy must support data owners, application developers, and product managers in understanding how they can safeguard the data. This consists of guidance to manage the entire data lifecycle, data archival, duration of data storage, etc. The data

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

management tools provided by the CSP should be utilized for automatically migrating the data to various regions or to delete unused data.

hide01.ir

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



Establishing Cloud Governance

Cloud governance is the extension of IT governance. To govern cloud services and the cloud environment, the existing IT governance process is enhanced. The following are some IT governance frameworks used in the industry.

hide01.ir

- **Control Objectives for Information and Related Technologies (COBIT):** The COBIT framework defines processes for managing IT. It is used for developing, managing, monitoring, and improving IT governance. COBIT focuses on risk. Any organization that adopts risk can choose the COBIT framework.
- **Information Technology Infrastructure Library (ITIL):** The ITIL framework demonstrates the best practices for managing the IT services of an organization and is focused on the process. Organizations that are attempting to control the use of cloud services can choose the ITIL framework, and a governance process can be implemented on it.
- **Capability Maturity Model Integration (CMMI):** As the name indicates, CMMI focuses on maturity. Enterprises can adopt this framework if they wish to mature in the cloud at an enterprise level.

The above-mentioned frameworks are optional, and many organizations implement cloud governance by creating their own framework.

In general, cloud governance is established in the following phases.

- **Plan:** In this stage, the following activities are performed.
  - Vision and scope are defined.
  - The service catalog is defined.

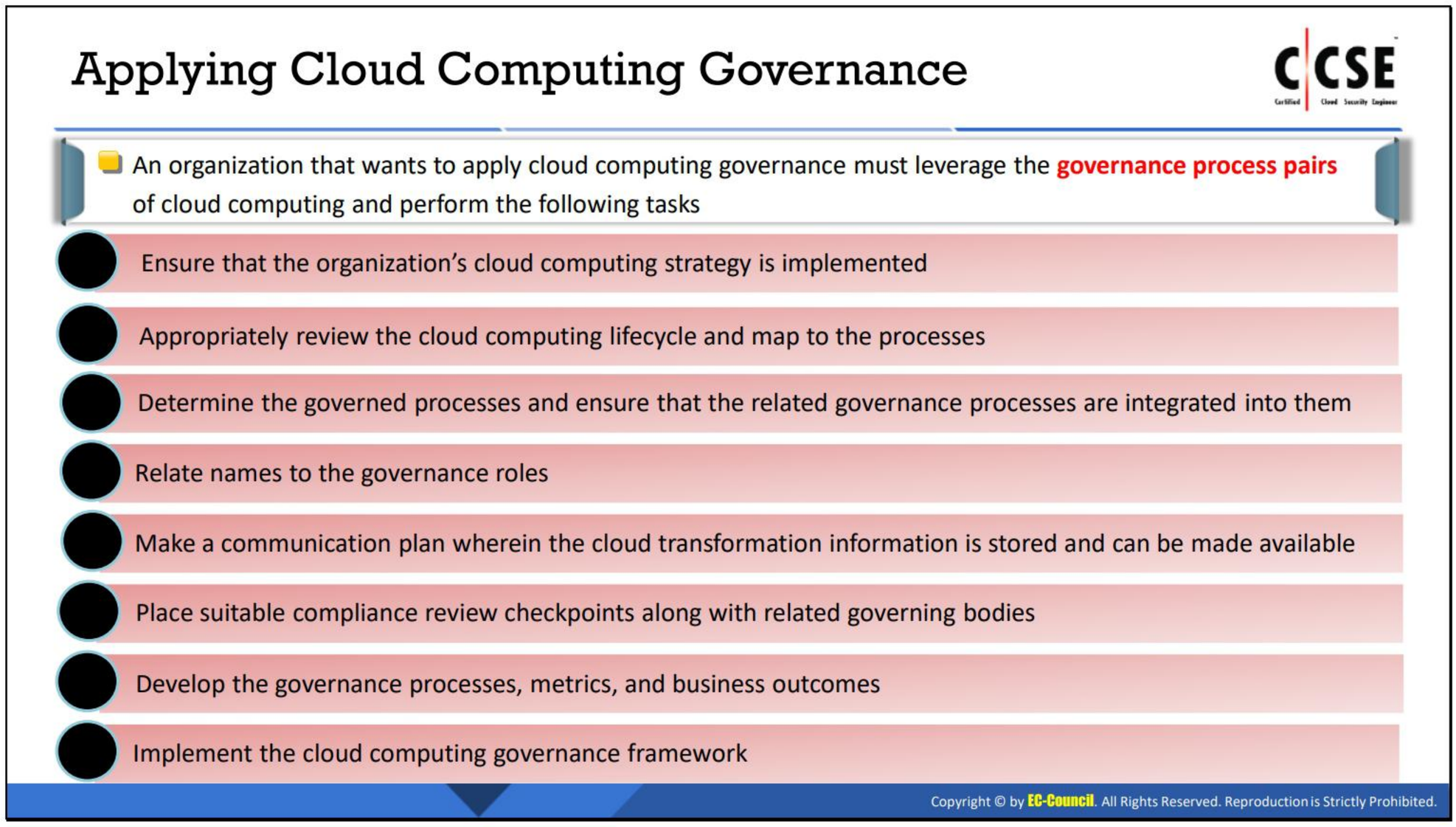
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The cloud governance framework and tools are defined.
- Key performance indicators (KPIs) are defined to measure the effectiveness of cloud governance.

- **Build:** During the build phase, the following activities are performed.
  - Reference architectures are defined.
  - The required tools are configured.
  - Governance organization is built.
  - The templates, policies and procedures, and standards are defined.
- **Operate and Manage:** The following activities are performed during this phase:
  - Monitoring
  - KPI measurement
  - Cloud governance framework optimization

hide01.ir

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



Applying Cloud Computing Governance

An organization that wants to apply cloud computing governance must leverage the process pairs of cloud computing governance and perform the following tasks.

- Ensure that the organization's cloud computing strategy is implemented.
- The cloud computing lifecycle should be appropriately reviewed and mapped to the processes. Then, determine the gaps that should be closed to fulfill the new cloud governance requirements.
- Determine the governed processes and ensure that related governance processes are integrated into them.
- Relate names to the governance roles. To execute governance processes, improve the existing governance bodies or define new governance bodies.
- Create a communication plan wherein information on the cloud transformation is stored and can be made available.
- Place suitable compliance review checkpoints along with related governing bodies.
- Develop the governance processes, metrics, and business outcomes.
- Implement the cloud computing governance framework.

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

Implementing Governance as a New Concept

- For setting up and implementing a new **governance structure**, consider the following key components

- **Preliminary tasks**: By performing the following tasks, the organization can lay a solid foundation for building a successful governance program.
  - **Identify the stakeholders**: Identify the individuals or groups that have an absolute interest in the governance structure and can be involved directly
  - **Define the governance board**: After identifying stakeholders, identify which individuals or groups should be and are willing to be on the governance board. Then, define their roles and responsibilities
  - **Review the key success factors**: Some key success factors must be considered for the success of the IT governance program; they include top management investiture, change management, and customization of the governance framework

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

Implementing Governance as a New Concept (Cont'd)

hidis01.ir

- **Adopt a governance implementation methodology**: To start the governance function, consider the following governance implementation methodology:
  - **Phase 1 (initiate the program)**: This phase identifies the **change drivers** that create a desire to realize changes at executive management levels
  - **Phase 2 (define problems and opportunities)**: This phase aligns **business strategies** and **risks** with IT objectives and prioritizes essential IT processes and goals
  - **Phase 3 (define the roadmap)**: This phase involves setting a **target** for improvement and then performing a gap analysis to identify possible solutions
  - **Phase 4 (plan the program)**: In this phase, suitable and **practical solutions** are planned by defining the projects that are supported by justifiable business cases and then developing a change plan
  - **Phase 5 (execute the program)**: In this phase, the **proposed solutions** are implemented in day-to-day activities
  - **Phase 6 (realize benefits)**: In this phase, the improved **management practices** transition to normal business operations
  - **Phase 7 (review effectiveness)**: This phase involves reviewing the overall **success** of the initiative, detecting any further governance requirement, and bolstering the need for regular improvement

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

Implementing Governance as a New Concept

An organization must choose an implementation methodology to create an effective and robust governance strategy for cloud computing. If the organization has an existing governance strategy for IT and information security, it can extend IT governance to the cloud.

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

Implementing Governance as a New Concept

An organization that has no existing governance structure must handle several preliminary functions before considering cloud governance. It should first establish a governance structure for IT and information security. The following key tasks should be performed for setting up and implementing a new governance structure.

- **Preliminary Tasks**

  It is essential to perform a series of tasks before initiating the governance process. By performing these tasks, the organization can lay a solid foundation for building a successful governance program. The tasks include the following.

  - **Identify the Stakeholders**: Identify the individuals or groups that have an absolute interest in the governance structure and can be involved directly. These groups involve the following:
    - Executive management
    - IT audit
    - IT management, chief information officer (CIO), and IT process owners
    - Business management and business process owners
    - Information security (including compliance and risk)
  - **Define the Governance Board**: After identifying the stakeholders, identify which individuals or groups should be and are willing to be on the governance board. Then, define their roles and responsibilities. The following roles are required according to ISACA.
    - **Board and Executives**: They set the direction for the program, approve key program roles and specify responsibilities, ensure program alignment with enterprise-wide risk management and governance, and provide support and commitment. These members also communicate, sponsor, and promote the agreed-upon initiative.
    - **Business Management**: It offers suitable stakeholders and champions that drive commitment and support the program. It is responsible for nominating key program roles and defining and assigning responsibilities.
    - **IT Management**: It ensures that executives understand and cherish the high-level objectives. It not only helps in nominating key program roles and defining and assigning responsibilities but also nominates a person to run the program in line with the business.
    - **IT Audit**: It provides audit participation as per the role and reporting arrangements and ensures that a sufficient level of audit participation is offered throughout the program.
    - **Risk and Compliance (InfoSec)**: It ensures that a sufficient level of participation is offered throughout the program.

hideo1.ir

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

- **Review the Key Success Factors**: Some key success factors must be considered for the success of the IT governance program. These key success factors are as follows.
    - **Top Management Investiture**: The executive management must show that they are dedicated to the governance process by establishing the purpose and direction of the governance function.
    - **Understanding of the Objectives and Outcomes**: All stakeholders must understand the purpose of implementing governance, including the IT, business, and InfoSec objectives and expected governance outcomes.
    - **Change Management**: To make any change effective, communicate clearly the expected results from the governance effort and enable them.
    - **Customizing the Governance Framework**: Carefully adopt any governance framework to ensure that it meets the organization's ability and needs. Maximize compatibility by carefully implementing tailored procedures and practices.
    - **Pick the Low-Hanging Fruit**: Identify activities that have clear benefits and can be easily performed. For example, an executive explaining cloud InfoSec issues is an activity that can be performed quickly and easily.

- **Adopt a Governance Implementation Methodology**: To start the governance function, consider the following governance implementation methodology.
    - **Phase 1 (Initiate the Program)**: This phase identifies the change drivers that create a desire to realize changes at executive management levels. This desire is then expressed in a business case outline. Change drivers are external or internal events, key issues, or conditions that act as a stimulus for change. Events, performance pitfalls, trends, software implementations, and goals of the organization can serve as change drivers.
    - **Phase 2 (Define Problems and Opportunities)**: This phase aligns business strategies and risks with IT objectives and prioritizes essential IT processes and goals. The COBIT framework helps in selecting goals by mapping business goals to IT goals to IT processes. If the IT goals are defined, critical processes can be defined, managed, and controlled to ensure successful, expected outcomes.

      The management can determine its present capabilities and weaknesses by performing an assessment based on the Capability Maturity Model of particular controls and processes.
    - **Phase 3 (Define the Roadmap)**: This phase involves setting a target for improvement and then performing a gap analysis to identify possible solutions. Give priority to projects that are easily achievable and provide the greatest benefits.

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

- **Phase 4 (Plan the Program)**: In this phase, suitable and practical solutions are planned by defining the projects that are supported by justifiable business cases and then developing a change plan. A sophisticated business case helps ensure that the benefits of the project are identified and monitored.
- **Phase 5 (Execute the Program)**: In this phase, the proposed solutions are implemented in day-to-day activities. Measures and monitoring systems are created to achieve business alignment and measure performance.
- **Phase 6 (Realize Benefits)**: In this phase, the improved management practices transition to normal business operations. The achievement of improvement is also monitored by measuring metrics and expected results.
- **Phase 7 (Review Effectiveness)**: This phase involves reviewing the overall success of the initiative, detecting any further governance requirement, and bolstering the need for regular improvement.
- Although reporting is not explicitly mentioned in the above phases, it is a part of all phases and iterations.

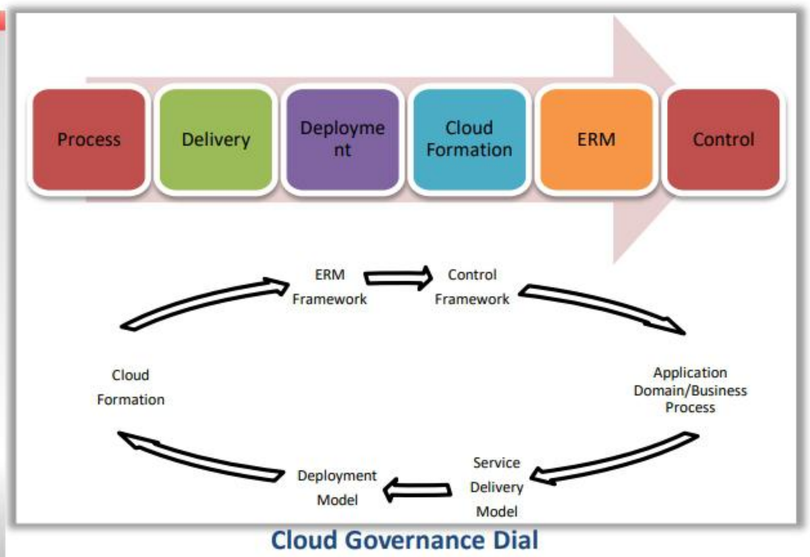
hide01.ir

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

Extending IT Governance Framework in Cloud with Cloud Governance Dial

- The IT cloud governance dial identifies the **steps** necessary for implementing appropriate IT governance for a cloud environment
- An organization can effectively extend its IT governance framework to the cloud environment. The components or processes of cloud governance can be viewed in the form of the following **six dials**

- **Process**: What is migrating to the cloud?
- **Delivery**: How it will be delivered (via PaaS, SaaS, IaaS, or BPMaaS)?
- **Deployment**: How it will be deployed (private, public, hybrid, or managed)?
- **Cloud Formation**: Proprietary/open, internal/external, insourced/outsourced, parameterized/de-parameterized
- **ERM**: What risk factors arise from the previous steps?
- **Control**: What are the control changes needed for this cloud solution?



Cloud Governance Dial

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

Extending IT Governance Framework in Cloud with Cloud Governance Dial

The IT cloud governance dial identifies the steps that are necessary for implementing appropriate IT governance for a cloud environment. An organization can effectively extend its IT governance framework to the cloud environment.

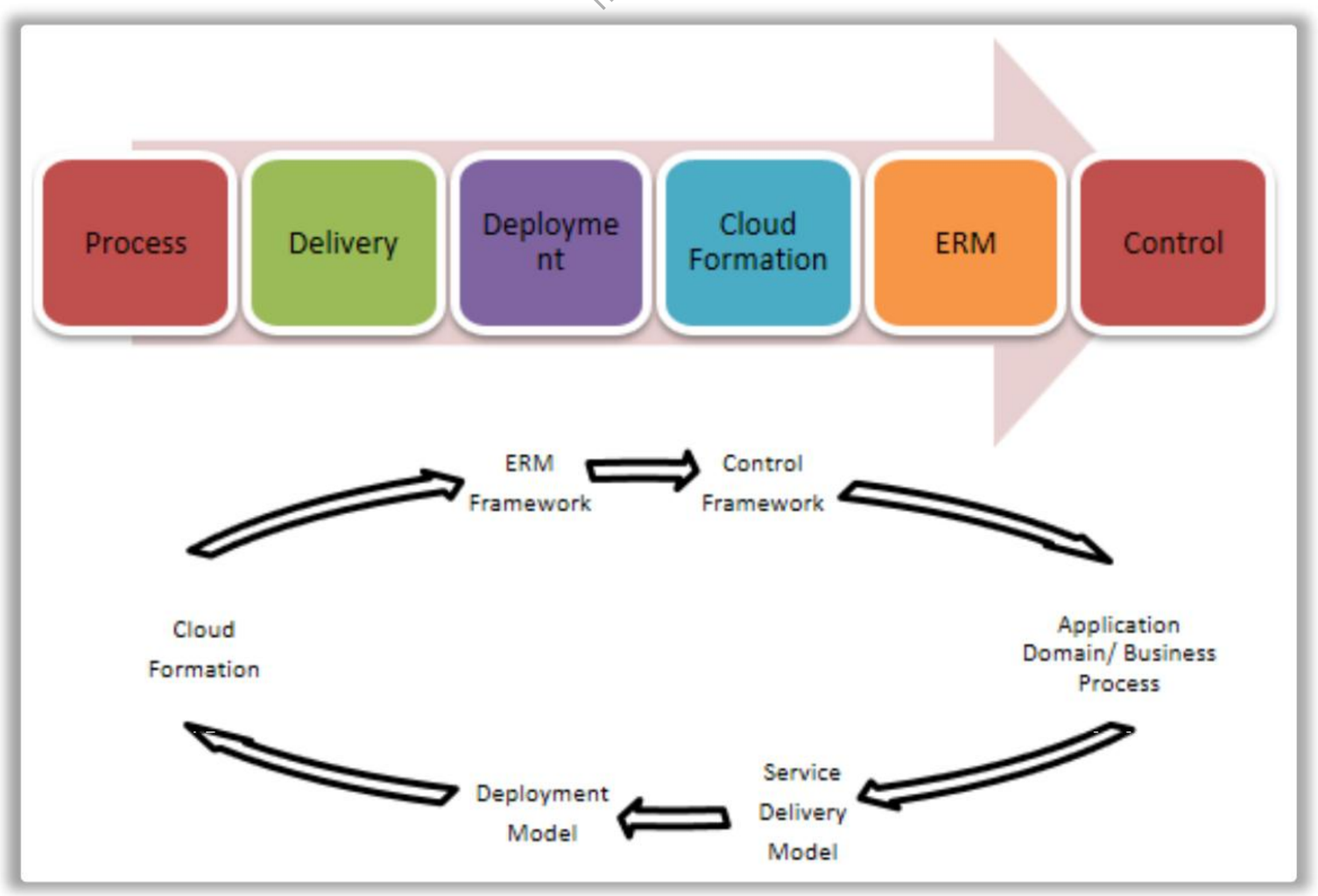


Figure 10.8: Cloud Governance Dial

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

The components or processes of cloud governance can be viewed in the form of the following six dials.

- **Process**: What is migrating to the cloud?
- **Delivery**: How will it be delivered (via PaaS, SaaS, IaaS, or BPMaaS)?
- **Deployment**: How will it be deployed (private, public, hybrid, or managed)?
- **Cloud Formation**: Proprietary/open, internal/external, insourced/outsourced, and parameterized/de-parameterized
- **ERM**: What risk factors arise from the previous steps?
- **Control**: What are the control changes needed for this cloud solution?

The applicable governance framework is created by aligning appropriate categories present on each dial. To govern the proposed cloud solution effectively, necessary changes should be made to the current IT governance framework. With the cloud governance dial, the organization can align the cloud solution with its defined business values and deliver added value via performance management and optimal resource allocation. This dialed solution can be evaluated further to specify the associated deliverables to achieve business agility/flexibility, business growth, asset utilization, and cost-effectiveness. These factors specify the necessary adjustments to the enterprise risk management (ERM) and control framework to eliminate or reduce cloud risk issues.

IT Governance Application to Cloud Deployment

ebook.ir

Various challenges exist for effective IT governance in cloud environments. Successful cloud migration depends on the organization's ability to evaluate the impact of the cloud migration and identify the required/suitable governance framework to achieve alignment with organizational goals and extract business value.

In the following scenario, the processes/components mentioned above are applied to payroll services through the cloud.

- **What is Moving to the Cloud?** Consider and evaluate technical results of both cloud delivery and in-house provision. Choose a business application that is common across all business types (not unique to the organization). Take payroll as an example.
- **Identify Objectives and Deliverables of the IT Governance Domain**: Cloud payroll solutions offer flexible, fast implementation as well as alignment with present and future IT objectives and business growth. With proper CSP selection and SLAs, the organization can obtain a reliable delivery of cloud applications and address risk concerns and compliance requirements.
- **How It Will Be Delivered?** The cloud delivery model is SaaS, regardless of whether the current payroll software is migrated to the cloud or a new payroll application is adopted. If additional HR applications are integrated, the model would become a business process solution (BPMaaS).

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

- **How It Will Be Deployed?** Payroll applications are generally deployed using a public cloud service (a multitenant environment). Companies that need enhanced security and reliability can choose a private cloud that is reserved for them. Organizations such as the military and universities may want to leverage a community/managed cloud for their HR and payroll applications.
- **Determine the Cloud Formation**: This payroll example assumes complete cloud deployment with payroll data stored outside the organization (external), where other tenants and applications can utilize the technology, services, and interfaces (open). The software application payroll subscription provides data sharing for government document filing and reporting (de-parameterized and outsourced).

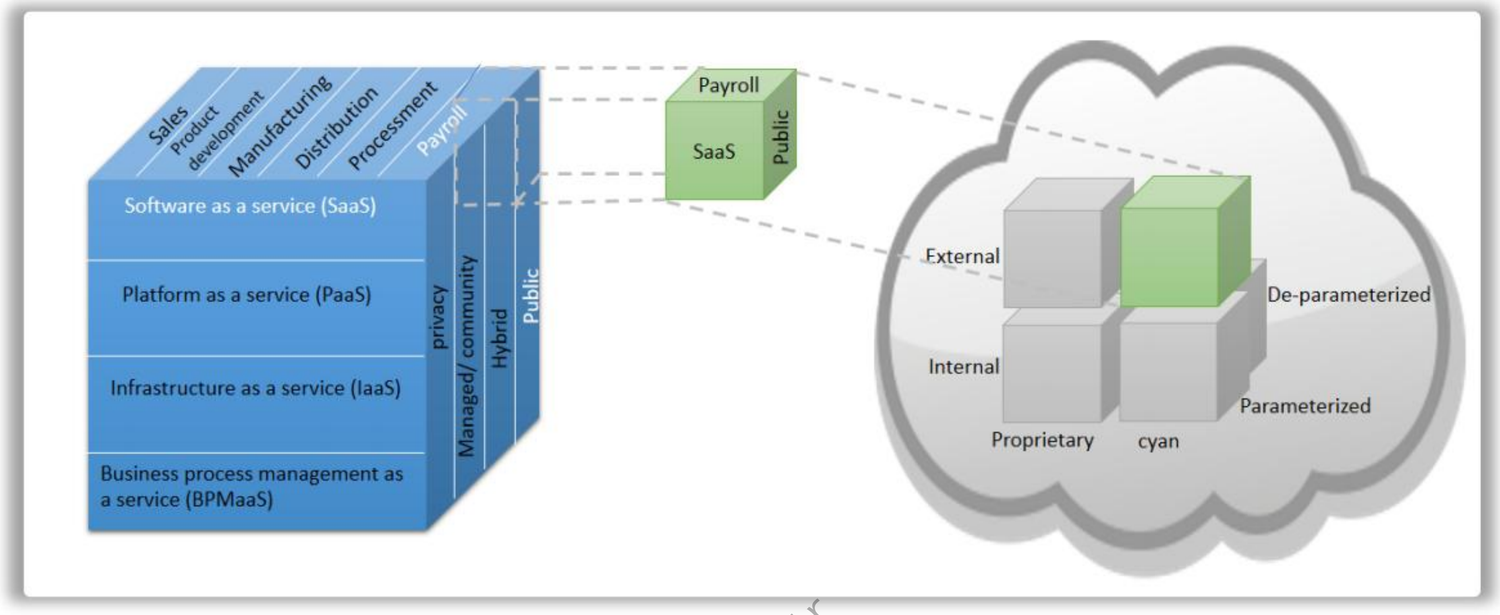
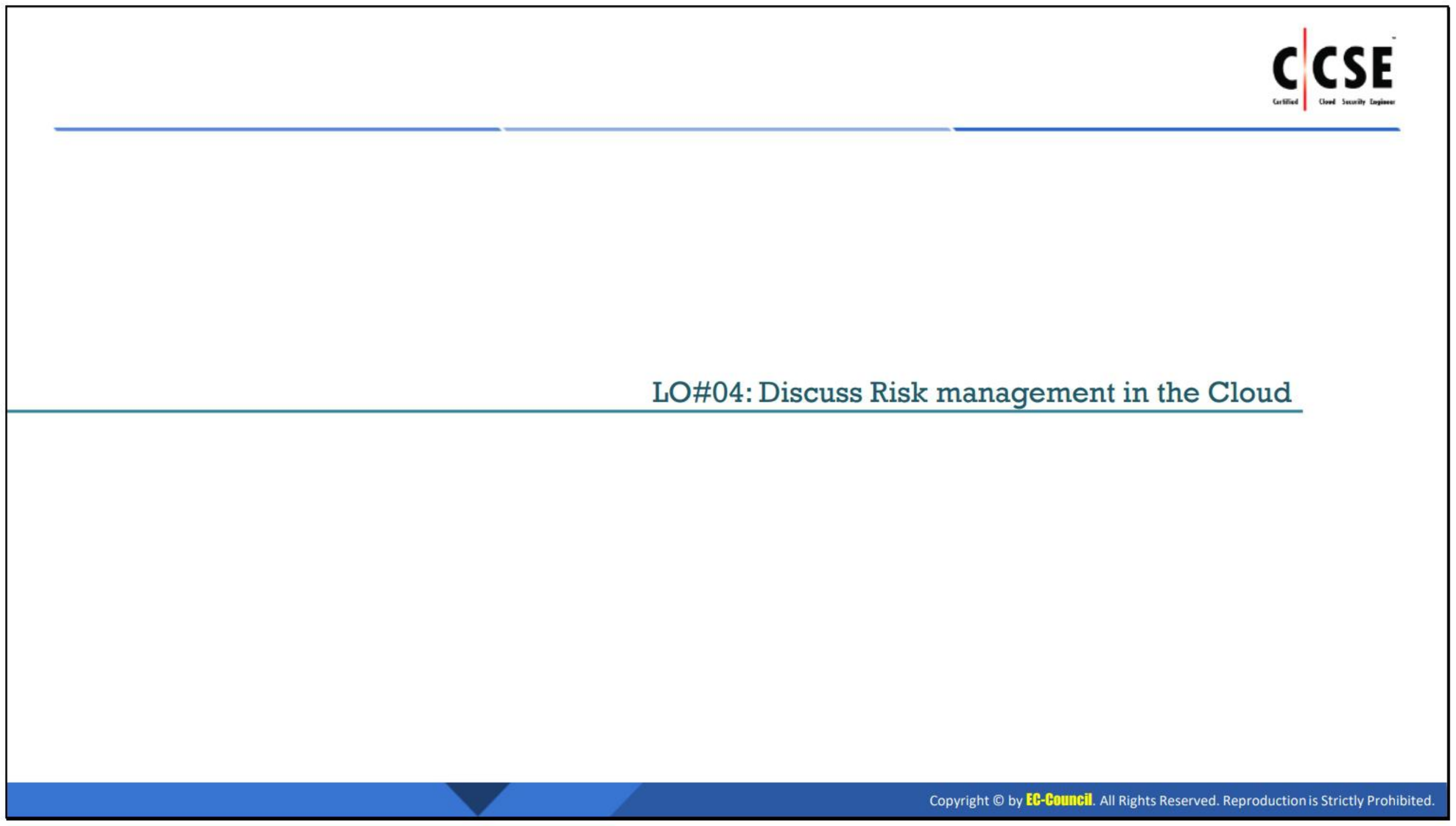


Figure 10.9: Visualization of the Steps for Migrating Payroll Services to the Cloud

- **Cloud Governance**: The IT governance framework of the organization must now be reviewed and modified based on the results (if needed). Do not replace an effective governance framework. Issues arising from the cloud deployment of the payroll application must be addressed. In this example, the governance framework should address the following risks.
  - **Contractual Risks**: Risks regarding SLAs and CSPs wherein governance agreements should be explicitly mentioned.
  - **Availability and Performance Risks**: Risks related to performance-level expectations, availability, and critical access concerns.
  - **Integration Risks**: Risks related to interoperability with other processes and apps that need the sharing of employee and payroll data.
  - **Audit and Compliance Risks**: Risks related to a storage location, data access, auditability, and jurisdiction.
  - **Security Risks**: Risks including data confidentiality, data integrity, and privacy.
- **Evaluation, Improvement, and Adaptation**: Cloud IT governance is not a static framework, because changes in the organizational structure, technology, laws, and regulations impact its effectiveness. The organization must monitor and update the governance framework periodically over time.

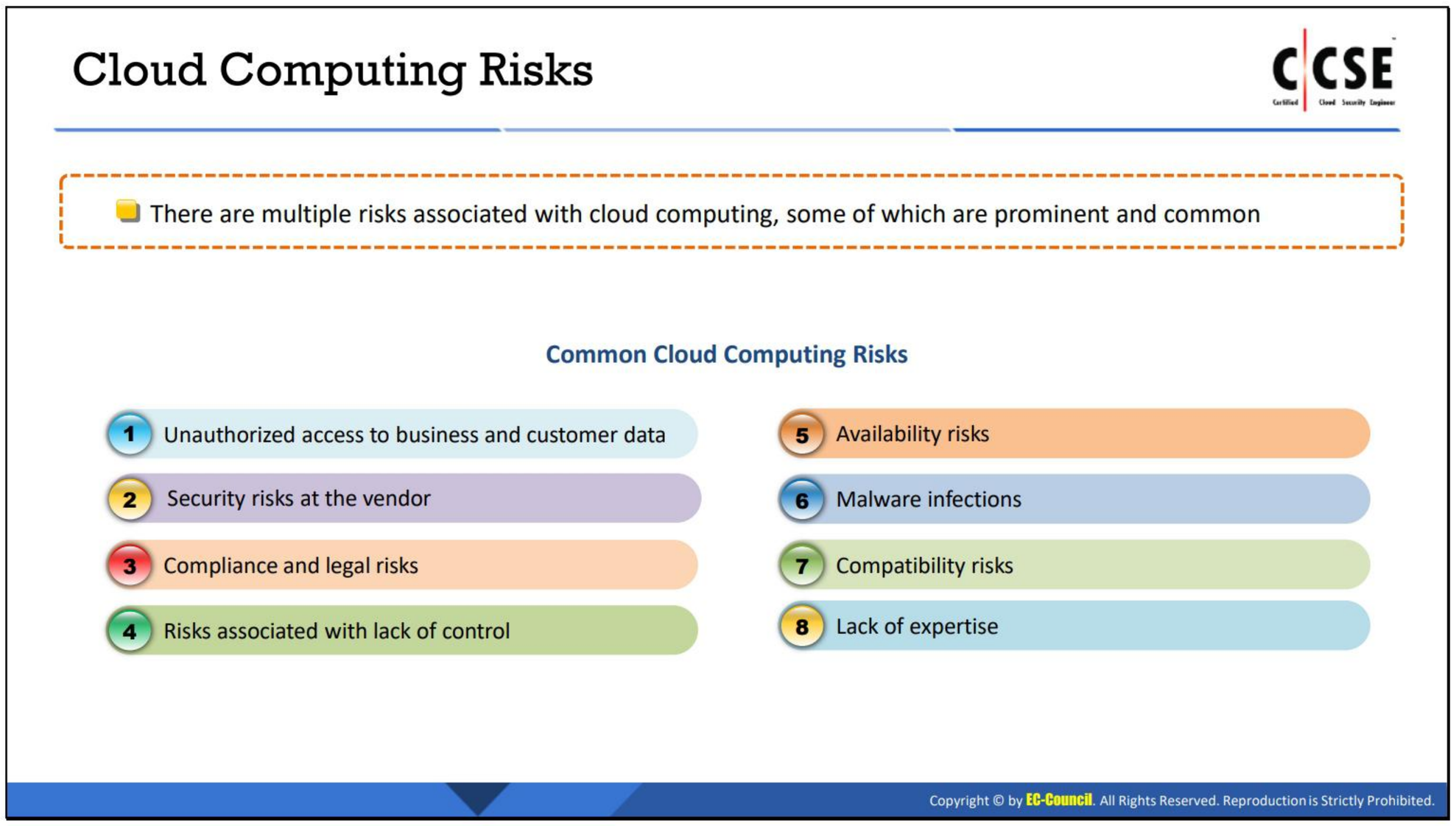
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Discuss Risk Management in the Cloud

To identify unforeseen risks in the cloud and the various technologies used, a cloud security engineer should have an understanding of risk management in the cloud. The objective of this section is to explain various risks and their management in detail, along with the risk mitigation processes and resources that help in establishing GRC in the cloud.

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



Cloud Computing Risks

Although there are multiple risks associated with cloud computing, some risks are relatively more prominent and common. The following are the common cloud computing risks.

hide01.ir

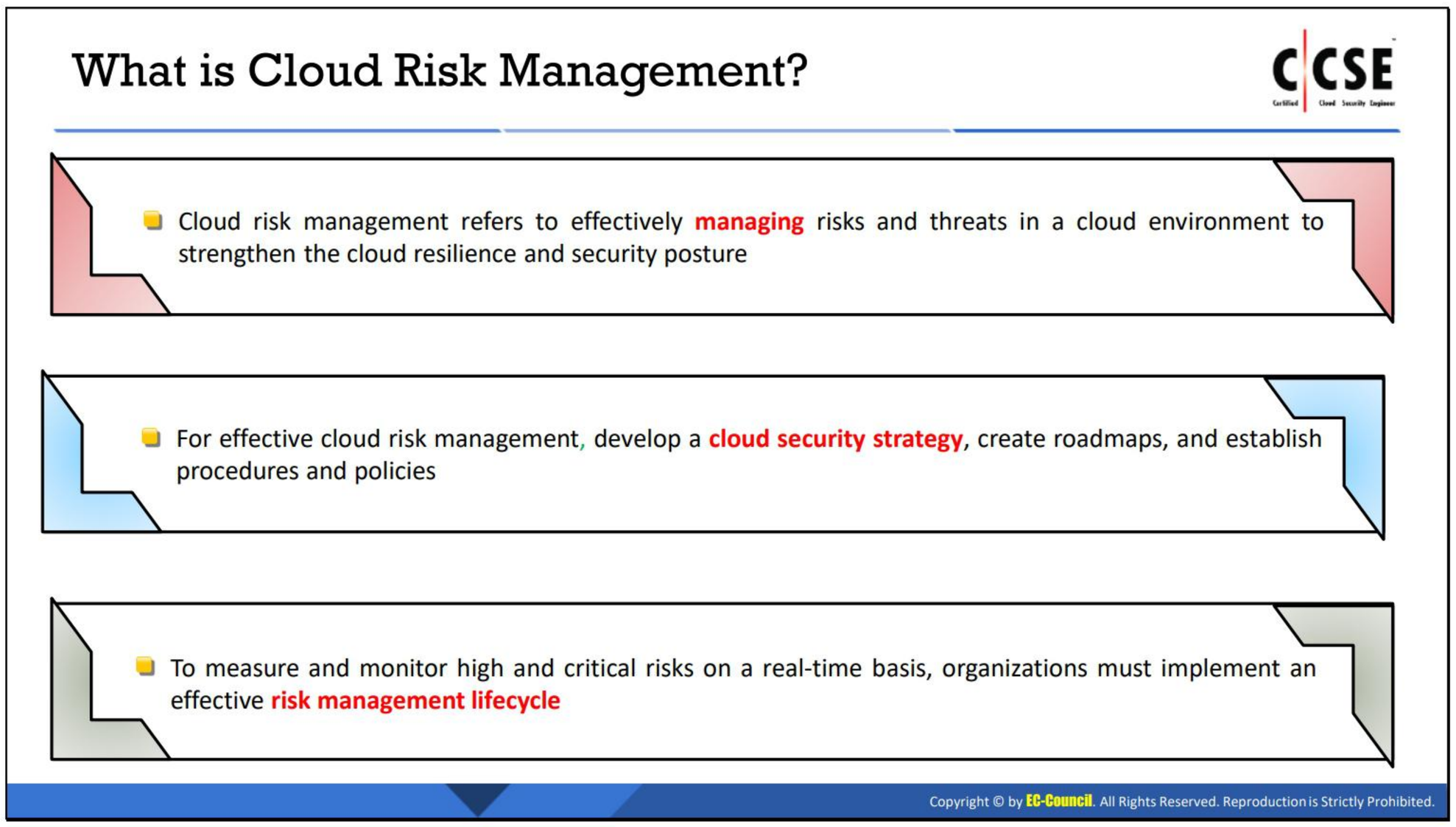
- **Unauthorized Access to Business and Customer Data:** Organizations outsource their data and services under the impression that the data and services are more secure in the cloud. As the cloud stores a huge volume of data, it could be an easy target for attackers. Hence, there arises a risk of the cloud becoming a single point of failure. The cloud faces the risk of unauthorized access not only from attackers and malware but also from insiders (internal employees). When organizations outsource their services or data, more people (that support cloud services) have access to their services or data. This means that organizations must even trust people they have never met. Moreover, government agencies can also access data stored in the cloud in certain situations.
- **Security Risks at the Vendor:** Many organizations use the cloud for storing business-critical data such as financial details (e.g., credit card information). By storing such critical information, they place their trust in the cloud provider. Small businesses may not even know about the technology and people involved in cloud computing. By depending on cloud services for business-critical tasks, they place their businesses at risk under CSPs. Therefore, CSPs play an important role in securing or damaging the reputation of such businesses.
- **Compliance and Legal Risks:** Organizations that process or store regulated data such as healthcare or creditcard information must comply with certain industry regulations. These regulations ensure that customer data are protected. If organizations outsource such regulated data to the cloud, they must ensure that CSPs also protect the data as per industry regulatory and compliance requirements. Organizations must also have

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

legal protections (in writing) with CSPs. If organizations do not have an agreement with CSPs about data protection, they will be held responsible for any data exposure due to a cloud service breach.

- **Risks Associated With Lack of Control:** Organizations can have full control over their data when they store the data in a local, self-managed network. However, when they store the data in the cloud, they have no such control over the data. CSPs control the data, and organizations have little information on how they do so. CSPs can modify the fee for their offered services on the basis of their complete control over the data. They may even limit access to the data if they have not paid the specified amount.
- **Availability Risks:** CSPs cannot guarantee 100% uptime at all times. When an organization uses cloud services for its business-critical tasks, the success or failure of its businesses depends on the CSP and ISP. If either of them fails, the organization suffers losses. Although most CSPs have downtimes, the business can be adversely affected if the downtime occurs during business hours.
- **Malware Infections:** As an Internet connection is used to store large amounts of data on the cloud, customers that use cloud services are at risk of cyberattacks. The most common threat is distributed denial of service (DDoS) attacks, in which attackers direct large volumes of traffic to web applications that cause servers to crash.
- **Compatibility Risks:** Migrating data to the cloud may cause compatibility issues with the existing IT infrastructure or with organizational policies and security requirements. Before considering data or service migration to the cloud, it is essential to cover all aspects that relate to compatibility.
- **Lack of Expertise:** As cloud computing is gaining prominence, organizations are moving their data and workloads to the cloud. Cloud technologies are rapidly becoming sophisticated and advanced. This makes it difficult for organizations to keep up with the advanced tools and technologies. They may not use the cloud to an optimum level owing to a lack of expertise or skilled workforce.

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



What is Cloud Risk Management?

Cloud risk management refers to the effective management of risks and threats in a cloud environment to strengthen cloud resilience and the security posture. It is a systematic process for handling threats or risks in an organization's cloud environment to enable it to identify the events that may cause damaging consequences and to create the best course of action for detecting, evaluating, responding to, and communicating risk issues. Cloud risk management ensures that cloud risks are effectively addressed (mitigated) by implementing sufficient security controls.

Organizations must be aware of vulnerabilities and risks they will face in a cloud environment while migrating their apps or data to the cloud. Effective cloud risk management requires a comprehensive and holistic approach including developing a cloud security strategy, creating roadmaps, and establishing procedures and policies.

Risk Management Objectives

- Identify the potential risks.
- Identify the impact of risks to develop improved risk management strategies and plans.
- Depending on the impact/severity of the risk, prioritize the risks and use established risk management methods, tools, and techniques.
- Understand and analyze the risks and report identified risk events.
- Control the risk and mitigate the risk impact.
- Create awareness among the security staff; develop long-term, reliable strategies and plans for risk management.

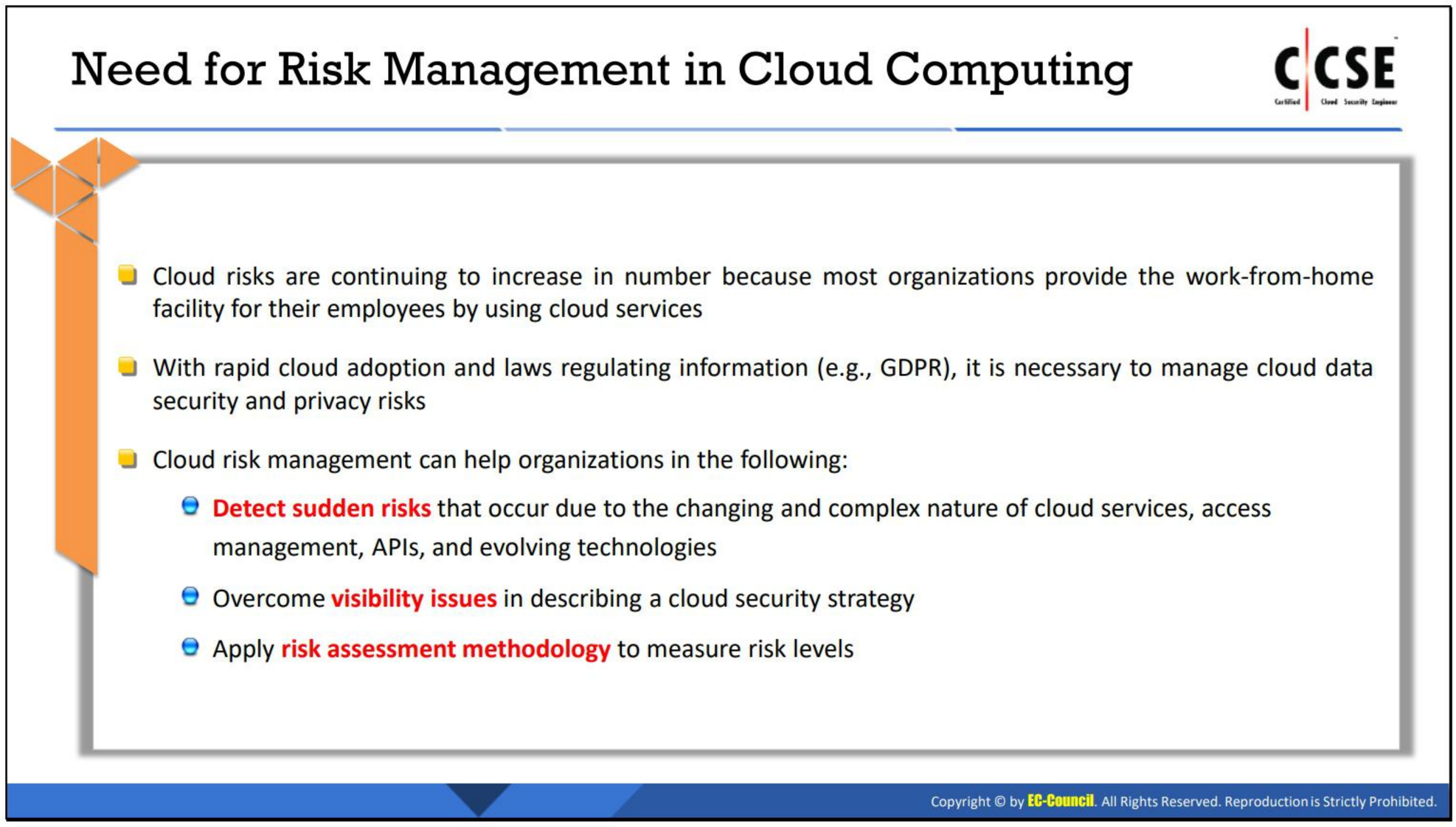
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To measure and monitor high and critical risks on a real-time basis, organizations must implement an effective risk management lifecycle. They should define what exactly should be measured and the acceptable variance to ensure that risks are mitigated in a timely manner. External audits can also help manage cloud risks. The following tools can be used for cloud risk management:

- NIST Risk Management Framework
- CSA Cloud Controls Matrix (CCM) framework
- ISO 27701 and ISO 27017/18 frameworks
- SOC reports that cover CCM controls

hide01.ir

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



Need for Risk Management in Cloud Computing

As many organizations are adopting cloud computing in one form or the other, cloud risk management has become important. Organizations face multiple risks that must be managed in a cloud environment to keep their business data and services secure and running. Cloud risks are continuing to increase in number because most organizations provide the work-from-home facility for their employees by using cloud services. Misconfigured cloud servers are prone to data breaches.

With the rapid cloud adoption and laws regulating information (e.g., the General Data Protection Regulation (GDPR)), it is necessary to manage cloud data security and privacy risks. Organizations using the cloud must adopt a risk management framework and implement basic security concepts such as privacy by design and security by design. Small and medium enterprises do not have risk lifecycle management or even a dedicated team to handle cloud risks. In the absence of effective risk monitoring, these organizations face threats to cloud security, privacy, and data security.

Cloud risk management can help organizations to:

- Detect sudden risks due to the changing and complex nature of cloud services, access management, application programming interfaces (APIs), and evolving technologies.
- Overcome visibility issues in describing a cloud security strategy.
- Apply the risk assessment methodology to measure risk levels.

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

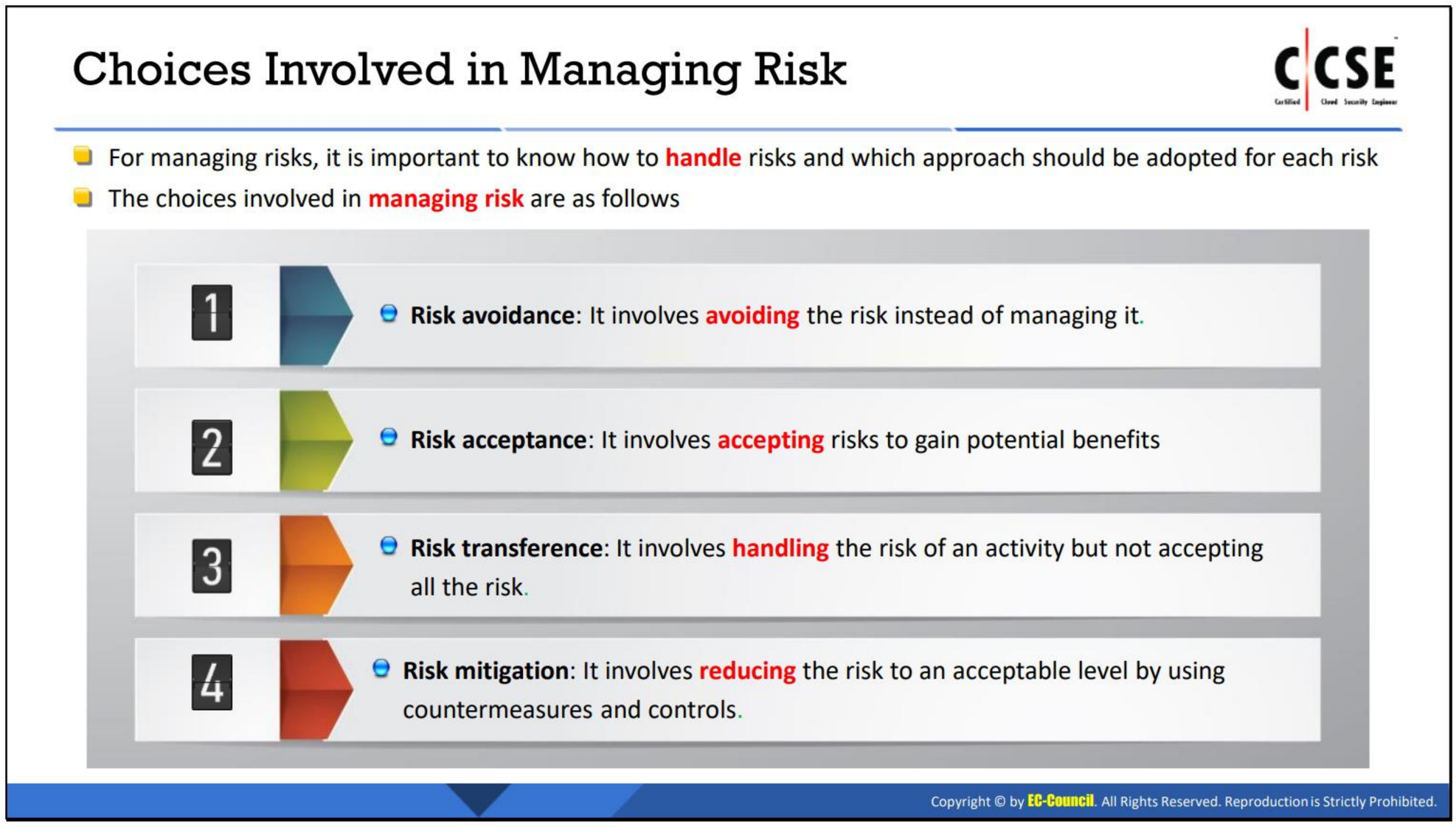
Risk Management Benefits

Risk management provides a structured approach to identifying risks. Having a clear idea of all risks allows an organization to analyze, prioritize, and take appropriate actions to reduce losses. The following are some benefits of cloud risk management:

- Focuses on the potential risk impact areas
- Addresses risks according to their level
- Improves the risk handling process
- Allows security officers to act effectively in adverse situations
- Enables the effective use of resources
- Minimizes the impact of risk on an organization's revenue
- Identifies suitable controls for security

hide01.ir

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



Choices Involved in Managing Risk

For managing risks, it is important to know how to handle risks and which approach should be adopted for each risk. The choices involved in managing risk are as follows.

- **Risk Avoidance:** Risk avoidance involves avoiding the risk instead of managing it. If an organization finds a risk in which the likely benefits of an activity are less than its costs (risks), the organization can opt not to perform the activity that would put it at risk. Not performing the risky activity is the most successful approach for removing a specific risk.

  For example, consider the activity of transporting a package from one side of the sea to another. The potential costs (risks) of the activity are drowning, losing both the package and the ship, etc., whereas the likely benefits include $10 per package for every successfully transported package. In this case, the organization may consider not to start or continue this trans-oceanic delivery business as the reward or benefit is far less than the potential costs (risks). This is referred to as risk avoidance.

- **Risk Acceptance:** Risk acceptance is the opposite of risk avoidance and involves accepting risks to gain the potential benefits. If an organization finds the risk of an activity minimal and its reward (potential benefit) substantial, it can proceed to perform the activity without any further consideration. This is referred to as risk acceptance.

  For example, consider the same activity of transporting a package from one side of the sea to another. If the organization determines that there is no risk in transporting the package based on historical evidence (e.g., no package, ship, or person was ever lost in the sea) and the likely benefit is substantial ($200), the organization may perform this activity. Thus, the organization opts for risk acceptance when the risk of the activity is within its risk appetite.

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

- **Risk Transference:** Risk transference involves handling the risk of activity but not accepting all the risk. Risk transference allows an organization to transfer the risk to someone at a nominal cost. An example of risk transference is insurance. The organization pays only a fraction of the cost of the worst outcome to prevent the damage or risk of the worst outcome. This is referred to as risk transference.

  For example, if an organization faces losses due to the risk of an activity that is covered under insurance, the losses will be compensated for by the insurance authority based on the agreement. This means that the organization shares the risk with the insurance company by paying a premium.

- **Risk Mitigation:** Risk mitigation is the last approach of managing risk. It involves reducing risk to an acceptable level by using countermeasures and controls. Risk mitigation is the approach used by most security practitioners on a daily basis. As a part of risk mitigation, the organization implements security controls to bring the risk level within its risk appetite.

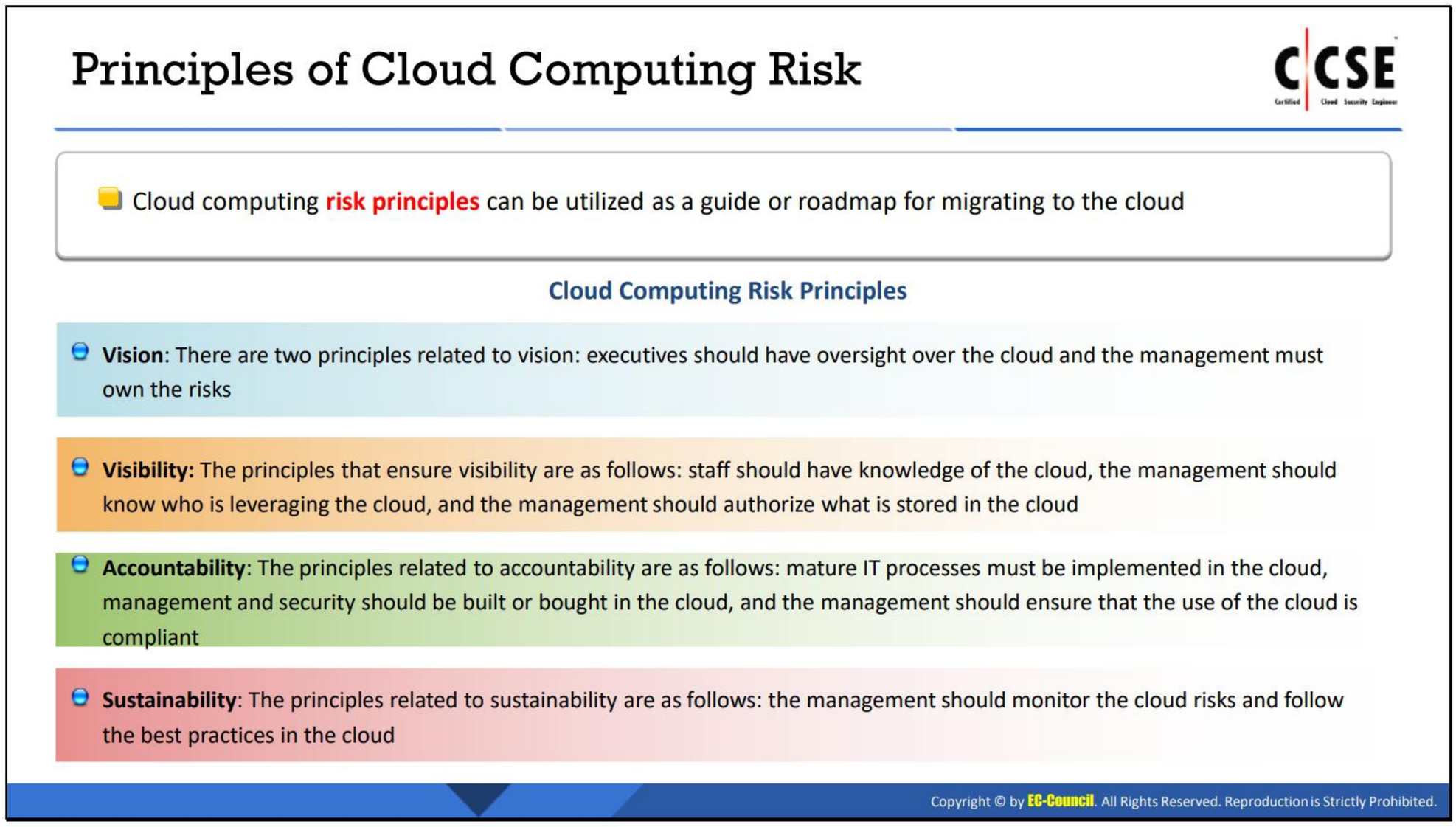
  For example, the organization may choose to reduce the risk associated with the package to be shipped across the sea by packing it into an airtight container, fixing a tracking device, etc. Once the organization determines that it has implemented sufficient controls and countermeasures to mitigate the risks associated with shipping the package, it can be confident about the success of its business.

  The following two aspects of risk mitigation should be taken into account.

  - It is not possible to eliminate risk, because risk can be reduced but not eliminated.
  - The cost of controls should not exceed the likely benefit of a business activity or process.

hite01.ir

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



Principles of Cloud Computing Risk

Cloud computing risk principles provide context to the framework for assessment (ISO/IEC 9126). These principles can be utilized as a guide or roadmap for migrating to the cloud. This roadmap has the following four guiding principles.

- **Vision**: It helps to create and communicate a vision for the cloud at a business-unit and enterprise level. The following are the two principles that relate to this vision.
  - **Executives Should Have Oversight Over The Cloud**: The organization must understand the value of data and the cloud-based technology. The The risk to information assets must be continuously monitored. This includes complying with applicable policies, regulations, and frameworks.
  - **Management Needs to Own the Risks**: The organization's management should own the risk associated with using cloud services and establish, monitor, and evaluate risk management on a regular basis.
- **Visibility**: It is beneficial to provide visibility of what should be done and the risk of doing it. The following are the three principles that ensure visibility.
  - **Staff Should Have Knowledge of the Cloud**: All cloud users must be well aware of the cloud and its associated risks, understand their responsibilities, and be liable for their cloud use.
  - **Management Should Know Who is Leveraging the Cloud**: The management of the organization should be aware of the users of the cloud. It should also ensure that appropriate security controls are implemented for all types of cloud use.

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

- **Management Should Authorize What is Stored in the Cloud**: The organization must formally classify the data and cloud-based technology for confidentiality, availability, and integrity and assess them for risk in terms of business. It should also ensure that technical controls and business best practices are included and tested to eliminate the risk throughout the asset lifecycle.

- **Accountability**: Through the following principles, the accountability extends to architecture, process, and culture.
  - **Follow Mature IT Processes in the Cloud**: The organization must ensure that all processes related to cloud-based system development and technical infrastructure are documented and communicated to all stakeholders, are in line with policy, are properly resourced, and satisfy the agreed-upon business requirements.
  - **Build Or Buy Management And Security in the Cloud**: The organization's management should consider monitoring and managing information as well as its risk and security while making all cloud decisions.
  - **Management Should Ensure That the Use of the Cloud is Compliant**: Cloud users and providers must comply with the applicable legal, regulatory, and contractual obligations, stand by the values of client commitment and integrity, and ensure that all cloud uses are authorized and appropriate.

- **Sustainability**: The following are the principles related to sustainability:
  - **Management Should Monitor the Cloud Risks**: The management of the organization must monitor the cloud risks. It should ensure that all acquired or developed cloud-based technology provides the timely and transparent reporting of information risk and has well-defined and well-communicated monitoring and escalation processes.
  - **Follow the Best Practices in the Cloud**: For all cloud-based systems development and technical infrastructure processes, the organization should consider modern technology and controls. This helps in addressing the latest information risks identified via external and internal monitoring.

mdeh.ir

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

Cloud Computing Risk Categories

- **Risks in a cloud environment can be classified into the following categories**

Policy and Organizational Risks

- These are business-IT-related risks that are faced by organizations while **selecting CSPs**
- Some of the policy and organizational risks are as follows:
  - Lock-in
  - Loss of governance
  - Compliance challenges
  - Business reputation loss
  - Cloud service failure or termination

Technical Risks

- These are IT-related risks that directly impact cloud systems that **store customer data**
- Some of the technical risks include the following:
  - Availability of service
  - Resource exhaustion
  - Intercepting data in transit
  - Data transfer bottlenecks
  - DDoS

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

Cloud Computing Risk Categories (Contd.)

hide01.ir

Operational Risks

- Operational risks are related to the **execution of the tasks** and IT services on which a business depends
- Some of the operational risks are as follows:
  - Suboptimal uptime and service reliability
  - Lack of customized service levels
  - Reduced control over QoS
  - Reduced control over availability and DR

Legal Risks

- These are IT-related risks that adversely impact organizations that use cloud services
- These risks are legal in nature and include the following:
  - Subpoena and e-discovery
  - Changes of jurisdiction
  - Data privacy
  - Licensing

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

Cloud Computing Risk Categories

Risks in the cloud environment can be classified into the following categories.

- **Policy and Organizational Risks**

  Policy and organizational risks are the business- and IT-related risks faced by organizations while selecting CSPs. The following are some policy and organizational risks.

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

- **Lock-in**: Lock-in refers to the inability of a cloud customer to move their data to another CSP for various reasons such as difficulty.
- **Loss of Governance**: An organization using the cloud does not have sufficient control over its data stored in the cloud. Many CSPs do not take the responsibility for the data stored on their platforms.
- **Compliance Challenges**: Organizations using the cloud do not know where their data are stored and what regulations and laws are applicable to the data. They also face difficulty in determining whether the CSP complies with the applicable regulations and laws.
- **Business Reputation Loss**: If one tenant is involved in malicious activities on the cloud, it affects the provider as well as other tenants. This leads to a loss of business reputation.
- **Cloud Service Failure or Termination**: CSPs may not provide services all the time. They may have service failures and terminations, which can affect the quality of service offered to cloud customers and cause them to face investment loss.

- **Technical Risks**

Technical risks are IT-related risks that directly impact cloud systems that store customer data. The following are some technical risks.

- **Availability of Service**: CSPs cannot provide a cloud service with 100% uptime. The availability of a service can be affected by failures, network performance, etc.
- **Resource Exhaustion**: If cloud resources are not allocated as per the requirements, resource exhaustion occurs. In cloud computing, resources are allocated based on statistical projections.
- **Intercepting Data in Transit**: The interception of data is a technical risk in which data are intercepted in transit to or from the cloud. Possible threats include man-in-the-middle (MITM) attacks, sniffing, replay attacks, and side-channel attacks.
- **Data Transfer Bottlenecks**: Transferring data between cloud environments is expensive and difficult.
- **Distributed Denial of Service (DDoS)**: DDoS attacks are considered a major challenge in cloud computing. Attackers can easily target cloud services to launch DDoS attacks using botnets.

- **Operational Risks**

Operational risks are the risks related to the execution of tasks and IT services on which a business depends. With cloud migration, a new concept of DevOps has been introduced to tackle operational risks. It is an approach in which operations and development responsibilities are merged. This reduces deployment times. However, the IT operations and development teams should be trained on cloud deployment and systems management in a cloud environment.

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

Operational risks in a private cloud include the following.

- **Suboptimal Uptime and Service Reliability**: Organizations may not employ all latest technology and upgrades for the cloud due to increased operational cost. This will result in suboptimal service reliability and uptime.

Operational risks in a public cloud include the following.

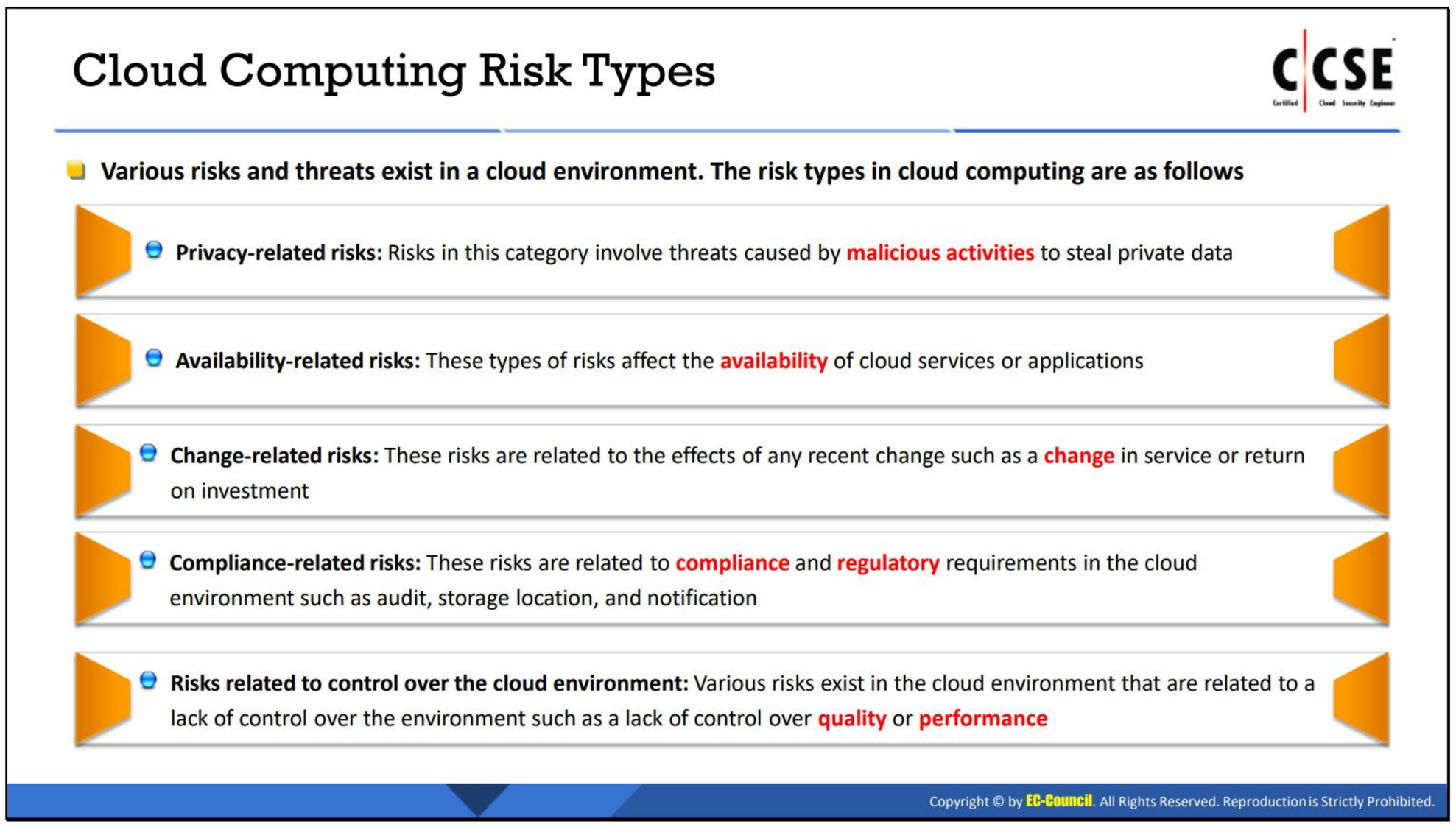
- **Lack of Customized Service Levels**: In cloud computing, organizations may have to select a near-acceptable service level for different IT services owing to a lack of customized service levels. In such as scenario, they cannot customize their apps and services to meet their specific needs.
- **Reduced Control Over QoS**: Organizations have reduced control over the quality of service.
- **Reduced Control on Availability and DR**: Organizations have reduced control over the availability and disaster recovery of their critical applications in cloud computing.

- **Legal Risks**

Legal risks are IT-related risks that adversely impact organizations that use cloud services. These risks are legal in nature and include the following.

- **Subpoena and E-Discovery**: In legal cases where law enforcement agencies confiscate the physical hardware of cloud computing, the data of tenants on the hardware will be disclosed to unauthorized parties.
- **Changes of Jurisdiction**: This risk affects cloud customers whose data are stored at multiple geographical locations that are under different jurisdictions. If their data are stored in data centers located in high-risk areas (jurisdictions where the rule of law is absent, international agreements are not respected, etc.), the data can be forcibly exposed by local authorities.
- **Data Privacy**: It is difficult for cloud customers to check how their data are processed and stored by CSPs. CSPs may not notify their customers about data breaches that affect their data privacy. Moreover, cloud customers do not have control over the data processed by CSPs.
- **Licensing**: Licensing conditions are very complex in cloud computing. Online licensing checks do not work in a cloud environment. Organizations using the cloud may need to pay extra to license instances hosted on CSPs.

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



Cloud Computing Risk Types

Various risks and threats exist in cloud computing. These risks can be categorized into the following types.

hide01.ir

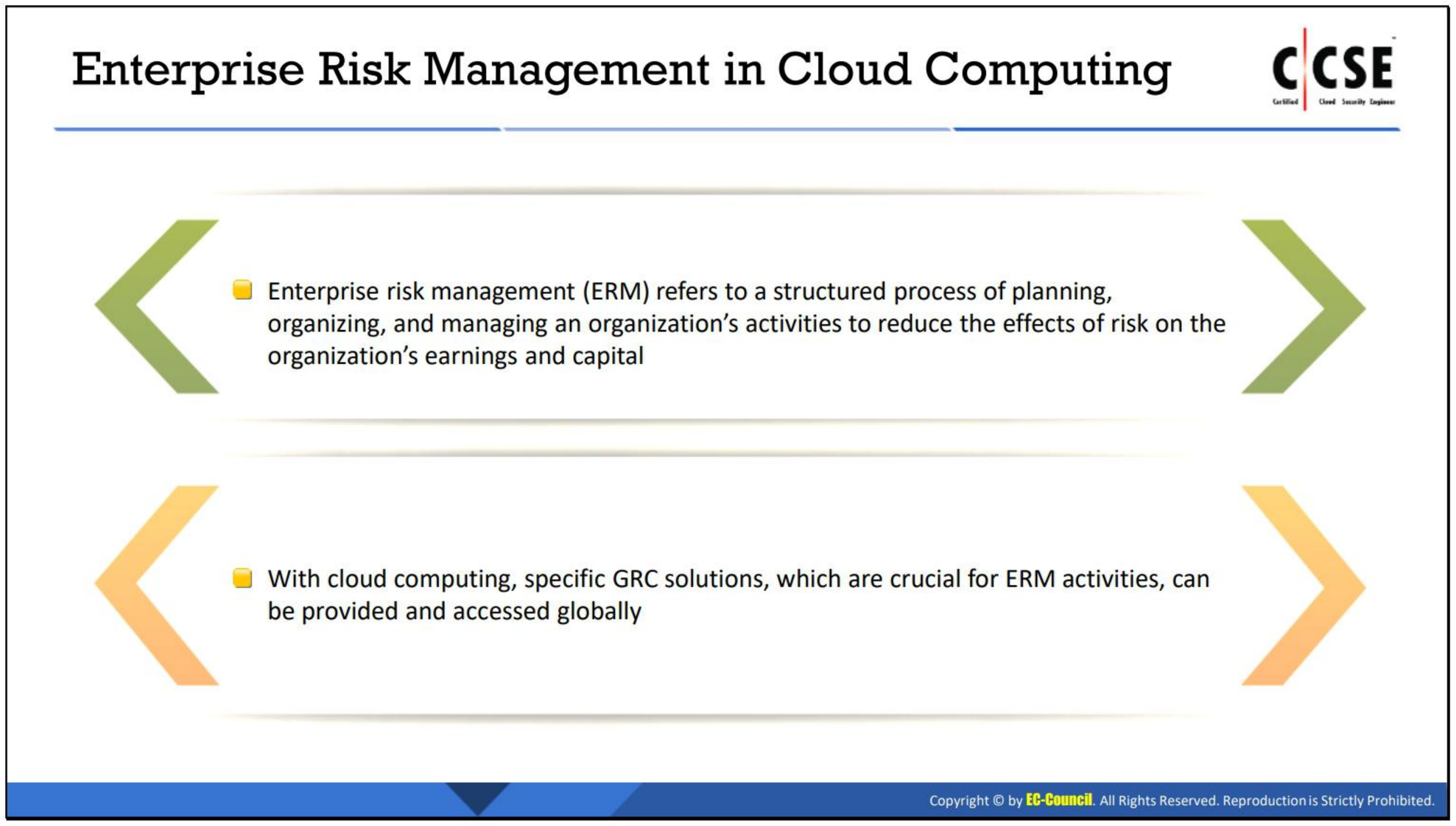
- **Privacy-related Risks:** Risks in this category involve threats caused by malicious activities aimed at stealing private data. The following are some risks related to privacy.
  - **Controlled Access**: Sensitive data stored in the cloud may be accessed by the CSP's staff if access is not controlled properly.
  - **Segmentation**: Multiple subscribers or tenants may exist in a cloud environment. The data of one organization can be accessed by another organization if subscription accounts are not properly segmented.
  - **Ownership Claims**: Ownership issues may arise in a cloud environment. The ownership of data can be inadvertently transferred to the CSP if the organization does not read the agreement properly.
  - **Confidentiality**: Organizations generally choose not to store sensitive data in the cloud to protect the confidentiality of the data. Usually, it is difficult to assign liability for data leaks between two parties (cloud providers and consumers).
- **Availability-related Risks:** This type of risk affects the availability of cloud services. The following is one such risk.
  - **Service Disruption**: Service disruptions can be caused by various factors, including faulty internet connections, degraded service quality, DDoS attacks, and service outages.

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

- **Change-related Risks:** These risks are related to the effects of any recent change. Some of the risks related to change are as follows.
    - **Change in Service**: This includes instances where the service becomes unavailable because of the closure of a CSP or its acquisition by another provider. If the CSP is acquired by another provider, the service may be unavailable for a short time.
    - **Return on Investment**: Organizations move to the cloud to save money. If the cost of a cloud subscription is more than the benefits received from it, the cloud subscription does not meet the purpose of migration to the cloud.
- **Compliance-related Risks**: These risks are related to compliance and regulatory requirements in the cloud environment. The following are some risks related to compliance.
    - **Audit**: Some CSPs do not follow external audit processes, which are important for the customer organizations. This places the organizations or cloud users at risk.
    - **Storage Location**: Customer data in the cloud are stored in various servers located in diverse regions or countries. Cloud customers do not know exactly where their data are stored. Compliance issues may arise for the data stored in different countries where different laws apply. Furthermore, sensitive data belonging to one country may be accessed by a rival country where the data are stored.
    - **Notification**: Customers may not be notified of any data breach by the CSP. This places them at risk because they cannot assess the damage caused by the breach.
- **Risks Related to Control Over the Cloud Environment:** Various risks exist in the cloud environment that are related to a lack of control over the environment. The following are some of them.
    - **Lack of Control Over Quality**: CSPs occasionally do not maintain quality standards. Customer organizations have little control over service quality standards as they are offered by the provider. Customer organizations must also determine how easy it will be to change the CSP in the case it offers services of degraded quality.
    - **Lack of Control Over Performance**: It may not be possible for a CSP to offer high-quality services all the time. As customer organizations have no direct access to the cloud infrastructure, they must rely on CSPs to resolve any service performance issues promptly.

hide01.ir

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



Enterprise Risk Management in Cloud Computing

Enterprise risk management (ERM) refers to a structured process of planning, organizing, and managing an organization's activities to reduce the effects of risk on the organization's earnings and capital. It includes strategic, financial, and operational risks as well as risks associated with accidental losses.

hide01.ir

Optimizing organizational governance, risk, and compliance (GRC) activities is essential to understand the important role of cloud computing in the ERM architecture. Cloud computing simplifies data center operations, improves resource utilization, and offers alternate backup and disaster recovery tools, eliminating the traditional complexities associated with on-premises, physical computing and data-storage operations. With cloud computing, specific GRC solutions that are crucial for ERM activities can be provided and accessed globally, depending on the organization's requirements.

Cloud computing helps organizations adopt feasible ERM architectures and best practices by reengineering and/or rationalizing GRC business processes, resource specialization, information enhancement, data management, etc.

Benefits of ERM in Cloud Computing

Using the cloud helps organizations implement ERM effectively. The following are some of the benefits of using the cloud for ERM.

- **Specialized Personnel**: CSPs hire and manage the finest, skilled personnel of the industry because their business model is based on offering IT resources. Organizations can often retain skilled resources owing to various reasons.
- **Operational Expenses (Opex)**: Organizations in many countries cannot receive immediate tax benefits for purchasing IT equipment for internal use. With capital

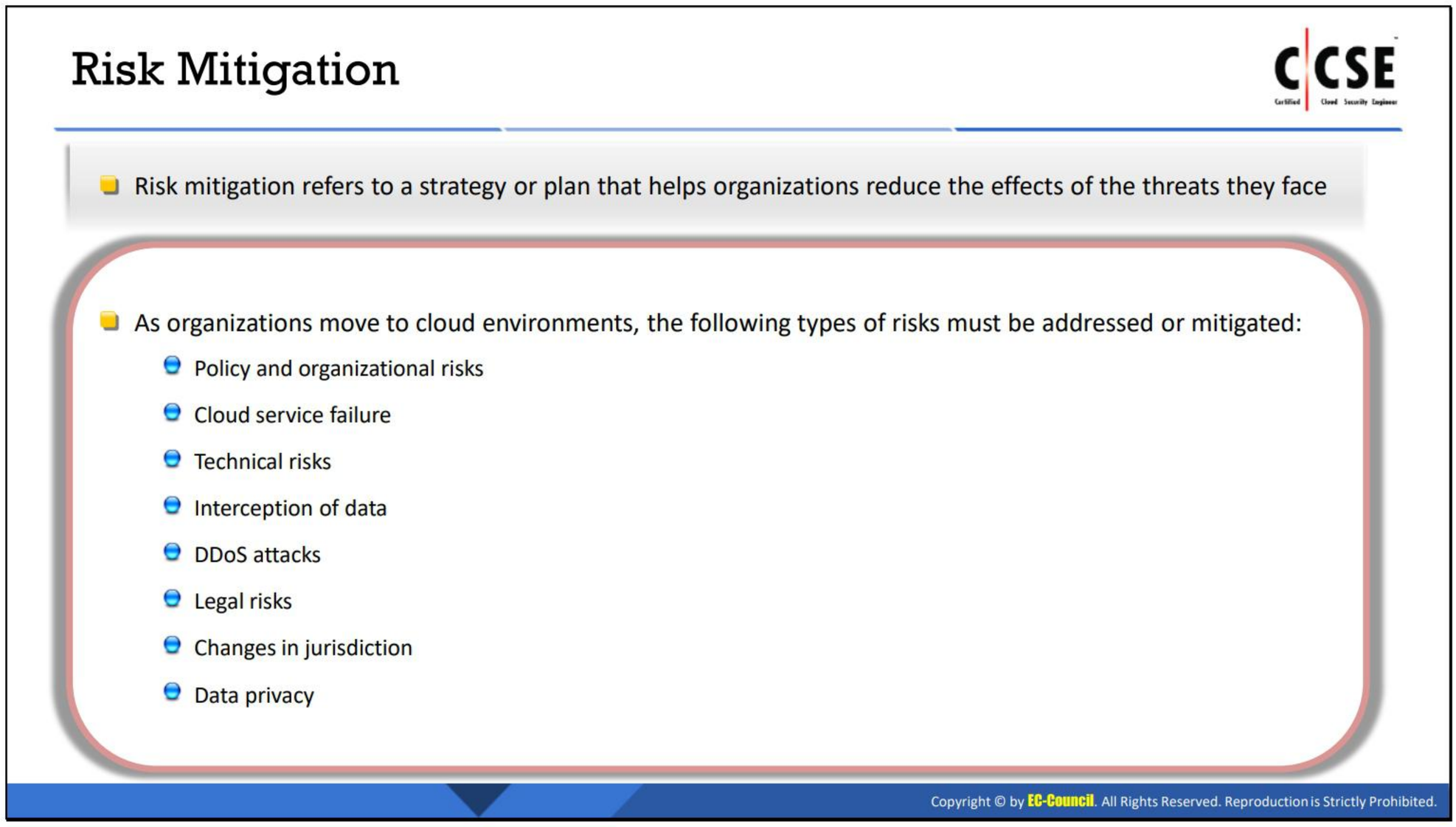
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

expenditure (capex), they receive staggered benefits spanning over five years. In contrast, they can receive instant tax benefits by using CSPs' resources because investments in cloud resources are treated as operational expenses (opex).

- **Platform Support**: For reasons such as the lack of sufficient knowledge, time, and testing infrastructure, many enterprises fail to roll out patches on time or even fail to detect the patches that should be applied. Cloud providers ensure that all applications and setups are updated on their platforms in a timely manner.
- **Backup and Recovery**: Most organizations take backups regularly, but only a few of them attempt to check if the restoration from those backups is successful. CSPs offer backup and recovery services to organizations. They test both data backup and recovery processes and ensure that everything works as expected to avoid unpleasant last-minute surprises. Using the cloud helps organizations implement ERM effectively.
- **Disaster Recovery (DR)**: DR is essential for all organizations that serve customers. For many organizations, implementing a DR process may be challenging if they do not have adequate IT infrastructure and/or skilled staff. Cloud platforms have in-built redundancy and DR capabilities that help organizations in the event of a disaster or failure.
- **Power Savings**: Organizations that move to the cloud can reduce their expenses on power and electricity. This leads to a reduction in costs and increase in profits.
- **Thin Clients**: Organizations that use cloud environments store their applications on the cloud to avoid investing in powerful desktops or laptops (clients) for running their applications. Moreover, they need not worry about information risk factors, as their confidential data are not stored on internal systems.

hi2e01.ir

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



Risk Mitigation

Risk mitigation refers to a strategy or plan that helps organizations reduce the effects of the threats they face. It involves taking various steps to reduce the adverse impacts of disasters and threats on business continuity. It is an essential element of risk management.

As organizations move to the cloud environment, they must address several risks in the cloud. The following are the types of risks that must be addressed or mitigated.

- **Policy and Organizational Risks**: Organizations face the risk of vendor lock-in (dependency on the vendor for products and services) with the use of proprietary interfaces as well as other challenges such as compliance with several regulations.
- **Cloud Service Failure**: Organizations should handle the risk of cloud service failures in the cloud environment and must mitigate these risks via BC/DR planning.
- **Technical Risks**: Companies that deploy cloud solutions often face technical risks such as resource exhaustion. Technical risks can occur if an organization does not manage cloud resources effectively or provision additional resources automatically when required.
- **Interception of Data**: Interception of data is a technical risk in which data are intercepted in transit to or from the cloud. The interception of data can be mitigated by encrypting the transmitted data and authenticating endpoints to ensure that they are legitimate.
- **DDoS Attacks**: DDoS attacks also occur in the cloud. The CSP and their ISP are responsible for the mitigation of DDoS attacks. Cloud customers (organizations) must ensure through discussions with their CSPs that proper security controls are implemented to promptly address the risk of DDoS attacks.

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

- **Legal Risks**: Legal risks must be considered while using the cloud environment. Maintaining compliance with various applicable regulations (e.g., HIPAA and PCI DSS) and laws is the most critical legal risk. Organizations often find it difficult to comply with these regulations while using the cloud. Before migrating to the cloud, organizations should thoroughly research the laws and regulations that apply to them on the cloud.
- **Changes in Jurisdiction**: Changes in jurisdiction are a major challenge faced by organizations. As cloud servers have different geographical locations where different laws apply, it is difficult for organizations to comply with all laws.
- **Data Privacy**: Data privacy can become a legal risk in the cloud because some CSPs have terms in their contracts that allow them to monitor customer data stored on the cloud and even sell the data to third parties. This can cause data privacy issues.

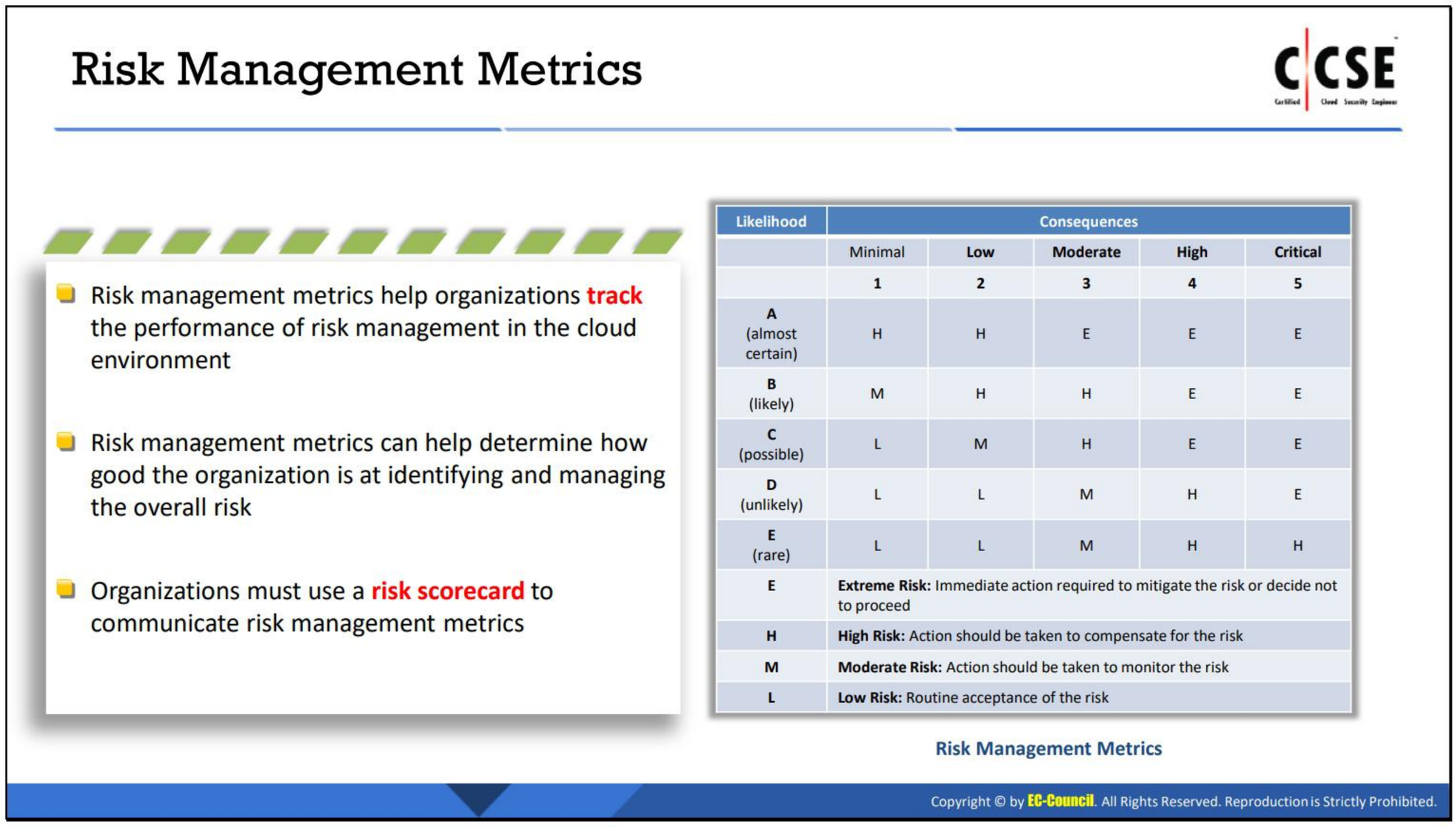
Actionable Risk Mitigation Steps

Organizations can achieve risk management (with risk mitigation) in multiple frameworks. Risk mitigation is included in risk management processes. The following are the steps of the risk mitigation process.

- **Examine the Risk Mitigation Steps**: This includes assessing the types of data and services (prescription, credit card numbers, and personnel records) handled and then identifying the threats against these services and data. IT leaders must analyze these threats to determine appropriate solutions.

  This step of risk mitigation involves implementing basic operational and management security tools for securing data and services. These controls can be security policies, SLAs, basic audit controls, and various forms of governance.
- **Review App Security**: In risk mitigation, evaluating the security of applications is important. It is necessary to identify which features of an application can be used for risk mitigation. IT managers must confirm the robustness of these features. For example, if an app encrypts data at rest for protecting confidentiality, identify the key length and encryption algorithm utilized as well as how powerful the combination of algorithm and key is. Employ additional security controls such as a virtual private network (VPN) if the app is developed to meet strong security requirements.
- **Develop a Data-Centric Governance Plan**: Data governance involves managing data throughout the enterprise by performing backups, handling e-discovery requests, and archiving old data. The absence of a data governance policy can increase the risk of data being misplaced, which makes the data easy to compromise. Organizations must develop a data-centric governance plan to address data management issues. They can use data leakage prevention (DLP) solutions to stop the unwanted proliferation of confidential data to unknown locations. Ensure that only authorized individuals have access to the data stored in the cloud.
- **Test and Retest**: Periodically test the data governance plan after implementing it. Testing includes actions such as ensuring that archived data are securely stored and unwanted data are destroyed properly. Regular testing is essential to ensure that all controls work as intended.

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



Risk Management Metrics

Risk management metrics help organizations track the performance of risk management in the cloud environment. Risk management approaches help manage risks actively within a specified area of the business. However, risk management does not help in determining how good an organization is at detecting and managing risks effectively. To determine how risk is managed, tracking is required. Risk management metrics can help determine how good the organization is at identifying and managing the overall risk.

Organizations can understand risk exposure better when they know whether organizational risks are managed effectively. Project management tools can be used to identify risks and improve risk awareness. Some risk metrics that help track risk management are listed below. All these metrics cannot be tracked simultaneously, as some of them can only be tracked once the risk becomes a real incident.

- **Number of Risks Detected**: Risks can be detected per project or program. The number of risks that a project can have depends on the project type. A project that was implemented multiple times will have a lower number of risks than a newly implemented project.
- **Number of Risks That Occurred or Became Issues**: The number of risks that turned into real issues or incidents on a project can be tracked. This step helps identify how well the risk analysis is being performed. For example, if multiple risks are tracked that turn into real issues, the team analyzing the risks should be informed that these issues might cause problems. If no tracked risk turns into an issue, the team should be informed that it is not tracking the relevant risks.

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

- **Number of Risks That Occurred Multiple Times**: The occurrence of a risk more than once in a single project or in different projects indicates that the team did not learn from its past experience.
- **Expected Risk Severity Vs. Actual Severity**: When a risk transforms into an issue, its impact on the project should be identified, and its severity should be compared with the predicted severity. Furthermore, organizations must check whether mitigation plans had the desired impact on minimizing the risk. Moreover, organizations should check whether residual risks are properly identified and mitigated.
- **Number of Unidentified Risks**: Issues that occurred but were not identified as risks should be tracked. The issue log can be checked to find the issues that had to be tracked as risks but were not.
- **Risk Management Cost**: The investment on risk management activities should be compared with the expected expenses. This measure can help estimate or determine the cost of risk on upcoming projects.
- **Number of Closed Risks**: Organizations must check how many risks passed by without turning into real issues and whether any active measures were taken to manage them. Identifying and tracking multiple risks can help track the key risks a project is facing. This shows that active risk management is being performed. However, a large number of detected risks with no closed risks indicates that the risk analysis was not effectively performed throughout the project lifecycle.

h1901.ir

Include the above risk management metrics in the project closure report. Check the key metrics from the start of a project for spotting trends and taking practical steps to improve risk management.

Organizations must use a risk scorecard to communicate risk management metrics. Assess the probability and impact of every risk separately and then consolidate the results to show exposure by using the following risk-level scale:

- Minimal
- Low
- Moderate
- High
- Critical

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

Likelihood	Consequences				
	Minimal	**Low**	**Moderate**	**High**	**Critical**
	1	**2**	**3**	**4**	**5**
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H
E	**Extreme Risk:** Immediate action required to mitigate the risk or decide not to proceed				
H	**High Risk:** Action should be taken to compensate for the risk				
M	**Moderate Risk:** Action should be taken to monitor the risk				
L	**Low Risk:** Routine acceptance of the risk				

Figure 10.10: Risk Management Metrics

The above risk scorecard offers a clear representation of potential risks.

hide01.ir

Monitoring Risk in a Cloud Ecosystem

Multiple cloud applications are used by organizations. These applications, which are used often, must be monitored based on the risk they pose to organizations and the purpose they serve. Risks in a cloud ecosystem can be monitored in the following ways.

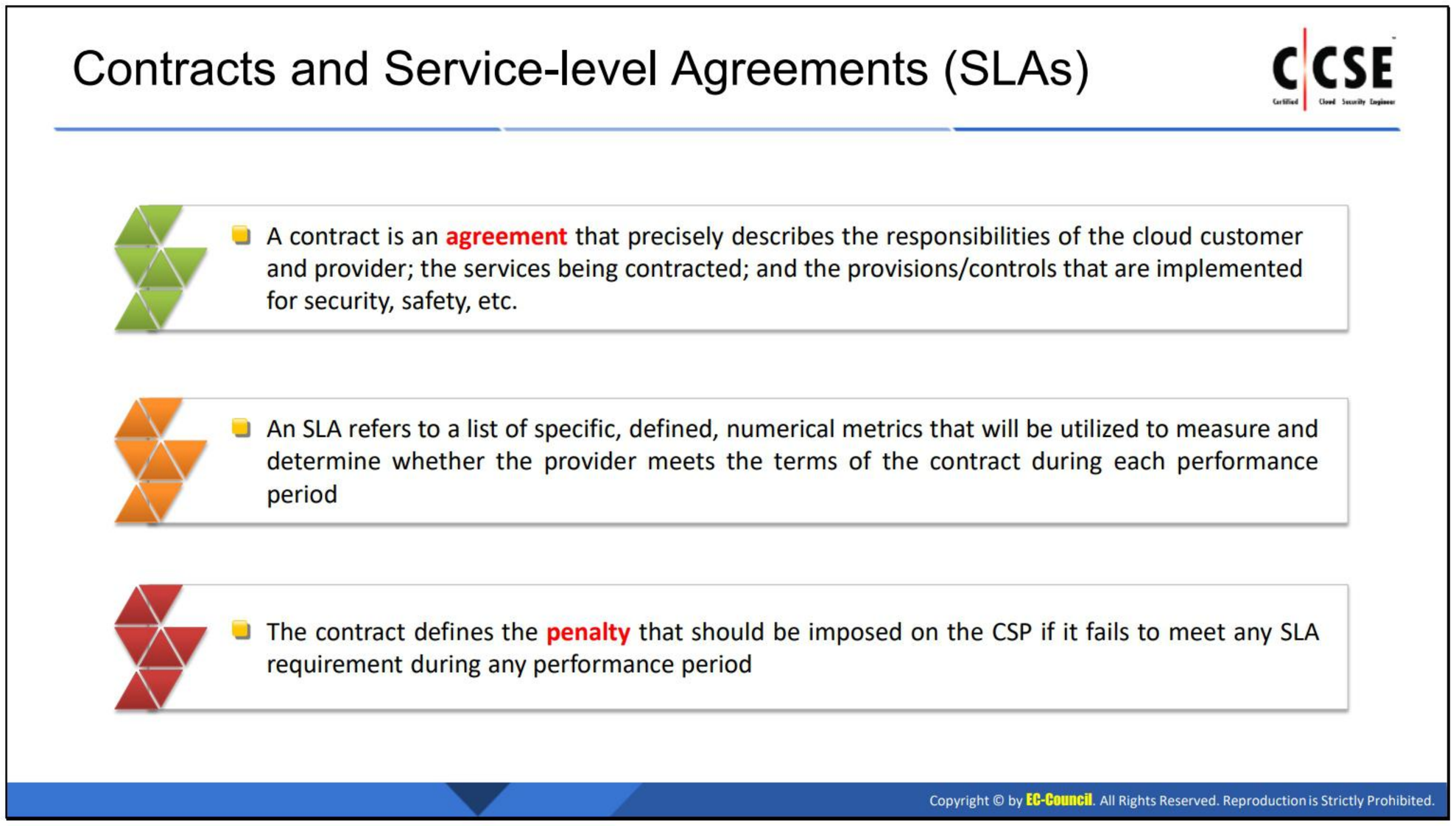
- **Cloud Apps in High-Risk Zones**: Use risk classification parameters to detect high-risk cloud applications. Examples are applications that do not have a well-defined privacy policy and apps hosted outside the EU.
- **Unauthorized Cloud Apps**: In organizations, some employees use or download cloud services without informing their IT staff. This is referred to as shadow IT, which poses data security risks to organizations. Consider the ratio of unauthorized/authorized cloud apps that are being used.
- **Redundant Cloud Apps**: Check the number of duplicate or unnecessary cloud apps based on the application discovery and use case. For example, cloud-based file storage can be combined to a single app such as Dropbox or Google Drive.
- **Sensitive Information Exposure**: Use a metric to detect the files accessed by unauthorized users via the on-premises intranet or the Internet.
- **Collaborations by External People**: Organizations should track (have complete details) of outsiders collaborating on files or content having sensitive data hosted inside or outside the domain.

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

- **Cloud Services Accessing Sensitive Information**: Identify the number of cloud services that process or store sensitive data.
- **Cloud Services By Category**: Organizations must classify cloud services that are in use by their category. Examples are social media and file sharing.
- **Cloud Policy Violations**: Closely monitor policy violations and exceptions. Examples are unmanaged cloud apps that are not tracked and unmanaged devices that have access to sensitive information.
- **Privileged Logins**: Identify the number of users that have privileged logins for authorized cloud apps.
- **Using Cloud Access Security Brokers (CASBs)**: The measurement of the above-mentioned metrics can be automated by deploying CASBs, which also generate reports for these metrics.

hide01.ir

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



Contracts and Service-Level Agreements (SLAs)

Contracts and SLAs are official agreements that define, establish, and enforce the relationship between a CSP and customer. Contracts and SLAs are briefly defined below.

Contracts: A contract is an agreement that precisely describes the responsibilities of the cloud customer and provider; the services being contracted; and the provisions/controls that are implemented for the security, safety, integrity, and availability of these services.

SLAs: An SLA refers to a list of specific, defined, numerical metrics that will be utilized to measure and determine whether the provider meets the terms of the contract during each performance period.

Although contracts and SLAs are different, they are related to each other. The contract defines the penalty that should be imposed on the CSP if it fails to meet any SLA requirement during a performance period. For example, if one month is taken as a performance period and an SLA metric allows not more than 5 s of downtime, then the provider can have a downtime of only up to 5 s during each month. If the downtime during any month is greater than 5 s, the customer is allowed to withhold payment for that particular month as the provider failed to meet the SLA requirement. Furthermore, the provider cannot discontinue the services offered to the customer, although the customer does not pay for that month.

The contract between the customer and provider must have the following essential elements and activities:

- Performance
- Availability (e.g., 99.99% of data and service uptime)
- Portability of databases

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

- Data location
- Logging and reporting (e.g., ability to report on key requirements and indicators as well as audit trails of all instances of access)
- Data format and structure (e.g., retrieving data from the CSP in an intelligent and readable format)
- Security and privacy of data (e.g., encrypting data at rest and in transit)
- Identification and problem resolution
- Dispute mediation (e.g., consequences and escalation process)
- Change management (e.g., new services or updates)
- Exit strategy options
- Components' activity
- Uptime guarantees (the five 9s principle)
- Penalties (for both the provider and customer)
- Penalty exclusions (e.g., scheduled downtime)
- Suspension of service
- Provider liability
- Disaster recovery
- Data protection requirements
- Security recommendations

hide01.ir

The SLA assigns particular numerical values (metrics) to the performance objectives mentioned in the contract. SLAs may have details such as those mentioned below.

- The customer will have constant, full access to their data and account(s) at all times. However, a service interruption of less than 24 h is allowed per calendar quarter (the provider will be responsible for the interruption).
- Data transferred from or to the CSP's resources and control at a specified rate should not exceed 40 GB/h. If the data transfer speed is greater, additional charges will be levied as per the rates specified in the standard rate sheet.
- All inquiries from the customer will be addressed by the provider within 3 h via telephone or email.

Key Cloud SLA Elements

Assess the below key elements while reviewing and accepting the SLA.

- **Risk Environment Assessment**: What are the risk types the enterprise may face?
- **Risk Profile**: What is the potential effect of risks and the number of risks?

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

- **Risk Appetite**: What is the acceptable/tolerable level of risk?
- **Regulatory Requirements**: Will these requirements satisfy the SLA?
- **Responsibilities**: Who will be responsible for what?
- **Risk Mitigation**: Which type of mitigation controls and techniques can minimize risks?
- **Risk Frameworks**: Which frameworks will be used to evaluate the ongoing effectiveness? How will cloud risk management be performed by the provider?

The cloud customer must address quality of services (QoS) issues to ensure that they receive services of high overall quality from the provider. Some of the QoS issues that should be considered are as follows:

- Capacity metrics
- Performance metrics
- Availability
- Outage duration
- Storage device metric
- Response time metric
- Storage capability
- Completion time metric
- Server capability
- Server capacity metric
- Meantime to switchover

hide01.ir

Business Requirements

Before migrating applications or systems to the cloud, an organization must have a comprehensive understanding of how its systems are built and configured and how they interact with other systems. This will help the organization understand whether it can move the intended application or system to the cloud. It can also determine whether the application requires any changes in code to work in the cloud environment as well as the possible impact it may have on compliance and regulatory requirements.

This analysis can help an organization develop and document specific business requirements for the cloud environment. The organization should create an organizational cloud strategy before signing the contract with a CSP. For developing the strategy, it needs to evaluate all key organizational assets for suitability to the cloud environment because not all systems and applications are cloud-ready. It is highly likely that not all business requirements of the organization can be met by the cloud provider. The organization must perform a gap analysis with the help of the security staff and operations staff to estimate the level of risk associated with moving to the cloud.

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

The organization's management can then analyze if the identified risk lies within acceptable levels. During the analysis, the management must consider its business continuity and disaster recovery (BCDR) plans and the impact of moving to the cloud on these plans. Any potential risks, restrictions, or exceptions must be highlighted and documented. All regulatory and compliance components that must be satisfied (either by the CSP or both parties) must be documented.

Service-level agreements (SLAs) play a vital role in cloud computing between the cloud customer and CSP. The organization must ensure that all components that are essential for its business, compliance, and regulatory needs are present in SLAs. In the cloud environment, cloud customers do not have the same level of access they have to conventional data centers. With SLAs, CSPs are contractually bound to fulfill the agreed-upon requirements of the customer organization. CSPs must allocate sufficient resources, as promised in SLAs, and respond to issues promptly to meet the business requirements of the organization.

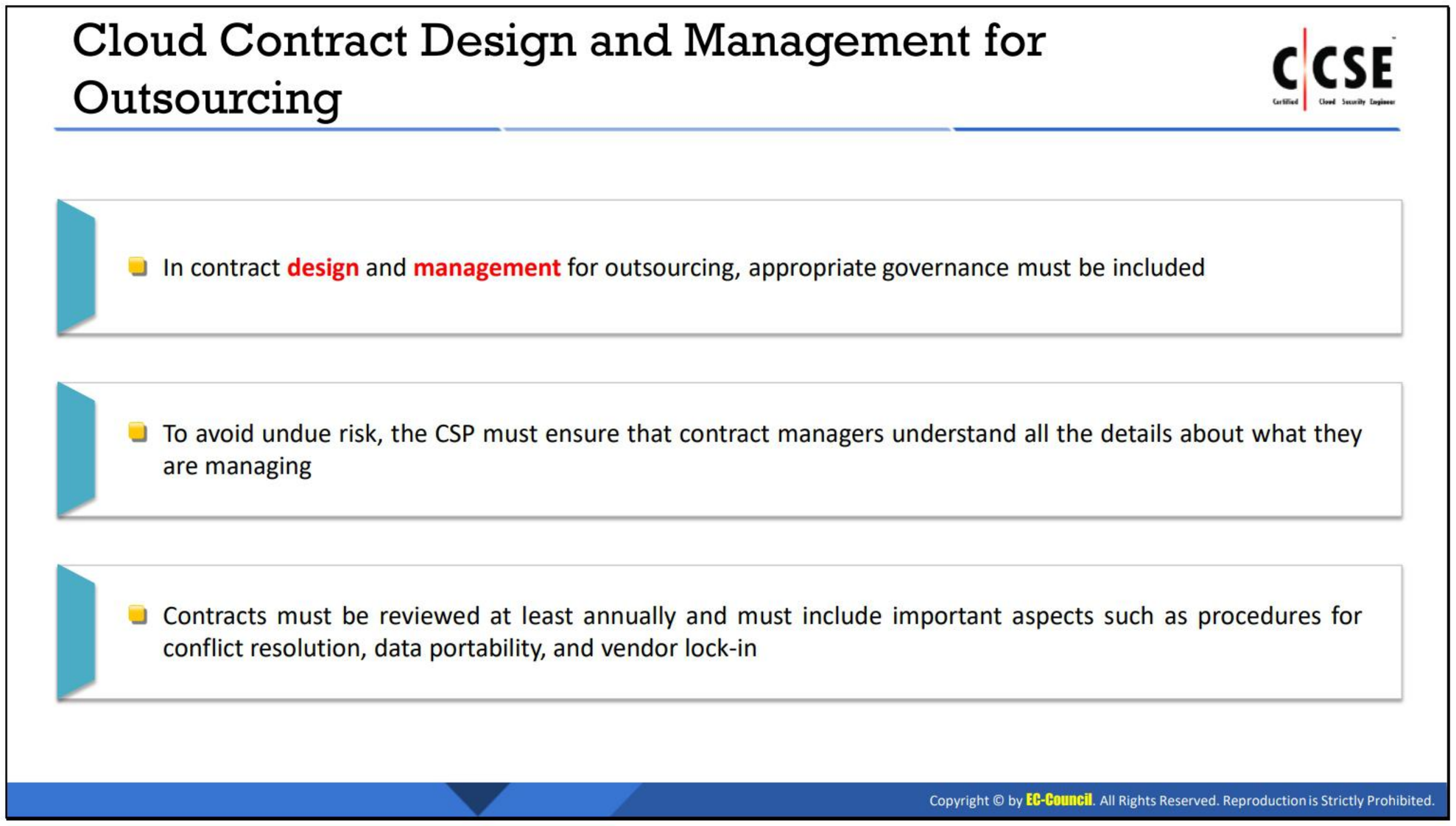
Cloud Migration Checklist

An organization must consider the items in the following checklist to evaluate whether the cloud can meet its business requirements.

- **Consider Business Outcomes With Financials**: Understand the business and financial drivers that are important for the business. Then, consider how they will impact the business when the target application or system is moved to the cloud.
- **Evaluate the Suitability of Applications**: Assess the suitability of the application that must be moved to the cloud. This assessment will help in identifying potential constraints and choosing the appropriate deployment model.
- **Review Business Processes**: The organization's business and operational processes will be affected by the implementation of cloud services. Identify the processes that will be affected. Review the current business processes to check where improvements can be made using cloud services.
- **Insourcing or Outsourcing Cloud Management**: Decide whether the migration process and cloud management will be handled by an in-house team or outsourced to a managed IT service provider.

h1de01.ir

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



Cloud Contract Design and Management for Outsourcing

In contract design and management for outsourcing, appropriate governance must be included. It is essential to have a deep understanding of contracts and contract management. Large organizations have a dedicated department to handle these aspects. Procurement and legal departments are generally responsible for understanding and appraising outsourcing. The outsourcing of a single role and function or complete business functions can fill skills gaps, increase cost benefits, and ensure the efficient and smooth movement of entities.

To achieve this, understand the reasons, business drivers, rationale, requirements, and potential impacts of cloud adoption. Moreover, the ability to coordinate, interpret, and communicate the challenges that lie ahead is essential while migrating to cloud computing. To avoid undue risk, the CSP must ensure that contract managers understand all the details about what they are managing. Ensure adequate governance in contract design and management for outsourcing.

An example of adequate governance is how frequently contracts are reviewed. Contracts must be reviewed at least annually and must include important aspects such as procedures for conflict resolution, data portability, and vendor lock-in. Vendor lock-in refers to the inability of a cloud customer to move away from their CSP due to some technical limitations or detrimental contract terms. Customers desire data portability to avoid vendor lock-in. Data portability refers to the ease of moving data from one CSP to another. The lower the portability of data, the higher is the chance of vendor lock-in.

Cloud outsourcing is more complex than conventional IT outsourcing as it involves many factors that must be considered while moving to the cloud. The CSP must act as an informed advisor to ensure that this process is smoother and more efficient by highlighting risks and issues before any unexpected event occurs.

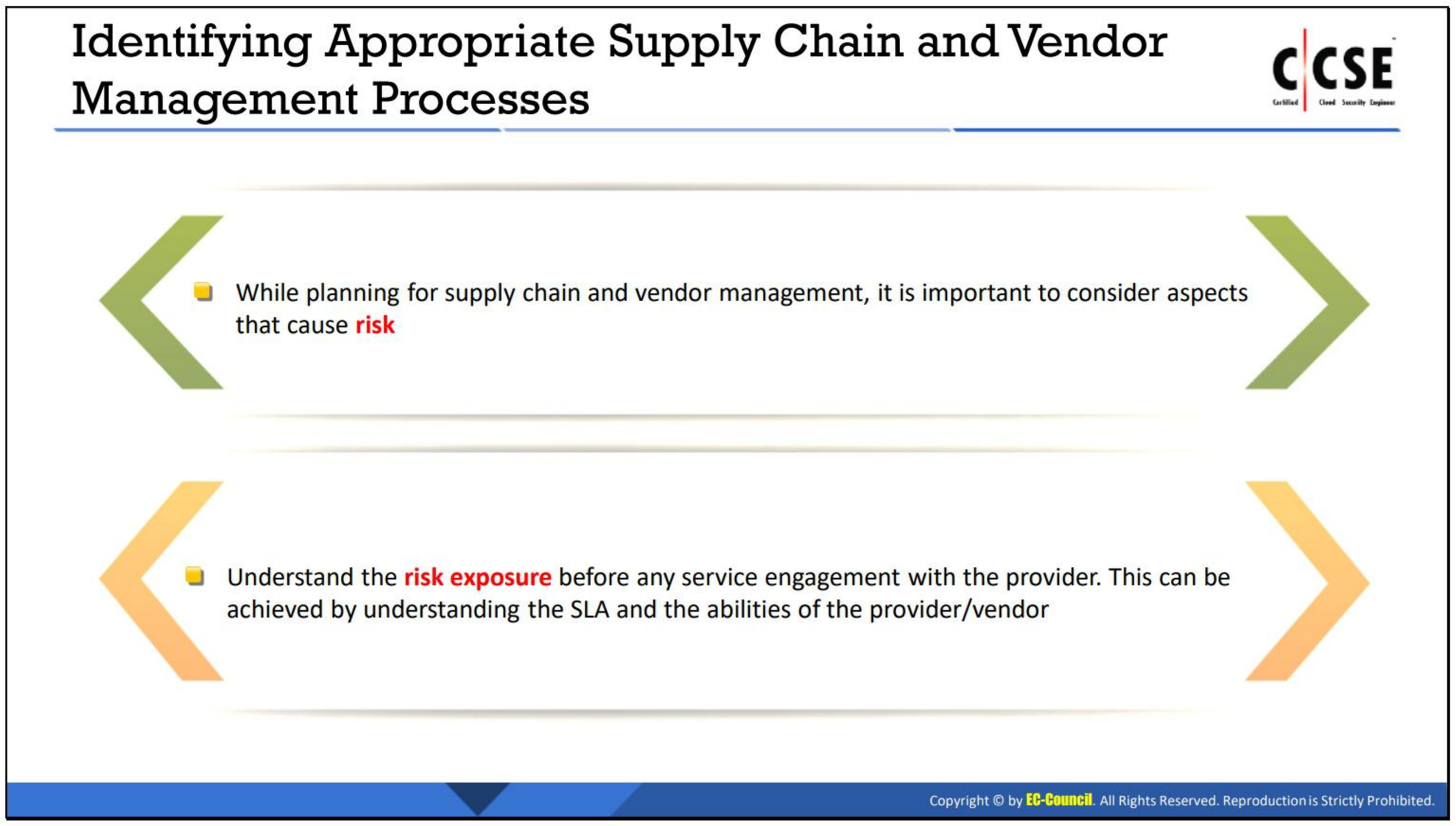
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following questions are important and should be considered while managing outsourcing contracts.

- If a change in CSP is desired, what will happen to the data? Will the data be transported?
- Can the data be transported to another CSP?
- Will the data be in a universal format so that it can be used?
- If conflicts are unresolved, will there be sufficient time to move data?
- Are there adequate data deletion arrangements via techniques such as crypto-shredding?

hide01.ir

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



Identifying Appropriate Supply Chain and Vendor Management Processes

While planning for supply chain and vendor management, it is important to consider aspects that cause risk. For example, when using conventional servers for application delivery to end users, outages can be quickly handled because the staff can solve problems instantly. However, in a cloud scenario, it is not possible to reach the cloud environment to solve problems.

Additionally, factors such as availability play an important role in the cloud. Multiple parties may be involved in a supply chain for delivering a cloud service. These parties include the following.

- **Cloud Carriers**: They are the ISPs between the CSP and cloud customer.
- **Platform Provider**: It is the vendor that supplies the OS used in the cloud service.
- **Application Provider**: It is the vendor that supplies the software used in the cloud service.

The above-mentioned entities may be different but are part of the supply chain. Problems may arise if any one of these becomes unavailable or creates issues in accessing resources. These supply chain risks must be handled carefully.

It is important to understand risk exposure before any service engagement with the provider. This can be achieved by understanding the SLA and the abilities of the provider/vendor. Ensure that the SLA contains the following elements:

- Performance
- Logging and reporting
- Security and privacy protections

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

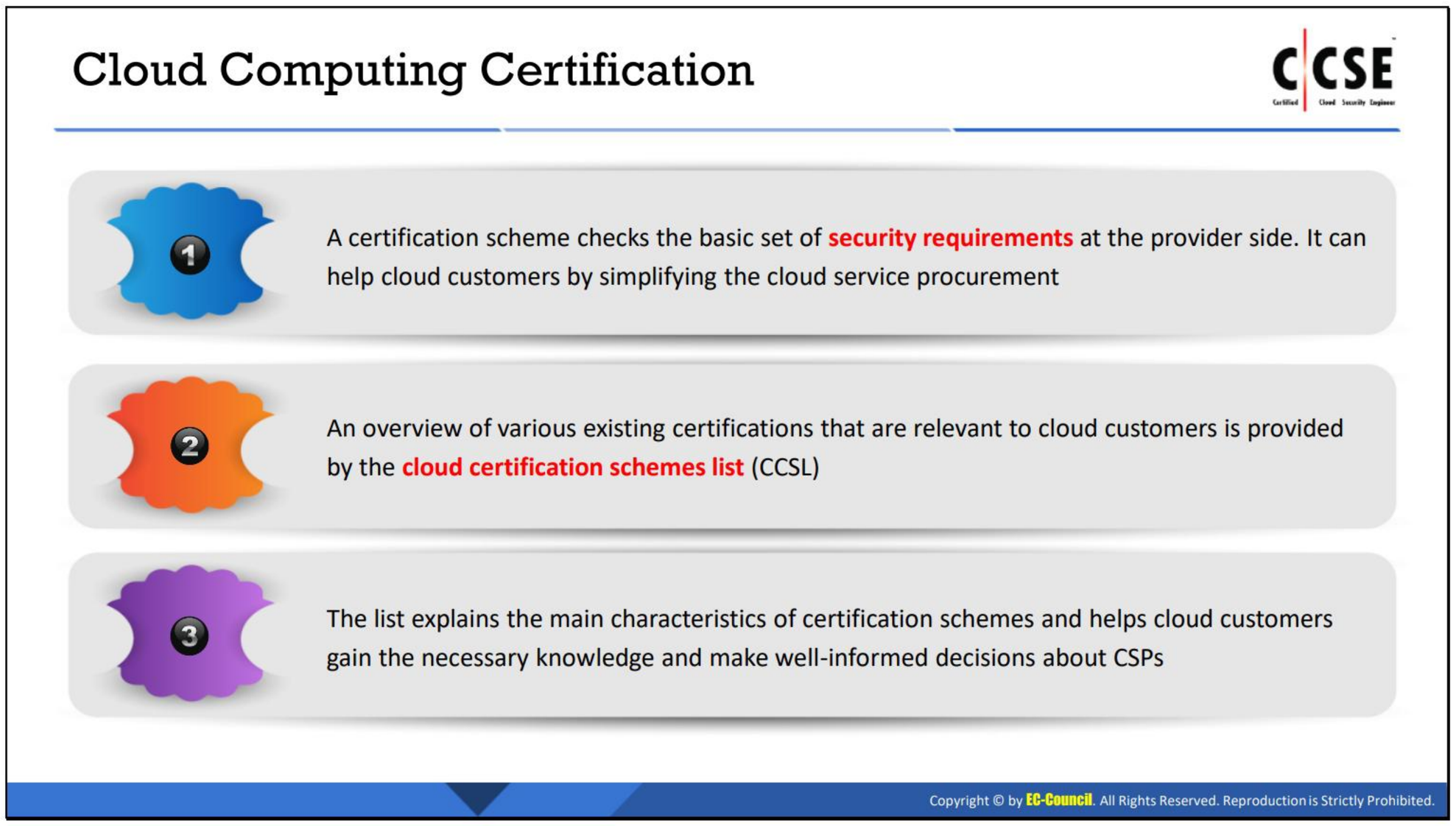
- Data location
- Data portability
- Change management process
- Dispute mediation process
- Data format and structure
- Problem identification and resolution processes
- Exit expectations
- Disaster recovery metrics
    - Recovery time objectives (RTOs)
    - Maximum period of tolerable disruption (MPTD)

The following are some questions that can help in understanding the risk exposure.

- Is this provider established for technology?
- Is the cloud service a main business for the provider?
- What is the provider's location?
- Is the provider financially stable?
- Is the provider certified against relevant professional and security standards and frameworks?
- Does the provider have adequate business continuity and disaster recovery (BCDR) processes in place?
- How will the provider meet the applicable regulatory, compliance, and legal requirements?
- Are there any reports of recent events that had an impact on the availability of cloud services?
- Does the provider offer interoperability to make the transition between CSPs easy?
- Are there any unexpected regulatory-driven compliance requirements?

hide01.ir

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



Cloud Computing Certification

Cloud customers may want to ensure that the cloud services they intend to procure are reliable and safe. As cloud services are complex and supported by various information and communications technology (ICT) components (data centers, cables, software, etc.), customers cannot check all the technical details by themselves. They cannot even perform an independent on-site audit for a CSP, because the CSP cannot allow each customer to audit them.

A certification scheme checks the basic set of security requirements at the provider side. It can help cloud customers by simplifying the cloud service procurement. However, this does not mean that the certification would replace due diligence exercised by customers while procuring cloud services.

An overview of various existing certifications that are relevant to cloud customers is provided by the Cloud Certification Schemes List (CCSL). The list explains the main characteristics of certification schemes and helps cloud customers gain the necessary knowledge and make well-informed decisions about CSPs. The CCSL attempts to answer the following questions.

- What are the underlying standards?
- Is the provider audited?
- Who provides certifications?
- Who performs audits?

The CCSL list comprises the following certification schemes:

- Certified Cloud Service – TUV Rhineland
- CSA Self-Assessment – OCF Level 1

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

- CSA Attestation – OCF Level 2
- CSA Certification Level 2
- EuroCloud Self-Assessment (ECSA Self-Assessment)
- EuroCloud Star Audit Certification (ECSA Audit)
- LEET Security Rating Guide
- Payment Card Industry Data Security Standard (PCI DSS) v3.2
- AICPA SOC 1
- AICPA SOC 2
- AICPA SOC 3

As an extension to CCSL, the Cloud Certification Schemes Metaframework (CCSM) provides a high-level mapping of the customer's security objectives to security objectives in current cloud security schemes. Cloud customers can access the CCSM tool online on the European Union Agency for Cybersecurity (ENISA) website. The CCSM tool provides customers with 27 CCSM objectives to select. Customers can select objectives by cross-referencing them against the certifications provided by CCSL.

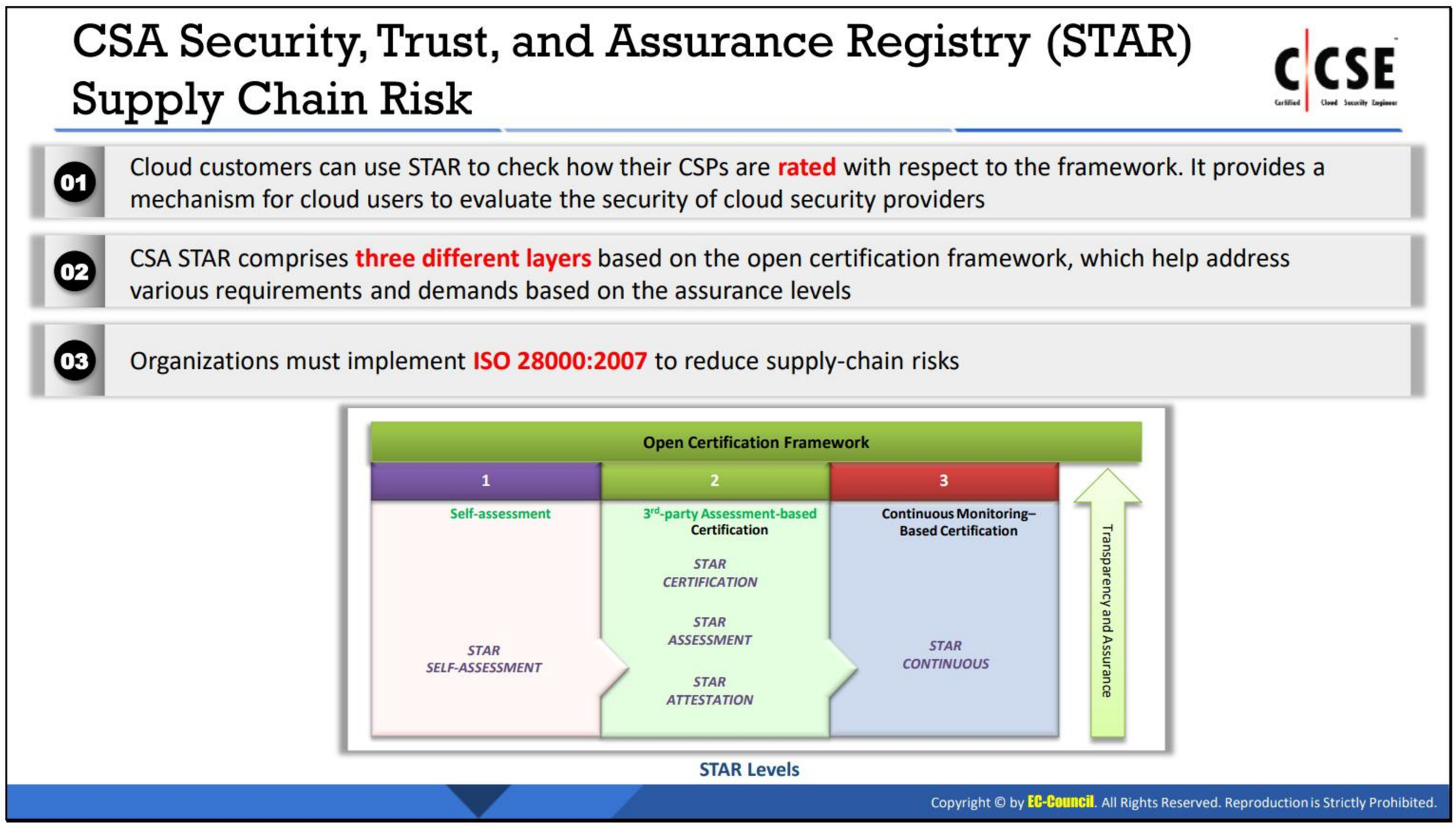
The figure below is a sample of how the resulting comparision matrix appears.

CCSM Security Objectives	Certified Cloud Service – TUV Rhineland	CSA Attestation OCF Level 2	EuroCloud Self-Assessment	ISO/IEC 27001 Certification
Risk Management	•	•	•	
Cloud Data Security	•	•	•	
Cloud Software Security	•	•	•	•
Cloud Monitoring and Log Access	•	•	•	•

ripeem.ir

Figure 10.11: Comparison Matrix of the CCSL and CCSM Objectives

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



CSA Security, Trust, and Assurance Registry (STAR) Supply Chain Risk

The Cloud Security Alliance (CSA) introduced the Security, Trust, and Assurance Registry (STAR) program to evaluate CSPs. Cloud customers can use STAR to check how their CSPs are rated with respect to the framework. It provides a mechanism for cloud users to evaluate the security of cloud security providers. CSA made STAR a publicly available and accessible registry to ensure cloud adoption and use throughout the cloud industry.

CSA STAR consists of the following components.

- **Cloud Controls Matrix (CCM)**: CCM is a list of security principles and controls suitable for a cloud environment and cross-referenced to various other frameworks such as NIST pubs, ISO standards, and COBIT.
- **Cloud Assessments Initiative Questionnaire (CAIQ)**: CAIQ is a self-assessment performed by CSPs in which they evaluate control groups and practice areas they utilize while offering their services.

CSA STAR Layers

CSA STAR comprises three different layers based on the open certification framework.

- **Self-assessment (Level 1)**: It demands the release and publication of due-diligence self-assessment against the CSA CCM or CSA CAIQ.
- **Attestation (Level 2)**: It demands the release and publication of the results of an assessment performed by a third party based on CSA CCM and AICPA SOC2 or ISO 27001:2013.
- **Ongoing Monitoring Certification (Level 3)**: It demands the release and publication of security properties monitoring results based on the cloud trust protocol (CTP).

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

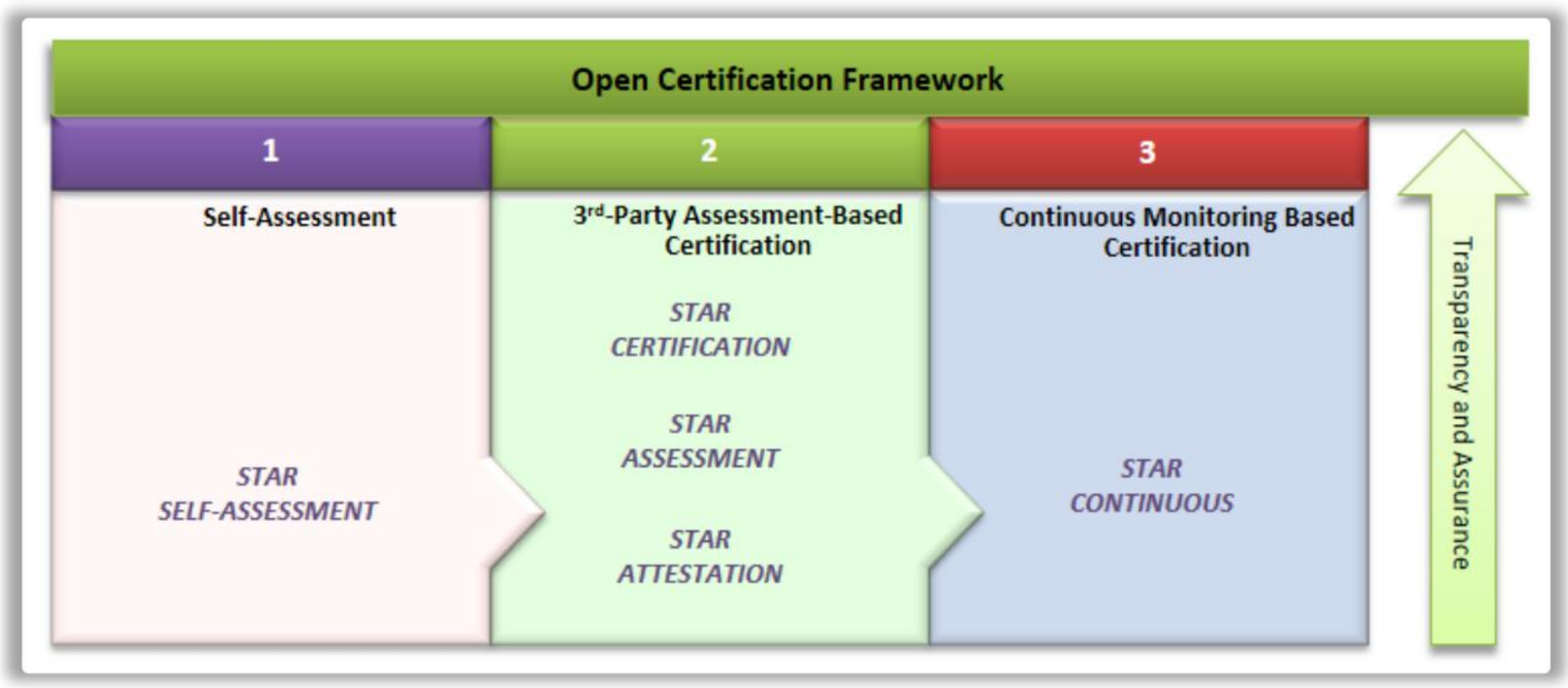


Figure 10.12: STAR Levels

Based on the assurance of levels, all levels allow addressing different requirements and demands.

Supply Chain Risk

Cloud customers must seriously consider business continuity and disaster recovery when evaluating supply chain risk. Ensure that all risks are properly identified and sufficient arrangements are implemented to tackle them. Some prevalent supply chain risks include the following:

hide01.ir

- Data breaches
- Provider's financial instability
- Single point of failure
- Data loss
- Malware infestations

All risks cannot be eliminated or reduced. Some risks such as natural disasters are too large to handle and cannot be removed or overlooked. In cases where the risk is too large to be removed, it needs to be transferred or avoided. One example of transferring the risk is insurance. Insurance helps in situations where the chance of a disaster is small but the effects/consequences of it would be huge.

Organizations must implement ISO 28000:2007 to reduce supply chain risks. This standard defines a collection of security management requirements that can help avoid risks in the supply chain. The contracting enterprise is responsible for ensuring the stability of each vendor in the supply chain for meeting ISO 28000:2007 requirements. Furthermore, this standard offers a certification against the following elements that are related to supply chain risk:

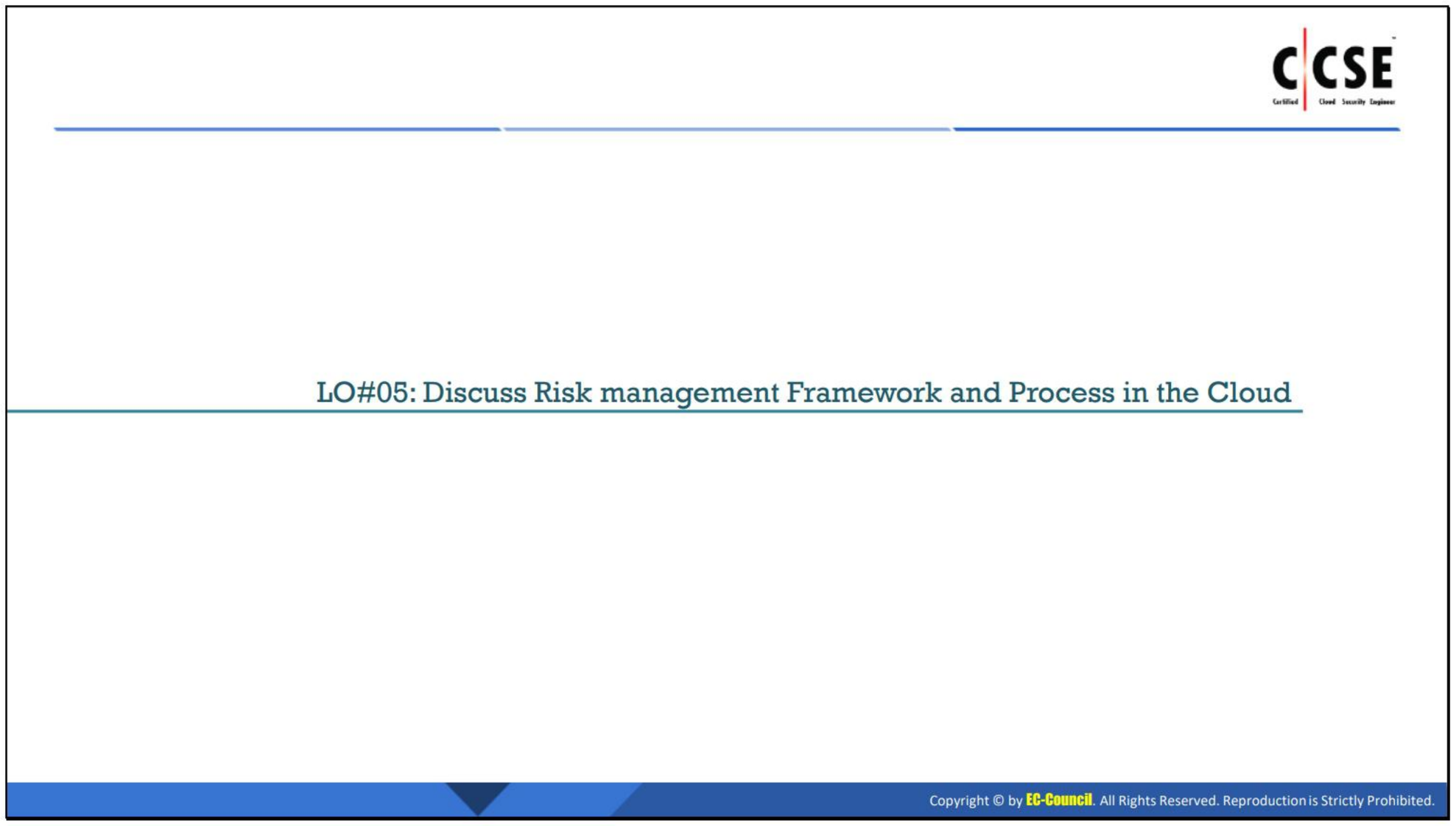
- Organizational objectives
- Security management policy
- Supplier relationships

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

- Risk management practices
- Documented records and practices
- Roles, responsibilities, and authorities
- Organizational processes and procedures

hide01.ir

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

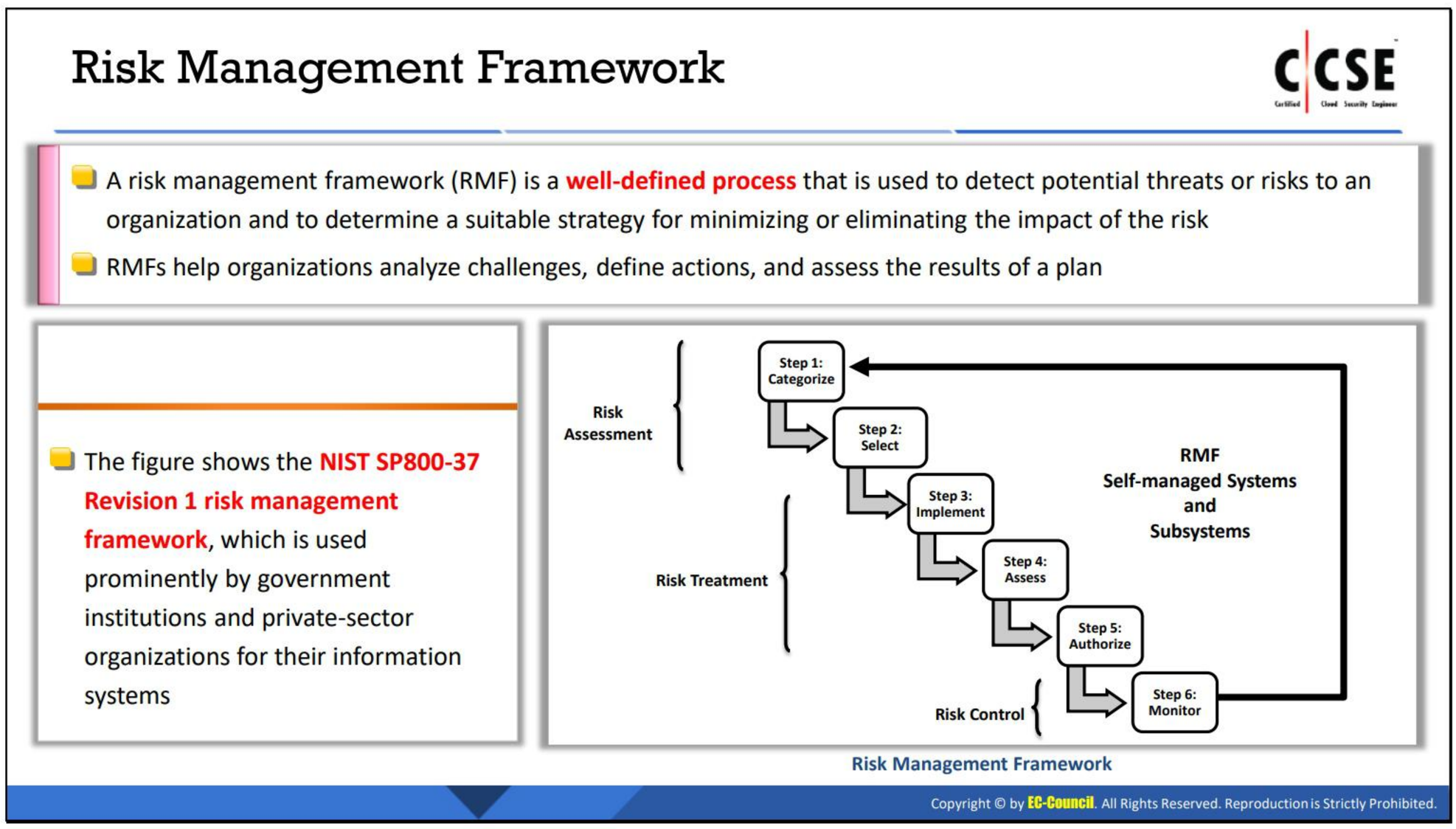


LO#05: Discuss Risk Management Framework and Process in the Cloud

This section explains in detail the risk management framework and processes used in GRC to secure the cloud.

hide01.ir

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



Risk Management Framework

A risk management framework (RMF) is a well-defined process that is used to detect potential threats or risks to an organization and to determine a suitable strategy for minimizing or eliminating the impact of the risk. It also helps define mechanisms to monitor and assess the strategy effectively. International organizations use RMFs to determine plausible foreign-exchange risk management strategies. RMFs help organizations analyze challenges, define actions, and assess the results of a plan. Effective risk management plays a crucial role in ensuring an organization's financial stability and performance.

An RMF offers a structured and disciplined process that combines InfoSec and risk management activities into the system development lifecycle (SDLC). In the risk management hierarchy, an RMF works primarily at tier 3 but can have interactions at tiers 1 and 2, such as providing feedback to the risk executive based on ongoing monitoring and authorization decisions.

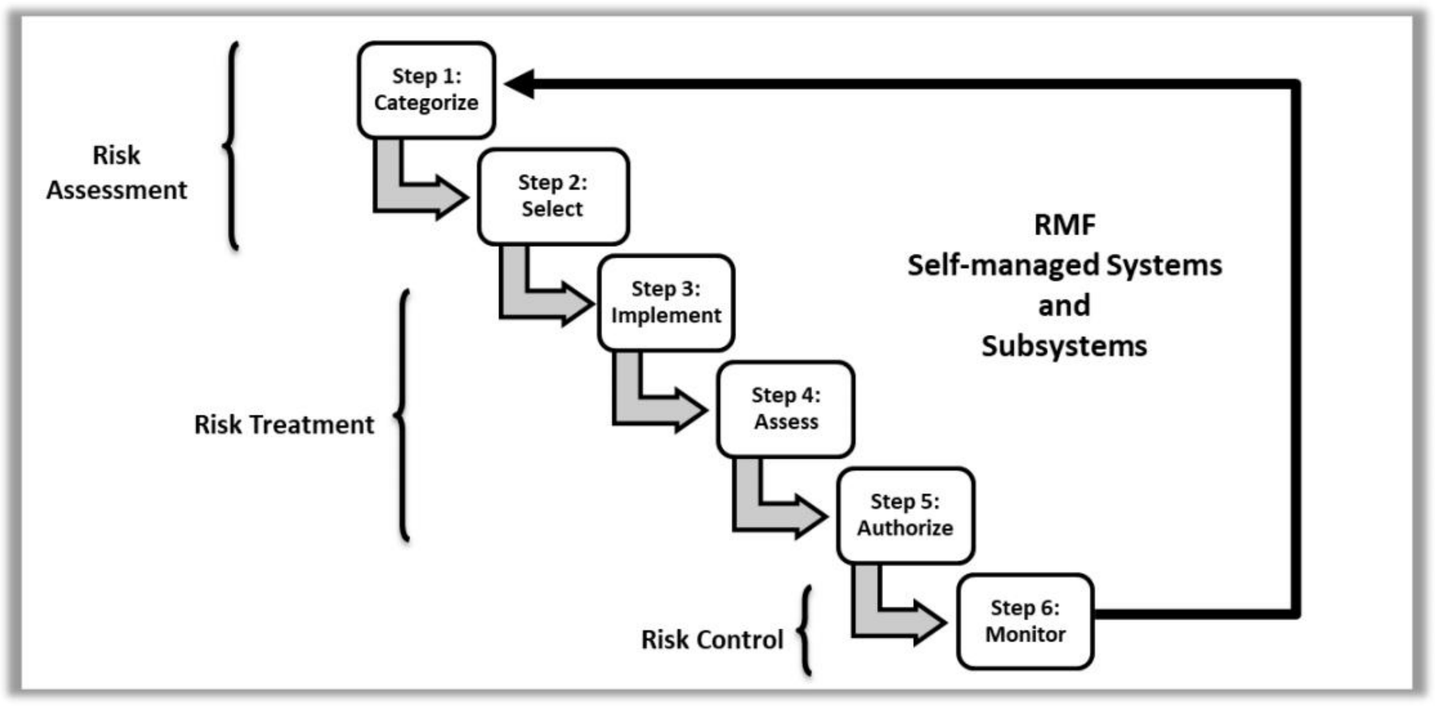


Figure 10.13: Risk Management Factor

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

The above figure shows the NIST SP800-37 Revision 1 RMF, which is used prominently by government institutions and private sector organizations for their information systems. Security requirements must be integrated into the SDLC along with the functional and non-functional requirements. For this purpose, security requirements must be defined and suitable solutions must be researched and created from the beginning of the system's development.

Risk Management Activities and RMF Steps (NIST SP800-37 Rev.1)

- **Risk Assessment:** Risk assessment involves analyzing the cloud environment to detect potential vulnerabilities and defects. Risk assessment includes the following steps.
  - **Categorize**: Perform a system impact analysis to categorize the information system and the information that is processed, stored, and sent by that system. Detect operational, security, performance, and privacy requirements.
  - **Select**: Based on the security categorization, choose an initial set of security controls (known as baseline security controls) for the information system. Then, customize the baseline controls as per the organizational risk assessment and operational environment conditions. Develop a strategy to monitor the effectiveness of security controls continuously. Ensure that all controls are documented in the security plan. Review and approve the plan.
- **Risk Treatment:** Risk treatment involves creating mitigation plans and policies. It includes the following steps.
  - **Implement**: Implement the security controls and define how they can be leveraged inside the information system and its operational environment.
  - **Assess**: Use suitable assessment procedures as described in the assessment plan to assess the security controls. This assessment ascertains if the controls are correctly implemented and whether they are effectively yielding the expected outcomes.
  - **Authorize**: Authorize information system operations based on the identified risk and risk tolerance. The assessment is conducted considering the risk to organizational assets, individuals, organizational operations, and other organizations.
- **Risk Control:** Risk control involves risk monitoring, identifying policy adjustments, and reviewing events. Monitoring is performed as follows in risk control.
  - **Monitor**: Monitor the security controls within the information system on a regular basis. Monitoring includes evaluating the effectiveness of these controls, documenting the changes made to the system or its operational environment, performing system impact analyses for these changes, and reporting the system's security state to the concerned organizational officials.

Ensure that these RMF steps are executed concurrently as part of the SDLC by the designated individuals or groups. The CSP applies the RMF steps to the lower part of the functional stack that is built as part of the services provided, whereas the cloud consumer applies them to the

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

upper part of the stack (upper functional layers) that are built and deployed on top of cloud infrastructure that is offered as a service.

Cloud consumers remain responsible for protecting the data and system when they orchestrate a cloud ecosystem for a cloud-based information system. However, based on the cloud deployment model, the consumers' level of control and direct management differ significantly.

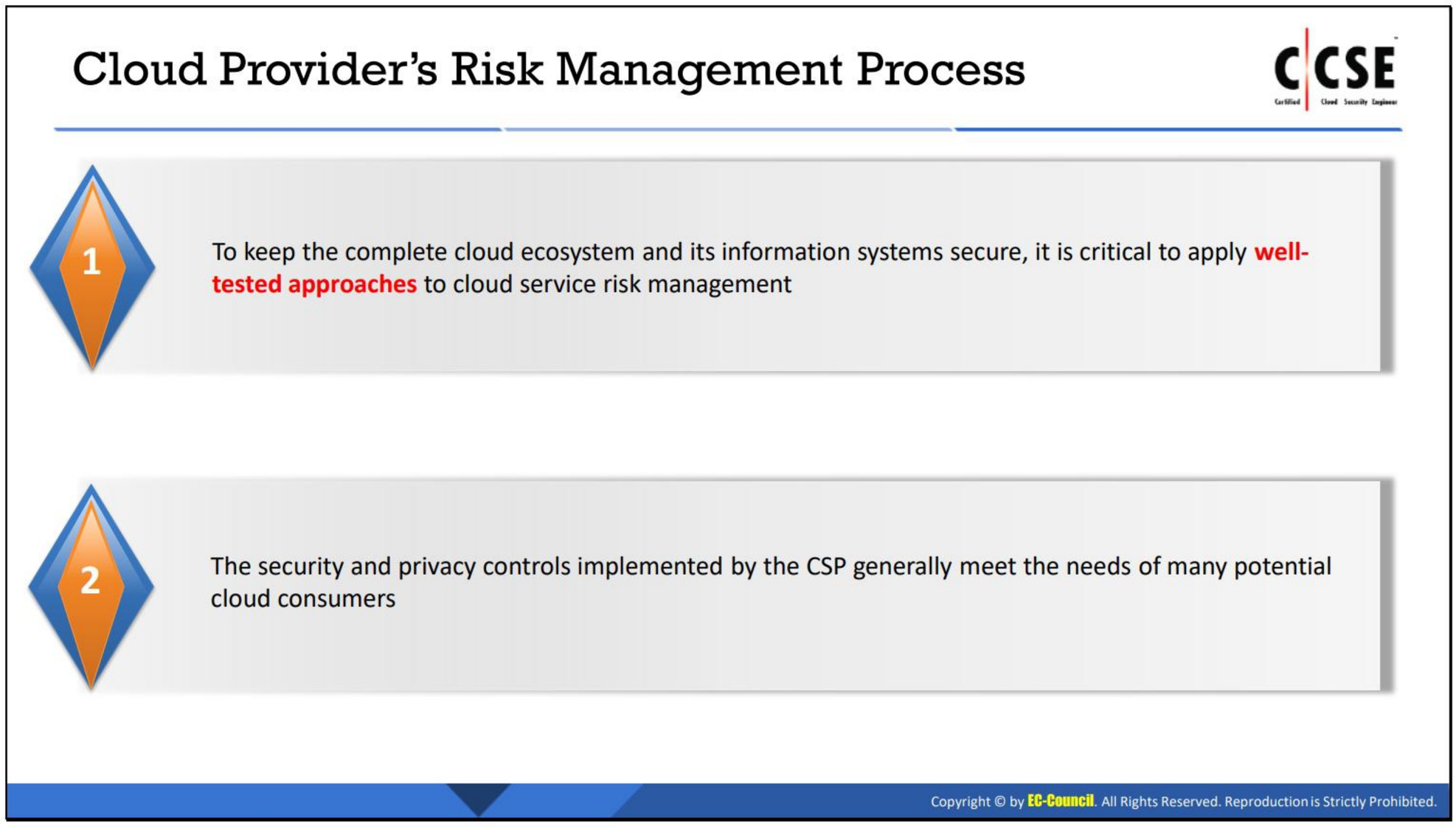
The RMF is applied to different layers of the cloud functional stack. The cloud consumer manages all the layers above the hypervisor for an IaaS cloud. The customer-managed functional stack is decreased proportionally in a PaaS cloud and reduced to a minimum for an SaaS cloud ecosystem.

Before starting a cloud service, a cloud consumer must analyze the risk associated with using a cloud-based solution for a specific information system and prepare for risk treatment and risk control activities. Therefore, the customer must acquire a perspective of the complete cloud ecosystem. Cloud consumers should also use the RMF in a personalized manner to perform the following tasks.

- Conduct a risk assessment.
- Determing the best-fitting cloud architecture.
- Choose the most suitable cloud service.
- Gain the required visibility into the cloud offering.
- Define and negotiate essential risk control and risk treatment mitigations prior to finalizing the SLA and progressing to security authorization.

hadeeb.ir

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



Cloud Provider's Risk Management Process

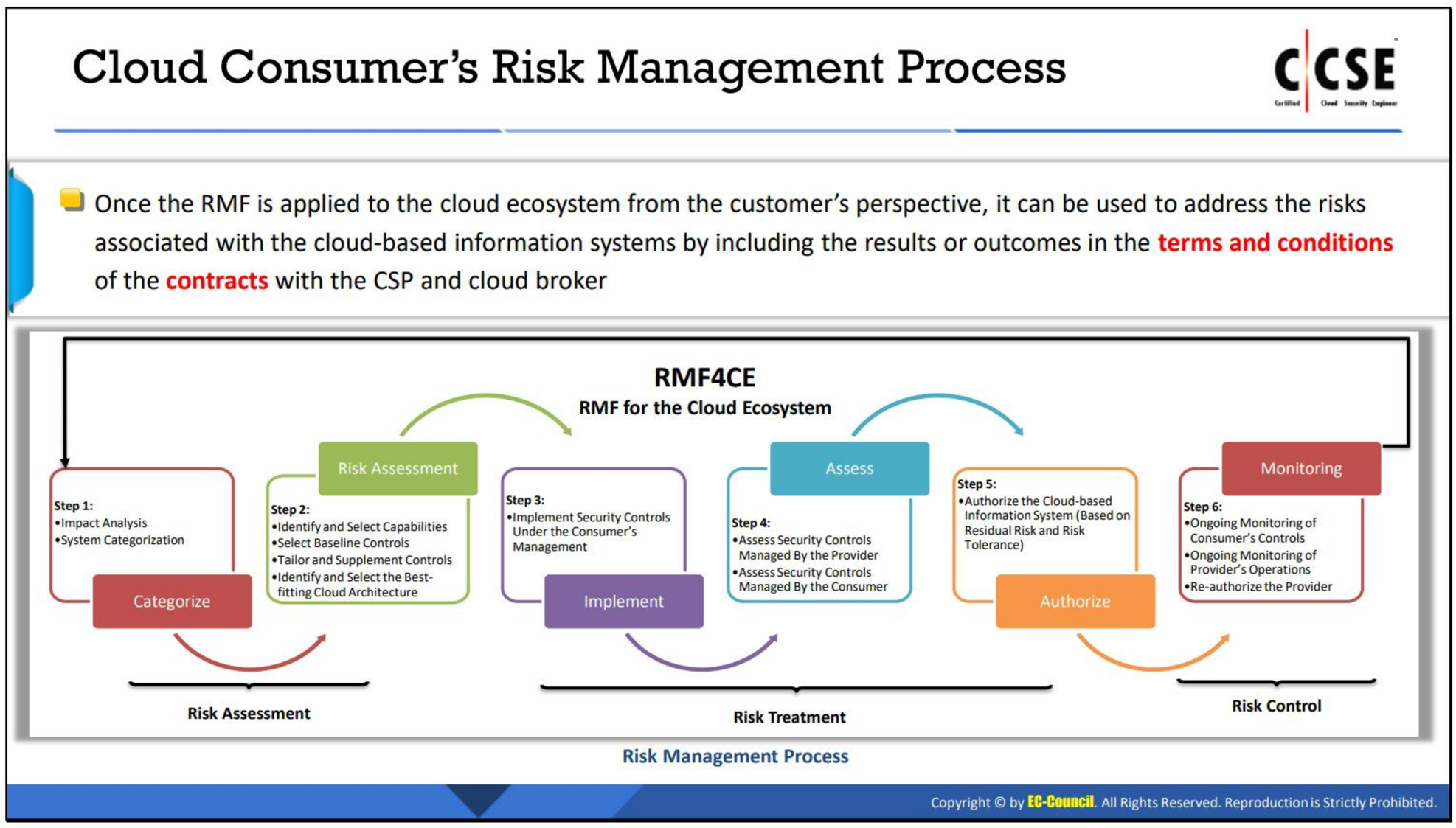
Along with the core functionality, CSPs incorporate operational features such as privacy and security controls that meet baseline requirements while developing cloud architectures and creating cloud services. They aim to meet the needs of numerous cloud consumers in a way that needs minimum customization. The selection and implementation of the security controls is performed by the CSP after considering their efficiency, effectiveness, and constraints based on the applicable policies, laws, directives, standards, or regulations. Specific requirements of cloud consumers are not known to the CSP; therefore, they are outlined as a generic core set.

CSPs can only assume what kind of data their consumers will generate when the system is implemented. The security and privacy controls implemented by the CSP generally meet the needs of many potential cloud consumers. With the help of the centralized nature of the cloud service it provides, the CSP can develop highly specialized, technical security solutions that offer a better security posture than in conventional IT systems.

To keep the complete cloud ecosystem and its information systems secure, it is critical to apply well-tested approaches to cloud service risk management. The CSP can easily apply the RMF to this system because it directly manages and controls the cloud service. The CSP can use the risk management framework (NIST SP800-37) as it is a broadly accepted and well-tested approach.

By applying the RMF, the CSP attempts to compensate for possible weakness in its cloud solutions used by consumers because the reputation and business continuity of the provider heavily depend on the performance and smooth operation of its consumers' solutions.

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



Cloud Consumer's Risk Management Process

The cloud consumer should clearly understand the architectural components for all service types and deployment models, cloud-specific characteristics of the system, and roles of the cloud actor in creating a secure cloud environment. This is essential for the successful adoption of a cloud-based solution. The consumer must also have the ability to do the following:

- Detect all cloud-specific security and privacy controls.
- Take help from the CSP and brokers when needed and via contracts (SLAs and service agreements).
- Evaluate the implementation of the privacy and security controls.
- Monitor the identified security and privacy controls regularly.

As cloud consumers directly manage and control the functional capabilities they implement, they can easily apply the RMF to these functional layers. They face multiple challenges in determining the cloud service offering that can address their cloud requirements effectively while supporting their mission-critical processes, services, and business in an efficient and secure manner. Generally, a cloud consumer who is adopting a cloud-based solution must follow the steps below:

- Define the application or service for which the cloud-based solution will be used.
- Identify functional capabilities that should be used for this service/app.
- Identify the privacy and security requirements and security controls required to secure the service/app.

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

- Analyze and choose the most suitable cloud architecture by combining a cloud service model (SaaS, PaaS, or IaaS) and deployment model (public, hybrid, private, or community):
  - Public SaaS, public IaaS, and public PaaS
  - Private SaaS, private IaaS, and private PaaS
  - Hybrid SaaS, hybrid IaaS, and hybrid PaaS
  - Community SaaS, community IaaS, and community PaaS
- Choose cloud actors that will be involved in orchestrating the cloud environment (e.g., brokers and/or providers).
- Understand the brokers' and CSPs' security posture and their security and privacy controls. Tailor these controls to meet the security and privacy requirements for a specific use case or determine additional compensating controls if necessary.
- Assign certain values to organization-defined security parameters by using selection statements and explicit assignments.
- Supplement security baselines with extra privacy and security control enhancements if required.
- Give any additional specific information for the implementation of these controls.

Application of RMF to a Cloud Ecosystem (Customer's Perspective)

Once the RMF is applied to the cloud ecosystem from the customer's perspective, it can be used to address the risks associated with the cloud-based information systems by including the results or outcomes into the contract's terms and conditions with the CSP and cloud broker. The contractual terms must specify that the customer can access cloud audit logs, user access logs, and continuous monitoring logs.

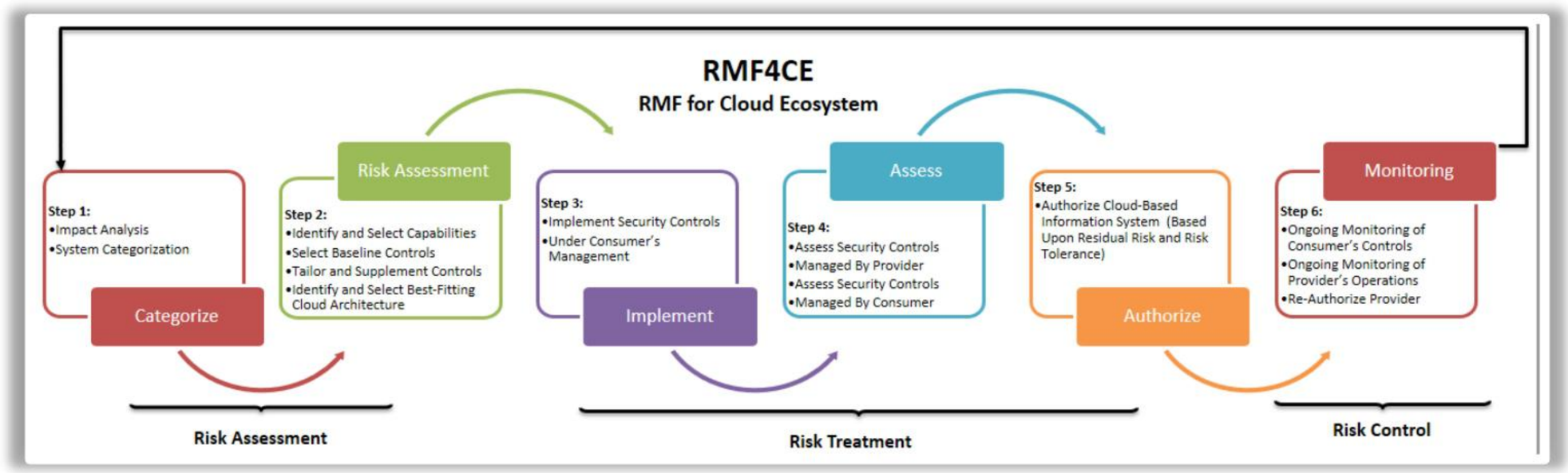


Figure 10.14: Risk Management Process

The above figure shows risk management activities that correspond to the steps in NIST SP800-37 rev.1 from the cloud consumer's perspective.

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

RMF Activities and Steps

The following are the RMF steps and activities that cloud customers must follow.

- **Risk Assessment:** Risk assessment involves analyzing the cloud environment to detect potential vulnerabilities and defects. It comprises the following steps.
  - **Categorize**: Perform a system impact analysis to categorize the information system and the information that is processed, stored, and sent by that system. Detect operational, security, performance, and privacy requirements.
  - **Select**: Selection involves the following activities:
    - Based on the system impact analysis, security control enhancements, and privacy controls, identify and choose the functional capabilities for the information system and the baseline security controls.
    - Determine and select the most suitable cloud architecture for this information system.
    - Select the CSP that best meets the expected architecture and security requirements. Moreover, determine the controls that will be implemented by the provider and consumer as part of the offering as well as the ones that need to be tailored.
    - Review or evaluate CSPs that satisfy the customer's criteria (e.g., controls, architecture, and functional capabilities).
    - Negotiate metrics and SLAs and sign service agreements as part of the procurement process.
    - Ensure that all controls are documented in the security plan. Review and approve the plan.
- **Risk Treatment:** Risk treatment involves creating mitigation plans and policies. It comprises the following steps.
  - **Implement**: Implement the privacy and security controls the customer is responsible for.
  - **Assess**: Assess the implementation of security and privacy controls of the CSP and the customer.
    - Assess the CSP's implementation of the tailored privacy and security controls.
    - Assess the customer's implementation of the controls and detect any dependency and inheritance relationships between the consumer's controls and CSP's controls.
  - **Authorize**: Authorize the cloud-based solution (information system) to work.

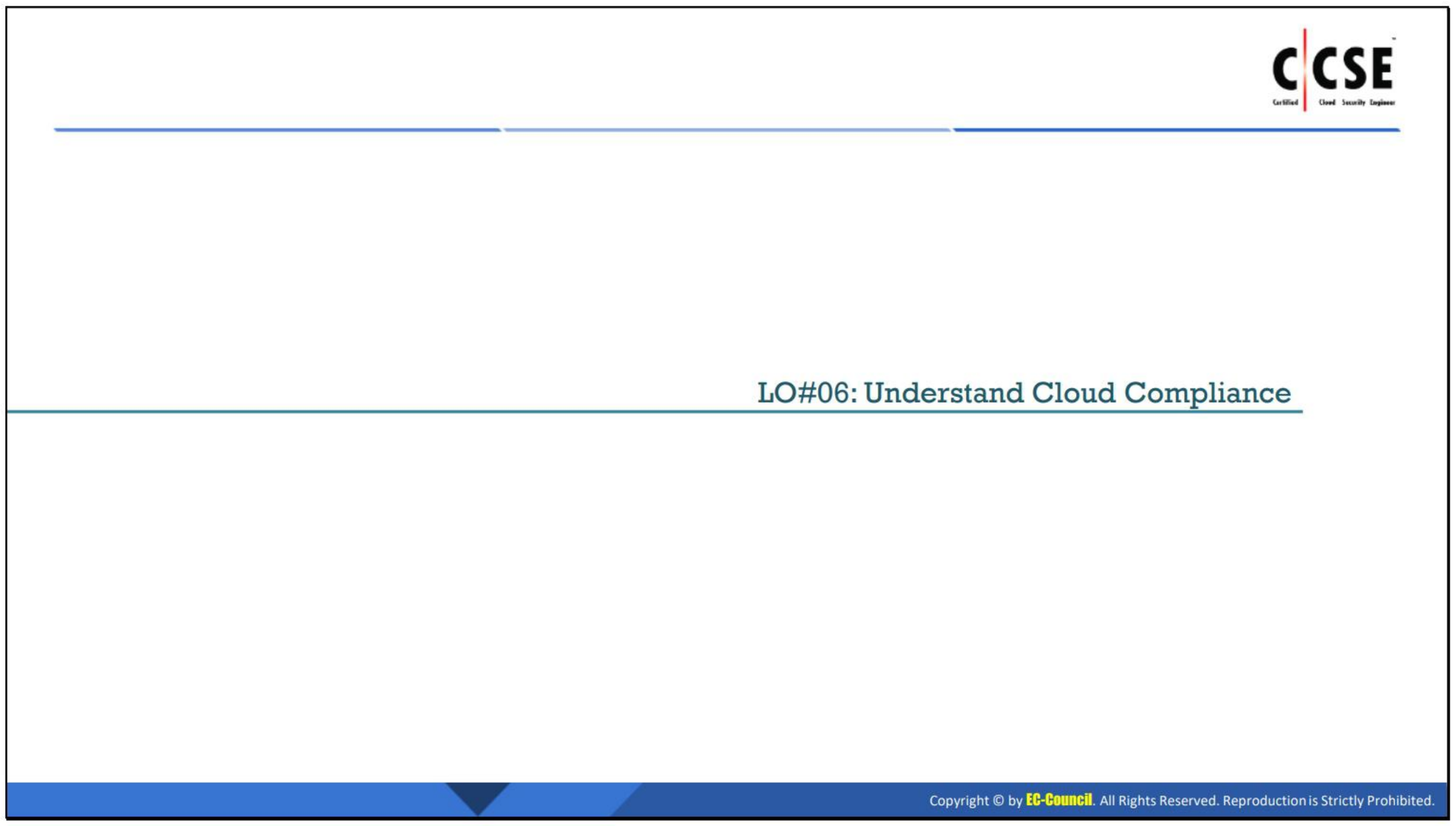
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Risk Control:** Risk control involves risk monitoring, identifying policy adjustments, and reviewing events. Risk control comprises monitoring.
    - **Monitor**: Monitoring involves the following:
        - Continuously monitor operations and the effectiveness of the controls under the management of the customer.
        - Continuously monitor the CSP's operations related to the cloud-based solution and evaluate the system's security posture.
        - Reassess and reauthorize the CSP's service.

The above-mentioned risk management approach enables the organization to systematically detect their hybrid, common, and system-specific security controls as well as other required requirements and highlight these to CSPs, procurement officials, carriers, and brokers.

hide01.ir

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

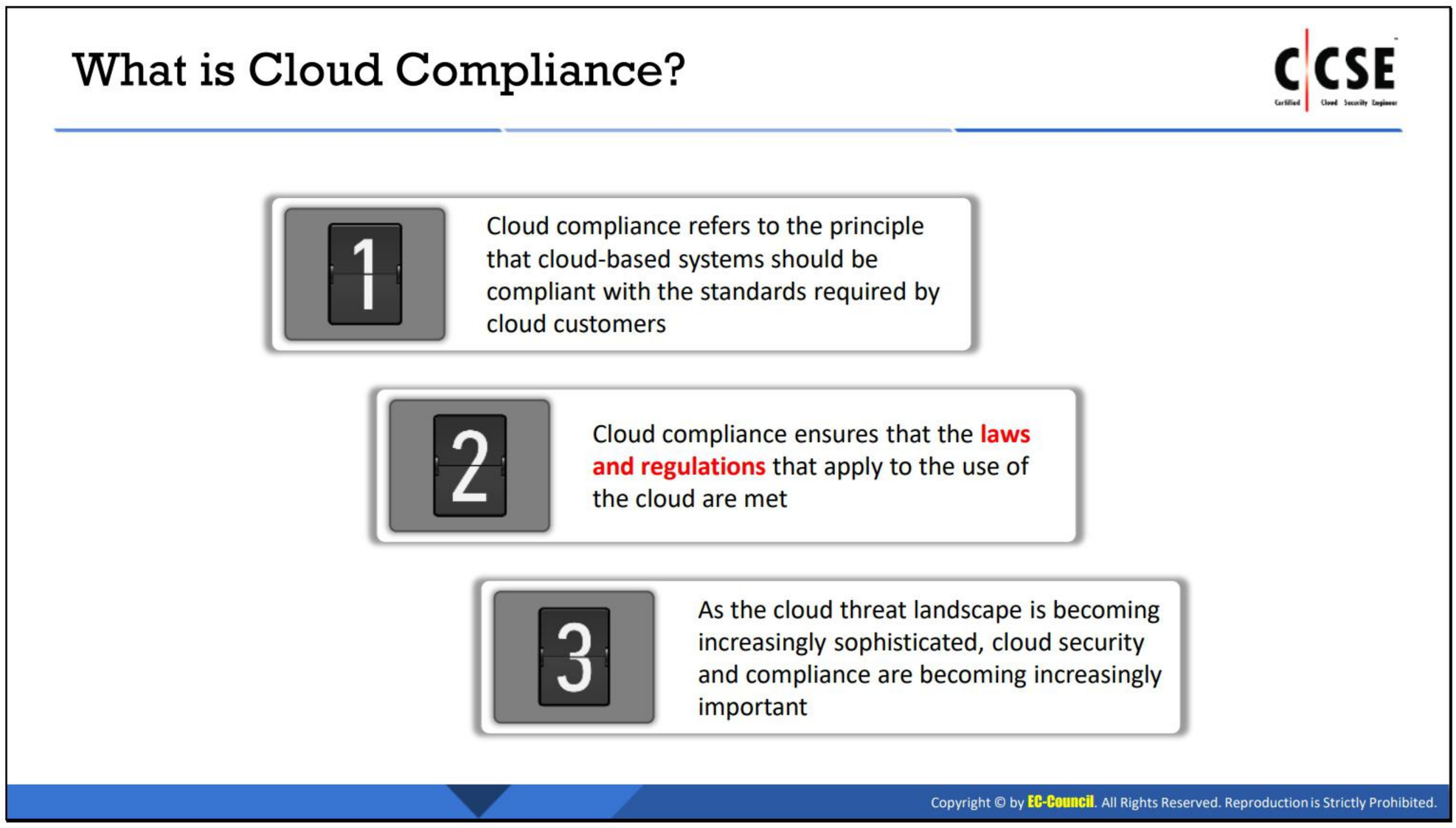


LO#06: Understand Cloud Compliance

This section briefly explains cloud compliance. It highlights the need for and design of a cloud compliance framework to secure a cloud environment from risks and threats and ensure compliance with the help of GRC.

hide01.ir

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



What is Cloud Compliance?

Cloud compliance refers to the process of ensuring that the cloud systems meet the cloud customer's compliance requirements. It ensures that all cloud services satisfy compliance requirements. Organizations are moving to the cloud because cloud computing offers multiple benefits. Cloud service providers (CSPs) store data in various data centers globally, but cloud customers must know where their data will be stored, what laws are applicable to their data, and what impact they will have on the data. Various types of laws apply to data stored in the cloud, such as data localization laws, data protection laws, and data sovereignty laws. Cloud compliance ensures that the laws and regulations that apply to the use of the cloud are met.

Cloud customers must consider various other laws such as access to information laws or inception laws because these laws allow governments or others to access their data stored in the cloud. Additionally, different laws apply to cloud data in different countries; therefore, it is essential to know what security measures are taken or should be taken to ensure that the data are compliant with those laws. Cloud customers must closely evaluate prospective CSPs to determine whether they provide services that meet the compliance they need. They can achieve this by asking CSPs for compliance certifications or by assessing the CSPs' security measures to confirm whether they comply with industry standards and regulations.

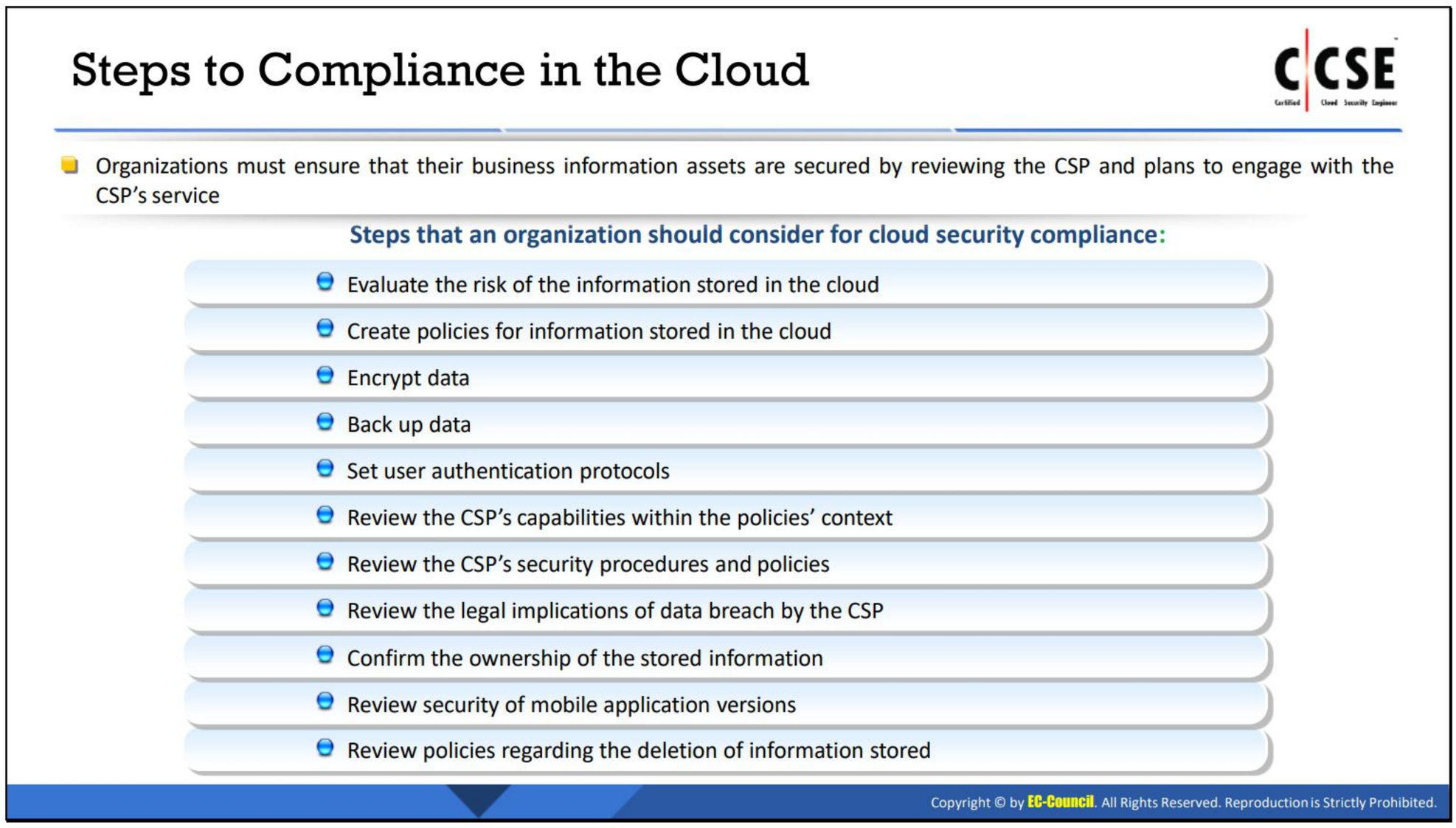
Cloud compliance has evolved with the increase in cloud security adoption. Cloud platforms and services should comply with several federal, state, international, and local security standards, laws, and regulations. If CSPs fail to ensure compliance in their services, they may face various challenges and legal actions (e.g., penalties and fines). Compliance regulations mandate how personally identifiable information (PII), payment card data, protected health information (PHI), and other regulated data can be treated. Examples of regulations are GDPR, HIPAA, Gramm–Leach–Bliley Act (GLBA), and PCI DSS.

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

Because the cloud threat landscape is becoming more sophisticated, cloud security and compliance are more important than ever. Although it is challenging for organizations to meet the different compliance requirements that are applicable to customer data stored in various regions/countries, they cannot ignore or overlook them. CSPs must assure their customers that their data are safe in the cloud by showing them various industry certifications for compliance with prominent industry standards and applicable laws and regulations.

hide01.ir

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



Steps to Compliance in the Cloud

Cloud compliance has become more important than ever because an increasing number of organizations are adopting cloud-based solutions for processing and storing their customers' data. Organizations must ensure that their business information assets are secured by reviewing the CSP and plans to engage with the CSP's service. The following are the steps that an organization should consider for cloud security compliance.

- **Evaluate the Risk of the Information Stored in the Cloud**: The organization must identify the types of information it wants to store in the cloud. As the data are stored remotely, the organization should analyze the consequences of a data breach by asking the relevant questions to the CSP. The organization can use a private cloud for storing risk-sensitive information if there are unacceptable risks associated with a public cloud. However, it can store non-risk-sensitive information on the public cloud. The organization should identify the various types of assets that it can control on a cloud platform while selecting a cloud storage provider. This helps focus on the assets over which the organization does not have much control.
- **Create Policies for Information Stored in the Cloud**: Once the risk of information stored on the cloud is evaluated, the organization must create a cloud security policy for the identified risks. This helps in implementing controls around these risks. The cloud security policy should be kept simple and easy-to-understand for the staff. An example policy contains the goal statement, scope, data classification, responsibilities, and policy. After preparing the policy, the organization can choose a suitable cloud-based application that can help it implement the policy. Before selecting a CSP, the organization must understand what internal controls the provider can offer for the stored information.

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

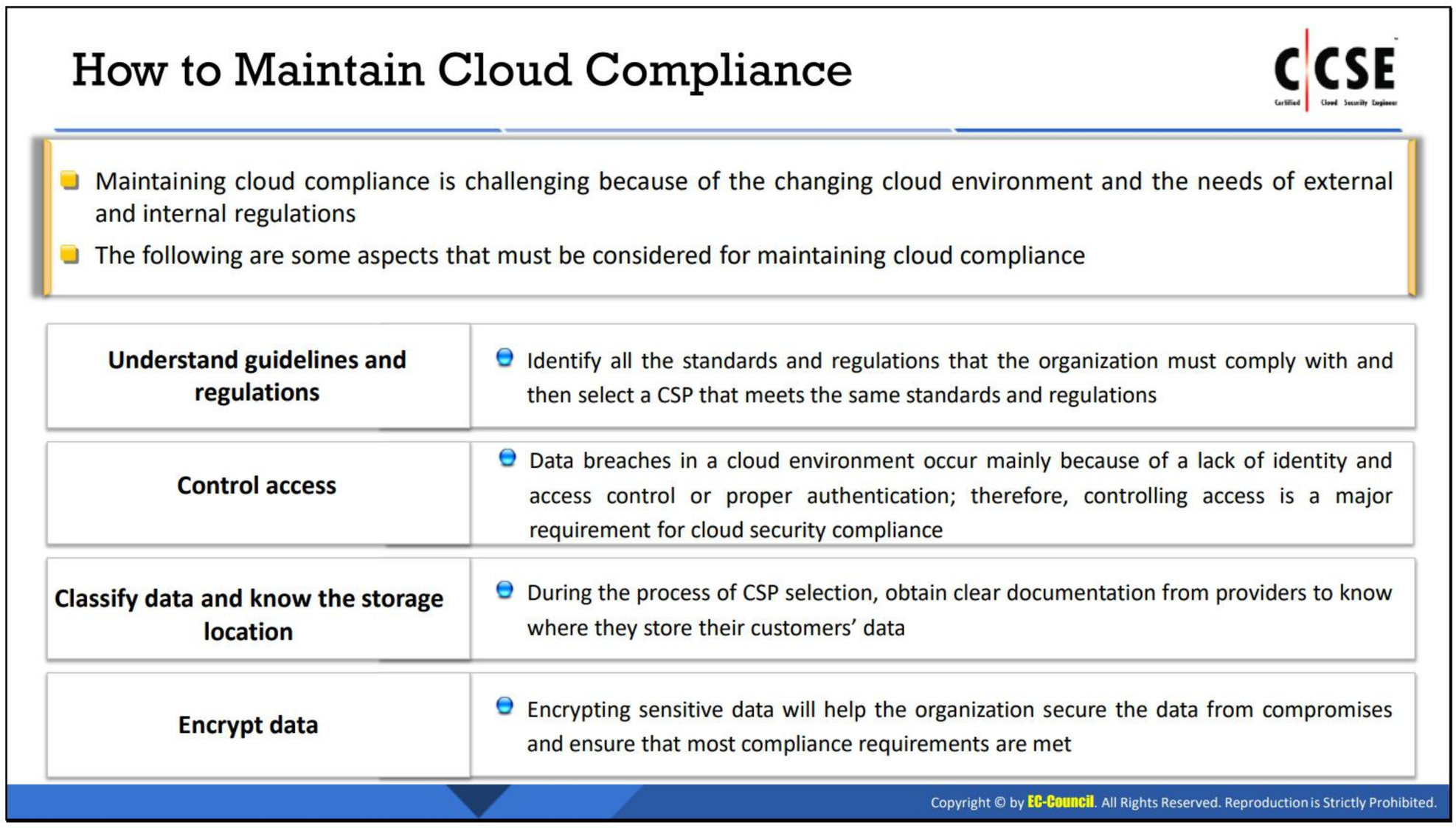
- **Encrypt Data**: The encryption of data is the main protection against cyber threats. Relying completely on the CSP for encrypting data is risky. Although cloud providers offer the "bring your own key" encryption method, it carries the risk of losing keys, which can make the information non-decryptable. The organization should identify the best possible method for securing its information while using the cloud.
- **Back Up Data**: With the help of cloud storage, information can be accessed and managed anywhere instantly. However, controls must be implemented to back up data as part of a good cloud security compliance program. Cloud storage can offer scalability and accessibility only when cloud apps are running. The organization must have a backup of data and BCDR plans for situations where cloud apps face an outage.
- **Set User Authentication Protocols**: Authentication protocols play a crucial role in cloud compliance. Based on the information needs, the organization should identify the appropriate authentication protocol. Understand the protocols used by the CSP before reviewing a prospective CSP. The organization can use mutual authentication protocols for authentication, which require the CSP and the organization to prove their identities to one another for authentication. The following authentication protocols can be used as per the organization's requirements.
  - **Secret Sharing**: This protocol requires both parties (the CSP and cloud customer) to share the information necessary to complete authentication. It can protect against DoS, replay, and MITM attacks.
  - **Smart Cards and Passwords**: This method requires the user to have a card and a password to gain access to the server. It can protect against offline guessing attacks.
  - **Elliptic Curve Cryptography**: This method involves the initialization phase, user-registration phase, and phase of mutual authentication with key agreement. It can protect against outside attacks, insider attacks, impersonation attacks, and attacks on mutual authentication.
  - **Steganography**: This method or protocol embeds encrypted information into a data piece or an image to hide it from third parties. This helps in preventing malicious users from accessing secrets.
- **Review the CSP's Capabilities Within the Policies' Context**: The organization should understand the various types of capabilities provided by the CSP to be able to choose the appropriate types of capabilities it requires. As the cloud services are subscription-based, the organization is charged depending on the plan for using them and the number of people with access to them. CSPs offer mainly three types of services: SaaS, IaaS, and PaaS. Based on the cloud security policy and risk assessment, the organization must choose the appropraite product/service after reviewing their cloud service requirements.
- **Review the CSP's Security Procedures and Policies**: The organization should look for CSPs that conform to the ISO/IEC 27001 and 27002 standards, which are not cloud-

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

specific but applicable to cloud computing. While selecting a CSP, ensure that it is ISO/IEC 27017 certified. Furthermore, the CSP must be ISO/IEC 27018 certified if it processes and stores personally identifiable information. In addition, the organization must review policies and processes that affect security, such as the privileged access policy, log retention policy, and change management process, while choosing a CSP.

- **Review Legal Implications of Data Breach By the CSP**: The data security and privacy laws that are involved in cloud compliance reviews include security issues, breach notifications, and forced information disclosure to government authorities. Review closely the contract signed with the CSP to understand the division of legal responsibilities. Some CSPs do not provide transparency into their security programs, which makes it difficult for a cloud customer to know if they comply with the federal regulations and statutes. Therefore, it is essential for the organization to clearly understand the contract terms and the liability section of the contract while selecting a CSP.
- **Confirm the Ownership of the Stored Information**: The cloud service contract explicitly defines the ownership of data stored in the cloud. When stakeholders have access to the stored data, the ownership of cloud data becomes confusing. The contract document must be reviewed in detail because the language used in the contract is usually standardized. This will ensure the security of the organization and its data.
- **Review the Security of Mobile Application Versions**: Cloud services are widely used because of their information and access portability. Employees use applications to access cloud services irrespective of their locations. This necessitates a compliance review for mobile apps. Although the Open Web Application Security Project (OWASP) is working on a comprehensive testing guide and security standard, no security standard currently exists for mobile apps. OWASP provides a mobile application security checklist that can help with the review process. The security impact of the CSP's mobile application can be determined using these resources.
- **Review Policies Regarding the Deletion of Information Stored**: Cloud compliance requires reviewing the processes and policies related to the deletion of information stored in the cloud. The deletion of information stored in the cloud comes under the purview of the data retention policy implemented by the CSP. Data encryption can cause some issues with data deletion. It may be difficult to trace data deletion if encryption is implemented. Some CSPs provide a solution to this issue by deleting the encryption keys after deleting the encrypted data. If the encryption keys are deleted, the encrypted data will be unreadable, even if the data remain in the cloud.

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



How to Maintain Cloud Compliance

Maintaining cloud compliance is challenging because of the changing cloud environment and the needs of external and internal regulations. Despite various challenges, organizations using the cloud need to maintain cloud compliance. The following are some aspects to be considered for maintaining cloud compliance.

hidan1.ir

- **Understand Guidelines and Regulations**: An organization using the cloud should comply with several industry standards and regulations. These regulations include local, national, and international standards that need to be followed. The organization must appoint a dedicated expert team to ensure continuous compliance. It must identify all the standards and regulations that it should comply with and then select a CSP that meets these standards and regulations. The following are some common regulatory requirements.
  - **HIPAA**: This standard is a collection of healthcare laws that provide security protocols and guidelines for storing patient health data and confidential information. This law is applicable to healthcare providers such as hospitals, doctors, and health insurance companies.
  - **PCI DSS**: This standard applies to companies that handle and process payment card information (e.g., credit card information). It ensures that the financial information of customers is secure.
  - **GLBA**: This standard offers guidelines to financial institutions regarding the protection of customers' confidential information. It states that financial institutions must update their customers on how their data are stored and protected.
- **Control Access**: Controlling access is a major requirement for cloud security compliance. Data breaches occur in cloud environments mainly because of a lack of identity and access

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

control or proper authentication. The organization should ensure that multi-factor authentication (MFA) is implemented in its cloud environment to prevent multiple security threats. Single sign-on is convenient to use but increases the risk of getting hacked. Similarly, a single username and password can be stolen or guessed easily if users use poor passwords. With MFA, users need to use their login credentials along with another type of authentication (e.g., a verification code sent to their email or mobile phone). This increases security and prevents any unauthorized user from gaining access to the cloud environment.

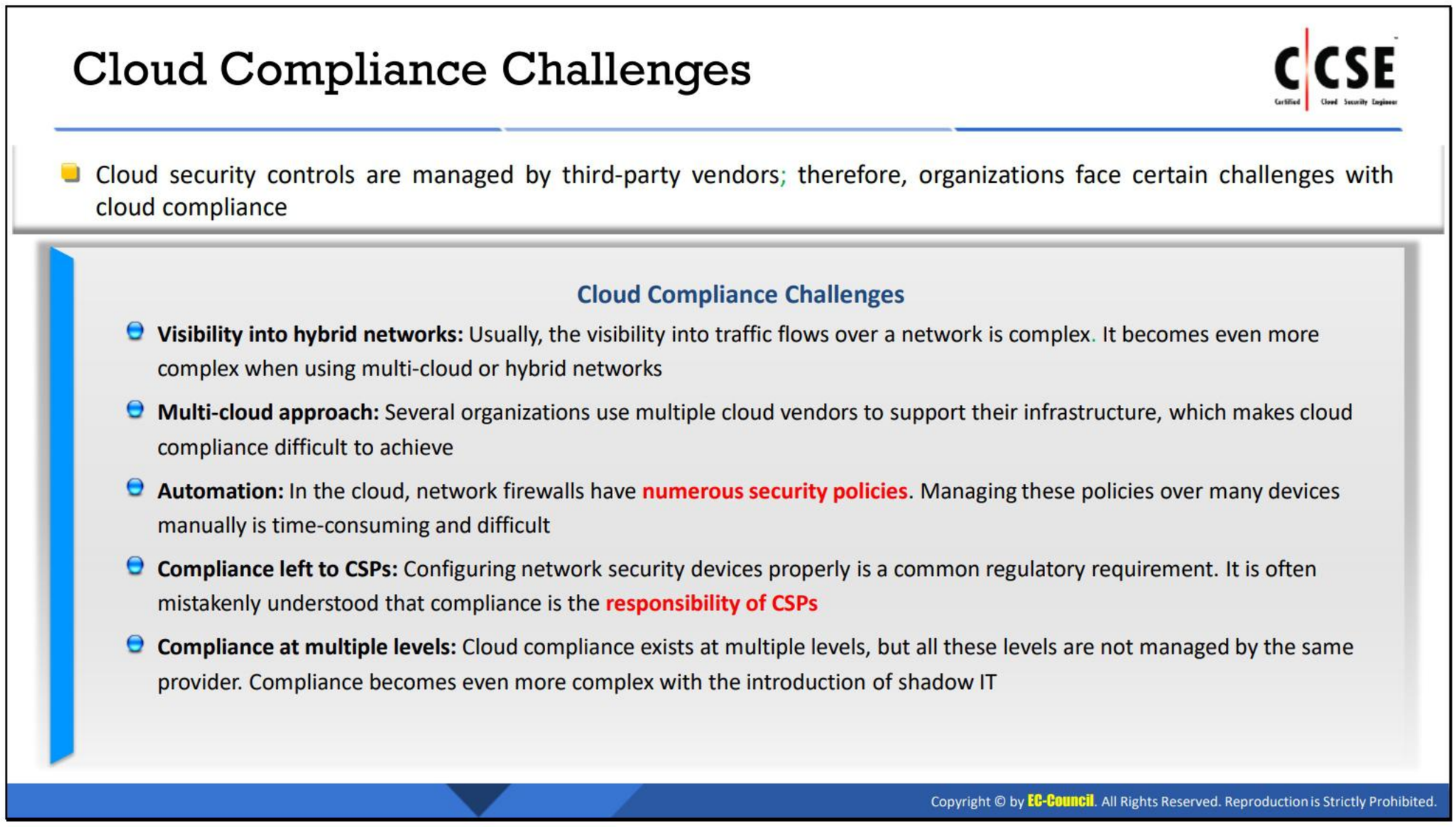
- **Classify Data and Know the Storage Location**: Knowing where the organization's data are stored (data location) is essential to maintain compliance. While auditing, the organization must show where its data are stored and what measures are implemented for its security. During the process of CSP selection, the organization should obtain clear documentation from CSPs to know where they store their customers' data. Most industry standards and regulations demand the storage of data in servers located in the US. After choosing a suitable CSP, the organization should classify the data to be moved to the cloud. Highly confidential data should be stored in a private cloud or the internal network as it is risky to store such data in the public cloud.
- **Encrypt Data**: Once the organization classifies the data to be moved to the cloud (including sensitive data), the data must be encrypted. Encrypting sensitive data will help in not only securing the data from compromise but also meeting most compliance requirements. The organization should use encryption services provided by the CSP as well as any other useful third-party software that offers encryption. The organization is responsible for protecting data in transit and at rest. Industry-standard protocols such as HTTPS should be used to secure data in transit.

  Most data breaches occur because of insider attacks, which are performed by internal employees. Encrypt all data between internal servers to add an extra layer of protection against malicious employees or those who accidentally access confidential files. CSPs allow setting up virtual networks to control access and secure the data within them. All traffic flowing between VMs inside a virtual network is encrypted. The organization can use the following to prevent insider threats.

  - Identity governance
  - Identity management
  - Security intelligence
  - Access management and risk authentication

hidden1.ir

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

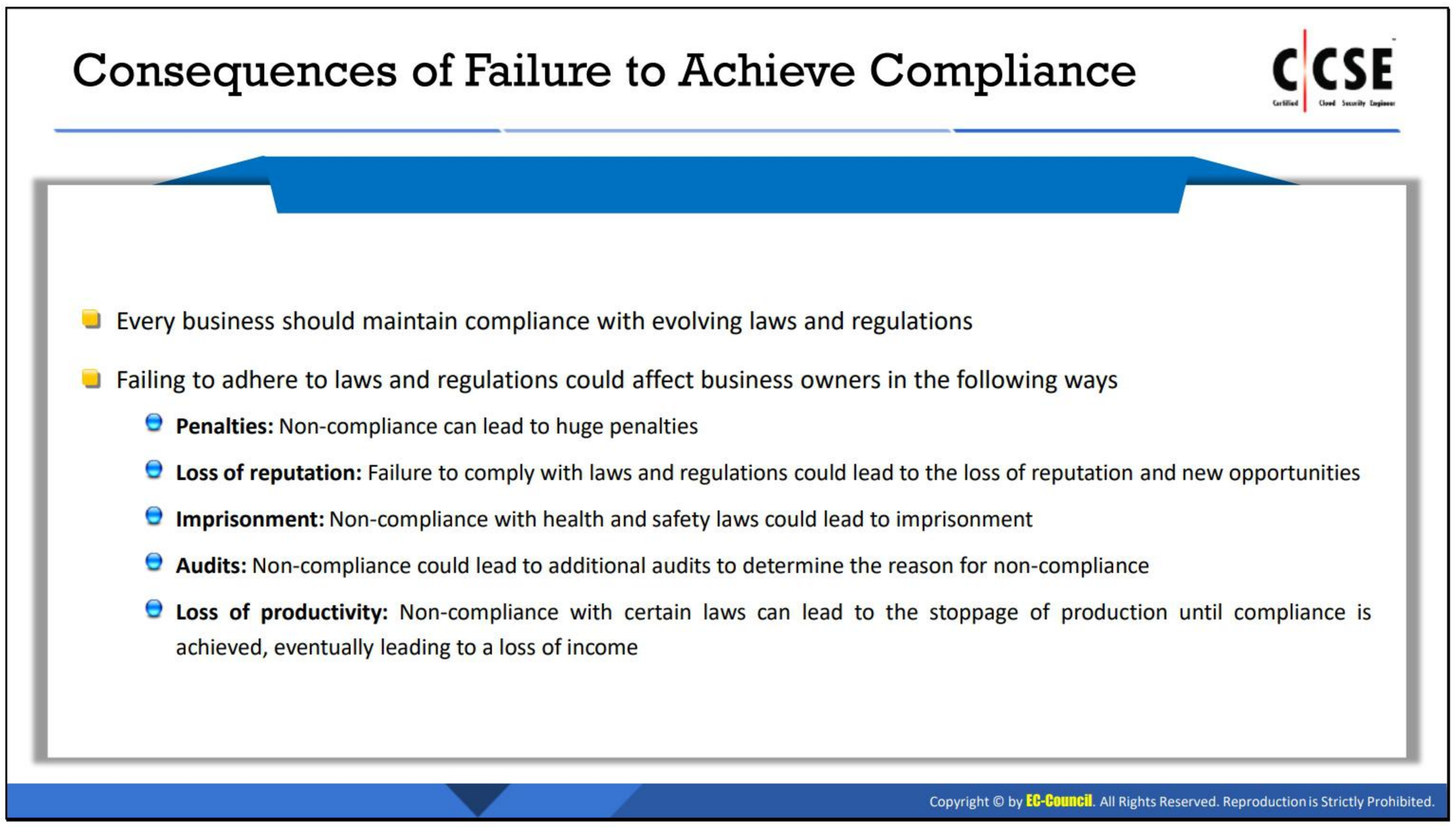


Cloud Compliance Challenges

Cloud security controls are managed by third-party vendors. Therefore, organizations face certain challenges with cloud compliance. These challenges include the following.

- **Visibility into Hybrid Networks**: Usually, the visibility into traffic flows over a network is complex. It becomes even more complex when using multi-cloud or hybrid networks. However, it is difficult to manage firewall policies without proper visibility into the traffic that flows across the entire network.
- **Multi-cloud Approach**: Many enterprises adopt multiple cloud service providers (CSPs) for their infrastructure. This makes cloud compliance difficult to achieve.
- **Automation**: In the cloud, network firewalls have numerous security policies. Managing these policies over many devices manually is time-consuming and difficult.
- **Compliance Left to Csps**: Configuring network security devices properly is a common regulatory requirement. However, in a cloud environment, it is often mistakenly understood that compliance is the responsibility of CSPs.
- **Compliance At Multiple Levels**: Cloud compliance exists at multiple levels, but all these levels are not managed by the same provider. Compliance becomes even more complex with the introduction of shadow IT. Many large industries have specific rules and regulations regarding cloud compliance, apart from the standard CSP compliance requirements to be followed by organizations using the cloud.

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



Consequences of Failure to Achieve Compliance

In recent years, adhering to laws and reviewing the compliance of business processes has become a concern for organization owners. Reviewing compliance involves identifying compliance violations. Every business must maintain compliance with evolving regulations. When an organization fails to adhere to laws and regulations, it faces serious consequences.

Achieving compliance is not an easy task, as regulatory bodies are implementing an increasing number of regulations. Monitoring the compliance of business processes with rules and regulations has become a major concern for every business. Organizations should keep monitoring compliance and stay up to date with regulations.

Non-compliance affects business owners in the following ways.

- **Penalties:** Non-compliance can lead to huge penalties. The penalties for large organizations could cancel out their profits. On the other hand, penalties may affect small businesses so severely that it can lead to business shut down. Apart from penalties, lawsuits and settlements can cost millions of dollars.
- **Damage to Reputation:** Any business that fails to achieve compliance with laws and regulations may face the risk of reputation loss. Based on the severity of non-compliance, it can seriously damage the business value and reputation. It could also lead to the loss of new opportunities. The damage caused to the organization's reputation could also last for a long time. Hence, the company should take proper measures to address compliance issues.
- **Imprisonment:** Non-compliance with health and safety laws could lead to imprisonment from months to years. Both employers and employees can be prosecuted for non-compliance.

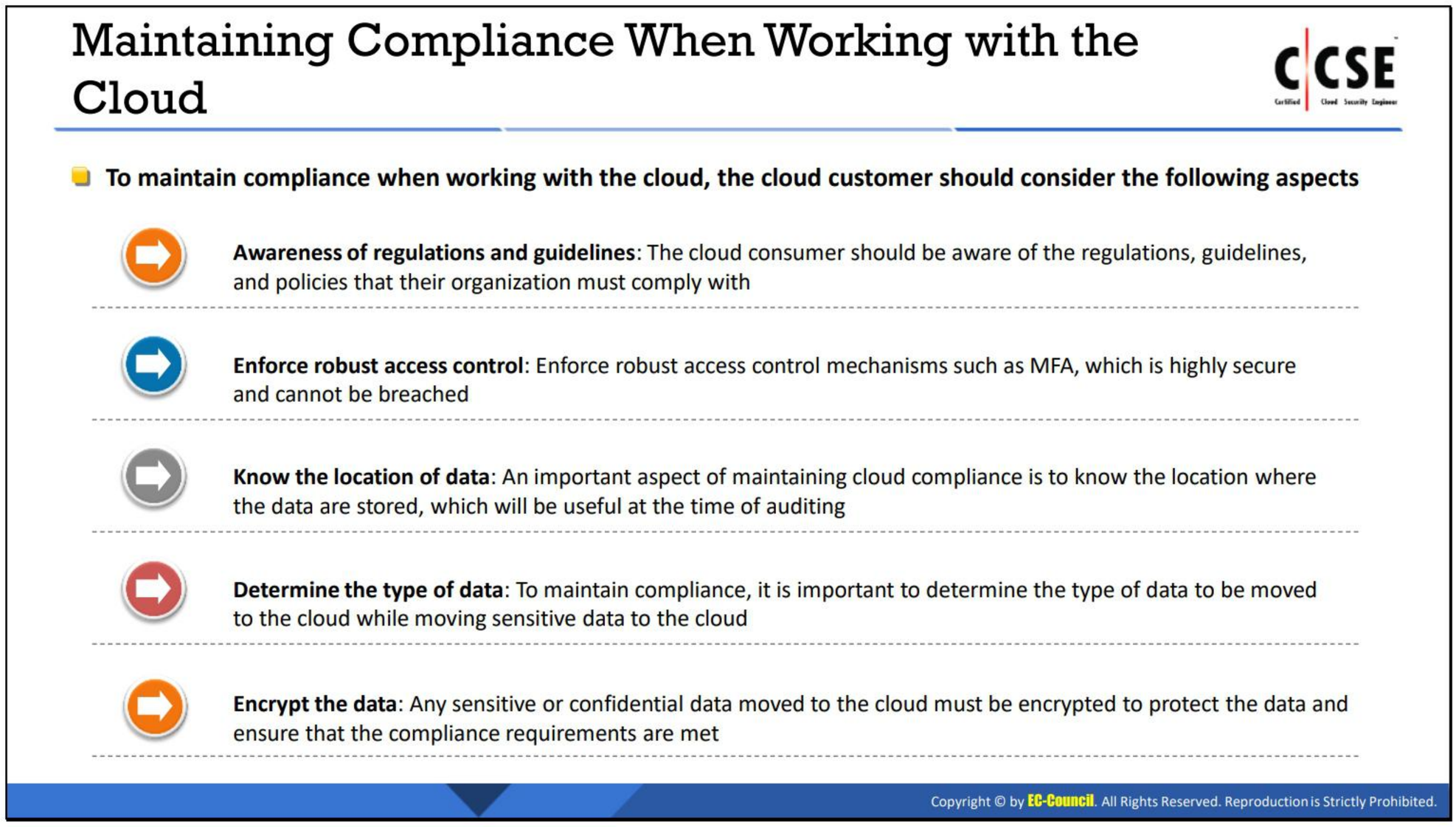
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Audits:** Non-compliance with laws and regulations could lead to additional audits, which are meant for understanding the reason for non-compliance. Additional audits are time-consuming and require extra effort.
- **Loss of Productivity:** Failing to achieve compliance with laws is considered illegal, and governing bodies could take serious actions. Non-compliance with certain laws can lead to the stoppage of production until compliance is achieved. The resulting loss of productivity eventually leads to a loss of income. In case of serious non-compliance issues, governance authorities may order companies to shut down.

Regulatory compliance is not a small matter. Achieving compliance with different compliance regimes can become difficult if no method is implemented to monitor the compliance at the business level. Therefore, using a smart method of running the business, the performance can be monitored using graphs, responsibilities can be assigned, and automated reports can be obtained.

hide01.ir

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



Maintaining Compliance When Working with the Cloud

Any business that works with sensitive data must manage and handle the data properly to comply with mandatory regulations. When a company adopts new technologies such as the cloud, it should ensure continued compliance with regulations.

Achieving compliance in the cloud is a major concern for many organizations. Both the cloud service provider (CSP) and the enterprise are responsible for maintaining compliance in the cloud. A clear understanding of how to achieve cloud compliance can help businesses operate in an ever-changing regulatory cloud environment. The CSPs can also help their customers achieve compliance in the cloud.

As the national and industry regulations for storing data in the cloud keep changing and updating, it is difficult to achieve compliance in the cloud. To maintain compliance when working with the cloud, the cloud customer should consider the following aspects.

Awareness of Regulations and Guidelines: A cloud user must comply with several industry standards and regulations. These regulations include local, national, and international standards that should be followed, which is cumbersome even for an intelligent employee. All CSPs are equipped to deal with different types of regulations and policies. They also have a team of experts that work extensively to ensure compliance. This is helpful for cloud customers as they can gain access to compliance infrastructure and make their team handle audits. Cloud customers can also download audit reports to demonstrate compliance.

The organization should be aware of the regulations and policies that the company should comply with. Each type of cloud infrastructure is developed on a different architecture and offers different services. A certain type of cloud infrastructure may not be designed to comply with certain regulations. The organization should find a CSP that offers the same business

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

compliance requirements. The CSP should provide documentation regarding how it meets compliance in the cloud. This information can be included in service-level agreement (SLA) or their website. The most common regulations include HIPAA, PCI, DSS, and GLBA.

Determine the Type of Data: After deciding on the type of cloud service required, it is important to determine the type of data to be moved to the cloud. While moving sensitive data to the cloud, cloud users must ensure that they maintain compliance. Owing to security and compliance regulations, the organization may decide to keep sensitive and confidential data in their internal network. If such data are moved to the cloud, the organization may maintain the data in an on-premises-hosted private cloud. The enterprise have to access logical infrastructure and physical infrastructure although it depends on cloud computing.

Enforce Robust Access Control: Improper authentication or identity and access control can be a source of data breaches for an organization. Although single sign-on is convenient and easy, it increases the risk of data breaches. Even a single password and username can be easily stolen.

Many companies consider multi-factor authentication (MFA) as a complex and time-consuming system, but it offers the best ways to prevent security threats. MFA is highly secure and cannot be breached. With MFA, users require not only a username and password but also a secondary authentication token such as a verification code sent to their mobile phone or email. The necessity of this extra step that can be performed only by an approved employee reduces data breaches.

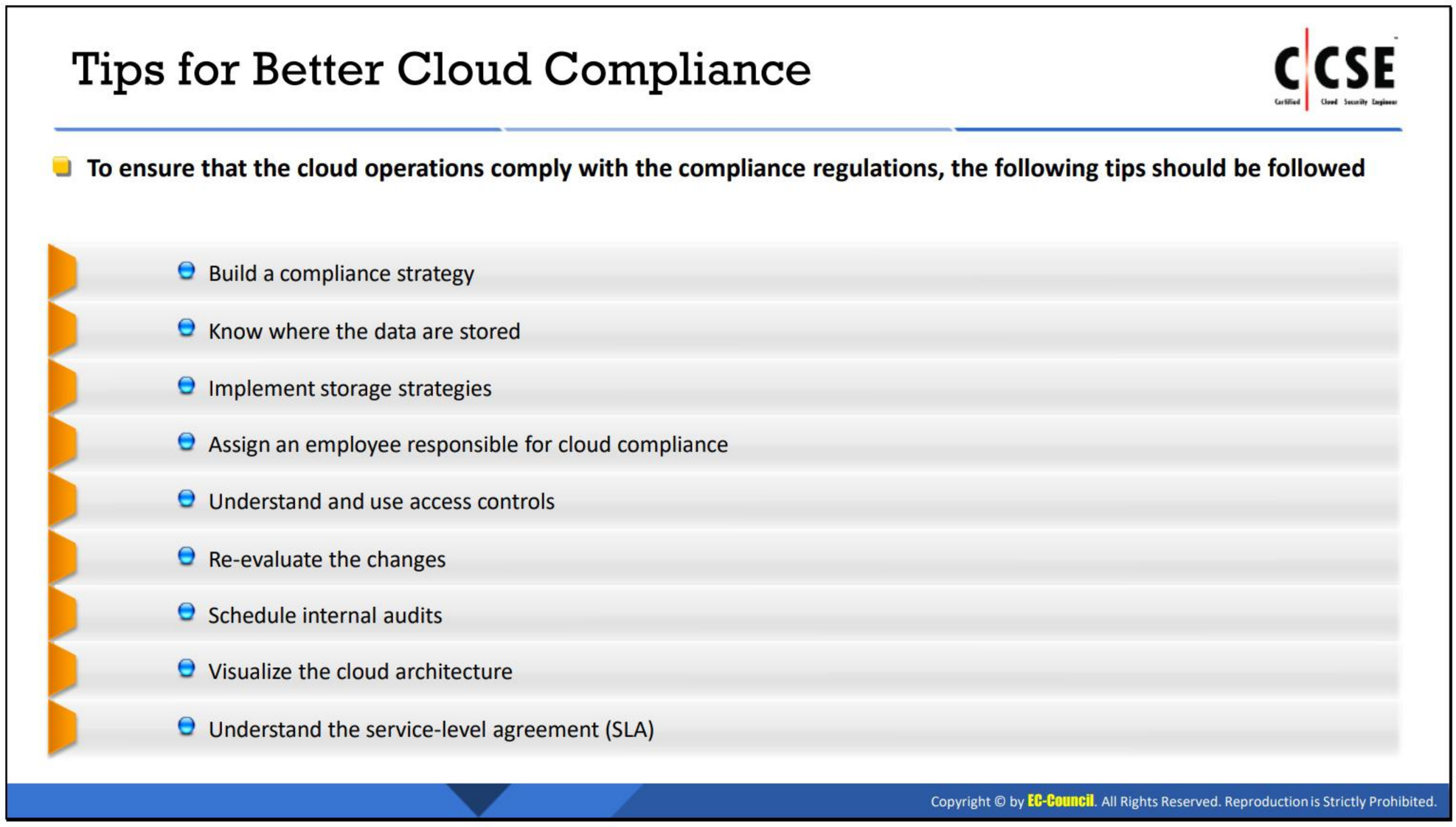
Know the Location of Data: An important aspect of maintaining cloud compliance is to know the location the stored data. When an audit needs to be performed, cloud customers must prove that the location of data is safe and secure by specifying the security standards that are implemented to protect the data. While researching CSPs, cloud customers must obtain documentation about the location of their servers.

Encrypt the Data: Although cloud data regulations do not strictly mandate data encryption, data encryption in the cloud is still essential for businesses. Any sensitive or confidential data moved to the cloud must be encrypted. Encrypting the data not only protects the data but also helps in meeting most compliance requirements. Most CSPs offer tools for encrypting data at rest as well as inbound and outbound traffic. Cloud customers can use those tools if they match the encryption requirements for data compliance.

Although CSPs offer encryption methods, the customers are responsible for protecting their data. Most data breaches are caused by insiders from the organization. The company should encrypt all the data between internal servers behind a firewall to protect against employees who are attempting to steal data. Cloud security providers use virtual networks, which cannot be accessed by anyone. It also ensures that the traffic between machines in the cloud is encrypted. The best method is to encrypt the data locally before moving the data to the cloud.

Irrespective of whether the organization uses a public or private cloud, certain guidelines should be met to ensure cloud compliance. Irrespective of the CSP the cloud user chooses, the data moved to the cloud must meet all the compliance guidelines and regulations.

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



Tips for Better Cloud Compliance

Cloud computing is an efficient method for improving the speed of infrastructure deployment. Hence, many organizations have started migrating to the cloud. This rapid migration has increased the need for greater data security regulations. The effect of data privacy compliance regulations on a company depends the industry in which it operates.

The range of compliance regulations is based on the organization's industry, location, and business function. It is important to understand how the applicable regulations affect data storage, password policies, data retention policies, etc.

To ensure that the cloud operations are compliant with the compliance regulations, the following tips should be followed.

Build a Compliant Strategy

Based on the business regulations, choose a CSP that is certified with the required business regulations. It is important to understand that using a compliant provider will not make the business fully compliant. It is essential to implement an independent compliance strategy. Many companies have the misconception that they are completely covered by what the CSP provides, and they fail to verify coverage; however, verification should be a part of the internal compliance method.

The customers should use the cloud service in alignment with compliance. The cloud users are responsible for ensuring that the CSP provides regulatory controls on a regular basis. The cloud users are also responsible for maintaining compliance with their own IT operations that connect to the CSP.

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

Know Where the Data are Stored

Some compliance regulations restrict the storage and processing of some data types to certain geographical locations. This could lead to additional challenges if the CSP stores the data across the world, but most CSPs are aware of these restrictions. CSPs allow customers to choose the geographical nodes for storing their data.

Implement Storage Strategies

By using dedicated storage solutions, the business can keep its data in a distinct cloud and differentiate their cloud from the hardware that holds other organizations' data. With such separation, the scope of regulation may be limited. Without any separation, it would be difficult to prove that the data are secure. Although the CSP separates the data, the cloud users must include such separation in the SLA.

Assign an Employee to Cloud Compliance

In the absence of a person in charge of handling cloud compliance, compliance tasks will be performed by employees who might have other cloud-related responsibilities. Without a compliance officer, it is not possible to achieve compliance. A compliance officer should be appointed to ensure that the compliance program is active. The officer is also responsible for reminding employees about the internal controls and regulatory expectations, negotiating and reviewing SLAs, and advising during architecture review.

Understand and Use Access Controls

hlo01.ir

Access controls are key for maintaining compliance, and it is essential to implement the proper controls. There should be strict policies about who can access, record, and use data. The controls should not allow anyone to collect or use data for unauthorized purposes.

During a compliance audit, it is necessary to prove that users have different levels of access to data. Furthermore, it is necessary to prove how those levels are maintained. The CSP should provide documentation mentioning how duties are separated for administrative functions.

Re-evaluate the Changes

After migrating to the cloud, the compliance should be checked again, as complying with some standards in the past does not guarantee that newly migrated data are automatically in compliance. Compliance officers are responsible for creating a compliance schedule.

Schedule Internal Audits

The compliance should be re-examined on a regular basis to ensure that regulatory requirements are met. Furthermore, the regulatory requirements themselves should be reviewed on a regular basis. Internal audits should be scheduled to conduct regular reviews of regulatory requirements. The frequency of such audits depends on the industry, applicable cloud regulations, and types of data used. The internal audit should be more stringent than the industry standard. Although such audits seem time-consuming, they save a lot of trouble in the future.

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

Visualize the Cloud Architecture

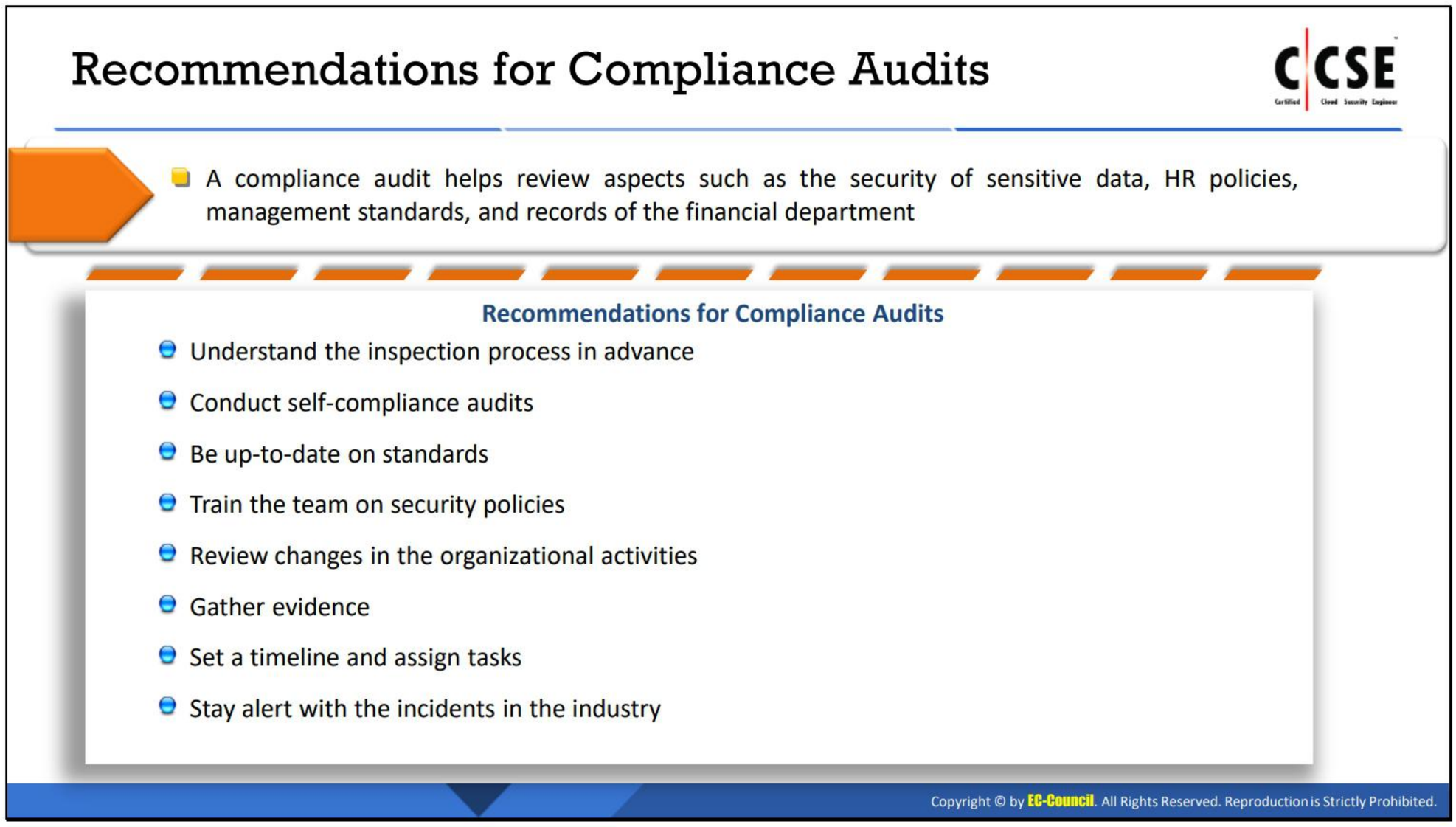
By examining the cloud architecture, the cloud users can understand how different parts of the architecture work together. Without a proper cloud architecture diagram, the decision-making relies on guesswork, which could cause serious issues.

Understand the Service-level Agreement (SLA)

Irrespective of the compliance regulations that apply to the organization, the cloud users should not assume that the CSP's terms and conditions alone will satisfy the requirements. The cloud users must know the details of the cloud services contract. The cloud users, rather than the CSP, have the sole responsibility for compliance. The SLA should define roles and responsibilities, data breach remediation, and the execution of incidence response. Every clause in the SLA should be aligned with the regulations governing the business.

hide01.ir

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



Recommendations for Compliance Audits

A compliance audit is an evaluation process conducted to ensure that an organization adheres to the external laws, rules, and regulations. It also reviews whether the organization complies with the internal rules, policies, procedures, and regulations. The aspects that are checked in a compliance audit are based on the organization type, the data it handles, and whether sensitive data are stored or transmitted.

A compliance audit helps in reviewing aspects such as the security of sensitive data, HR policies, management standards, and records of the financial department. Every business must comply with the regulations, and failure to comply could lead to consequences such as fines, imprisonment, and business shut down.

The recommendations for compliance audits are as follows.

Understand the Inspection Process in Advance

The organization must be aware of the audit process in advance. They can obtain an inspection checklist directly from the governing or regulatory agency. Industry associations may also offer audit guidelines, sample procedures, and policies. Using all these resources, the organization can prepare an internal audit program.

Conduct Self-compliance Audits

The best way to determine whether the organization would pass a compliance audit is to conduct a self-compliance audit. The organization can appoint an internal team or an independent auditor to perform a self-compliance audit and correct deficiencies. An external auditor can thoroughly review the internal audit system. The organization should be prepared with all the required documentation and processes to correct the required deficiencies to pass the audit.

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

Be Up-to-date on Standards

New changes in the compliance requirements can affect the enterprise's audit. It is essential to stay up to date on changes in the compliance requirements. This ensures that the data management and tracking are performed under the required parameters. The compliance should be assessed with the new guidelines.

Train the Team on Security Policies

The organization must ensure that all the users are aware of the security policies followed for handling, recovering, archiving, and destroying confidential data. In addition, all the users must be trained on Internet safety concerns and other security areas related to the organization.

Review Changes in the Organizational Activities

Recent changes to the organization such as new programs, new reporting requirements, or any troubleshooting issues should be reviewed. All these activities should be reported to the auditor.

Gather Evidence

Having well-organized data helps interpret the results of the compliance audit. Create subfolders for each cycle or category. This helps in keeping the relevant information together and ensuring easy access. Sensitive information should be protected with a password and maintained in a restricted network location.

ide01.ir

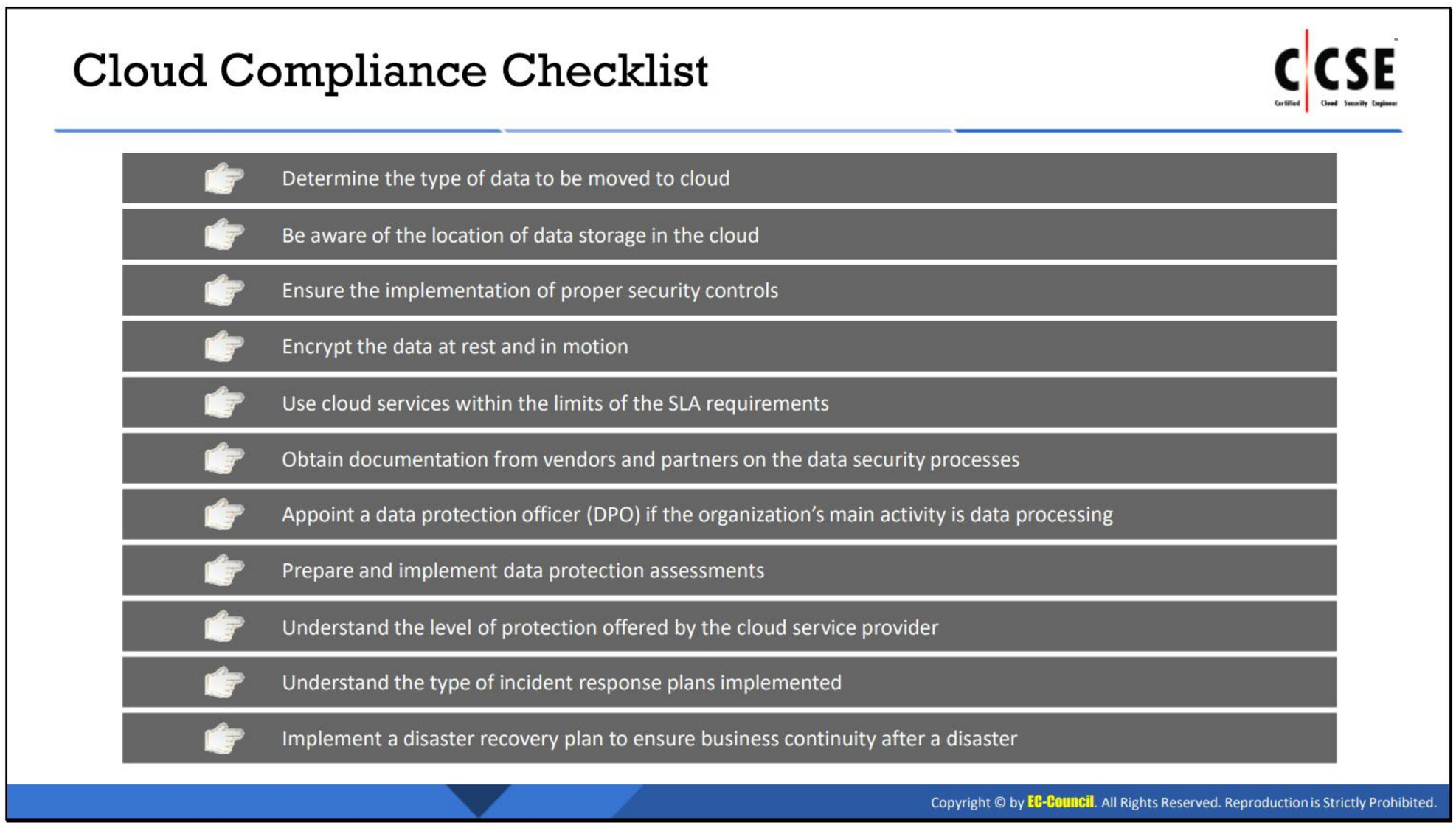
Set a Timeline and Assign Tasks

Any compliance audit requires proper preparation from inside and outside of the organization. Review the list of papers and schedules made by the auditor. Each task should be assigned to the respective team members with a due date. The due date should provide sufficient time for reviewing and correcting issues, if required. Difficult and time-consuming tasks should be given high priority. All the required financial statements should be made available to the auditors before the scheduled fieldwork.

Stay Alert with Incidents in the Industry

If a competitor experiences an incident, the organization must review its internal systems to ensure that its network is protected from such an incident. Security incidents in a company within the industry can motivate compliance auditors to investigate similar organizations to find inefficiencies.

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



Cloud Compliance Checklist

Achieving cloud compliance has become a major concern for cloud users. With the evolution of hacking, increased regulations and standards have been implemented by industries, governments, and individual organizations. When an organization migrates to the cloud, achieving compliance is difficult if it is not prepared. Cloud customers must choose the appropriate services to meet their requirements.

The following checklist helps achieve compliance in the cloud environment.

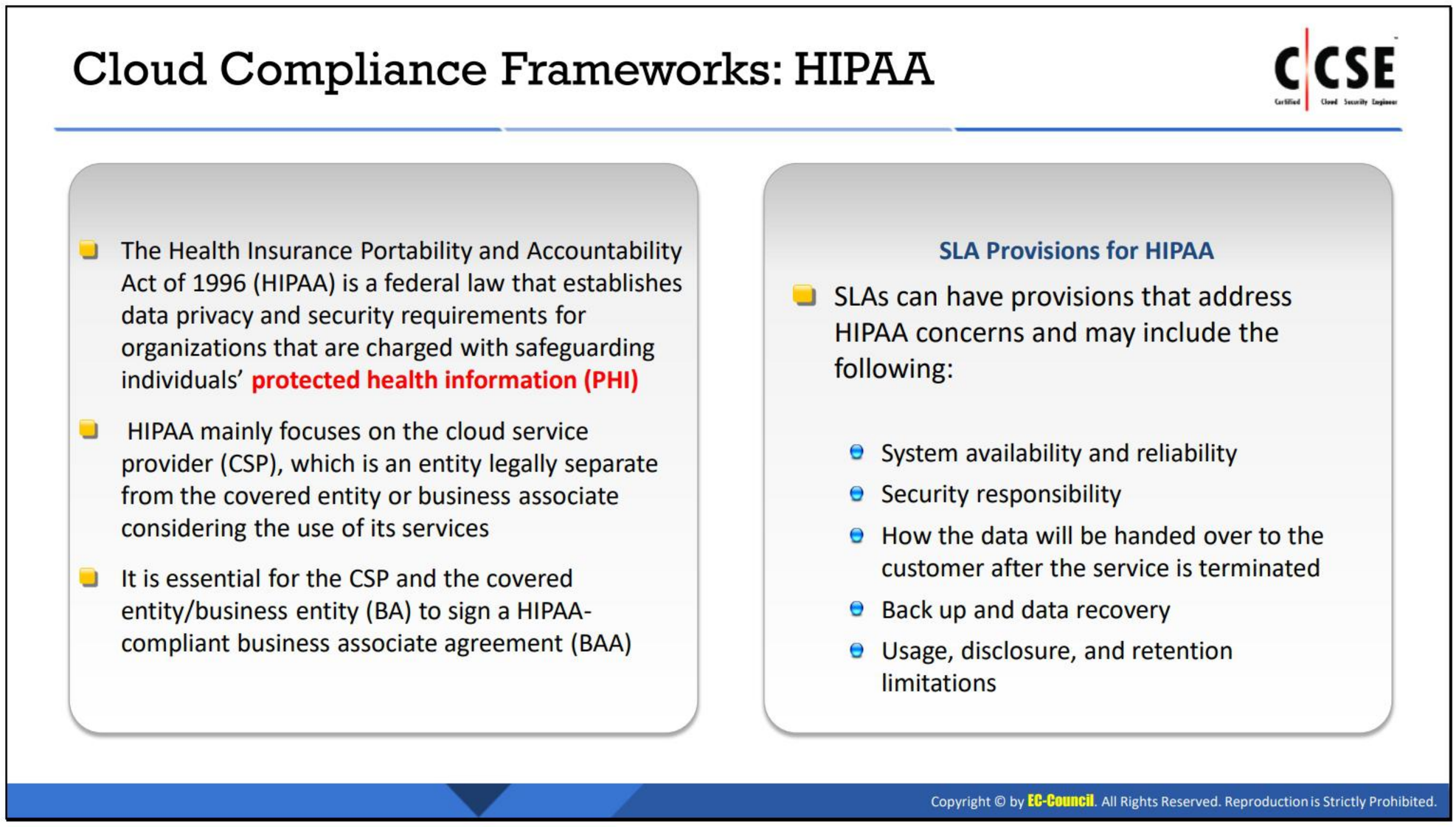
- **Data:** The cloud users must determine the types of data to be moved to the cloud and those that should not be moved to the cloud.
- **Location of Data:** During the audit, the users must prove the location of the data. The cloud customers should ensure that they are aware of the location of data storage in the cloud.
- **Data Access Control:** The organization must implement proper security controls. The organization must understand who has access to the data in the cloud and their level of access.
- **Data Encryption:** The data at rest and in motion in the cloud should be encrypted.
- **Required Resources:** Based on the company's compliance requirements, the organization may need a private data center inside the CSP data center.
- **Service-level Agreement (SLA):** The laws and regulations of a company may have requirements for the SLA. The SLA requirements may limit the usage of specific types of services. Therefore, the cloud service should be used as per the SLA.

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

- **Request Documentation:** The cloud users must request documentation from vendors and partners on the data security processes. This helps in demonstrating compliance and in conducting an audit trail.
- **Appoint a Data Protection Officer (DPO):** If the organization's main activity is focused on data processing, a DPO should be appointed. The DPO should be familiar with IT processes, privacy regulations, and data security.
- **Data Protection Assessment:** The organization must prepare and implement data protection assessments.
- **Data Protection:** The organization that adopts the cloud must understand the level of protection offered by the cloud service provider (CSP).
- **Security Requirements:** The cloud customers must understand the type of security the organization needs. For compliance requirements, it is important to understand the level of security required by the law or regulations.
- **Compliance Certifications and Legally Accepted Substitutes:** All CSPs can be certified. If a CSP cannot receive certifications, they attempt to achieve compliance by implementing a strict set of standards.
- **Auditors:** The organization must understand which third-party auditors perform the audit for cloud compliance. The organization must also determine whether it is entitled to a cloud compliance audit.
- **Incident Response:** The organization must understand the scope of incidents. It should also understand what type of incident response plans are implemented.
- **Disaster Recovery:** The laws and regulations applicable to the company may have certain disaster recovery requirements. The cloud customers must have a disaster recovery plan to ensure business continuity after a disaster.

hiox01.ir

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



Cloud Compliance Frameworks: HIPAA

Source: https://www.hhs.gov

The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule includes standards that address the use and disclosure of individuals' health information—called protected health information (PHI) by organizations subject to the Privacy Rule, which are themselves called "covered entities"—as well as standards for individuals' privacy rights to understand and control how their health information is used. The HHS Office for Civil Rights announces a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act to strengthen the privacy and security protections for health information established under HIPAA.

HIPAA focuses on the cloud resources offered by a CSP, which is an entity legally separate from the covered entity or business associate considering the use of its services. CSPs generally offer online access to shared computing resources with varying levels of functionality depending on the users' requirements, ranging from data storage alone to complete software solutions (e.g., an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs. Common cloud services are on-demand Internet access to computing (e.g., networks, servers, storage, and applications).

The HIPAA Privacy, Security, and Breach Notification Rules (the HIPAA Rules) establish important protections for individually identifiable health information (called protected health information or PHI when created, received, maintained, or transmitted by a HIPAA covered entity or business associate), including limitations on the use and disclosure of such information, safeguards against inappropriate use and disclosure, and individuals' rights with

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

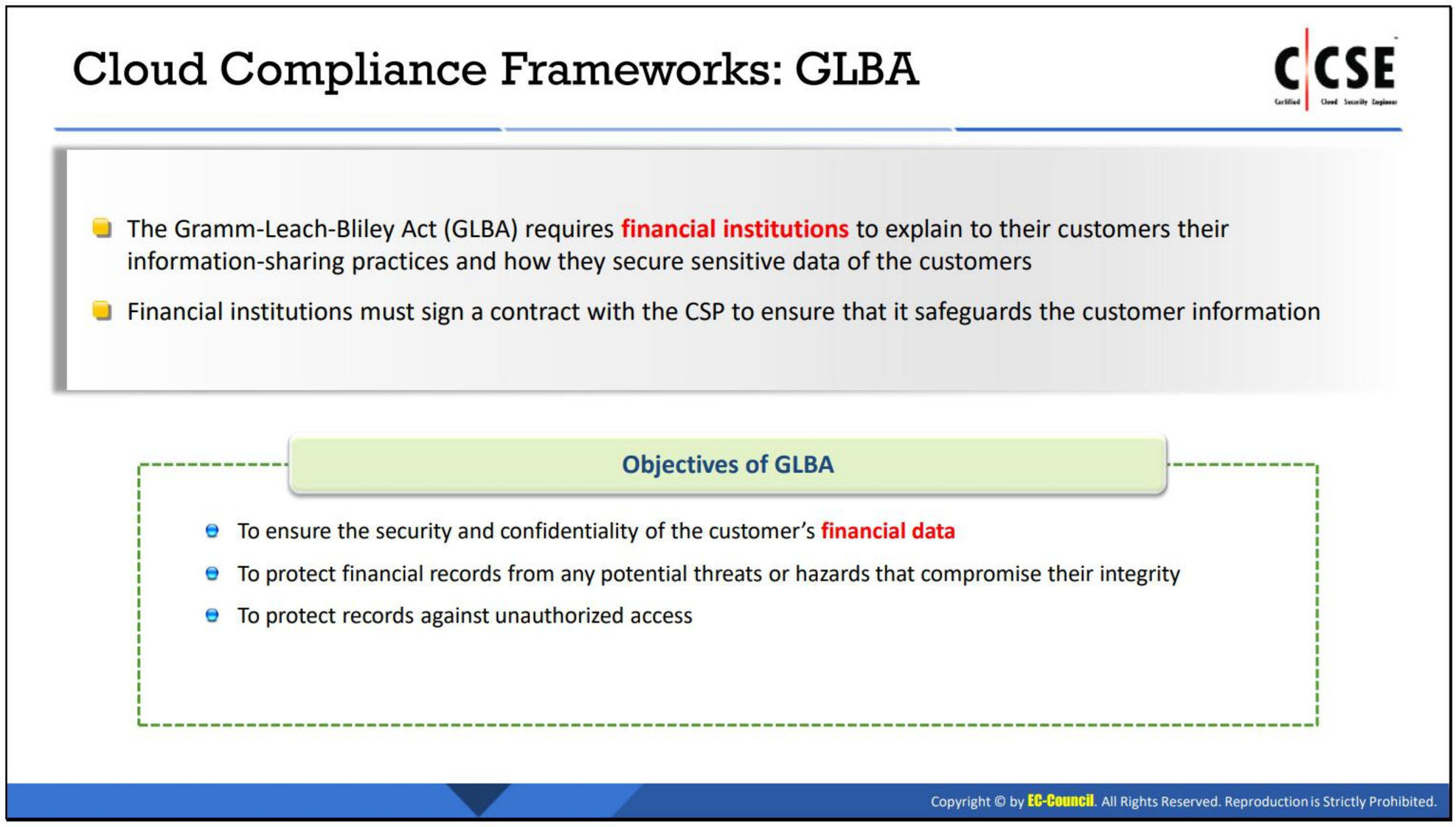
respect to their health information. Covered entities and business associates must comply with the applicable provisions of the HIPAA Rules. A covered entity is a health plan provider, healthcare clearing house, or healthcare provider that conducts certain billing- and payment-related transactions electronically. A business associate is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI. A business associate can also be any subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

When a covered entity engages the services of a CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate under HIPAA. Further, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit PHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the CSP processes or stores only encrypted PHI and lacks the encryption key for the data. Lacking an encryption key does not exempt a CSP from the status of a business associate and the corresponding obligations under the HIPAA Rules. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules. It should be ensured that the CSP analyzes the breach notification requirements under the HITECH act before disclosing PHI to CSPs.

A service-level agreement (SLA) is used to address more specific business expectations between the CSP and its customer, which may also be relevant to HIPAA compliance. SLAs can include provisions that address such HIPAA concerns as the following:

- System availability and reliability
- Back-up and data recovery (e.g., the ability to respond to a ransomware attack or other emergency situation)
- Manner in which data will be returned to the customer after service use termination
- Security responsibility
- Use, retention, and disclosure limitations

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



Cloud Compliance Frameworks: GLBA

Source: https://www.ftc.gov

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions – companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. The GLBA seeks to protect consumer financial privacy. Its provisions limit when a financial institution may employ third parties. The law covers a broad range of financial institutions and includes many companies not traditionally considered to be financial institutions, because they engage in certain financial activities. Financial institutions must notify their customers about their information-sharing practices and inform consumers of their right to opt-out if they do not want their information to be shared with non-affiliated third parties. In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and rediscloure of that information.

Cloud service providers (CSPs) should sign a contract with financial institutions to gain access to customer data. The collected data should be used only for the purposes stated in the contract.

The Privacy Rule protects a consumer's non-public personal information (NPI). NPI is any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.

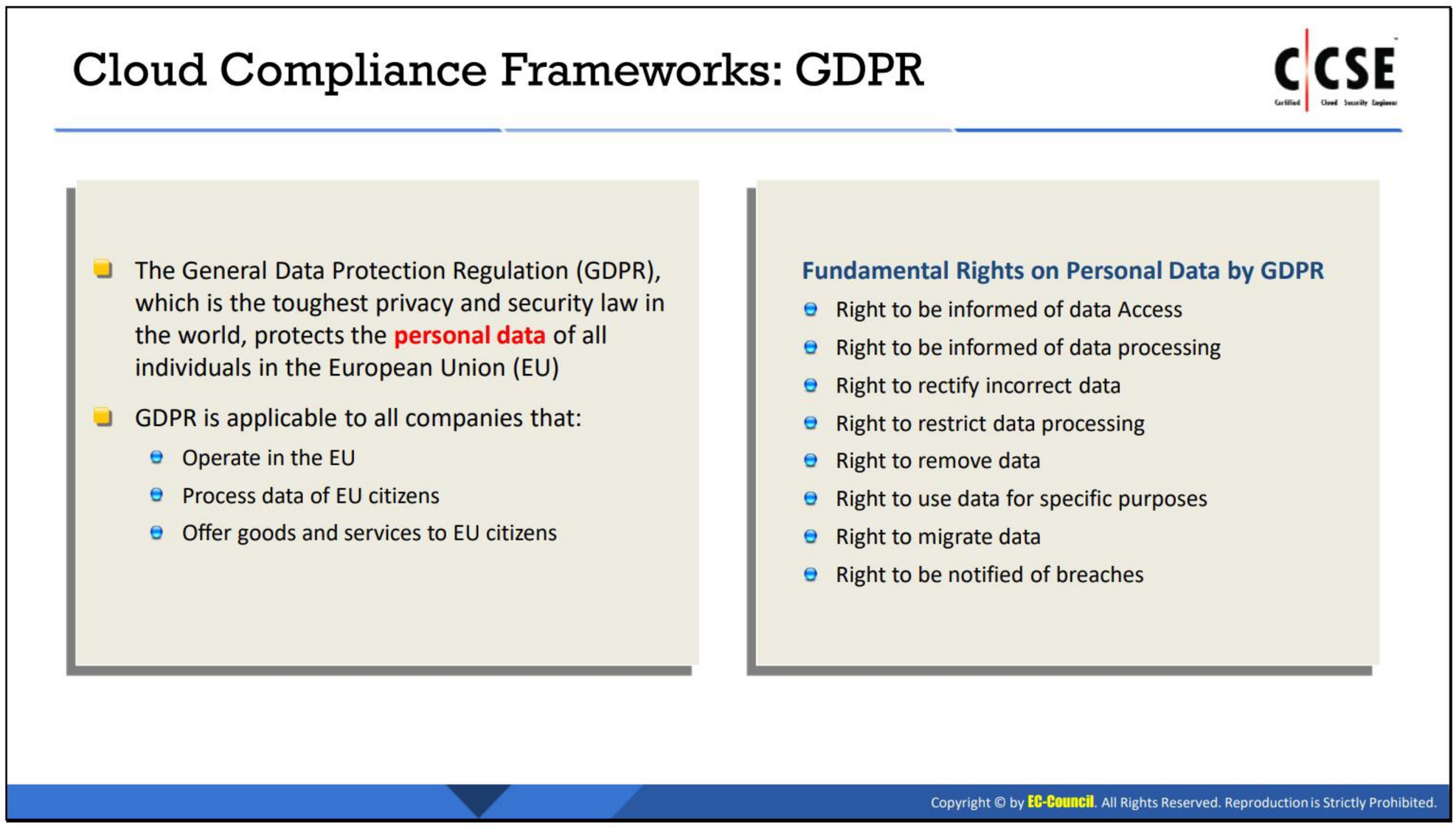
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NPI includes the following:

- Any information an individual provides to receive a financial product or service (for example, name, address, income, social security number, or other information on an application)
- Any information about an individual obtained from a transaction involving financial product(s) or service(s) (for example, the fact that an individual is a consumer or customer of a product, account numbers, payment history, loan or deposit balances, and credit or debit card purchases)
- Any information about an individual received in connection with providing a financial product or service (for example, information from court records or from a consumer report).

hide01.ir

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



Cloud Compliance Frameworks: GDPR

Source: https://gdpr.eu

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Although it was drafted and passed by the European Union (EU), it imposes obligations on organizations anywhere as long as they target or collect data related to people in the EU. GDPR is applicable to all companies that:

- Operate in the EU
- Process data of EU citizens
- Offer goods and services to EU citizens

Fundamental Rights on Personal Data by GDPR

- Right to be informed of data access
- Right to be informed of data processing
- Right to rectify incorrect data
- Right to restrict data processing
- Right to remove data
- Right to use data for specific purposes
- Right to migrate data
- Right to be notified of breaches

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

The GDPR defines an array of legal terms at length. The following are some of the most important factors in GDPR.

- **Personal Data:** Personal data are any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data.
- **Data Processing:** Data processing is any automated or manual action performed on data. Examples include collecting, recording, organizing, structuring, storing, using, and erasing data.
- **Data Subject:** It is the person whose data are processed.
- **Data Controller:** It is the person who decides why and how personal data will be processed.
- **Data Processor:** It is a third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations.

Data Protection Principles

- **Lawfulness, Fairness, and Transparency:** Processing must be lawful, fair, and transparent to the data subject.
- **Purpose Limitation:** Data processing must be performed only for the legitimate purposes specified explicitly to the data subject at the time of collecting the data.
- **Data Minimization:** It states that only required and relevant information should be collected and processed as per the specified purpose.
- **Accuracy:** Personal data must be kept accurate and up to date.
- **Storage Limitation:** It states that the personally identifying data should be stored for as long as necessary for the specified purpose.
- **Integrity and Confidentiality:** Processing must be performed in such a manner that security, integrity, and confidentiality are ensured (e.g., by using encryption).
- **Accountability:** The data controller is responsible for demonstrating GDPR compliance in accordance with all of these principles.

Accountability

The GDPR requires data controllers to be able to demonstrate compliance with GDPR. The following are some of the ways to achieve this:

- Designate data protection responsibilities to the team.
- Maintain detailed documentation of the data being collected, how the data are used, where the data are stored, which employee is responsible for the data, etc.
- Train staff and implement technical and organizational security measures.

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

- Implement data processing agreement contracts with third parties contracted to process data.
- Appoint a data protection officer (DPO).

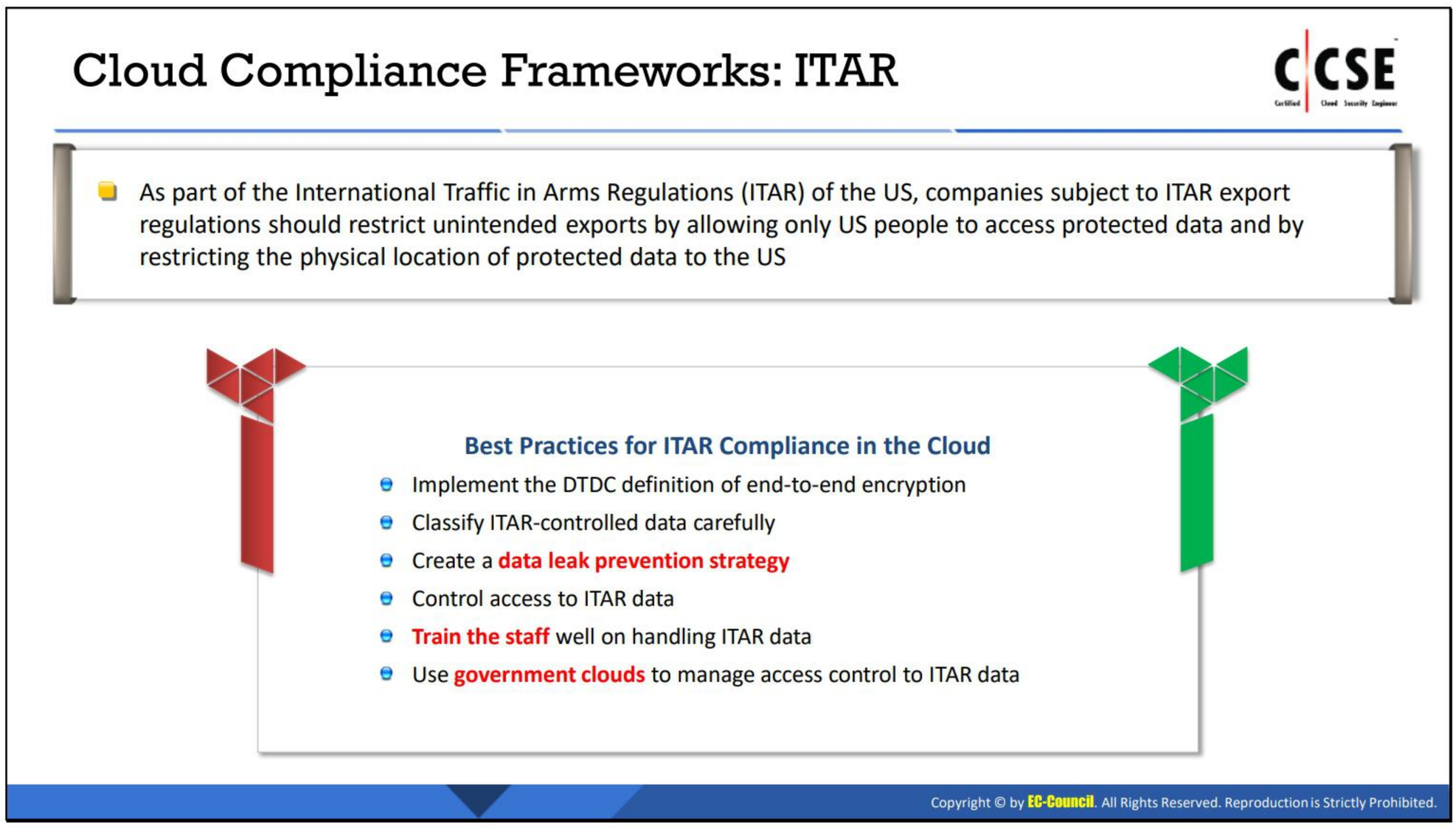
Data Security

- Handle data securely by implementing appropriate technical and organizational measures.
- Technical measures range from requiring employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.
- Organizational measures include staff training, adding a data privacy policy to the employee handbook, or limiting access to personal data to only those employees in the organization who need it.
- If a data breach occurs, inform the data subjects within 72 h, failing which penalties apply.

A cloud service provider (CSP) subject to GDPR requirements can appoint a data protection officer (DPO) even if it is not required. There are benefits to having a DPO, whose basic tasks involve understanding the GDPR and how it applies to the organization, advising people in the organization about their responsibilities, conducting data protection trainings, conducting audits and monitoring GDPR compliance, and serving as a liaison with regulators.

hide01.ir

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



Cloud Compliance Frameworks: ITAR

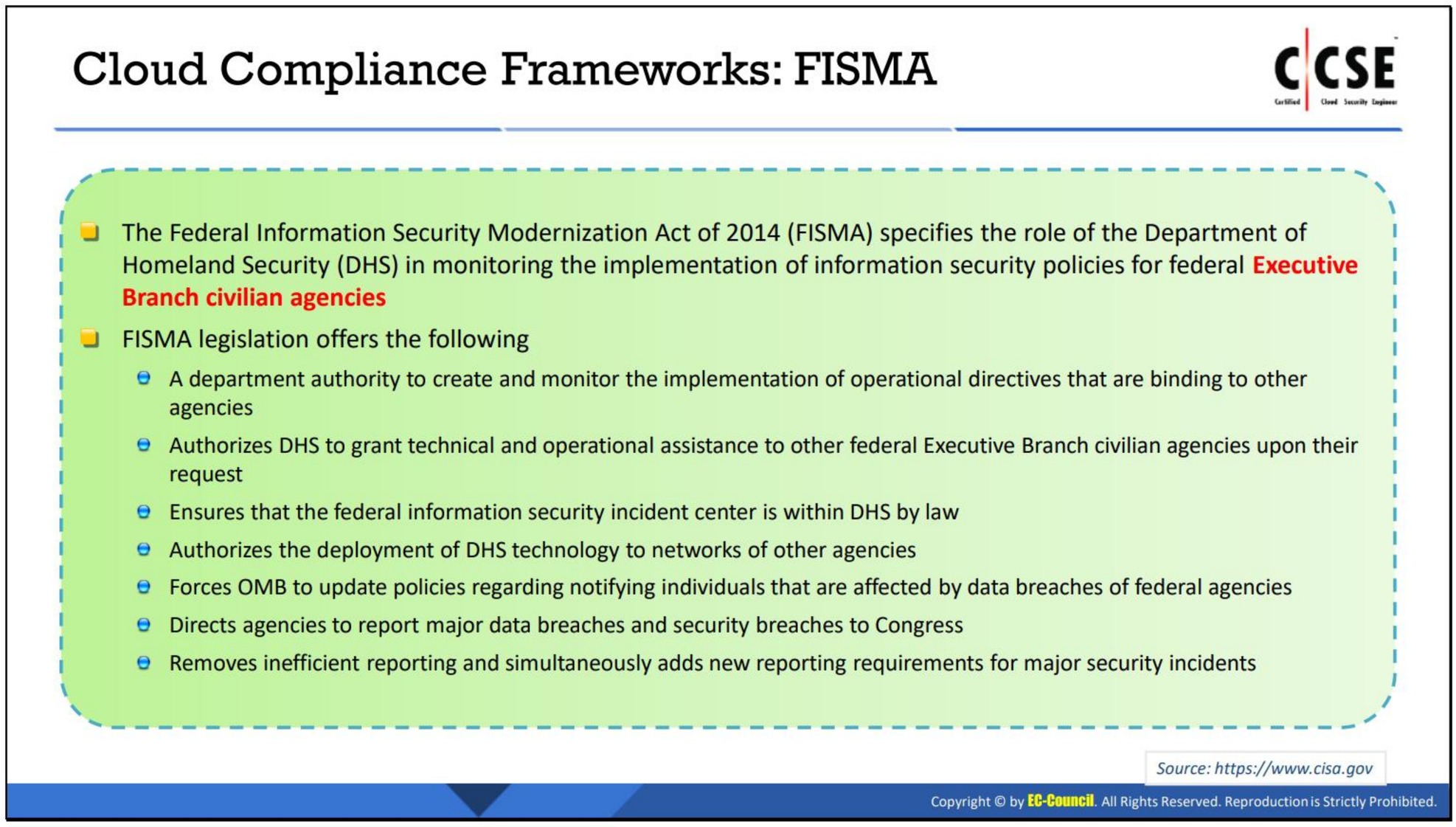
Source: https://www.pmddtc.state.gov

The US Department of State is responsible for managing the export and temporary import of defense articles (meaning any item or technical data designated under the US Munitions List, as described in Title 22 CFR 121.1) that are governed by the Arms Export Control Act (Title 22 USC 2778) and the International Traffic in Arms Regulations (ITAR) (Title 22 CFR 120–130). The Directorate for Defense Trade Controls (DDTC) is responsible for managing entities governed under these programs. As part of the US ITAR, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US citizens and by restricting the physical location of protected data to the US.

Best Practices for ITAR Compliance in the Cloud

- Implement the DDTC (Directorate of Defense Trade Controls) definition of end-to-end encryption for technical data related to defense.
- Classify ITAR-controlled data carefully into categories such as confidential, public use, and internal use.
- Create a data leak prevention strategy.
- Control access to ITAR data by following the principle of least privilege.
- Train the staff well on handling ITAR data.
- Use government clouds to manage access control to ITAR data.

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



Cloud Compliance Frameworks: FISMA

Source: https://www.cisa.gov

The Federal Information Security Modernization Act 2014 (FISMA) codifies the role of the Department of Homeland Security (DHS) in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing the agencies' compliance with those policies, and assisting the Office of Management and Budget (OMB) in developing those policies.

FISMA updates the federal government's cybersecurity practices in the following ways:

- Codifying the authority of DHS to administer the implementation of information security policies for non-national federal Executive Branch security systems, including providing technical assistance and deploying technologies to such systems
- Amending and clarifying the oversight authority of OMB over federal agency information security practices
- Requiring OMB to amend or revise OMB A-130 to eliminate inefficient and wasteful reporting

The legislation provides the Department authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistency with OMB policies and practices. It also performs the following:

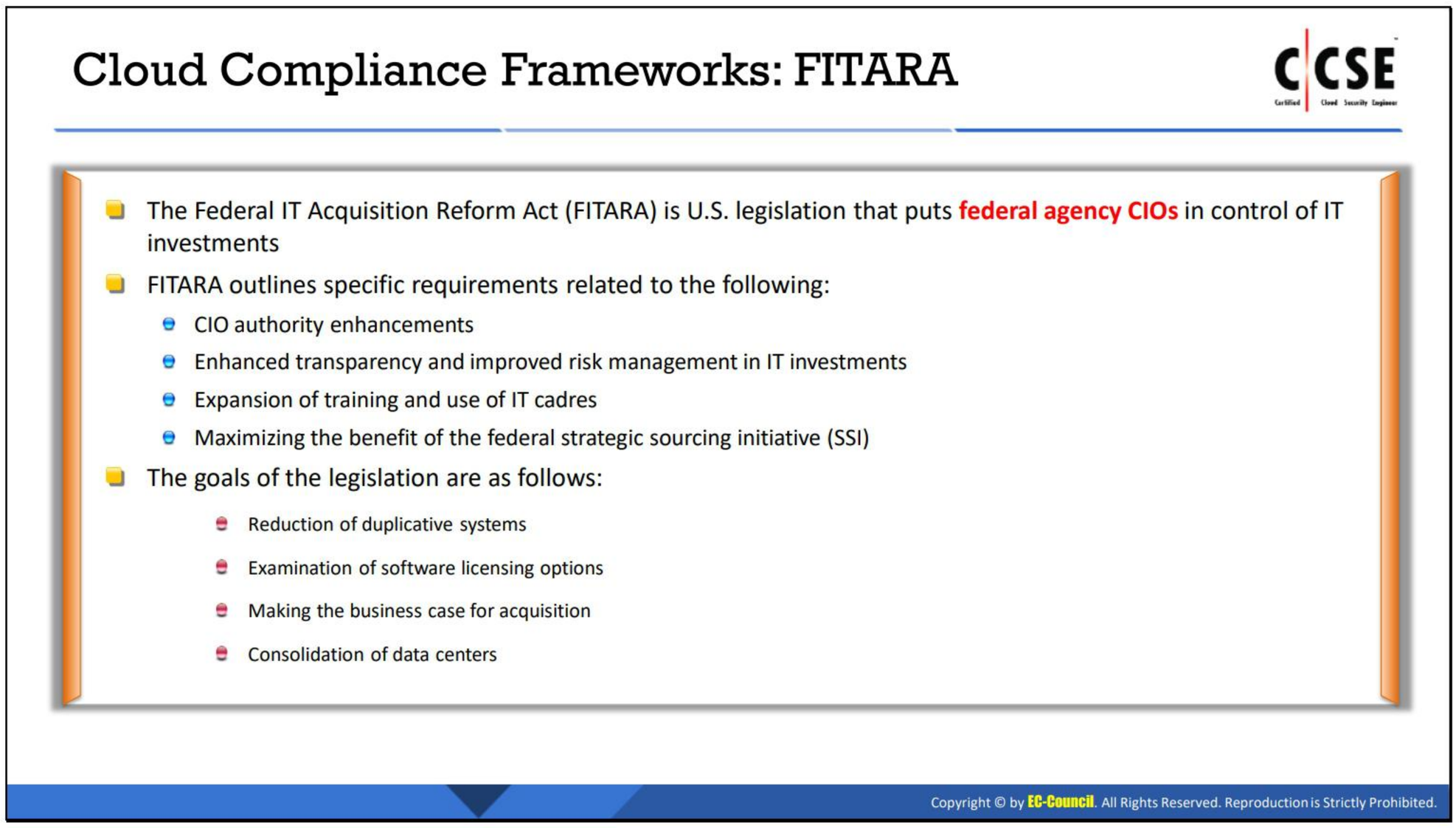
- Authorizes DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request

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

- Places the federal information security incident center (a function fulfilled by US-CERT) within DHS by law
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request)
- Directs OMB to revise policies regarding the notification of individuals affected by federal agency data breaches.
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually.
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information security incidents.

hide01.ir

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



Cloud Compliance Frameworks: FITARA

Source: https://handbook.tts.gsa.gov

The Federal IT Acquisition Reform Act (FITARA) is US legislation that puts the chief information officers (CIOs) of federal agencies in control of IT investments. Compliance with this act requires the CIO and chief technology officer (CTO) to provide the documented approval of an IT purchase.

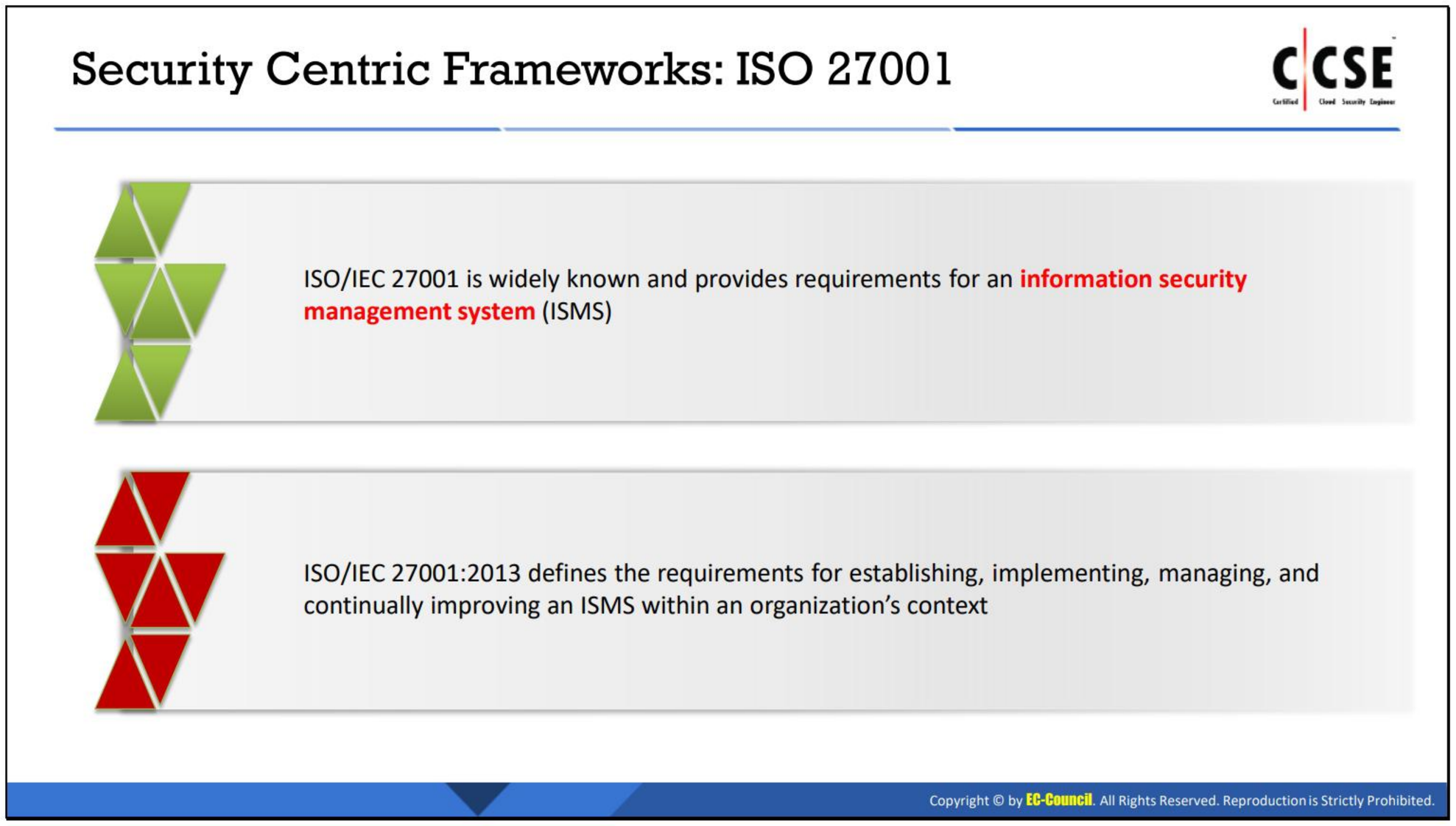
FITARA outlines specific requirements related to the following:

- CIO authority enhancements
- Enhanced transparency and improved risk management in IT investments
- Portfolio reviews
- Expansion of training and use of IT cadres
- Federal Data Center Consolidation Initiative (FDCCI), more recently known as the Data Center Optimization Initiative (DCOI)
- Maximizing the benefit of the federal strategic sourcing initiative (SSI)

FITARA aims to eliminate duplication and waste in IT acquisition for the federal government through the following specific goals:

- Reduction of redundant systems
- Examination of software licensing options
- Making the business case for acquisition.
- Consolidation of data centers.

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



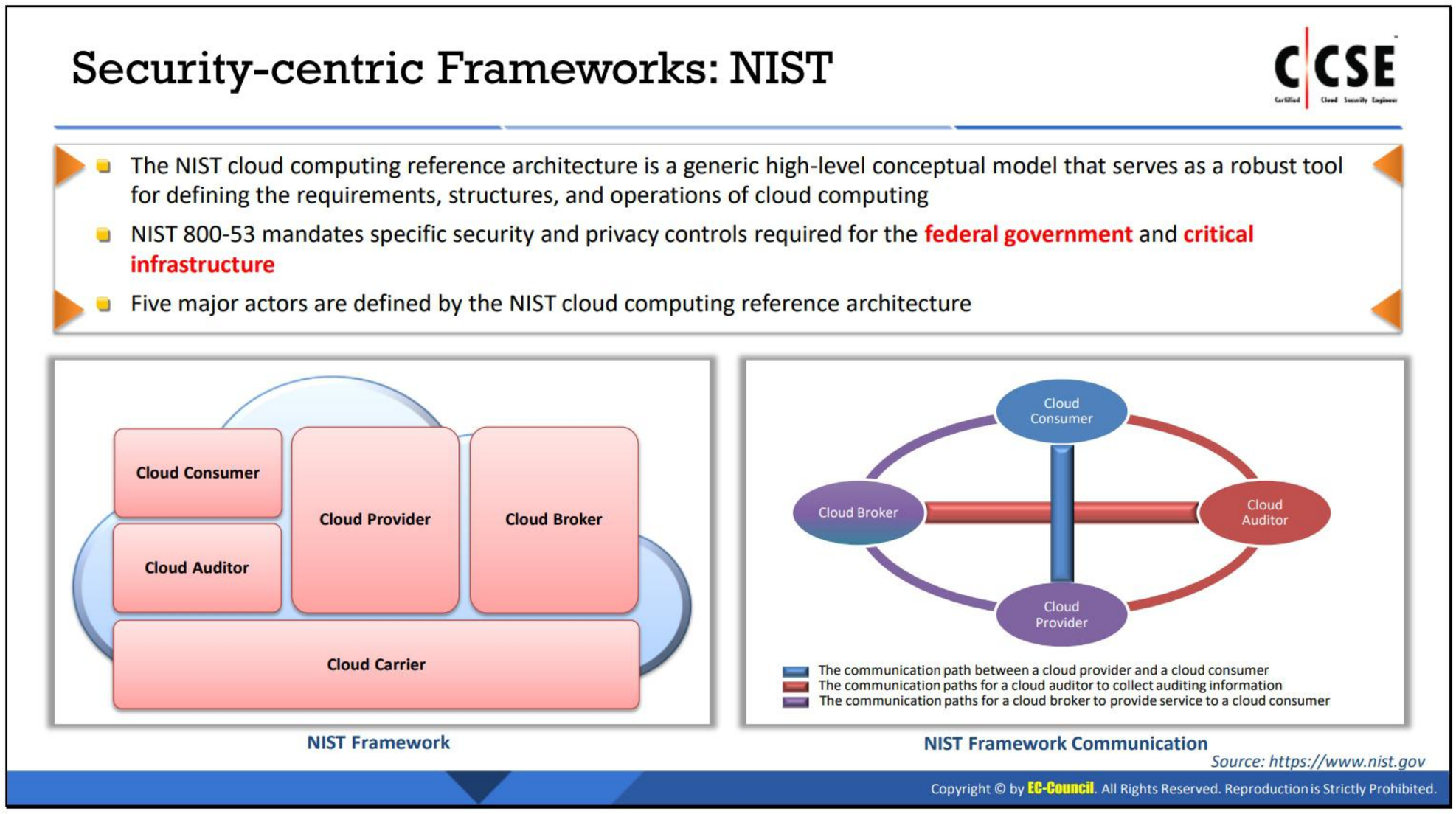
Security Centric Frameworks: ISO 27001

Source: https://www.iso.org

ISO/IEC 27001 is a widely known framework that outlines requirements for an information security management system (ISMS). Meeting these requirements enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details, or information entrusted by third parties.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size, or nature.

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



Security-centric Frameworks: NIST

Source: https://www.nist.gov

The National Institute of Standards and Technology (NIST), under the US Department of Commerce, creates standards and guidelines pertaining to information security. The 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:

- Illustrate and understand various cloud services in the context of an overall cloud computing conceptual model
- Provide technical references to USG agencies and other consumers to understand, discuss, categorize, and compare cloud services
- Communicate and analyze security, interoperability, and portability candidate standards and reference implementations

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

The NIST cloud computing reference architecture defines five major actors, which are described below.

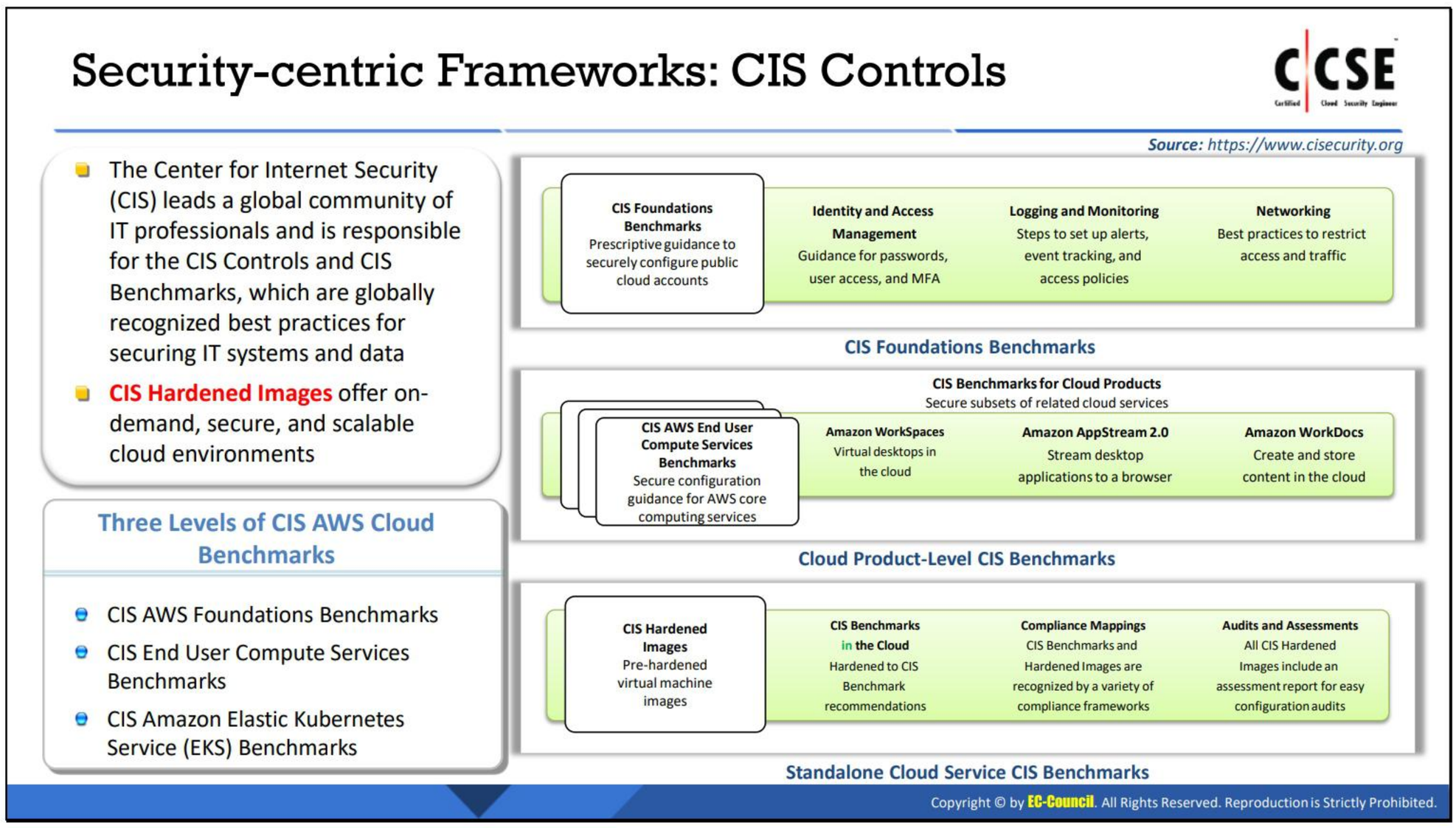
- **Cloud Consumer:** A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from, a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the 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 the 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 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 security requirements for the system. Security auditing should include the verification of compliance with regulations and security policies.
- **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 some 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 the secure movement of data between the cloud consumer and multiple cloud providers.
    - **Arbitrage**: Service arbitrage is similar to service aggregation except that the services being combined/consolidated are not fixed. Service arbitrage implies that a 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 SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers and may require the cloud carrier to provide dedicated and encrypted connections between cloud consumers and cloud providers.

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

NIST developed Special Publication 800-53 (NIST SP 800-53) to build on statutory responsibilities laid out in the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, which is a federal law that requires U.S. government agencies to create, review, and report on agency-wide practices that prioritize information security. NIST 800-53 mandates specific security and privacy controls for the federal government and critical infrastructure.

hide01.ir

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



Security-centric Frameworks: CIS Controls

Source: https://www.cisecurity.org

The Centre for Internet Security (CIS) responded with more resources to help secure these capabilities in the AWS cloud. It works with Amazon Web Services (AWS) to expand with new cloud products and services.

hiteb.ir

New Guidance from the CIS AWS Benchmarks Community

CIS expand their network volunteers to guidance for AWS Cloud. This effort resulted in CIS Benchmarks specific to AWS cloud products and services.

CIS honed resources and did not create CIS Benchmark for every unique service. Instead, CIS followed the lead of AWS, and grouped services by cloud product. AWS offers dozens of products, grouping cloud services based on the function they provide.

Three Levels of CIS AWS Cloud Benchmarks

The guide presents the three CIS AWS Benchmark categories applicable to the cloud:

- CIS AWS Foundations Benchmark
- CIS End User Compute Services Benchmark
- CIS Amazon Elastic Kubernetes Service (EKS) Benchmarks

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

CIS AWS Foundations Benchmark:

Provide an account-level starting point for configuring securely for the AWS Cloud. These resources cover identity and access management, logging and monitoring, networking, etc.

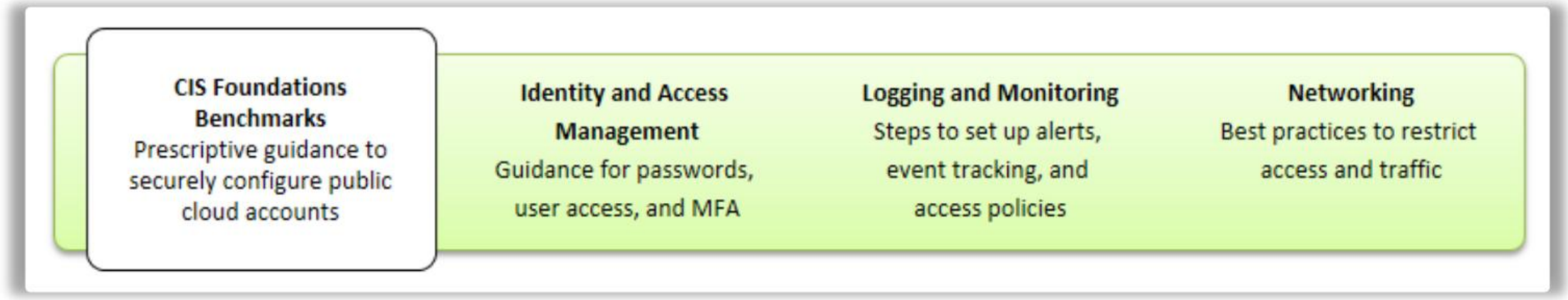


Figure 10.15: CIS Foundations Benchmarks

CIS End User Compute Services Benchmark:

The first release of cloud product-level CIS Benchmark is the CIS AWS End User Compute Service Benchmark. This includes configuration recommendations for Amazon WorkSpaces, Amazon WorkDocs, Amazon AppStream 2.0, and Amazon WorkLink. The user can choose the applicable services and configure them according to what is running in their environment.

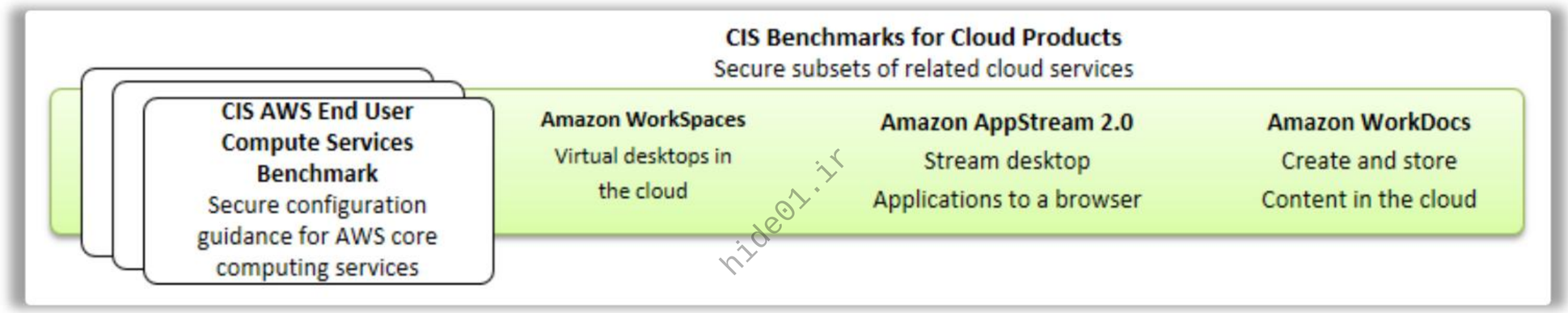


Figure 10.16: Cloud Product-Level CIS Benchmarks

CIS Amazon Elastic Kubernetes Service (EKS) Benchmarks:

The configurations needed for services warrants a CIS Benchmark specific to one cloud service. With this scenario, the product-level CIS Benchmark will include a section for the cloud service but will point to a separate CIS Benchmark for the service. An example of the standalone cloud service CIS Benchmark is the CIS Amazon Elastic Kubernetes Service (EKS) Benchmarks.

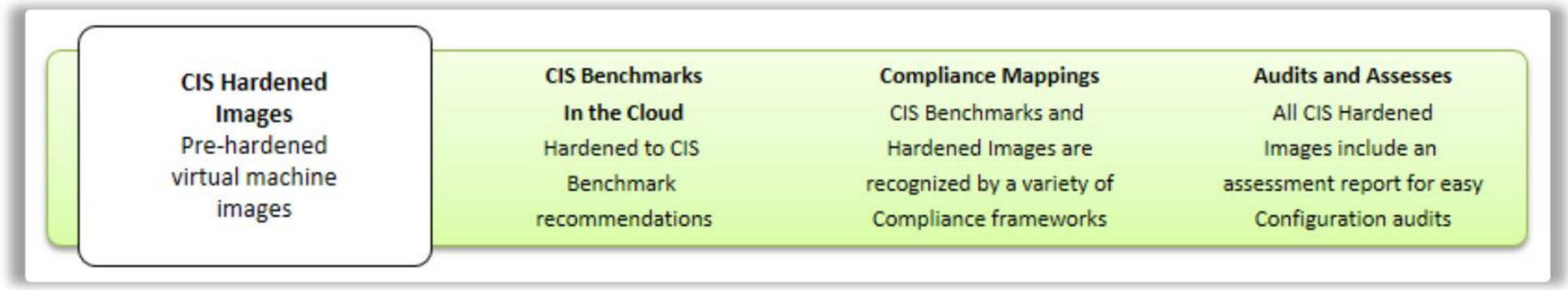


Figure 10.17: CIS Amazon Elastic Kubernetes Service (EKS) Benchmarks

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

Security-centric Frameworks: CSA STAR

- Cloud Security Alliance (CSA) Security Trust And Risk Assurance (STAR) is a **cloud security assurance program**
- Cloud service providers establish trust through transparency
- Cloud customers ensure privacy and security from providers

		Audit Frequency	Security	Privacy
Type of Audit	●—●—●	STAR Level 3	Continuous Auditing	----------
	●—●—○	STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment	----------
		STAR Level 2	3rd Party Certification	GDPR CoC Certification
	●—○—○	STAR Level 1 Continuous	Continuous Self-Assessment	----------
		STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment

Transparency and Assurance

Levels of STAR

Source: https://cloudsecurityalliance.org

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

Security-centric Frameworks: CSA STAR

Source: https://cloudsecurityalliance.org

Cloud Security Alliance (CSA) Security Trust And Risk Assurance (STAR) is cloud security assurance program. STAR program encompasses key principles of transparency, rigorous auditing, and harmonization of standards. STAR registry documents the security and privacy controls provided by popular cloud computing offerings. This publicly accessible registry allows cloud customers to access their security providers to make the best procurement decision.

Cloud Service Providers:

STAR registry is a cost-effective solution that decreases complexity while increasing trust and transparency. Demonstrate your adherence to security and privacy best practices to future and current customers by submitting to the registry.

Benefits of STAR for Cloud Service Providers:

- Accelerate sales cycle.
- Solidify position as a trusted provider of cloud services.
- Better build, establish and maintain a robust security program.
- Expand business by helping customers navigate secure cloud adoption.
- Be part of a global database that is becoming the marketplace for providers used by cloud users.

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

Cloud Customer:

Improve the security and privacy program within your organization. STAR lets you gain insight into the controls in place to protect your data. Assess both your internal level of assurance, and the level of assurance offered by your cloud providers. Whether you moved to the cloud or are considering migrating soon, STAR can help you manage your security and privacy programs more effectively.

Benefits of STAR for Cloud Customer:

- The STAR registry as a trusted source of information on the security and privacy posture of CSPs. It enforces accountability and lets you build a coherent GRC program.
- The STAR compliance program which lets you select the level of transparency and assurance you require from CSPs.
- The STAR Foundation tools (CCM, CAIQ, GDPR, COC) to support your own GRC approach and ensure language alignment between you and your CSP.
- If your provider is not listed on the STAR registry, please submit a request to have them verified using our ready-made editable template that you can revise and e-mail directly to your provider(s).

Level of STAR:

The level pursue depends on level of responsibility in the shared responsibility model and the levels of assurance and transparency provided:

hide01.ir

		Audit Frequency	Security	Privacy
Type of Audit	●—●—●	STAR Level 3	Continuous Auditing	----------
	●—●—○	STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment	----------
		STAR Level 2	3rd Party Certification	GDPR CoC Certification
	●—○—○	STAR Level 1 Continuous	Continuous Self-Assessment	----------
		STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment

Transparency and Assurance

Figure 10.18: Levels of STAR

Level 1:

- Operating in low-risk environment.
- Want to offer increased transparency into security control.

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

- Looking for cost-effective way to improve trust and transparency.

Level 2:

- Operating I medium high environment
- Already hold the following:
  - ISO 27001
  - SOC2
  - GB/T 22080-2008
- Looking for cost effective way to increase assurance for cloud security and privacy.

Level 3:

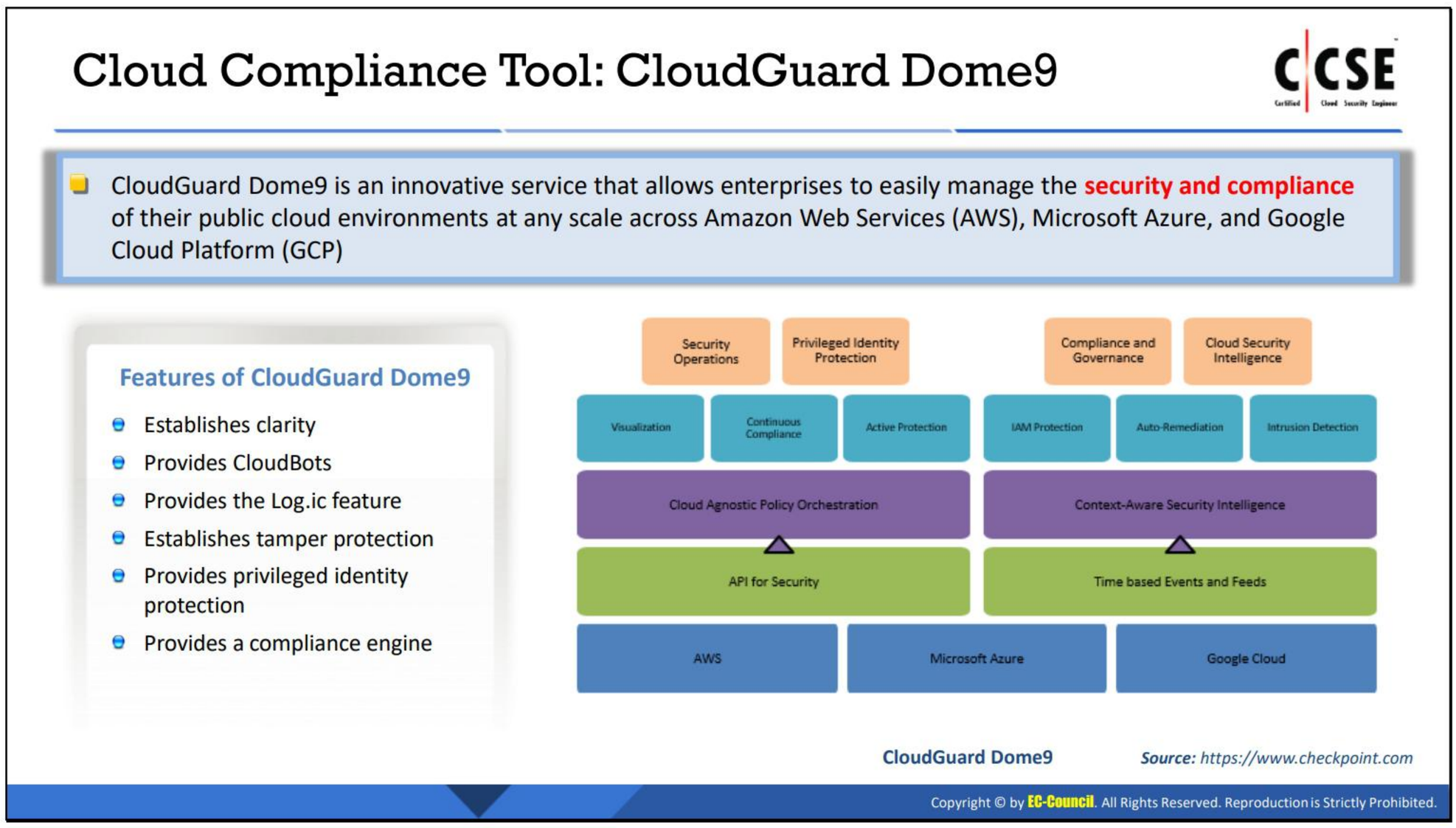
- Operating in high-risk environment.
- Want to offer a high-level transparency.
- Organisations full service cloud service provider (CSP).

How to Get Started with STAR:

Determine level of trust and transparency required:

- **Low-risk Organization:** Level 1 is good place to start. If it is decided later that you require greater assurance from your provider, you can request them to completer level 2.
- **Medium Risk Organization:** Level 2 is good for organization with a moderate amount of risk. You can request a self-assessment along with third party certification to provide your management with both transparency and assurance.
- **High-risk Organization:** Level 3 is designed for organization operating in high-risk environments. Continuous auditing offers organization the highest level of both transparency and assurance to keep organization safe on cloud.

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



Cloud Compliance Tool: CloudGuard Dome9

Source: https://www.checkpoint.com

CloudGuard Dome9 allows enterprises to easily manage the security and compliance of their public cloud environments at any scale across Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). CloudGuard Dome9 offers technologies to visualize and assess security posture, detect misconfigurations, model, and actively enforce gold standard policies, protect against attacks and insider threats, cloud security intelligence for cloud intrusion detection, and comply with regulatory requirements and best practices.

Features of CloudGuard Dome9:

- **Clarity:** Visualization of cloud assets, including network topology, firewalls and more.
- **CloudBots:** Auto-remediation solutions for AWS that accelerate the resolution of dangerous misconfigurations and enforce compliance.
- **Log.ic:** Cloud security intelligence that combines cloud inventory and configuration information with real time monitoring data from a variety of sources.
- **Tamper Protection:** Continuous monitoring and automation reversion of unauthorized modifications.
- **Privileged Identity Protection:** Just-in-time privilege elevation with out-of-band authorization for IAM actions.
- **Compliance Engine:** Comprehensive compliance management including automated continuous compliance to help assess and enforce regulatory requirements and security best practices.

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

Capabilities of CloudGuard Dome9:

- **Security Operations:** Visualize assets, assess security posture, fix misconfigurations and threats, manage the cloud firewall, and enforce security from a single source of network authority.
- **Privileged Identity Protection:** Protect against compromised credentials and identity theft using a cloud's native IAM capabilities to safeguard access to actions that can have a big impact.
- **Compliance and Governance:** Manage the compliance lifecycle for standards such as PCI DSS, from automated data aggregation and assessment to remediation and reporting.
- **Cloud Security Intelligence:** CloudGuard Log.ic is a cloudnative security intelligence technology that delivers cloud intrusion detection, network traffic visualization and user activity analytics.

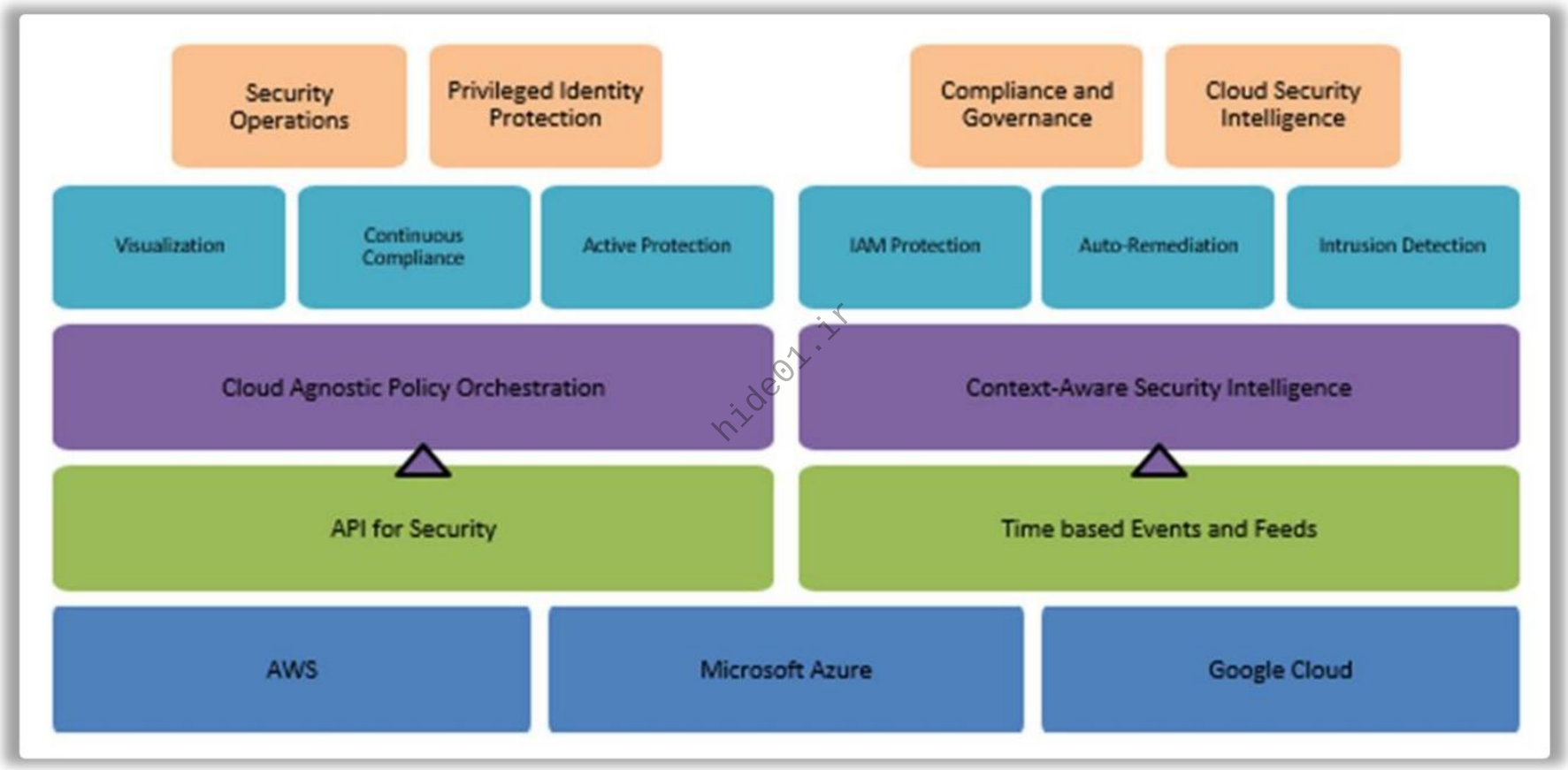


Figure 10.19: CloudGuard Dome9

Benefits of CloudGuard Dome9:

- **Agentless, Cloud-native Architecture for Today's Cloud:** The CloudGuard Dome9 service uses the native security controls provided by public clouds to protect all cloud resources, including built-in services such as AWS RDS, GCP compute engine instances, and Azure LBs, meeting the needs of today's public clouds that agent-based solutions cannot address. CloudGuard Dome9 allows you to protect multiple cloud environments by combining cloud-agnostic policy automation with cloud-native security capabilities.
- **Faster Time-to-Value with CloudGuard Dome9:** With no software to install and no agents to manage, you can secure your environment with CloudGuard Dome9 in under five minutes. You never have to worry about software updates and scaling problems. CloudGuard Dome9 integrates with your AWS accounts leveraging innovative cross-

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

account trust policy to gather security information, rather than sharing keys and credentials.

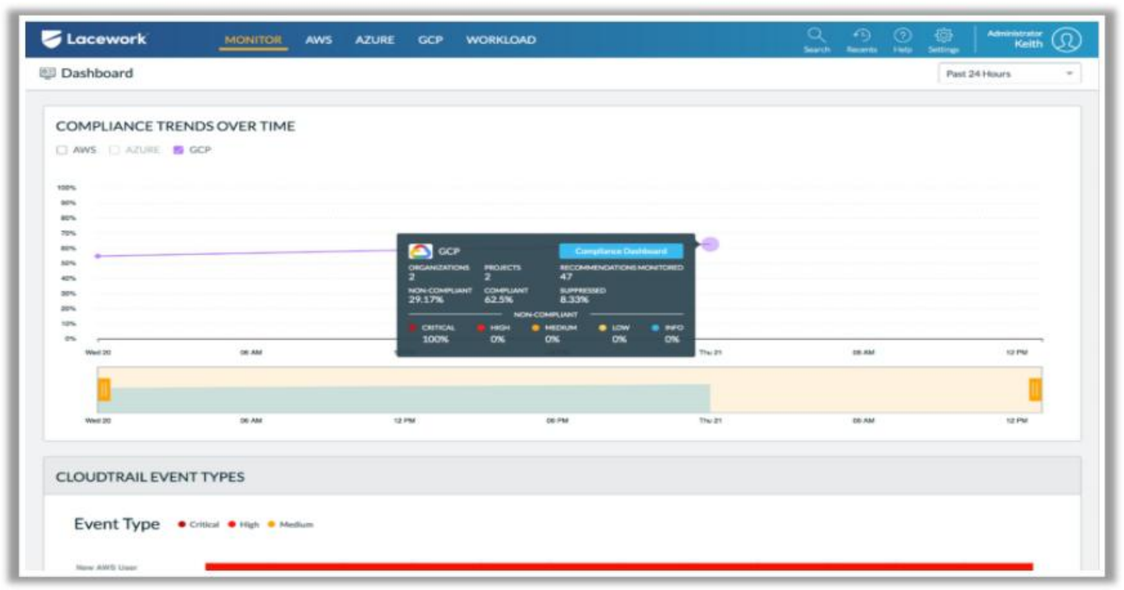
- **Remediate in Place — Find It, Fix It, Stay Fixed:** CloudGuard Dome9 is not just a monitoring solution. In addition to powerful visualization capabilities that allow you to review security posture in real-time to discover any vulnerabilities, compromised workloads, open ports, or misconfigurations, CloudGuard Dome9 also allows administrators to take the necessary actions to rapidly mitigate risk through remediation from a single platform.

hide01.ir

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

Cloud Compliance Tool: Lacework

- Lacework's centralized cloud security platform offers unprecedented visibility, delivers one-click investigation, allows automatic intrusion detection, simplifies cloud compliance across various cloud platforms (Azure, GCP, and AWS), and provides **a consolidated view of risk** across cloud containers and workloads



Lacework Dashboard

Source: https://www.lacework.co

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

Cloud Compliance Tool: Lacework

Source: https://www.lacework.com

Lacework's unified cloud security platform provides unprecedented visibility, automates intrusion detection, delivers one-click investigation, and simplifies cloud compliance across AWS, Azure, and GCP, providing a comprehensive view of risks across cloud workloads and containers.

Complexity is an enemy of security; a unified view is essential to simplify the complexity of having multiple configurations. Lacework does this across AWS, GCP, and Azure by bringing multiple clouds into one portal. This means no logging into different disparate tools to evaluate your stance. It is a single pane of glass to audit all your cloud platform configurations. As configurations change, Lacework will monitor and alert any time a configuration goes out of compliance. This ensures that security and compliance teams immediately become aware of issues so they can be fixed before data and cloud resources are compromised.

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

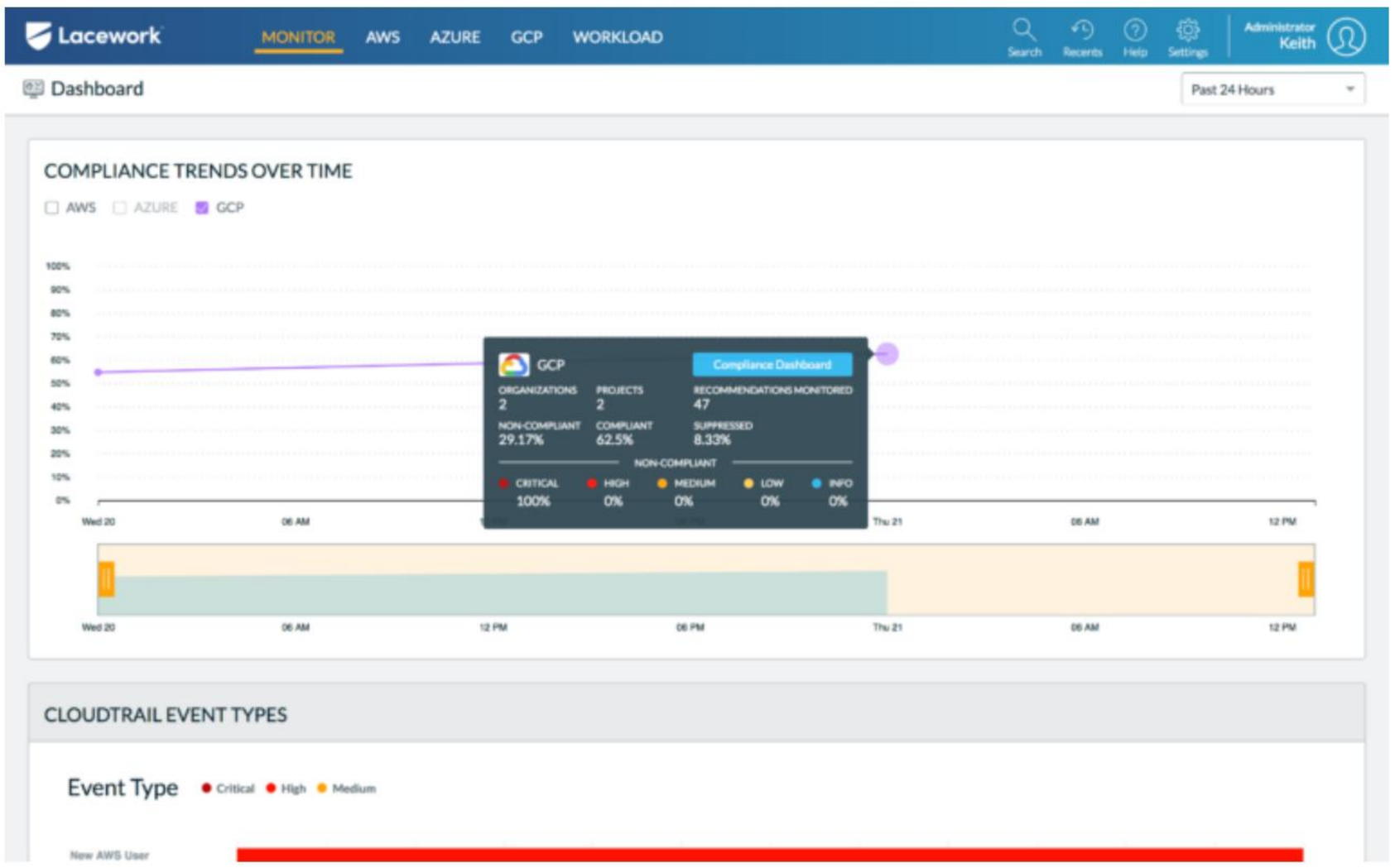


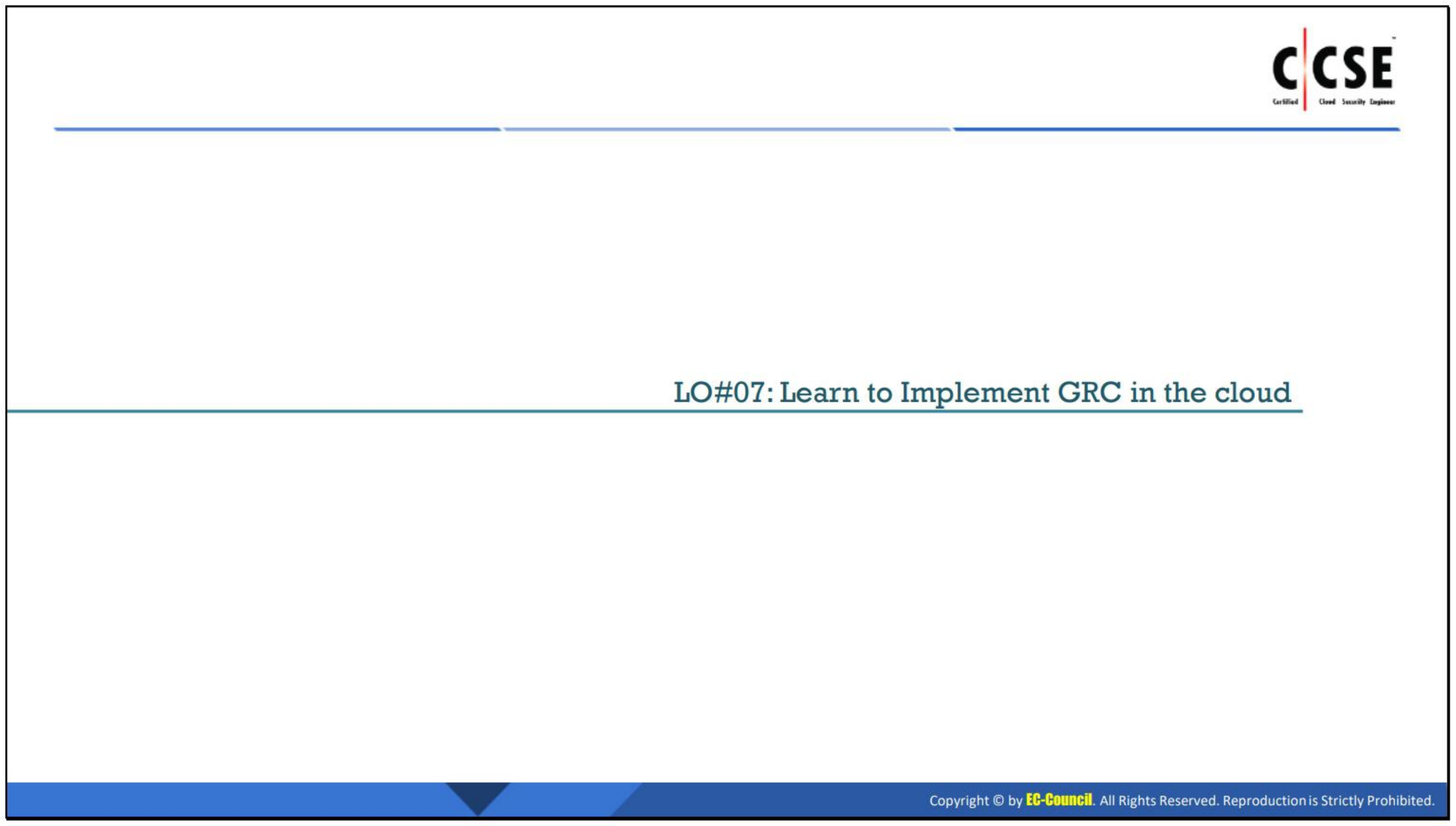
Figure 10.20: Lacework Dashboard

Configuration Compliance Management

Lacework checks across the industry-accepted CIS Benchmark for secure configurations for cloud accounts and workloads. Additionally, Lacework includes supplemental checks for common compliance frameworks like PCI-DSS, SOC 2, HIPAA, and others. Using Lacework, compliance and security teams have continuous analysis and historical reporting available so they can understand what is being checked, where problems exist, an analysis of the problem, and the steps needed to remediate the misconfiguration.

Lacework delivers deep visibility for configurations across all an enterprise's cloud accounts and workloads so organizations can ensure compliance with industry, governmental, and institutional standards. Operating on multiple cloud platforms can increase the threat vector of the overall infrastructure and add complexity to an already challenging task. Lacework operates as a comprehensive, centralized solution to identify, analyse, and alert on configuration issues.

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



LO#07: Learn to Implement GRC in the Cloud

The objective of this section is to teach the cloud security engineer the various considerations to implement the GRC in cloud.

hide01.ir

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

Considerations for an Effective IT GRC Cloud Program

- By leveraging the cloud, an organization can draw various **benefits** such as agility, cost, elasticity, and deployment of workloads within minutes

- At the time of migrating to the cloud, the organization faces many challenges, and one of the biggest challenges is to update the entire GRC program

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

Considerations for an Effective IT GRC Cloud Program (Cont'd)

hid001.ir

- **The important considerations for an effective IT GRC cloud program are as follows**

Security by design	The security-by-design framework offers the **automation** of security controls and streamlines the auditing process
Continuous control monitoring	It **operationalizes** the entire risk management effort and rationalizes the controls, compliance costs, changing regulations, rising risks, etc.
Organizational culture	Suitable organizational culture is required for GRC to thrive
Logging actions in the cloud	It simplifies audit preparation, minimizes the burden on control owners, and increases the efficiency of IT auditors

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.

Considerations for an Effective IT GRC Cloud Program (Cont'd)

Disaster recovery and business continuity	A BCDR solution should be developed as a part of GRC, and it should be designed to facilitate **operational continuity**, integrated IT risk management, industry-specific regulatory compliance, etc.
Vendor management	Vendor management helps in determining the **solution** to a business problems and then implementing the solution across the organization
Automated application performance management	Automated application performance management is very important as it allows the organization to provide a **seamless user experience**

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

Considerations for an Effective IT GRC Cloud Program

By leveraging the cloud, the organization can draw various benefits such as agility, cost, elasticity, deploying workloads within minutes, etc. At the time of migrating to the cloud, the organization faces many challenges, and one of the biggest challenges is to update the entire GRC program. The organization should have complete information about the important components and the associated risks, only then the organization can draw the benefits of cloud security and an efficient GRC framework. The important considerations for an effective IT GRC cloud program are as follows:

Security by Design

Security by design refers to a process in which the software engineer design secure software from the beginning to minimize the probability of flaws that would compromise the organization's information system. It aims to stop the cybersecurity breach and restore the system after an organization is a strike by a cybersecurity breach.

Security by design will make sure that the enterprise continuously manages, maintains, and monitors cybersecurity risk governance and management. Security by design is easily executed in the cloud environment. The cloud service provider (CSP) such as AWS is supporting security by design and validating it for cloud consumers. This approach allows the organization to design and automate its AWS ecosystem with robust security and governance. The techniques of security by design will expand the cybersecurity capabilities of an organization for real-time governance, risk, and compliance management.

The penetration testing in cloud and threat intelligence platforms helps in preventing the attack as well as identify the vulnerabilities in the system. A robust software will be designed by incorporating security, privacy, and compliance. Every organization should check that the

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

important information is masked when they are moving to a non-production environment where the security controls are inadequate.

Various organizations are adopting hybrid models of cloud (SaaS, private, etc.,) and on-premises. The ERP (enterprise resource planning) landscape has been changing at a rapid pace, which leads to new inherent risks that should be tackled by the controls framework. The control framework of an organization should be standardized across the organization regardless of the geography and support the organization to achieve compliance with legislation such as SOX, GDPR, etc. In ERP, the security by design should focus on continuous controls, the ERP is designed to meet regulatory compliance, accounting standards, and internal controls.

The security by design is cost-effective and provides various business benefits to the organization. The security by design framework offers automation of security controls and streamlines the auditing process.

Continuous Controls Monitoring

Continuous controls monitoring is a collection of technologies, which automate the process to minimize business losses and enhance the efficiency of the operation by continuously monitoring the business functions. It will minimize the cost of audits by continuously auditing the controls. Continuous control monitoring is implemented across the organization. In financial services, continuous control monitoring exists in the form of financial transaction monitoring or fraud monitoring. In technology, continuous control monitoring exists in the form of network security and cybersecurity monitoring.

hire01.ir

Continuous control monitoring is an important part of GRC, which supports an organization in improving risk management. It helps an organization to monitor Governance, Risks, and Compliance.

Due to the increase in the complexities of compliance and risk management, the organization should operationalize the entire risk management effort. Apart from this, the organization needs to rationalize the various overlapping and duplicated controls. Continuous control monitoring takes care of operationalizing the entire risk management effort, rationalize the controls, compliance costs, changing regulations, rising risks, etc.

Enforcing continuous control monitoring requires identification of controls or processes as per the applicable industry control frameworks like COBIT 5, ITIL, etc. At this point, the key control prioritization for continuous monitoring takes place. After this, goals or control objectives are defined. This is followed by the building of specific automated tests or metrics, then the process frequency is determined. At this juncture of time, the process for handling the alarms, rectifying the control weakness, investigation, and communicating are required.

For regulatory control monitoring as well as financial monitoring, continuous control monitoring delivers a modern, optimized, and automated framework. Continuous control monitoring will make an effective control environment.

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

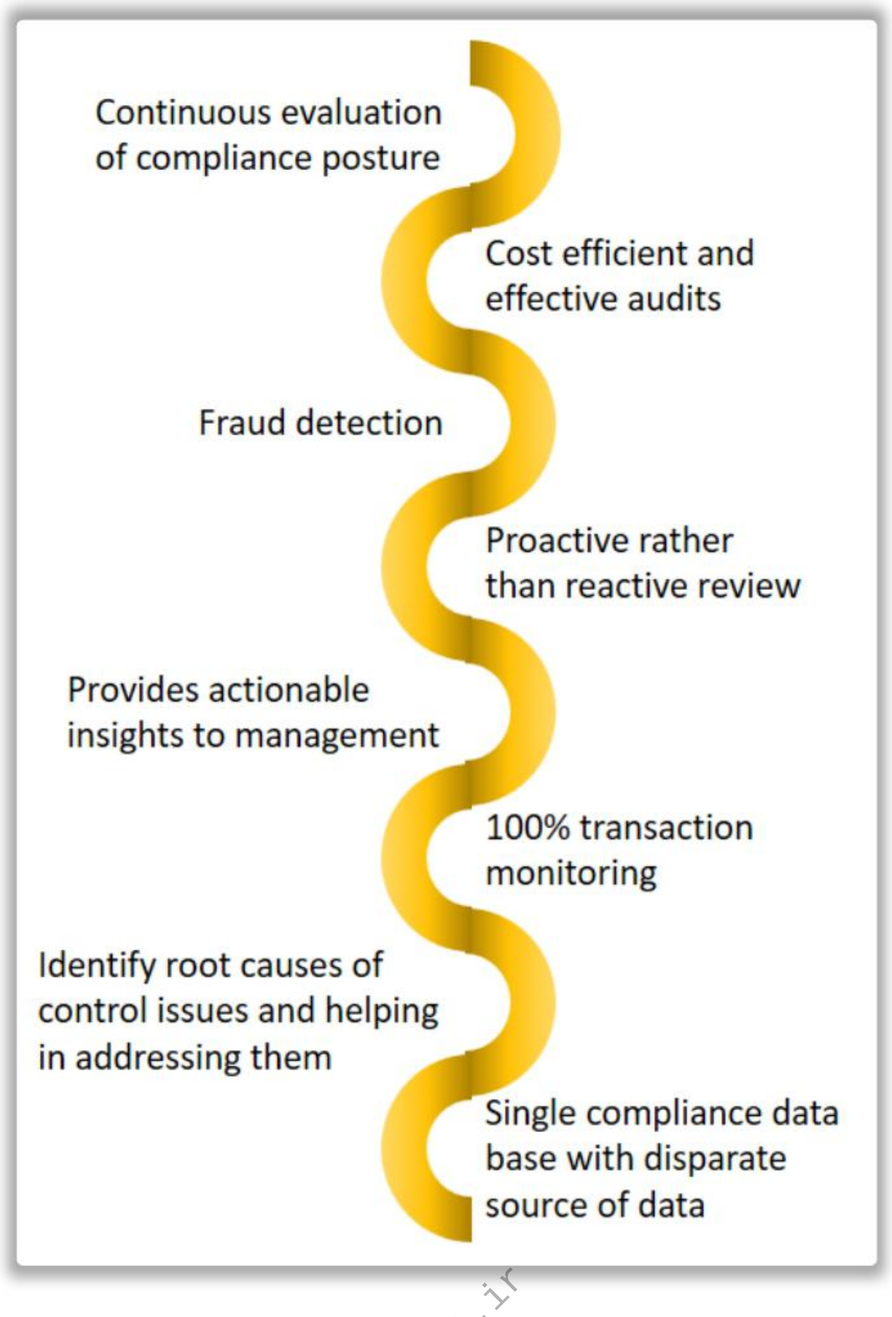


Figure 10.21: Continuous Control Monitoring

Continuous control monitoring allows an organization to continuously evaluate the compliance posture, perform cost-effective and efficient audits, detection of fraud, proactive review, offers actionable insights into managements, complete transaction monitoring, determine the cause of control issue and support in resolving them, provide single compliance database with separate sources of data.

Organizational Culture

The culture of an organization will play a significant role in the successful utilization of the cloud. Every risk cannot be fully mitigated; therefore, it is necessary to understand the organization's risk tolerance.

GRC increases the compliance levels, improves risk management, and delivers robust governance, but it requires an appropriate organizational culture to thrive. Some organizations observe very little improvement after implementing GRC, whereas other organizations find a lot of improvement after GRC implementation. This is due to differences in organizational culture.

If the employees of an organization are not utilizing or implementing the GRC technology, then the management should identify the reason why the employees are not enforcing GRC technology. Based on the organization and various factors, the result can vary. Most of the organizations could find that the issue is related to the knowledge of the technology. The maximum number of employees are not able to implement new technology, and they do not reveal it, as they are uncomfortable in admitting their inability to understand the new

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

technology. This issue can be resolved easily. If an organization is enforcing a GRC tool, then the organization should provide guides to the employees so that they can utilize it.

Provide training materials to the employees, so that the employee can refer to the training material if they face any issue. The organization should allow the employee to provide their feedback and convey their ideas so that the organization can modify the GRC solution, which enhance the efficiency and productivity.

While creating a suitable culture for GRC, the organization should remember that the culture cannot be enforced. GRC is a new approach to manage governance, risk, and compliance. The major enforcement issue is that it only works under monitoring or supervision. The employees will make the same mistakes if they are not monitored. Culture will consume a significant amount of time for formation, but it will lead to compliance with no need for monitoring or supervision.

If the organization wants the employees to interact efficiently with the new technology, then the organization should focus on its culture. The organization should provide appropriate environments, training, materials to the employees, then they will become more efficient and would not hesitate to implement new technology such as GRC.

Logging Actions in the Cloud

The actions that are performed by the organization in the cloud should be logged. It will provide a comprehensive view and an insight into all the activities that were performed by the organization in the cloud environment. It will simplify the audit preparation, minimizes the burden on control owners, and increase the efficiency of IT auditors.

hi101.ir

Disaster Recovery and Business Continuity

The cloud vendor should provide business continuity and disaster recovery provision to the cloud consumer. Few cloud vendors did not provide data backup services, the customer must contact another vendor for backup service or internally make an arrangement for data backup. Apart from this, the cloud service is proprietary to the cloud vendor. In case, the data is backed up, the value could be lost if the particular cloud service is unavailable. BCDR solution should be developed as a part of GRC, and it should be designed to facilitate operational continuity, integrated IT risk management, industry specific regulatory compliance, etc.

Vendor Management

Every vendor state that they are transparent and are perfect in providing robust cloud services, but most of them did not do the customers' jobs with the customer resources and tools. Vendor management helps in finding out the solution to resolve business problem, then implement the solution across the organization. Various questions are essential for an IT auditor to ask such as

- Where is the data?
- Who can see the data?
- Is the data untampered?

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

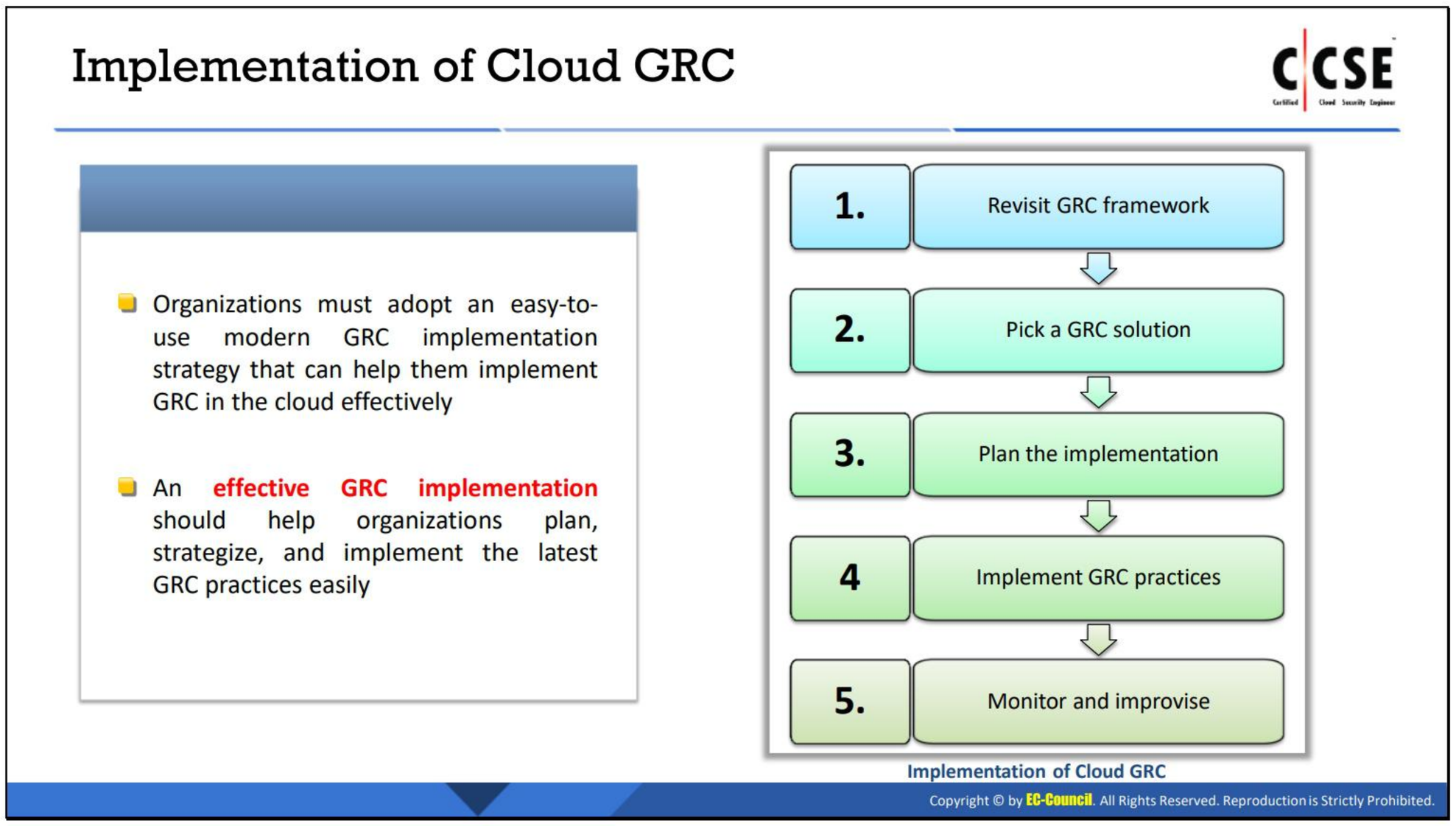
Apart from the above questions, many questions are specific to the business model of the organization.

Automated Application Performance Management

Application performance management is the process of managing the user experience, availability, and performance of an application. The technology and operation department should monitor the metrics that are aligned with the established SLA. Cloud performance management is offered by various cloud vendors to the cloud consumer. Automated application performance management is very important as it allows the organization to provide a seamless user experience. If the user is experiencing issues with logins, this would impact the revenue of the organization.

hide01.ir

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



Implementation of Cloud GRC

Organizations must adopt an easy-to-use modern GRC implementation strategy that can help them implement GRC in the cloud effectively. An effective GRC implementation should help organizations to easily plan, strategize, and implement the latest GRC practices. Consider the following steps for an effective GRC implementation in an organization:

- **Revisit/review the GRC Framework**

  Review the existing GRC framework and identify the technology gaps that must be filled. This may require redefining what GRC means for the organization. Have a clear understanding of the organization's key business objectives and business processes because this will help in choosing the right technology and create appropriate policies, guidelines, procedures for the business.

- **Select a GRC Solution**

  Choosing an ideal GRC solution and the right implementation partner for the organization is essential for the effective functioning of the GRC initiative. There are several cloud-based GRC tools/solutions and multiple vendors available in the market. For example, RSA Archer, Riskonnect, BWise, etc., are some of the popular GRC products. Choose a solution that meets all the features and requirements that you want after doing thorough research. Ensure that you select an experienced vendor that can implement GRC in the cloud environment within an acceptable period with optimal efficiency.

- **Project Planning**

  This step involving creating a suitable GRC implementation plan. The cloud vendor sends a project manager or business analyst to your organization to understand the business

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

processes and policies. A risk assessment is also conducted to identify the areas that should be protected. Based on the results, the analyst or manager develops an integrated GRC plan that suits the most to the organization. They provide a detailed demonstration of the chosen GRC product, assign roles and responsibilities and define timelines for the project.

- **Implement GRC Practices**

  Implement GRC practices in the organization after the development of the GRC plan. Most GRC programs are automated and cloud-driven and their implementation involve operational risk management, policy and document management, corporate compliance management, and IT risk management. Creating awareness about the newly implemented GRC policies and training employees to practice are part of the GRC implementation program because they are essential for the success of GRC implementation.

- **Monitor and Improvise**

  Implementing a GRC program is a continuous business practice that needs to be followed daily across all departments. To ensure its success, monitor and ensure that GRC practices are followed diligently inside the organization. Due to the dynamic nature of the business world, it is essential to modernize the GRC platform and periodically revise GRC policies to meet business, industry, and regulatory requirements.

Steps to Plan/update a GRC Initiative

hode01.ir

Organizations must follow these tips to plan/optimize their GRC program:

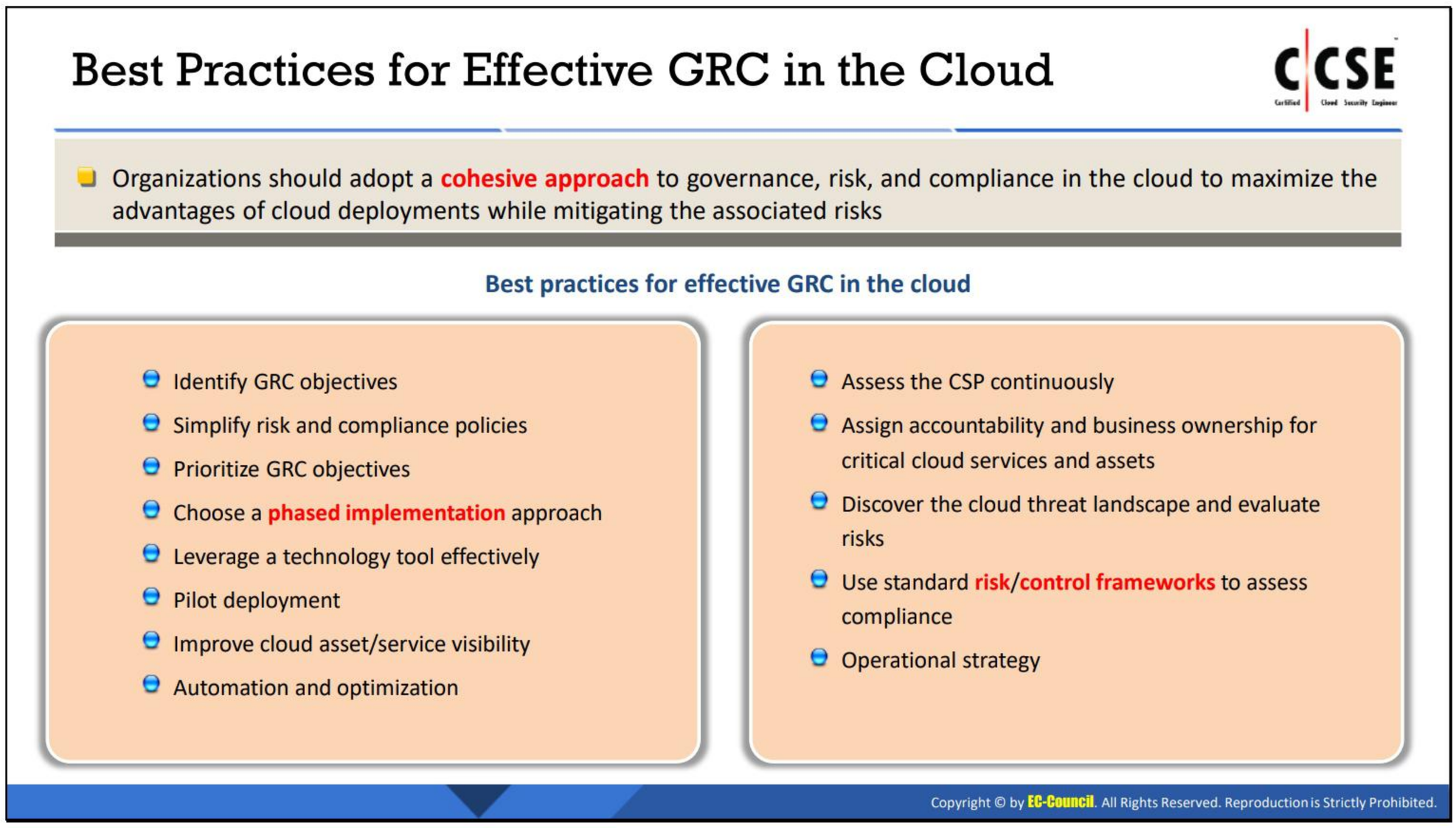
- Get full support from the senior management in this initiative.
- Develop a detailed GRC program, addressing all three components (governance, risk, and compliance) in a simple, easy-to-understand framework.
- Examine the present GRC environment carefully to identify areas for improvement.
- Set up a budget and save money for the program.
- Select individuals/professionals to join the team and prefer those with certifications.
- Understand the business objectives and goals of the organization from multiple perspectives (e.g., competitive position, financial, reputation, etc.).
- Identify and map all GRC factors that apply to the organization directly.
- Brief senior management on program findings and recommendations periodically.
- Ensure all team members have the same understanding of overall goals and objectives by having regular meetings.
- Have training and education sessions for management and employees on GRC activities.
- Conduct reviews and audits periodically to ensure that everything is working as intended.

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

- Look for ways to continually improve the GRC function by leveraging automated GRC software tools that can help streamline functions.

hide01.ir

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



Best Practices for Effective GRC in Cloud

Organizations should adopt a cohesive approach to governance, risk, and compliance in the cloud to maximize the advantages of cloud deployments while mitigating the associated risks. Following are some best practices for effective GRC in the cloud:

- **Identify GRC Objectives**: Design your business processes and set GRC objectives and goals. Then, choose the technology that can help you meet those goals.
- **Simplify Risk and Compliance Policies**: Ensure that risk and compliance policies are simple and easily understandable for all staff in your organization. Policies must be written in a way that employees can utilize them effectively. Keep the policies in a central location, making them accessible for everyone. Also, communicate policies across the organization and make sure that employees understand them well and know how to follow them.
- **Prioritize GRC Objectives**: Prioritizing GRC objectives is most important after defining the objectives. Identify the key objectives and ensure that they are addressed first followed by other objectives.
- **Choose a Phased Implementation Approach**: Ensure that the GRC implementation is done in a phased manner. Opting for a phased implementation approach helps organizations to achieve GRC goals easily.
- **Leverage a Technology Tool Effectively**: Before using tools for GRC implementation, evaluate them to identify whether they meet your GRC objectives and goals or not. This helps in selecting tools that facilitate faster GRC implementation. Generally, tools are selected depending on the ease of deployment, cloud presence, intuitive end-user interface, and ease of upgrades.

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

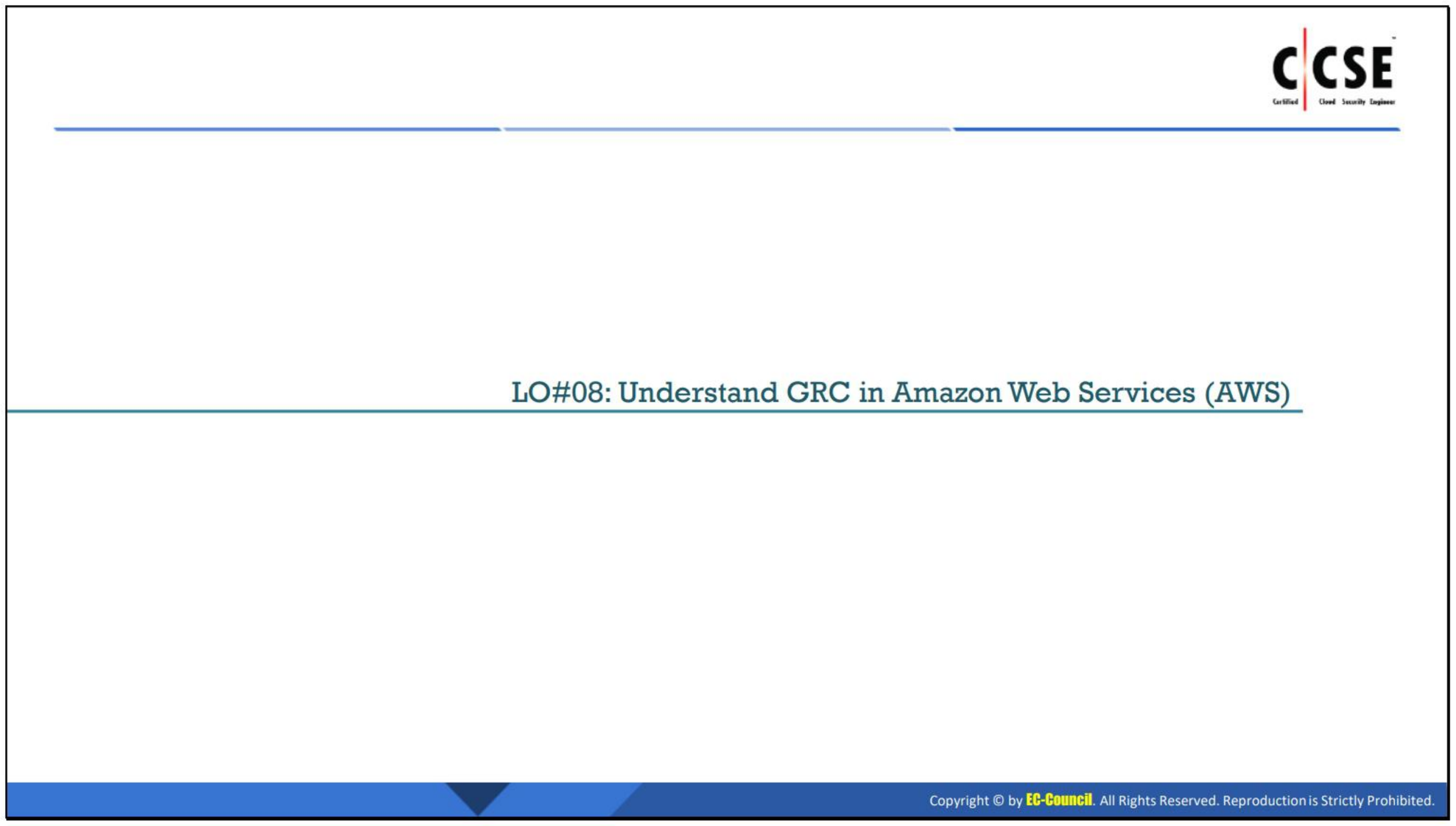
- **Pilot Deployment**: Measure the effectiveness of the deployment by setting up and configuring your initial use cases via the selected tools. Validate the deployment against the success criteria to know how effective it is.
- **Improve Cloud Asset/Service Visibility**: Understand the scope of cloud services used inside the organization and get visibility into the entire cloud environment. IT and infrastructure managers need to know about all processes that are running on cloud deployments, assets supporting them, and their ownership inside the organization. A well-defined policy should be adopted by organizations to deploy, manage, and run cloud applications and classify the data stored in them as per its sensitivity to ensure that sufficient controls are put in place to manage data effectively.
- **Assess the CSP Continuously**: Select a CSP that shows validation of security controls. This includes validating physical data center security, network security, and a standard audit framework that complies with the applicable regulatory standards. Organizations must ensure due diligence by establishing a due-diligence framework to evaluate the CSP's performance regularly to gain a complete understanding of the cloud environment.
- **Assign Accountability and Business Ownership for Critical Cloud Services and Assets**: Document all cloud assets, policies, business objectives, and business processes along with their operational relationships. Ensure that these policies and processes are accountable and explicitly assigned, and well-understood throughout the organization. Establishing accountability is essential when customer information is intertwined with the CSP's information. This includes defining SLAs, logical separation of data sets from other users/customers' data sets, and classifying the services consumed.
- **Discover the Cloud Threat Landscape and Evaluate Risks**: The organization should understand the cloud threat landscape, evaluate risks, and mitigate them effectively to protect it and its interested parties from being exposed. It should be always alert and aware of the latest developments because threats are evolving. This will help it to be prepared for security threats in the cloud.
- **Use Standard Risk/Control Frameworks to Assess Compliance**: Evaluate cloud compliance with regard to the organizational security, policies, and privacy practices. There are various risk frameworks available such as ISO/IEC 27017, NIST's Framework for Improving Critical Infrastructure Cybersecurity, CSA's GRC stack, etc. Use a standard risk/control framework that suits best for your organization to assess compliance.
- **Operational Strategy**: A GRC program needs to be evolved/updated continuously because the threats and risks faced by the organization change over time. Define an operational strategy around the program in the beginning stage so that a continuous feedback and improvement loop can be developed. Appoint a risk committee that can meet regularly to offer governance and oversight and suggest refinements for policy framework and risk definitions. Constitute a dedicated operations team that is responsible for initiating audit cycles, monitoring risks, and providing feedback and adequate reports to executives on your program's effectiveness.

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

- **Automation and Optimization**: The organization must use automation for a GRC program implementation. Using automation moves it towards proactive risk management.

hide01.ir

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

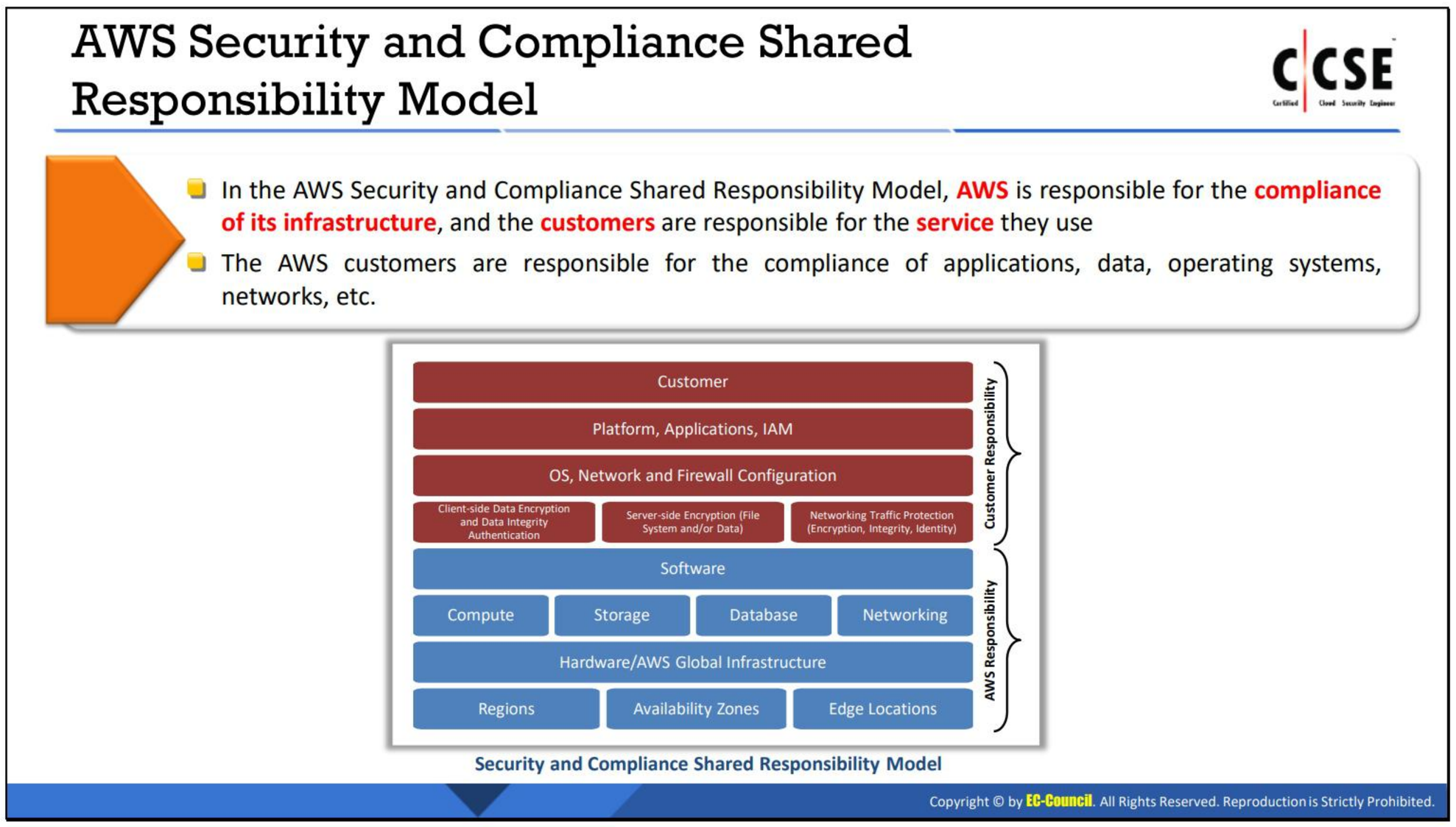


LO#08: Understand GRC in Amazon Web Services (AWS)

The objective of this section is to provide a overview of GRC features in AWS. Tt shows implementation of various GRC functionality with AWS tools and resources.

hide01.ir

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



Security and Compliance Shared Responsibility Model

AWS Security and Compliance Shared Responsibility Model

AWS Cloud Compliance makes the cloud users understand the controls in AWS that can be used for protecting the data and security in the cloud. In terms of compliance, both customers and AWS share the responsibilities. The responsibilities of the customers are based on the service they use. The customers are responsible for developing their environment according to the organization's security and compliance requirements.

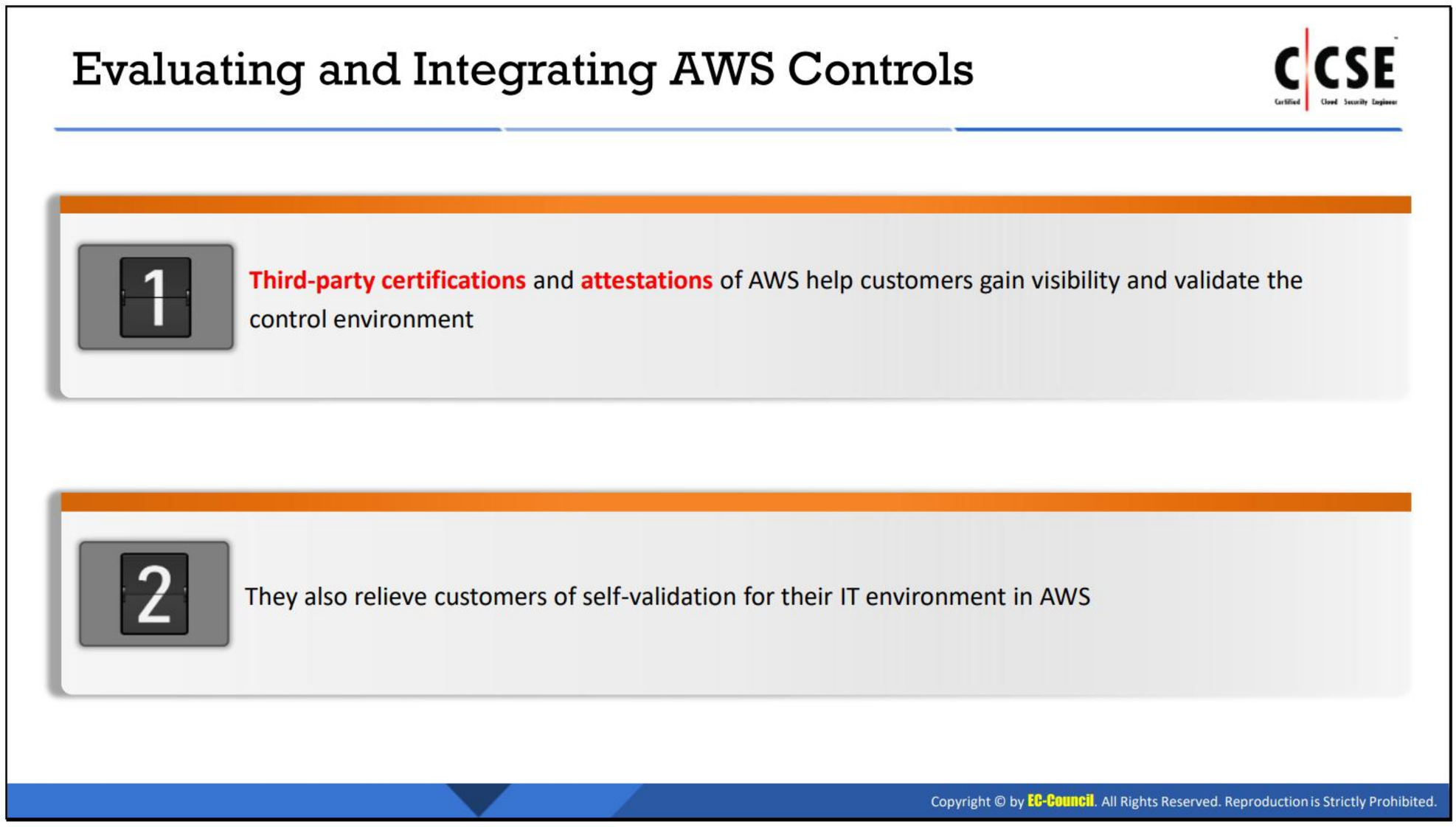
AWS provides the IT infrastructure to its customers by following the best practices and through IT security standards. AWS complies with the following assurance programs:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

AWS is responsible for the compliance of its infrastructure. The users are responsible for the compliance of applications, data, operating systems, and networks. Customers need to select the AWS services carefully because the responsibility changes as per the services integration into the IT environment and application laws. Customers can use host-based encryption, host-based firewalls, and intrusion detection to meet their complex compliance requirements.

The shared responsibility also offers flexibility and customer control to allow customers to deploy the infrastructure as per their industry-specific certification requirements. The shared responsibility also applies to IT controls. The management, operation, and verification of IT controls are shared between AWS and its customers. AWS manages controls related to deployed infrastructure in AWS. Using compliance and control documentation, customers can conduct evaluation and verification procedures.

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



Evaluating and Integrating AWS Controls

AWS provides information related to the IT controls using technical papers, certifications, reports, and any other third-party attestations.

hide01.ir

In general, the design and operational effectiveness of the controls are validated by the internal or external auditors using process walkthroughs and evidence evaluation. This type of evaluation is used to validate controls in traditional on-premises environments, whereas in AWS, customers can make a request for third-party attestations and certifications for evaluating them. The certifications and attestations assure customers about the design and effectiveness of controls validated by the third parties. With this, the controls environment becomes a unified framework where customers can ensure that the controls are working effectively.

Customers get the visibility and validation of the control environment through the third-party attestations and certifications of AWS. Customers also get relief from performing their own validation for organization's IT environment in AWS using both third-party attestations and certifications of AWS.

Following are some ways that provide the IT control information to the customers of AWS:

- **Specific Control Definition:** Key controls need external attestation of the effectiveness of the key controls. They are important for the control environment of the customer. External attestation is needed to ensure whether the key controls are aligned with the requirements of compliance (e.g., annual financial audit). For this reason, a huge range of IT controls are published by AWS in Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report is developed by the American Institute of Certified Public Accountants (AICPA) which is a recognized auditing standard. Formerly, the SOC1 report

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

is referred as Statement on Auditing Standards (SAS) No. 70, Service Organizations report, and commonly known as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report. The SOC1 audit comprises audit of the design and operating effectiveness of control objectives and control activities defined by AWS. Also, the SOC 1 Type II report indicates described controls from the report are tested for operating effectiveness by an external auditor.

AWS control environment should provide high levels of confidence to the controls described in the report due to the competence of the AWS external auditor. AWS controls can operate effectively for various compliance purposes such as Sarbanes-Oxley (SOX) Section 404 financial statement audits.

There are certain other specific control activities that relate to AWS Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance. PCI and FISMA standards need independent validation.

- **General Control Standard Compliance:** AWS' industry certifications may be evaluated if an AWS customer needs to meet a huge set of control objectives. Using AWS ISO 27001 certification, AWS follows best practices to maintain a secure environment and complies with a broad comprehensive security standard. AWS complies with the needed controls for organizations that process credit card information with Payment Card Industry Data Security Standard (PCI DSS).

  With FISMA standards, AWS compliance complies with the needed controls by US government agencies. Customers can know the information about the security process' nature and controls with that complying with general standards.

vid01.ir

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

AWS Risk and Compliance Program

- AWS integrated the risk and compliance program to **control risk** in every design and deployment phase and reevaluate the risk-related activities of the organization

Components of AWS Integrated Risk and Compliance Program

- **AWS Business Risk Management (BRM):** The BRM program identifies risks and implements controls to manage risks
- **Operational and business management:** AWS reviews **operational metrics** in weekly meetings and identifies risks before they affect business operations

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

AWS Risk and Compliance Program (Cont'd)

hide01.ir

- **AWS control environment and automation:** It includes standards, processes, and structures to guide customers for implementing **minimal security controls** in the AWS environment. It ensures the secure delivery of AWS services to its customers
- **Controls assessment and continuous monitoring**: **Review** of the AWS application security risk management, ongoing vulnerability management scanning, etc. help customers build a compliant solution on AWS services
- **AWS programs, certifications, reports, and third-party attestations:** These ensure that the control activities are operating as intended

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

AWS Risk and Compliance Program

AWS integrated the Risk and Compliance program to manage the risk in all design and deployment phases and reassesses the risk-related activities of the organization. It helps customers to build and operate in the AWS security control environment. AWS helps its customers to incorporate AWS controls into their governance framework by providing risk and compliance program information to its customers. The various components of AWS integrated risk and compliance programs are as follows:

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

AWS Business Risk Management

The AWS Business Risk Management (BRM) program partners with AWS business units to provide key risks in AWS environment to AWS Board of Directors and AWS senior leaders. This program conducts risk assessments and risk monitoring for the AWS functional areas. The BRM program identifies risks and implements controls to manage risks. Apart from this, known risks register is being maintained by this program.

To remediate the risks, the BRM program sends the reports of its efforts to the organization's vice presidents and directors for business decision-making.

Operational and Business Management

AWS makes use of weekly, monthly, quarterly reports for the communication of risks in all components of the risk management process. It also uses an escalation process to provide information to management about high-priority risks in the organization. All these things ensure that risk is consistently managed.

The business owners are responsible for the oversight of their business through a cascading responsibility structure. AWS reviews operational metrics in weekly meetings and identifies risks before it affects the business operations.

To establish AWS core values, executives, and senior leadership play an important role. Each employee receives the company's Code of Business Conduct and Ethics. AWS conducts complete periodic training for its employees. Compliance audits are performed on regular basis to help employees understand and follow the policies.

The organizational structure of AWS provides a framework to plan, execute, control, and handle business operations. The organization structure provides roles and responsibilities for adequate staffing, segregation of duties, and operations efficiency. Management also has appropriate ways for reporting key personnel. The company's verification processes for hiring include verification of education and previous work experience. In some cases, background checks are also permitted by the law and regulation to understand the abilities of the employee for the offered position. The company follows an on-boarding process for new employees to make them familiar with the AWS tools, processes, policies, and procedures.

AWS Control Environment and Automation

AWS implements various security controls such as policies, processes, and control activities to handle risks in the organization. The control environment of AWS includes standards, processes, and structures to guide customers for implementing minimal security controls in the AWS environment. The control environment ensures the secure delivery of AWS services to its customers.

The control environment includes people, processes, and required technology to establish an environment that supports AWS controlled framework. AWS also integrates required cloud-specific controls into the AWS environment. AWS assists its customers to manage their control environment by monitoring the industry groups.

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

Control automation helps AWS to reduce human intervention in case of recurring processes. It is the best way for implementing effective security control and associated risk management. Control automation focuses on reducing the inconsistencies in process execution caused by humans while conducting a repetitive process. It also eliminates process deviations and assures that the controls are applied as designed. Engineering teams at AWS are responsible for developing an AWS control environment that supports a higher degree of control automation.

Controls Assessment and Continuous Monitoring

AWS controls assessment and continuous monitoring strengthen the security team in safeguarding AWS services and application against the threat. AWS implements various activities before and after a service deployment to reduce the risks in the AWS environment. The activities integrate all the compliance and security requirements during the design of each AWS service. The activities also validate if the services are operating well and securely after moving them into production.

The activities in terms of risk and compliance include both pre-launch activities and post-launch activities. The pre-launch activities include:

- Review of the AWS Application Security risk management in order to confirm that the security risks are detected and alleviated.
- Review Architecture readiness to help customers in ensuring alignment with compliance rules.

During the deployment, each AWS service undergoes various assessments against security requirements to meet AWS high levels of security.

The post-launch activities include:

- AWS Application Security ongoing review helps to ensure that a security posture is maintained for each service.
- Ongoing vulnerability management scanning

All the above control assessments help customers to build a compliant solution on AWS services.

AWS Certifications, Programs, Reports, and Third-Party Attestations

To ensure that the control activities are operating as designed, AWS regularly undergoes various third-party attestation audits. AWS is audited against various global and regional security frameworks. It participates in almost 50 different audit programs.

The audit results are documented and are made available to all the customers through AWS Artifact. AWS Artifact is a self-service and central resource portal that contains AWS compliance reports. All the new reports are added to the AWS Artifact and customers can monitor the AWS security and compliance by accessing the new reports.

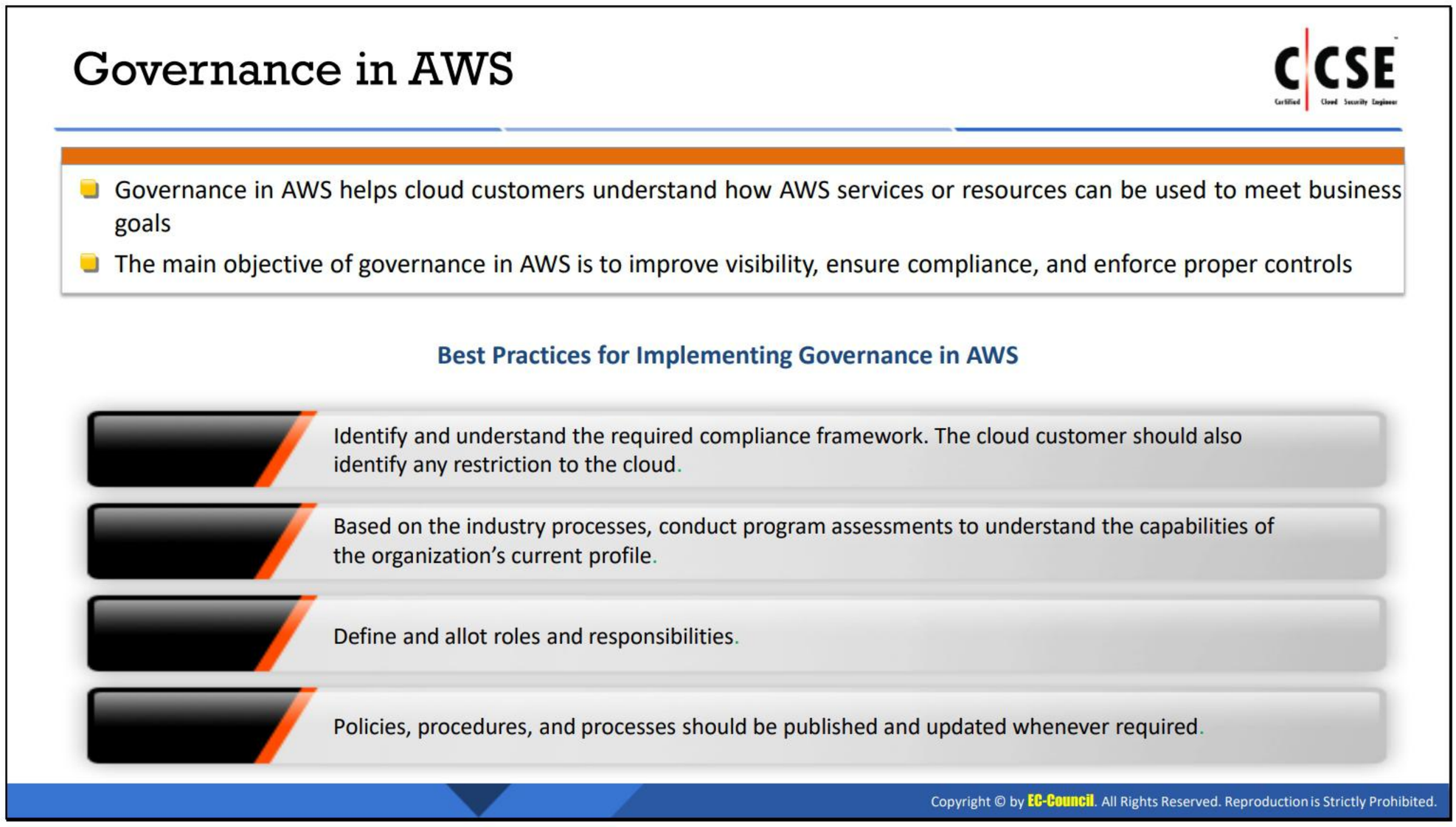
AWS may undergo audits with customers or governmental auditors based on a country's or an industry's regulatory requirements. All these audits provide additional supervision of the AWS

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

cloud environment. The audits also ensure that the customers have enough tools to operate in a confident and compliant manner using AWS services.

hide01.ir

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



Governance in AWS

Governance in AWS helps cloud customers to understand how AWS services or resources can be used to meet the business goals. It also focuses on controlling the costs and risks and improving efficiency. Governance includes people, processes, and technology related to AWS infrastructure. Enforcing governance in the AWS cloud is difficult due to the decentralized cloud environment. Hence, effective governance is essential to ensure that there are controls over cost, security, and performance.

The main objective of governance in AWS is to improve visibility, ensure compliance, and enforce proper controls. Apart from this, AWS governance also focuses on protecting from potential events that impact operations, security, and finance. By covering every aspect of AWS cloud activities in governance helps for the effective implementation of governance. Best practices are implemented based on the business assets, performance analysis against cost, and addressing risks.

The following are some of the best practices for implementing governance in AWS:

- **Define a Governance Strategy**

  For a successful implementation of governance in AWS, the end-users should have a governance strategy. The governance strategy includes choosing a framework and selecting stakeholders. A governance framework refers to a set of IT principles for managing and controlling the organization. Stakeholders are the people who are responsible for implementing a governance framework to reduce the risks in business.

- **Identify and Understand the Compliance Requirements**

  It is important to identify and understand the organization's compliance requirements. It is impossible to create a framework needed for compliance without understanding

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

the compliance requirements. Required compliance frameworks such as HIPAA and other contract or agreement obligations should be identified.

The cloud customers should also identify any restrictions to the cloud. The required and chosen standards such as NIST, ISO, COBIT, CSA need to be identified.

- **Perform Program Assessments**

  Based on the industry processes such as NIST Cyber Security Framework (CSF), program assessments should be conducted to understand the capabilities of the organization's current profile. The target profile which is the desired end state should be determined and a CCoE (Cloud Center of Excellence) team must be built. To allocate resources, gaps such as people, processes, and technology should be prioritized and documented. A cloud strategy including procurement, security, and management should be drafted and published. And finally, roles and responsibilities need to be defined and assigned to people.

- **Publish and Update Policies, Processes, and Procedures**

  Based on the objectives and desired capabilities, the cloud customers need to update the policies to align them with the business goals. The processes pertaining to modern organization and management techniques should be updated and should mention how to upgrade to old technologies. To integrate with the cloud services and other new emerging technologies, the procedures need to be updated. Technical governance standards should also be established for choosing the controls to monitor compliance.

hide01.ir

- **Use Global Tagging Policy**

  To allocate costs and identify trends, each resource can be tagged. A global tagging policy can be enforced to analyze costs and performance.

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

Steps to Implement Governance in AWS

The following are the steps to implement governance in AWS.

Define

- The cloud customer should define the provisioning and configuration of AWS resources. This can be achieved using CloudFormation and AWS Service Catalog
  - **CloudFormation**: CloudFormation is a service that can be used by cloud customers to describe and provision AWS infrastructure resources to the cloud environment
  - **AWS Service Catalog**: AWS Service Catalog helps in creating and managing catalogs of IT services . Using Service Catalog, deployed IT services can be centrally managed



CloudFormation AWS Service Catalog

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

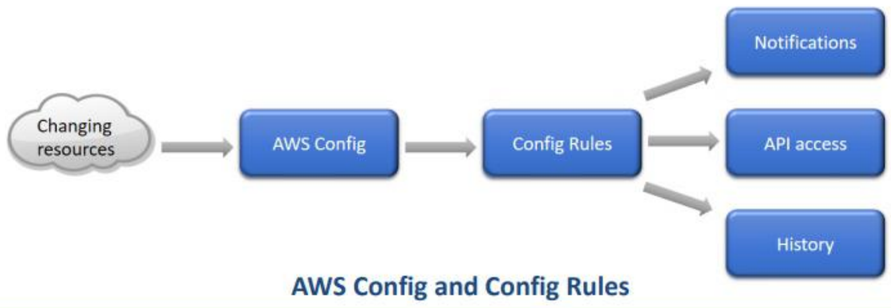
Steps to Implement Governance in AWS (Cont'd)

Discover and Monitor

- In this step, the cloud user must continuously discover new resources and changes to existing resources. The resources and operations should be monitored for compliance
- AWS CloudTrail, AWS Config and Config Rules, and EC2 Systems Manager can be used for discovering and monitoring resources
  - **CloudTrail:** CloudTrail increases the visibility of user activities and resource activities
  - **AWS Config and Config Rules:** It is a continuous assessment and recording service that helps cloud users assess, evaluate, and audit the configuration of AWS services
  - **EC2 Systems Manager – Inventory and State Manager:** It helps view and control the AWS cloud infrastructure



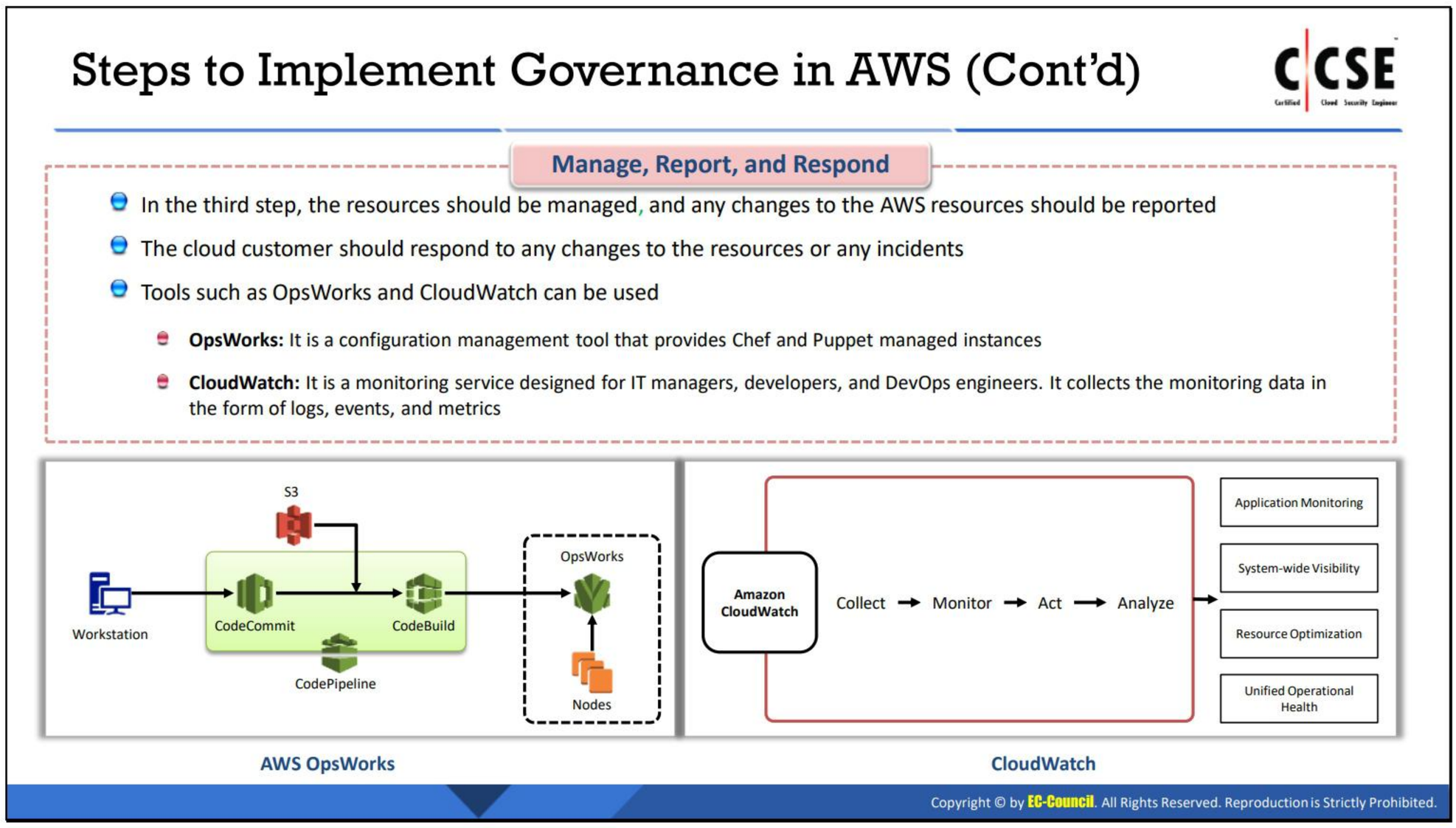
CloudTrail



AWS Config and Config Rules

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.



Steps to Implement Governance in AWS

The following are the steps for implementing Governance in AWS:

- Define
- Discover and Monitor Resources
- Manage, Report, and Respond

hide01.ir

Define

The cloud customer should define the provisioning and configuration of AWS resources. This can be implemented using CloudFormation and AWS Service Catalog.

- **CloudFormation:** CloudFormation is a service that can be used by cloud customers to describe and provision AWS infrastructure resources to the cloud environment. A cloud user can describe resources using a CloudFormation template. The template can be written in JSON or YAML to describe what resources need to be created and configured. All the required resources can be launched and configured as a stack using a template. Using the template, the cloud customer can delete, update, or create an entire stack as a single unit. Third-party application resources can also be provisioned along with the AWS resources using CloudFormation Registry.

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

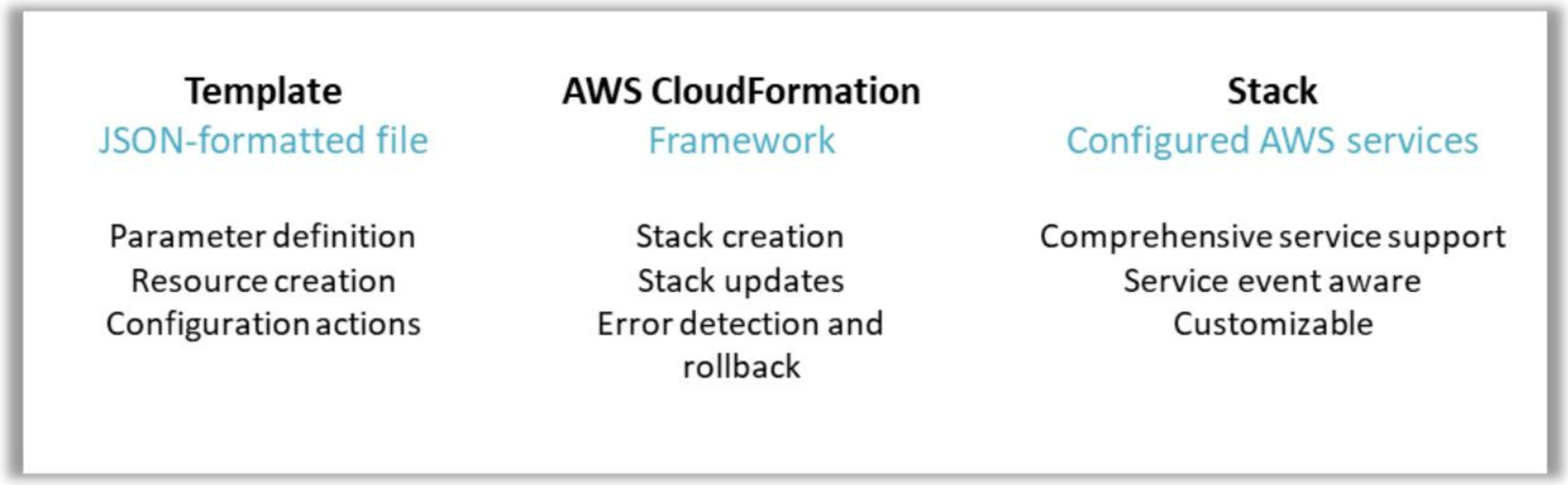


Figure 10.22: CloudFormation

- **AWS Service Catalog:** AWS Service Catalog allows creating and managing the catalogs of IT services. The IT services include everything from virtual machines, software, and databases. Using Service Catalog, deployed IT services can be centrally managed. This helps to meet the compliance requirements and achieve governance while allowing the users to deploy the approved IT resources. The applications and their metadata can be managed to track security and compliance at the application level.

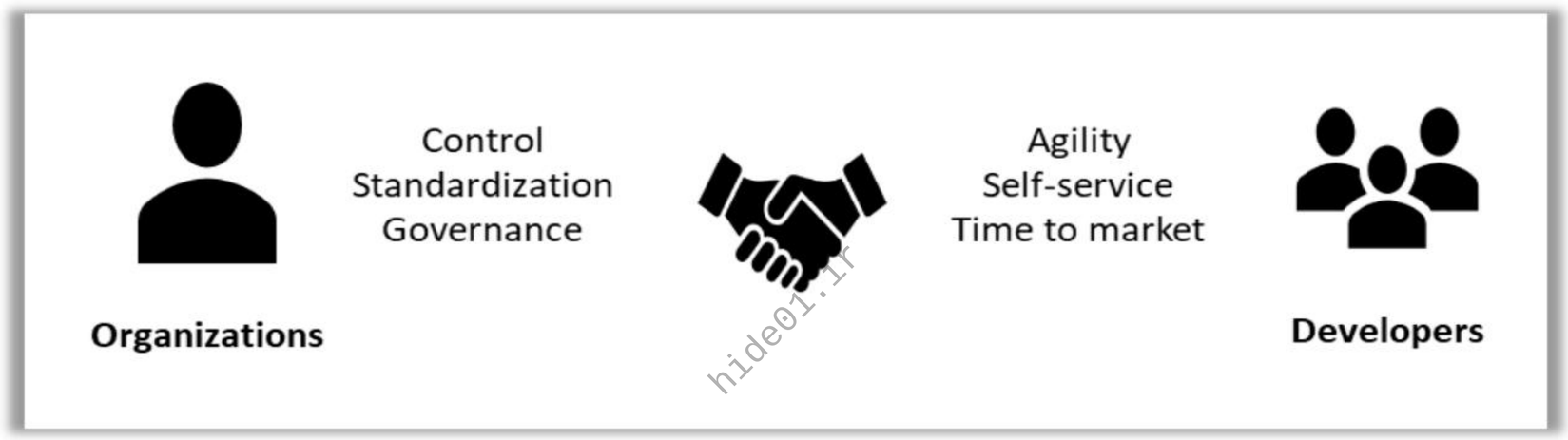


Figure 10.23: AWS Service Catalog

Discover and Monitor

In this step, the cloud user needs to continuously discover new resources and changes in the existing resources. The resources and operations should be monitored for compliance. AWS CloudTrail, AWS Config and Config Rules, and EC2 Systems Manager can be used for discovering and monitoring resources.

- **CloudTrail:** CloudTrail increases the visibility of user activities and resource activities. It provides the history of an AWS account activity. It also provides a history of actions performed through console CLI (Command Line Interface), AWS SDKs, etc. It enables governance, compliance, operational, and risk auditing for an AWS account. It helps to continuously monitor the account activity. Compliance can be simplified by automatically recording and saving the actions performed within the AWS account.

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



Figure 10.24: CloudTrail

- **AWS Config and Config Rules:** It is a continuous assessment and recording service. It helps the cloud users to assess, evaluate, and audit the configuration of AWS services. It can be done using Config rules to represent the organization's ideal configuration settings. AWS Config offers customizable and pre-defined rules. AWS Config tracks changes to the AWS resources and alerts when the changes are not compliant with the rules. This simplifies the compliance auditing and security analysis.

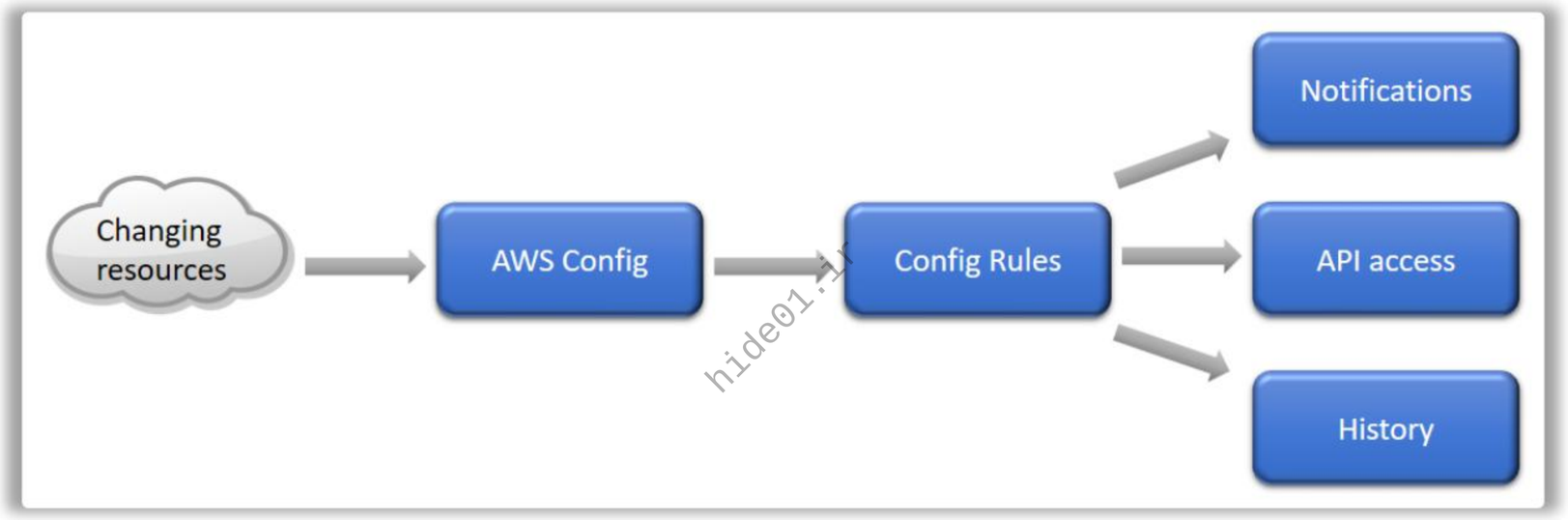


Figure 10.25: AWS Config and Config Rules

- **EC2 Systems Manager - Inventory and State Manager:** It helps to view and control the infrastructure on the AWS cloud. The Inventory provides visibility of the software catalog and configurations of EC2 instances and on-premises environment. State Manager can be used to define and maintain the configurations of applications running on AWS or on-premises. The policies can be reapplied on a defined schedule such as OS changes, local users, and permissions.

Manage, Report, and Respond

In the third step, the resources should be managed and any changes to the AWS resources should be reported. The cloud customer should respond to any changes to the resources or any incidents. Tools such as OpsWorks and CloudWatch can be used.

- **OpsWorks:** It is a configuration management tool that provides Chef and Puppet managed instances. With OpsWorks, Chef and Puppet can be used to automatically configure, deploy the servers across EC2 instances or on-premises. AWS OpsWorks for Chef Automate is a configuration management service to host Chef Automate. Chef Automate is a set of automation tools for compliance and security, configuration

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

management, and deployment. OpsWorks provides access to Chef Automate features such as compliance management and configuration.

- **CloudWatch:** It is a monitoring service designed for IT managers, developers, and DevOps Engineers. It collects the monitoring data in the form of logs, events, and metrics. Logs can be monitored, stored, and accessed from AWS services. CloudWatch Events provides a stream of system events. By creating a set of rules, the events can be routed to target functions. CloudWatch can be used to find unusual behaviour in the cloud, set alarms, analyze logs and metrics, and take automated actions.

hide01.ir

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

Governance Tools in AWS

AWS provides the following tools for governance:

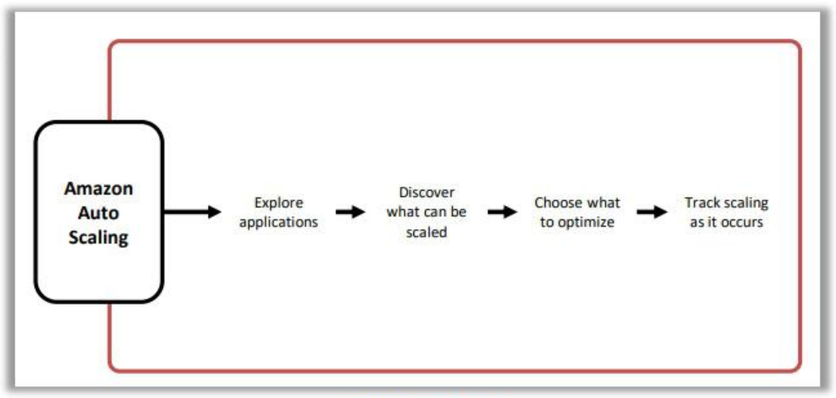
- AWS Auto Scaling
- AWS Managed Services
- AWS Trusted Advisor
- AWS Personal Health Dashboard
- AWS Control Tower
- AWS Console Mobile Application
- AWS License Manager

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

Governance Tools in AWS (Cont'd)

AWS Auto Scaling

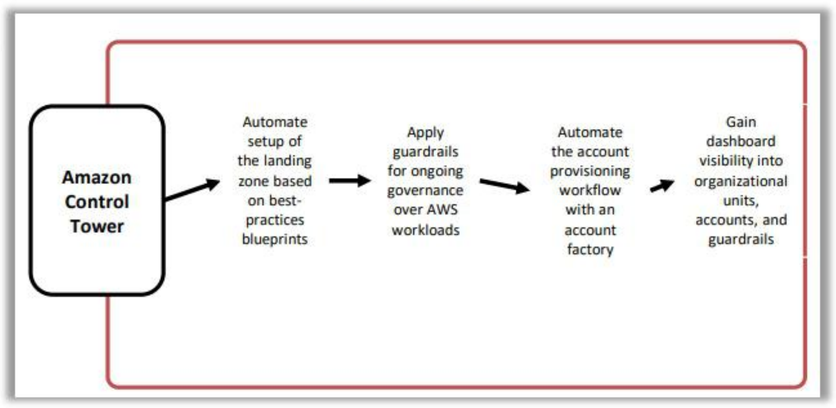
- **Monitors** the applications and automatically allots resources
- Provides easy-to-setup **application scaling** for various resources in different services
- Allows the optimization of cost and performance
- Can be combined with **EC2 Auto Scaling** to scale other resources for other AWS services



Auto Scaling

AWS Control Tower

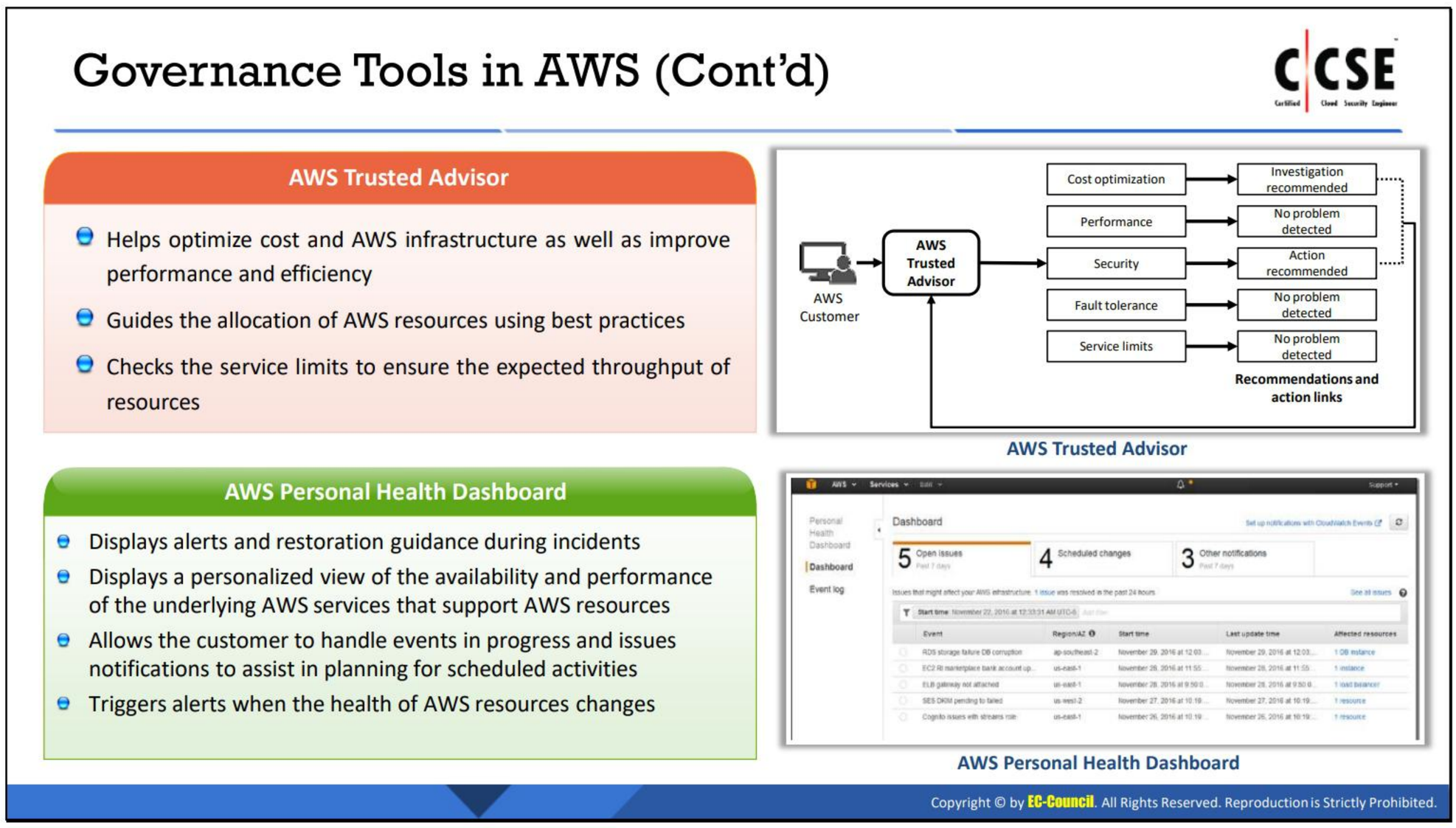
- Automates the setup of a baseline environment or a landing zone
- Provides an easy way to govern a safe, secure, and multi-account AWS environment
- Allows the organization to **create new AWS accounts** easily, all of which comply with the organization's policies
- Uses **guardrails** to enforce service control policies and to identify violations



AWS Control Tower

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.



Governance Tools in AWS

AWS offers various tools to handle governance such as:

- AWS Auto Scaling
- AWS Control Tower
- AWS Trusted Advisor
- AWS Personal Health Dashboard
- AWS Managed Services
- AWS Console Mobile Application
- AWS License Manager

hide01.ir

AWS Auto Scaling

AWS Auto Scaling keeps monitoring the applications and it automatically adjusts the resources to achieve expected performance at low cost. Auto Scaling makes it easy to setup application scaling for various resources in different services. Scaling becomes simple with AWS Auto Scaling and it lets to optimize cost and performance. It makes the application to have enough and right resources at the right time. AWS Auto Scaling can be combined with EC2 Auto Scaling to scale other resources for other AWS services.

AWS Control Tower

The setup of a baseline environment or a landing zone can be automated using AWS Control Tower. It automates the configuration of landing zone based on the best practices blueprints which are easy to govern workloads. AWS Control Tower provides an easy way to govern a safe,

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

secure, and multi-account AWS environment. Any enterprise that migrates to the cloud will have many applications and different teams. The organization needs to create multiple accounts for the teams and should maintain a consistent level of compliance and security. Using AWS Control Tower, the organization can create new AWS accounts with a few clicks and all the accounts will comply with the organization's policies.

Control Tower uses Guardrails to enforce service control policies and to identify violations. The policies apply while creating a new account or while changing an existing account. Control Tower also provides a report of how each AWS account obeys the enabled policies. This helps to have control over the AWS environment without compromising with the speed and agility.

AWS Trusted Advisor

AWS Trusted Advisor helps to optimize cost, AWS infrastructure, improve performance and efficiency. It provides guidance to allot AWS resources using best practices. The recommendation of a Trusted Advisor can be considered while developing new applications or workloads. It also checks the service limits to ensure the expected throughput of resources and to identify the overutilized instances.

AWS Personal Health Dashboard

When AWS experience incidents that affect the workloads, Personal Health Dashboard provides alerts and restoration guidance. It provides a personalized view of the performance and availability of AWS services in the AWS resources. The dashboard provides the required information to handle the events in progress and provides notifications to plan for the scheduled activities. When there are any changes in the health of AWS resources, Personal Health Dashboard automatically triggers alerts. This provides visibility of the events and guides to resolve the events quickly.

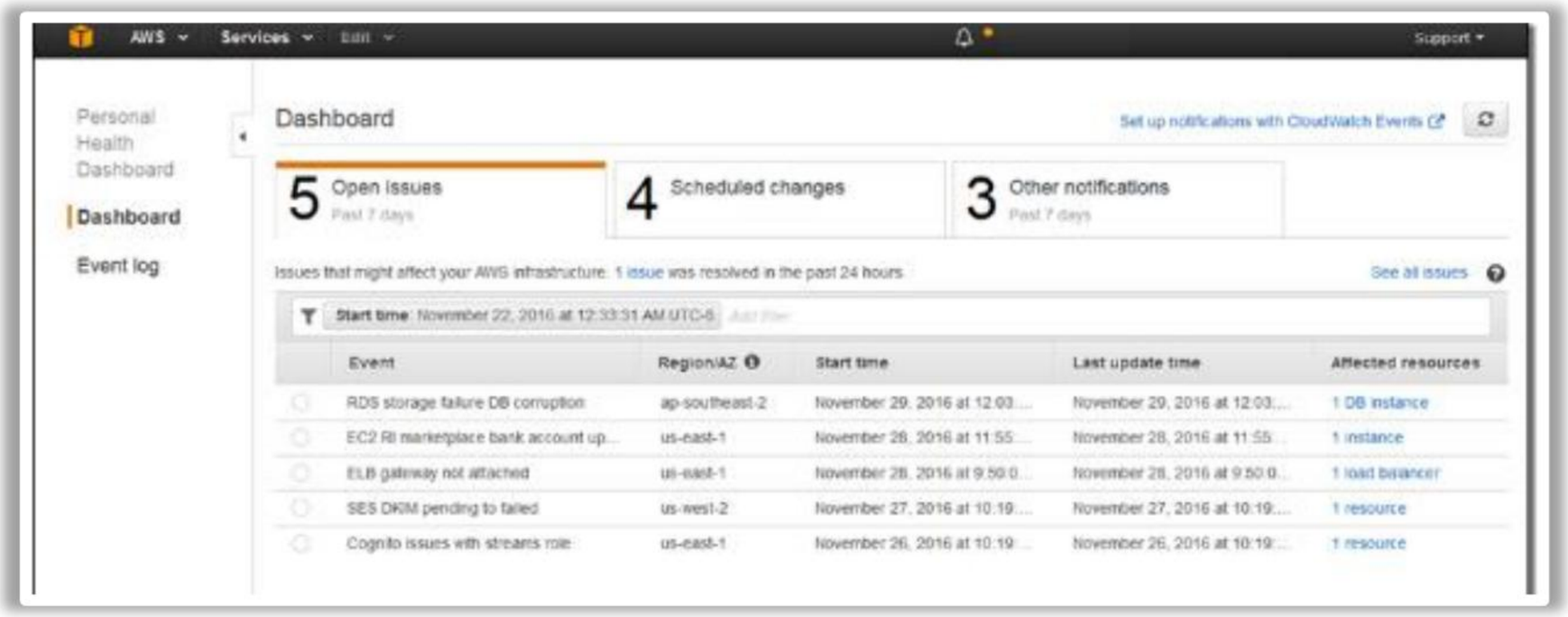
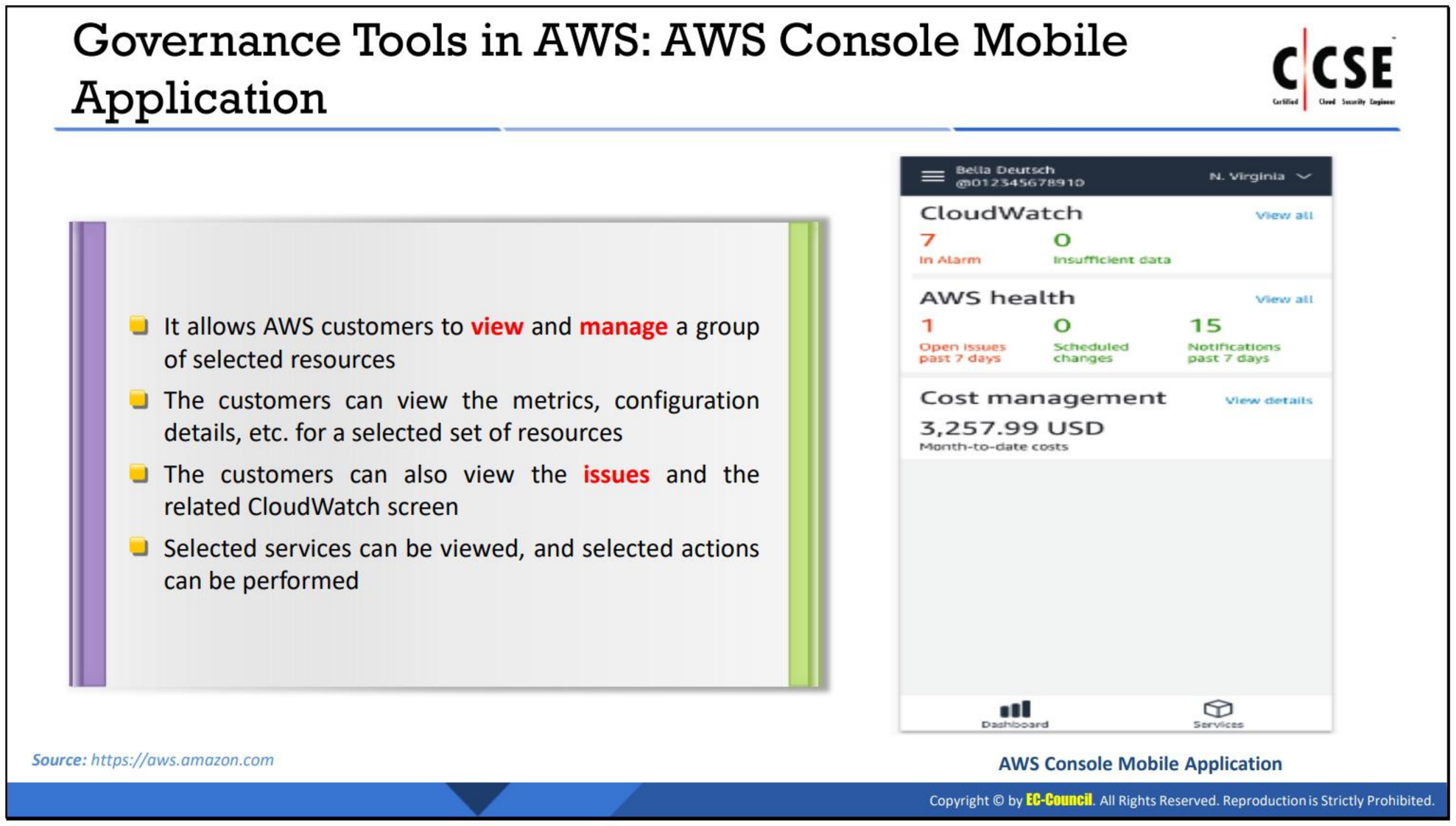


Figure 10.26: AWS Personal Health Dashboard

Source:https://aws.amazon.com

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



Governance Tools in AWS: AWS Console Mobile Application

AWS Console Mobile Applications lets the AWS customers view and manage a group of selected resources. The AWS customers can monitor the resources through a dedicated dashboard. They can view the metrics, configuration details, etc., for a selected set of resources. The permitted users can have a full view of account status including CloudWatch data, Personal Health Dashboard, Cost management, and billing. The customers can also view the issues and view the related CloudWatch screen to have a detailed view using graphs. Users can also view selected services and perform selected actions on them.

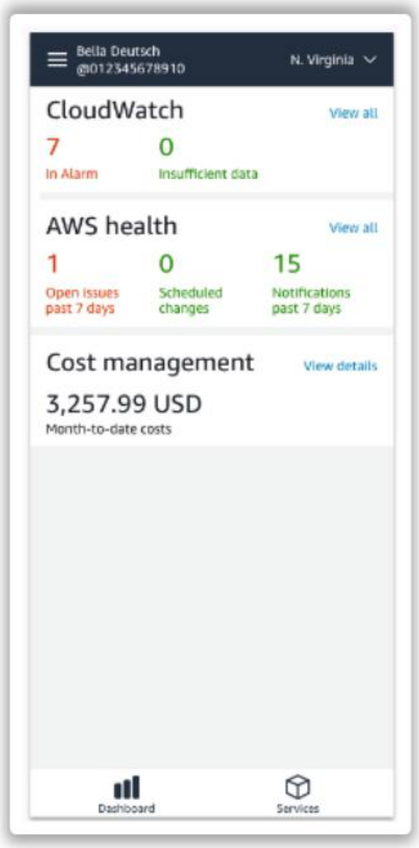
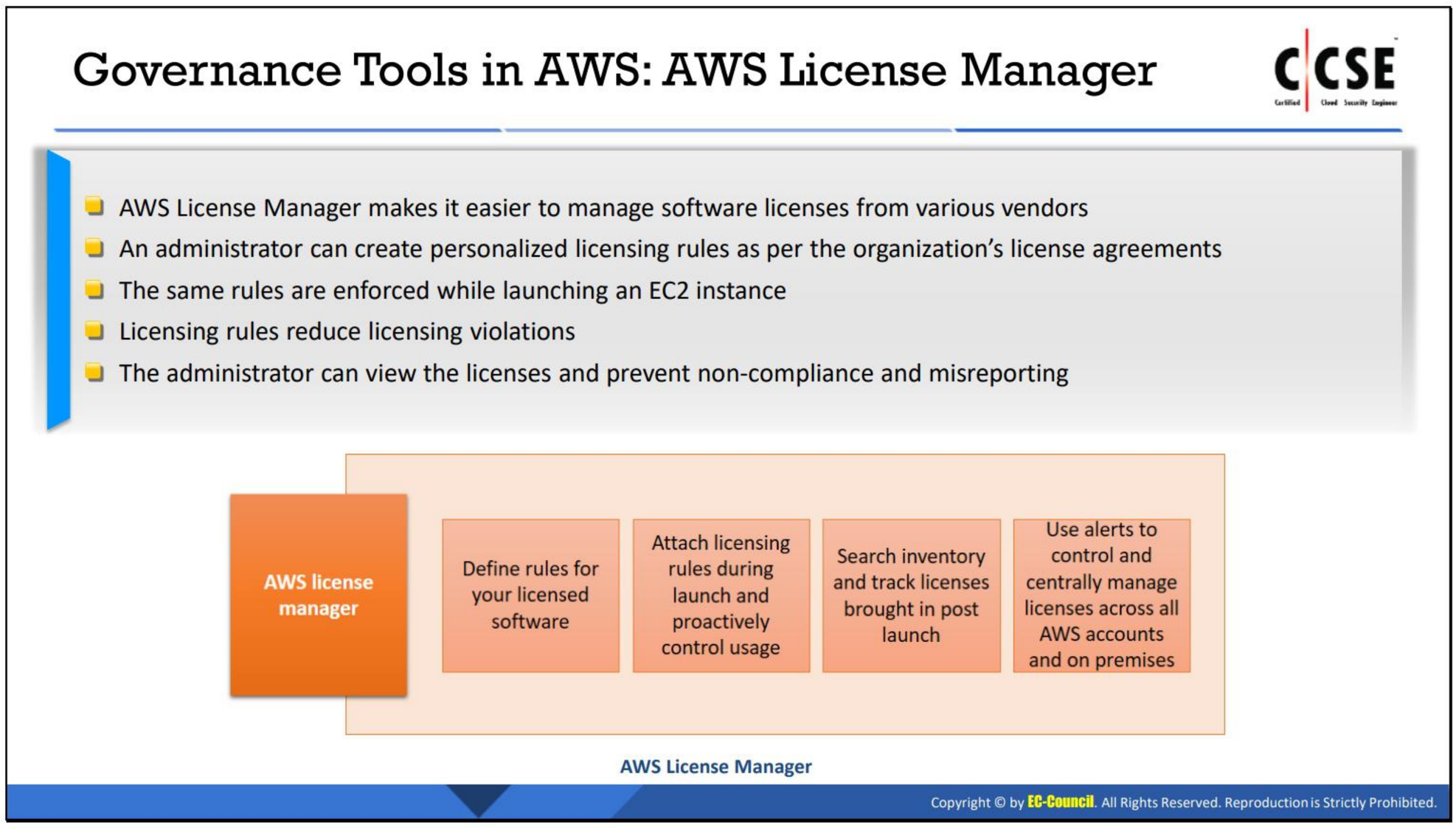


Figure 10.27: AWS Console Mobile Application

Source: https://aws.amazon.com

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



Governance Tools in AWS: AWS License Manager

AWS License Manager makes it easier to manage the software licenses from vendors namely SAP, Oracle, IBM in AWS, and on-premises environment. Using this tool, an administrator can create his own licensing rules as per the organization's license agreements. The same rules are enforced while launching an EC2 instance. These rules can be used to reduce licensing violations. Using these rules, a data breach can also be prevented by stopping the instance launch or by making the administrator aware of the infringement. From AWS License Manager Dashboard, the administrator can view the licenses and prevent costs for licensing overages, non-compliance, and misreporting.

AWS License Manager can also be integrated with other AWS services to manage licenses in multiple AWS accounts, and IT catalogs from a single AWS account.

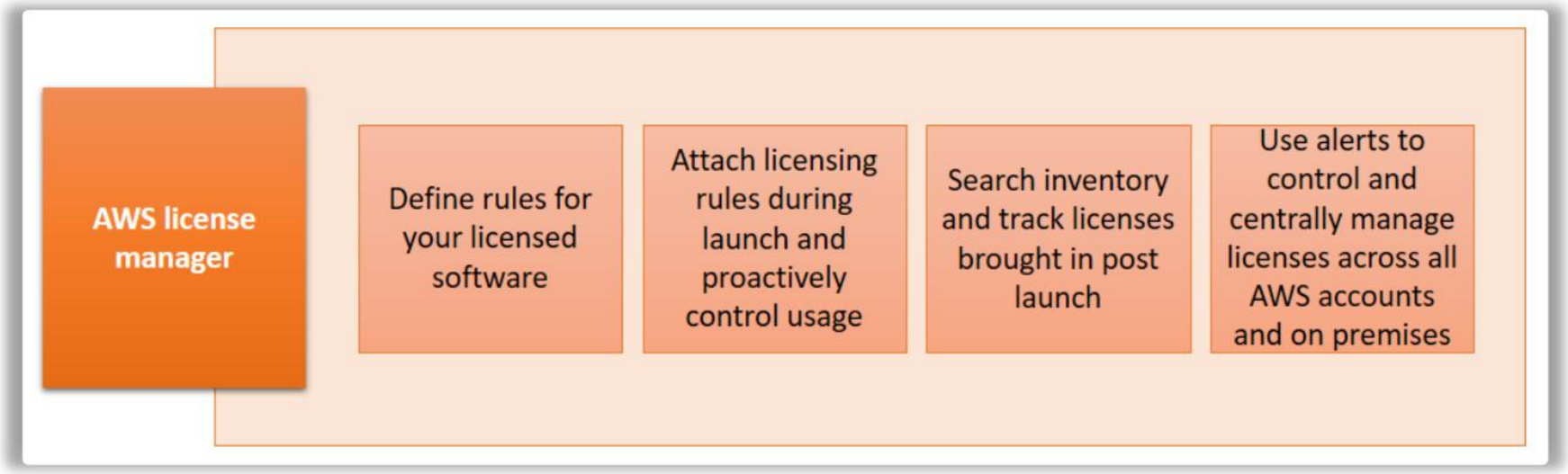
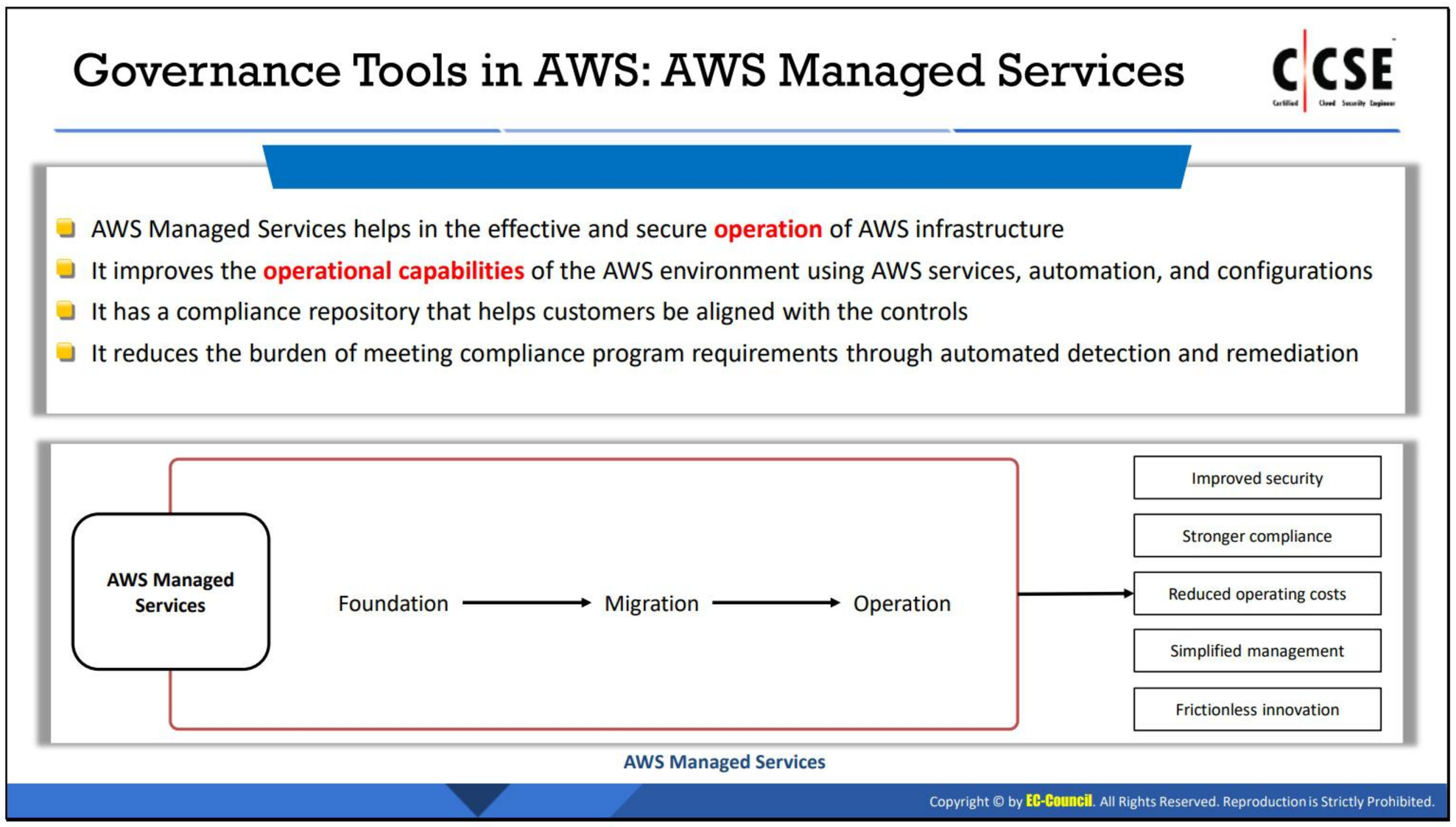


Figure 10.28: AWS License Manager

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



Governance Tools in AWS: AWS Managed Services

AWS Managed Services (AMS) help for effective and secure operation of AWS infrastructure. Using AWS services, automation, configurations, AMS can improve the operational capabilities of the AWS environment. It automates regular activities such as monitoring, patch management, changing requests, and backup services. It also provides lifecycle services to allocate, support, and run the AWS infrastructure. Corporate and security infrastructure policies can be enforced by using Managed Services controls. It reduces the burden of operating the infrastructure, improves agility, and reduces cost. AWS Managed Services has a repository of compliance, security, and guardrails to help customers aligned with the controls. Through automated detection and automated remediation, it also reduces the burden of meeting the compliance program requirements.

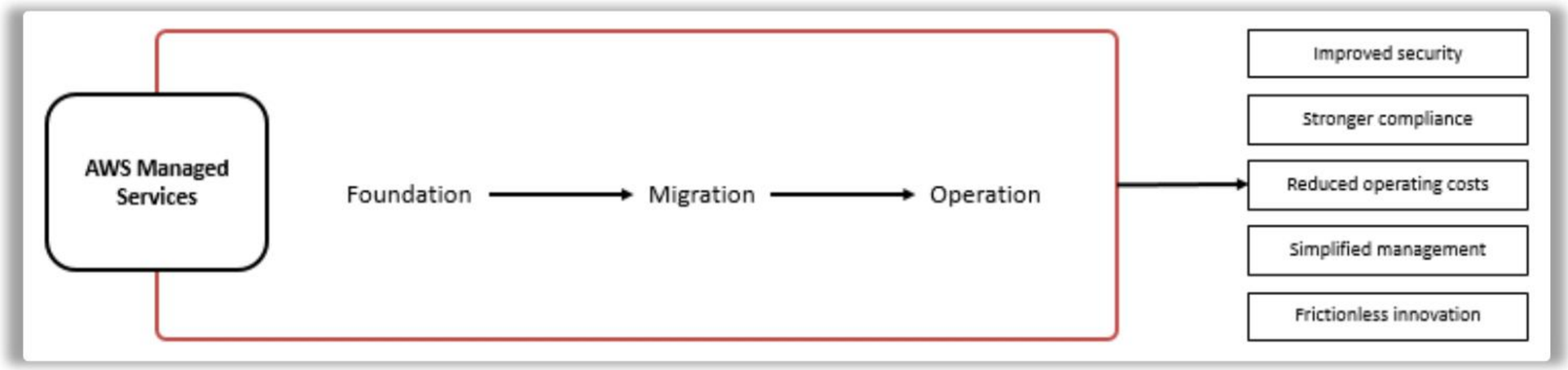
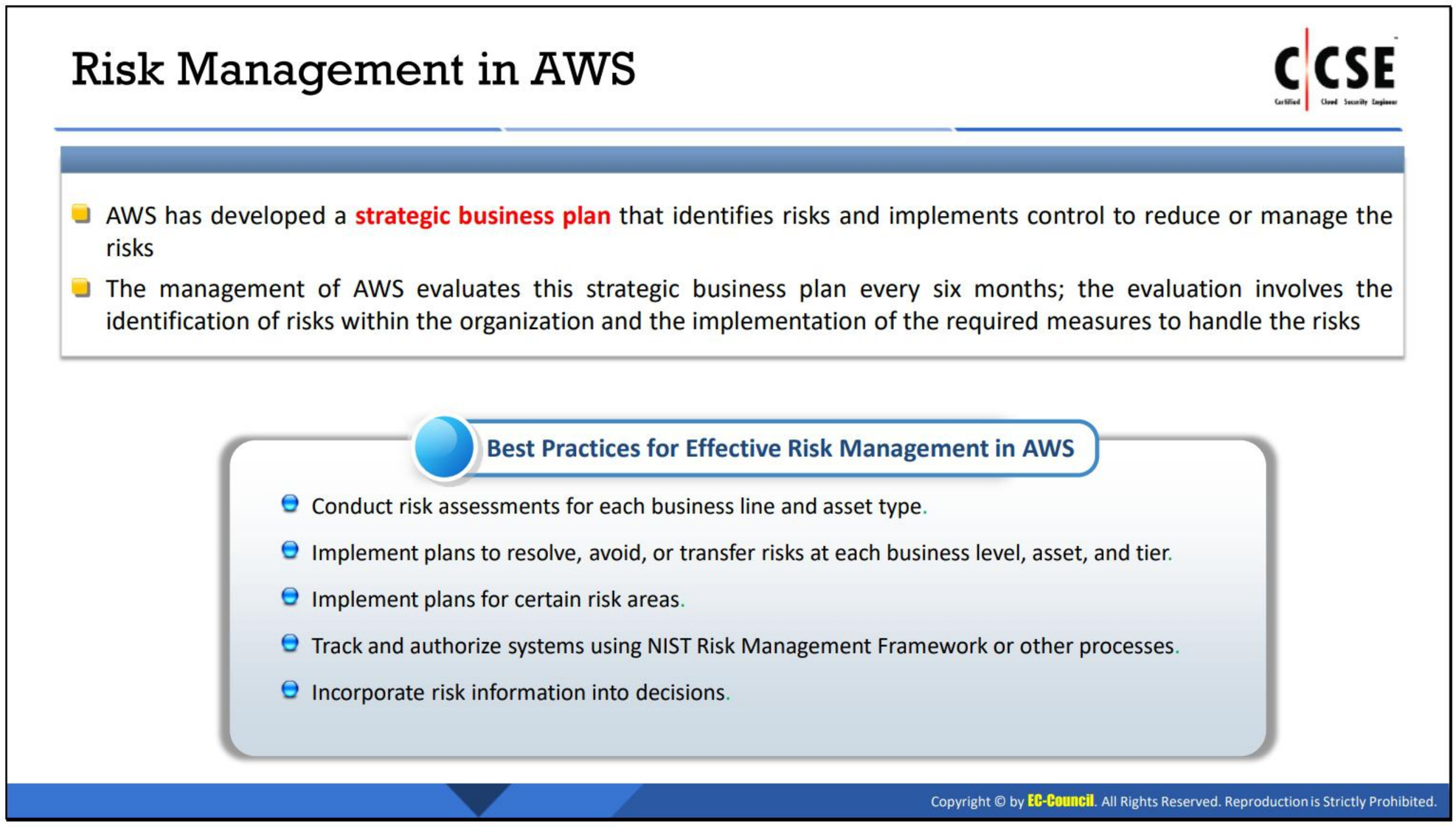


Figure 10.29: AWS Managed Services

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



Risk Management in AWS

AWS has developed a strategic business plan that identifies the risks and implements control to reduce or manage the risks. The management of AWS evaluates this strategic business plan every six months. The evaluation involves the identification of risks within the organization and the implementation of required measures to handle the risks.

AWS also undergoes various internal and external assessments. The Compliance and Security teams of AWS developed an information security framework and policies. This framework and policies are based on the Control Objectives for Information and related Technology (COBIT) framework. It is also integrated with the ISO 27001 certifiable framework. AWS provides security training to its employees, maintains security policies, and conducts application security reviews. These reviews evaluate confidentiality, integrity, and data availability.

AWS also identifies the vulnerabilities by scanning the service endpoint IP addresses that face the internet. The vulnerabilities will be notified to the relevant parties to resolve them. In addition to this, independent security firms also conduct regular external vulnerability threat assessments. The recommendations and finding from assessments are sent to AWS leadership after classification. All these scans are not for the customer's vulnerability scans, but for the health and viability of the AWS infrastructure. As long as the customers do not violate the AWS Acceptable Use Policy, they can also request permission to scan their specific compliance requirements.

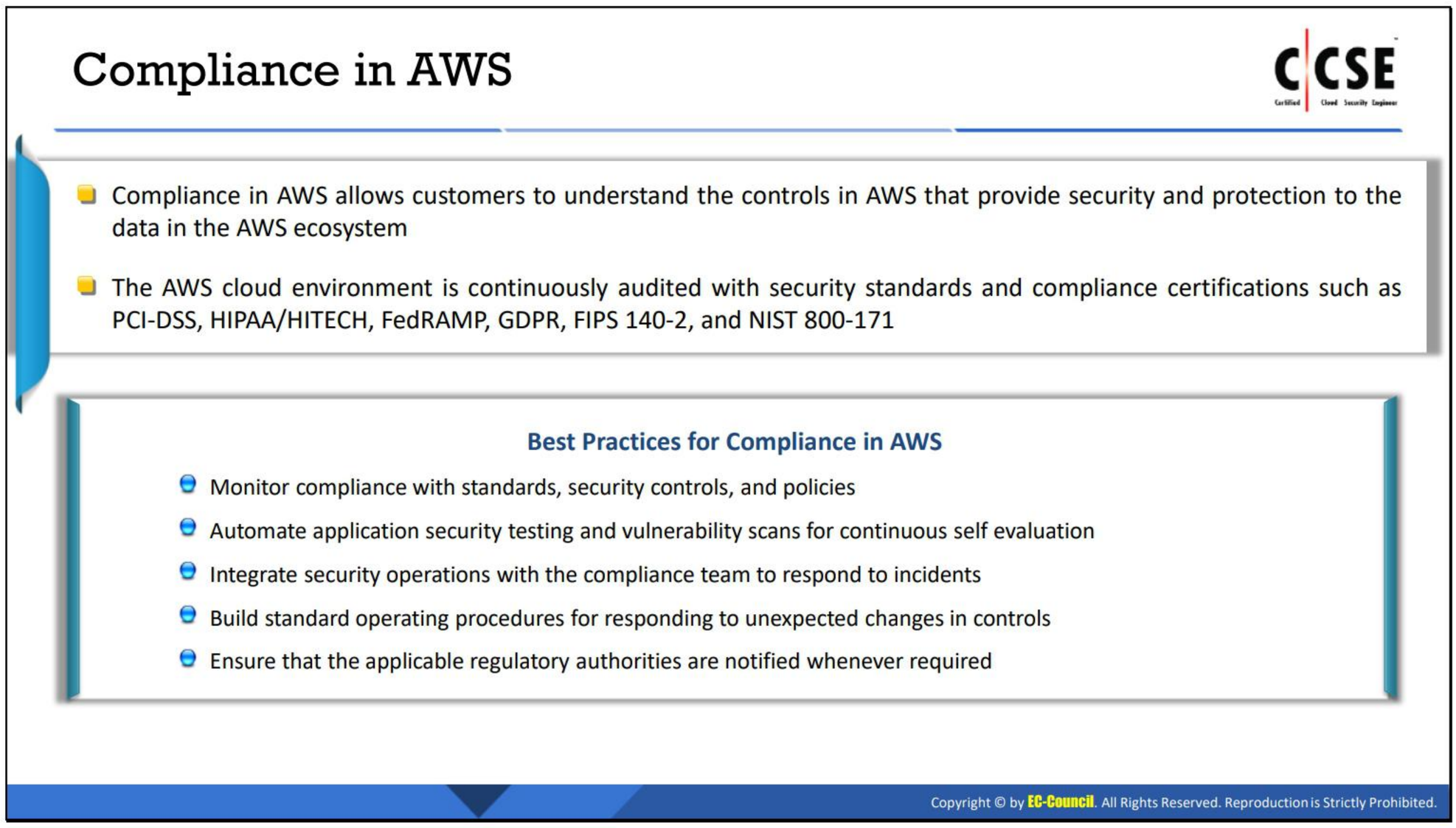
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following best practices can be followed for effective risk management in AWS:

- **Conduct a Risk Assessment**
  - The organizational risk assessments should be regularly conducted or updated
  - The risk assessments for each business line such as products or services, mission need to be conducted or updated
  - Risk assessment for every asset type should also be conducted or updated
- **Draft Risk Plans**
  - Cloud customers can implement plans to resolve, avoid, or transfer risks at each business level, asset, and tier
  - Customers can implement plans for certain risk areas
- **Authorize Systems**
  - The systems can be tracked and authorized using NIST Risk Management Framework or other processes
  - NIST Special Publication 800-53, ISO ISO/IEC 27002:2013 can be used to implement and evaluate controls based on risks
  - By employing automation to a great extent, continuous monitoring of risk and controls can be implemented
- **Incorporate Risk Information into Decisions**
  - System risk can be linked to the organization and business risk
  - Translation of continuous system risk monitoring and status to business and organizational risk can be automated

hiu01.ir

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



Compliance in AWS

Compliance in AWS allows the customers to understand the controls in the AWS that provide security and protection to the data in the AWS ecosystem. Compliance responsibilities are shared between the customers and AWS. AWS cloud environment is continuously audited with security standards and compliance certifications such as PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. This helps customers to meet compliance requirements for every regulatory agency around the world. AWS also offers assurance programs that offer control mappings and templates to customers for establishing compliance with their environments.

All the AWS services can be used in compliance with GDPR (General Data Protection Regulation). This allows AWS service customers to deploy their AWS services along with their GDPR compliance plans. Also, AWS provides its customer GDPR-compliant Data Processing Addendum (DPA) to comply with the GDPR contractual obligations. The GDPR DPA applies to all AWS customers automatically.

AWS continuously undergoes assessments for its underlying infrastructure. The assessments include both physical and environmental security of the data centers and hardware. This helps customers to make use of those certifications and inherit those controls. For validating compliance, AWS customers can make use of AWS automated tools such as AWS Config, and CloudTrail. These automated tools reduce the burden of performing audits as these tasks become automated.

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

The following are the best practices for compliance:

- **Monitor Compliance with Standards, Security Controls, and Policy**
  - Technical control monitoring and reporting should be automated
  - Non-technical controls can be manually monitored
  - Compliance monitoring can be linked with Security Information and Event Management (SIEM) and other tools
- **Continuous Self-assess**
  - Customers can continually self-assess by automating application security testing and vulnerability scans
  - Periodic self-assessments should be conducted from the sampling of controls
- **Respond to Events**
  - For response management, integrate security operations with the compliance team
  - To respond to unintentional changes in controls, standard operating procedures should be established
  - Impacts should be resolved and the affected controls should be reset
- **Communicate Events and Changes to Risk**
  - For each type of incident, a reporting tree and thresholds should be established
  - General counsel should be included in the reporting
  - Automation should be implemented wherever required
  - Ensure to notify the applicable regulatory authorities whenever required

hadeo1ir

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



Customer Cloud Compliance Governance

In AWS, customers are also responsible for maintaining proper governance in their IT control environment. The governance must be implemented irrespective of where and how the IT is deployed.

hide01.ir

The leading practices for implementing governance in the IT control environment include:

- **Compliance Objectives:** The cloud customers must understand the required compliance requirements and objectives from the relevant resources.
- **Build a Controlled Environment:** The AWS customers should build a controlled environment that should meet the required objectives and requirements.
- **Understand the Validation:** The AWS customers must understand the validation required as per the organization's risk tolerance.
- **Verify the Operating Effectiveness:** The AWS customers must verify the operating effectiveness of their IT control environment.

When the organization infrastructure is deployed in the AWS cloud, it offers various options to enterprises for applying different controls and verification methods.

The basic approaches for implementing strong customer compliance and governance include the following:

- **Reviewing AWS Shared Responsibility Model, Security Documentation, and Compliance Reports:** The cloud customers must go through the AWS Shared Responsibility Model, AWS compliance reports, and AWS security documents. By referring to those reports and documents, the cloud customers must understand the

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

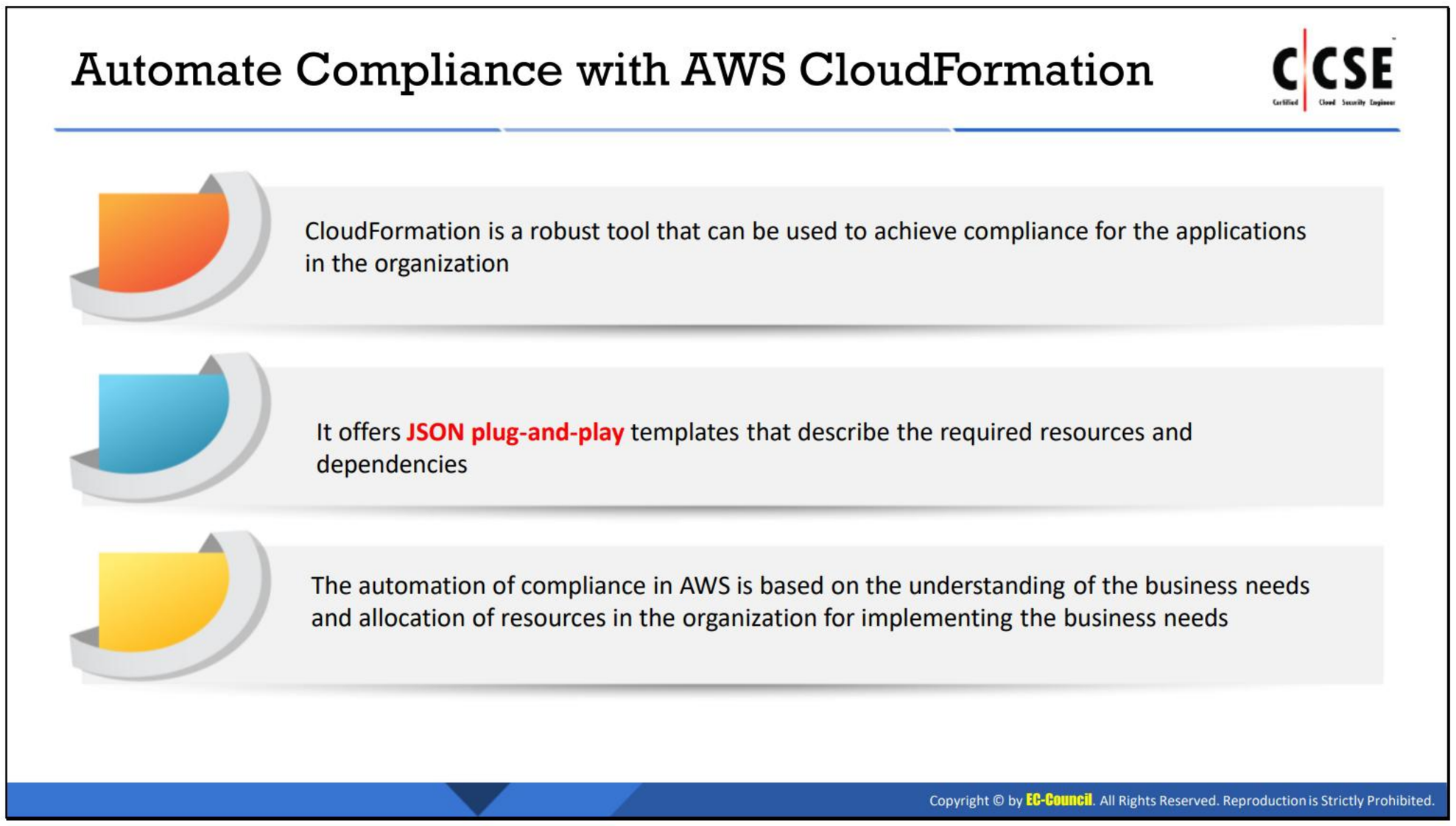
complete IT environment. Based on the understandings, all the compliance requirements should be documented into a cloud control framework.

- **Designing and Implementing Control Objectives:** The AWS customers should design and implement control objectives. The designed control objectives should meet the compliance requirements mentioned in the AWS Shared Responsibility Model.
- **Identifying and Documenting Controls From Other Parties:** The AWS customers should identify the controls from other parties and those controls should be documented.
- **Verifying the Control Objectives:** The AWS customers should verify that all the control objectives are met. They should also ensure that the important controls are designed and are working efficiently.

By following all the above approaches for compliance governance, cloud customers can have a proper understanding of their IT control environment. It also helps customers to clearly outline the verification activities that need to be performed.

hide01.ir

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



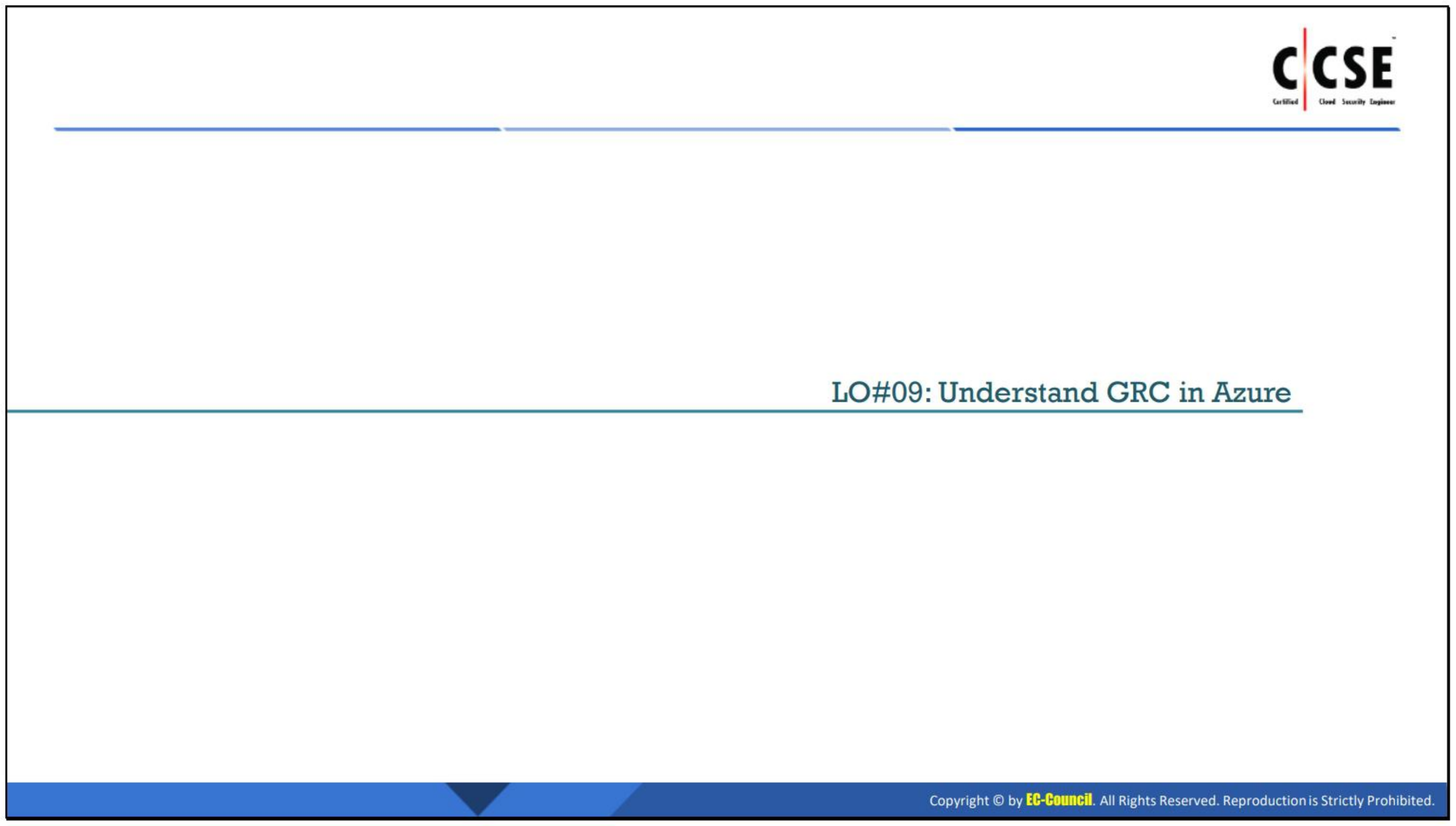
Automate Compliance with AWS CloudFormation

CloudFormation is a robust tool that can be used to achieve compliance for the applications in the organization. It helps to model AWS resources and other third-party resources and provision them consistently. It offers JSON plug-and-play templates that describe required resources and dependencies. Using this template, all the required resources can be launched as a stack. This allows for a smooth and continuous deployment of architecture.

A stack is also an important feature of CloudFormation. The stack is a set of resources that can be configured together to meet the specific compliance requirements of an organization. The stacks can be provisioned and managed across multiple AWS accounts and regions. Also, cloud customers can set the baselines for architecture and automate them like applications. Once stacks are created for every use case, cloud customers can combine them as a package. The package can be replicated and deployed as per the requirement. The following are the tips for automating compliance in AWS:

- **Use Modular Development:** The cloud customers must adopt modular development. The stacks should be nested into layers and then they can be packaged.
- **Define Compliance Parameters in Advance:** The compliance parameters should be defined in advance. By this, the customers know how to use a parameters file.
- **Implement Contingencies:** Contingencies must be implemented based on the dependencies and the requirements of the organization.
- **Use IAM:** Cloud customers should make use of IAM to control access to the stacks and to prevent users from deleting important stacks. The automation of compliance in AWS is based on the understanding of the business needs. It is also based on the allocation of resources in the organization for implementing the business needs.

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

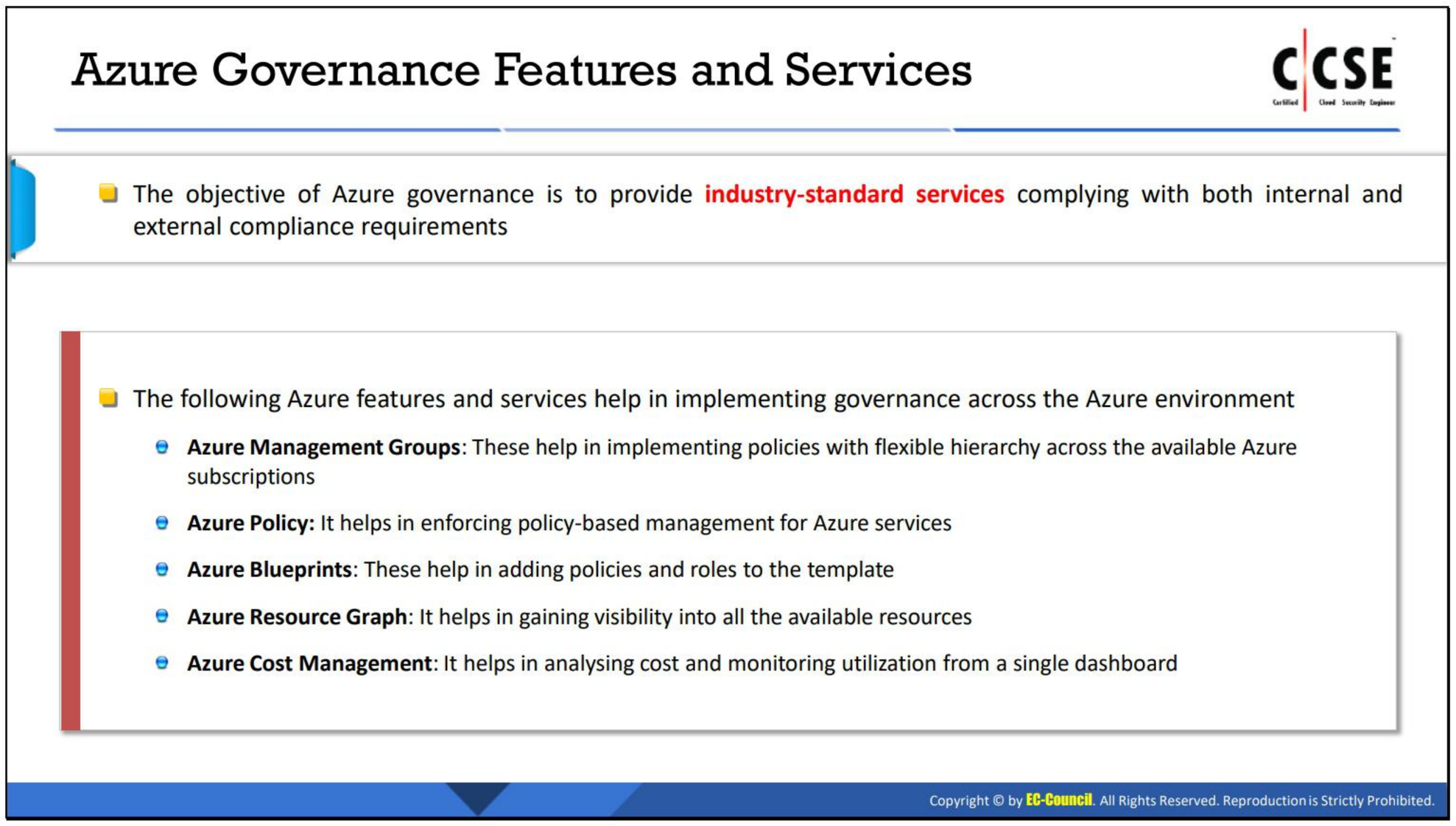


LO#09: Understand GRC in Azure

The objective of this section is to provide a brief overview of GRC in Azure Cloud with the help of tools and resources provided by Microsoft Azure. It shows how to manage governance, Risk management and compliance in Azure.

hide01.ir

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



Azure Governance Features and Services

As developers or other required teams are given unrestricted access to resources, any actions performed by them unintentionally may reflect in huge billing. To avoid these kinds of consequences, governance is enforced. It manages, monitors, and audits the Azure resources.

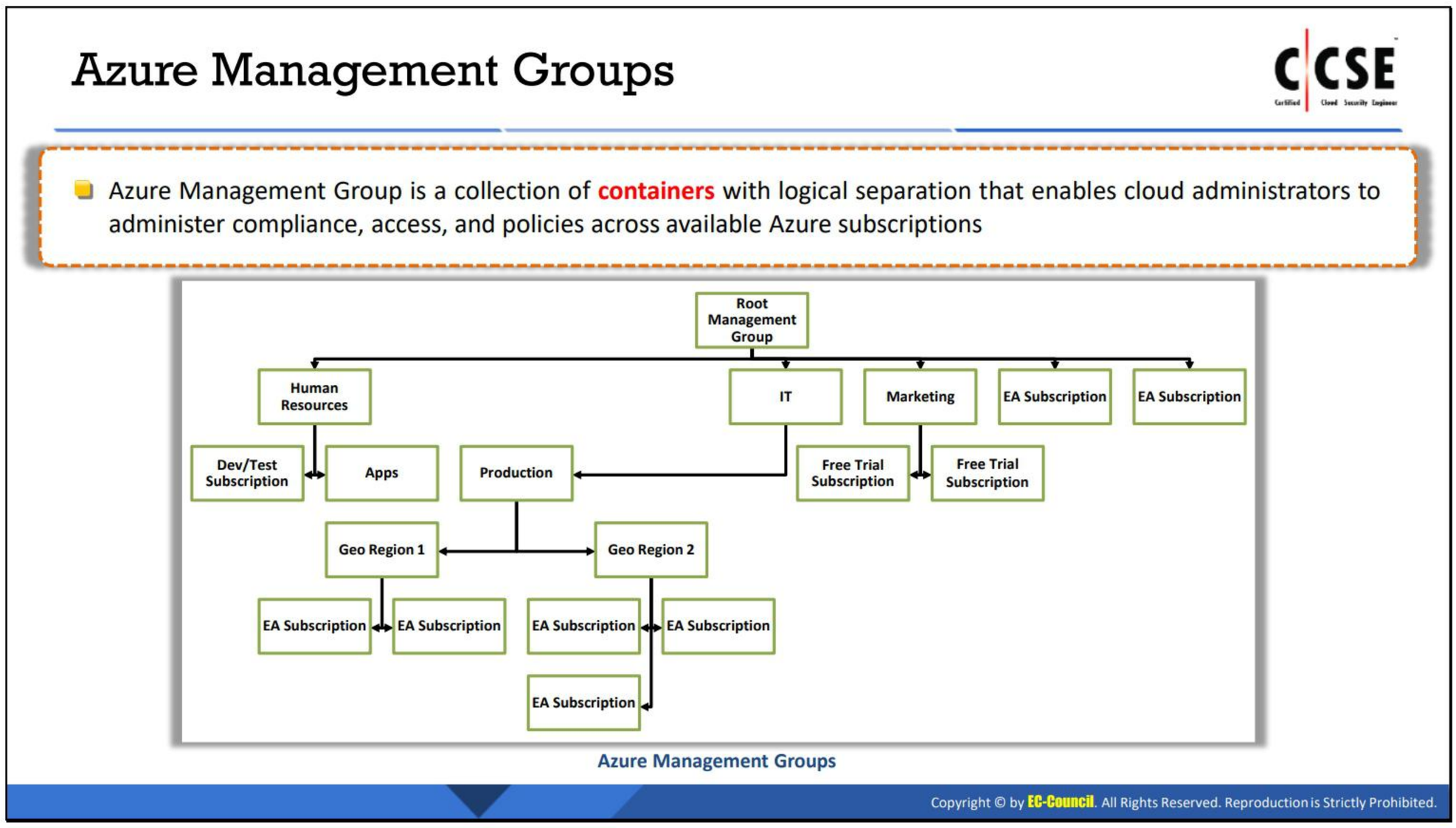
hidoo1.ir

The objective of Azure governance is to provide customers with industry-standard services that comply with both internal and external compliance requirements. The services provided by Azure governance are Azure Policy, Azure Blueprints, Azure Cost Management, and Azure Resource Graph. Not all the services are available directly, some of them available as preview services.

The following Azure features and services helps in implementing governance across the Azure environment:

- **Azure Management Groups**: It helps in implementing policies with flexible hierarchy across available Azure subscriptions
- **Azure Policy:** It helps in enforcing policy-based management for Azure services
- **Azure Blueprints**: It helps in adding policies and roles to the template
- **Azure Resource Graph**: It helps in getting visibility into all the available resources
- **Azure Cost Management**: It helps in analysing cost and monitoring the utilization from a single dashboard.

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



Azure Management Groups

Azure Management Group is a collection of containers with logical separation that enables cloud administrators to administer compliance, access, and policies across available Azure subscriptions. Azure subscription tree (chain of groups, subscription, regions, etc) can be built by Management groups which can be used by multiple services related to Azure. For example, Azure Role Based Access Control (RBAC) and Azure Policy. For the effective governance of the resources, Azure Management Groups can be extended up to six levels in the chain, this creates flexible management of access control, policy, and compliance.

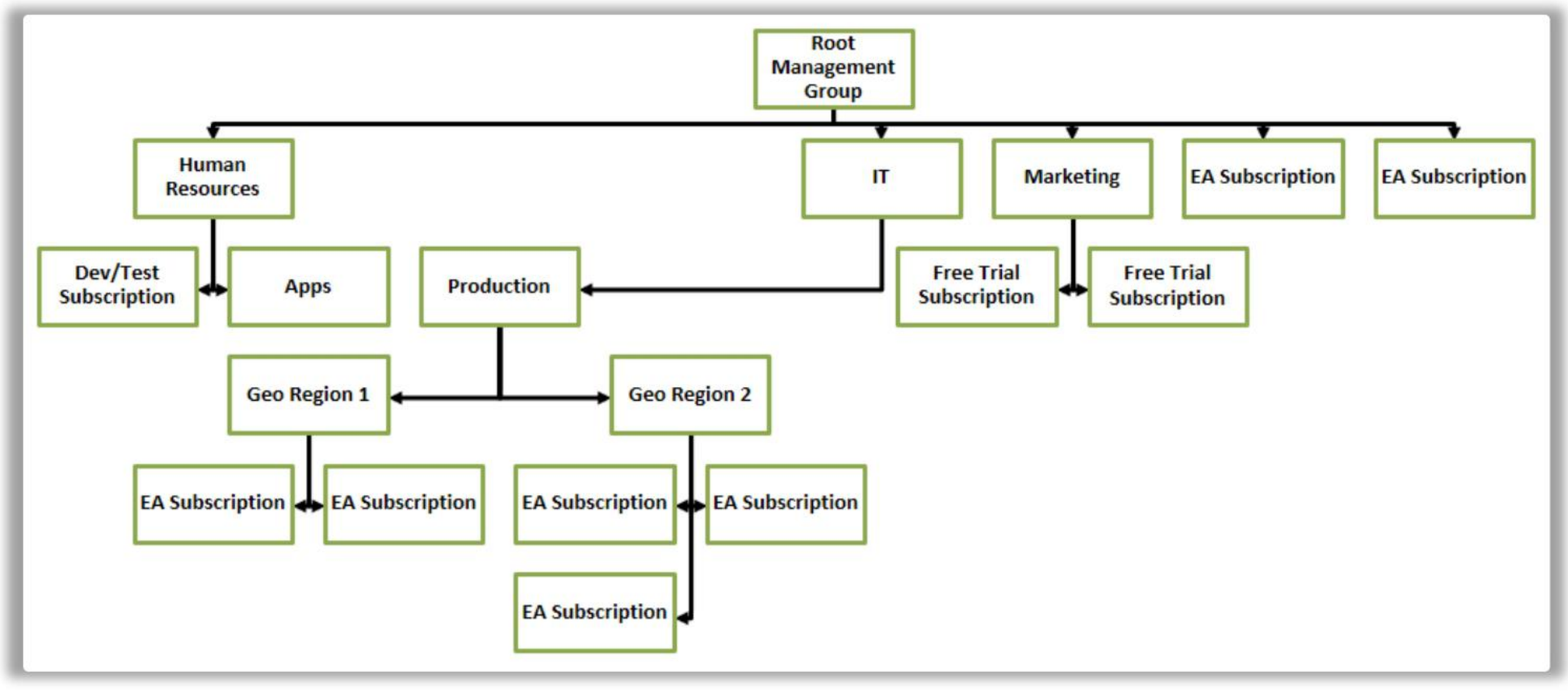
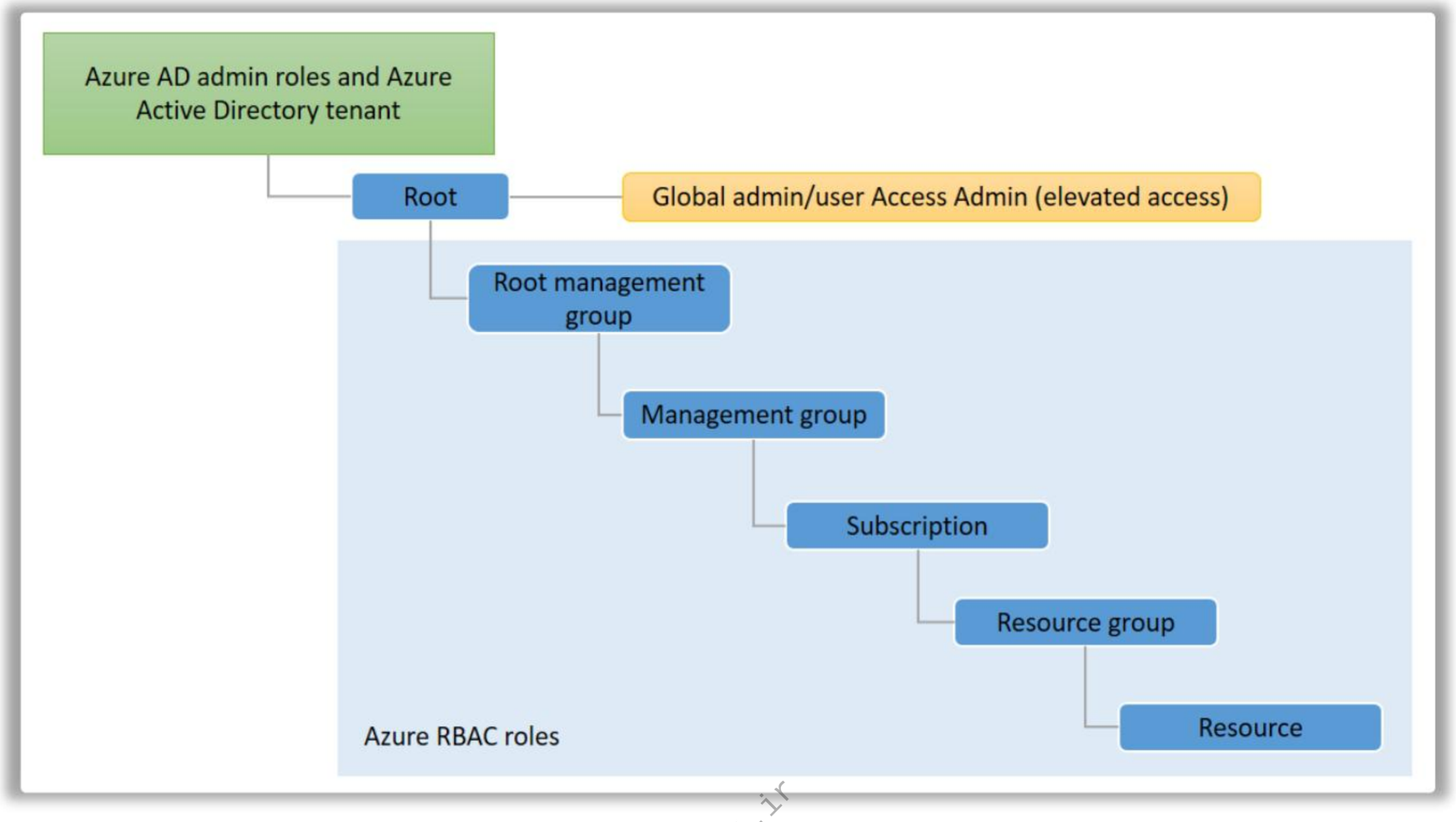


Figure 10.30: Azure Management Groups

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

Different Azure Subscriptions hold different resources that are assigned to them, and the Azure Subscription is connected to individual Azure Active Directory tenants. The permissions are reflected as configured at that level. To be precise, the Management Groups can contain multiple subscriptions as long as they belong to the same tenant (Active Directory) i.e the subscription of one tenant cannot contain the subscription of another tenant.



hidoo1.ir

Figure 10.31: Azure AD and Organizational Structure Relation

Resource Group maintains all the Azure resources associated with a particular subscription. After creating the required policy it can be applied to either Management Group or a subscription. The same policy can also be exempted at the Resource Group level. Imagining a tree of Management Group the first and top-level place belongs to the root Management Group which cannot be eliminated or moved. This will have the list of all other Subscriptions and Management Groups. Each Management Group supports only one parent (for each subscription) and multiple children in the tree. It is recommended to maintain two management groups i.e one for production and the another for non-production or testing environment. The root management group will enforce the default security policies. The lower levels in the hierarchy cannot change enforced policies at the higher level. The organizations having more (complex) Azure Subscriptions will be benefitted from the use of Management Groups, as this provides flexible control over them.

Use Root Management Group

To maintain consistency in the enterprise the Root Management Group (MG) is used, and ensure to take care while testing changes to minimize operational disruption. The consistency over the enterprise is achieved by applying permissions, tags, and policies in all subscriptions. It is recommended to take care during the planning and implementation of assignments to the root management group, as there are chances which might result in downtime of Azure resources. Due to errors productivity impact may also occur.

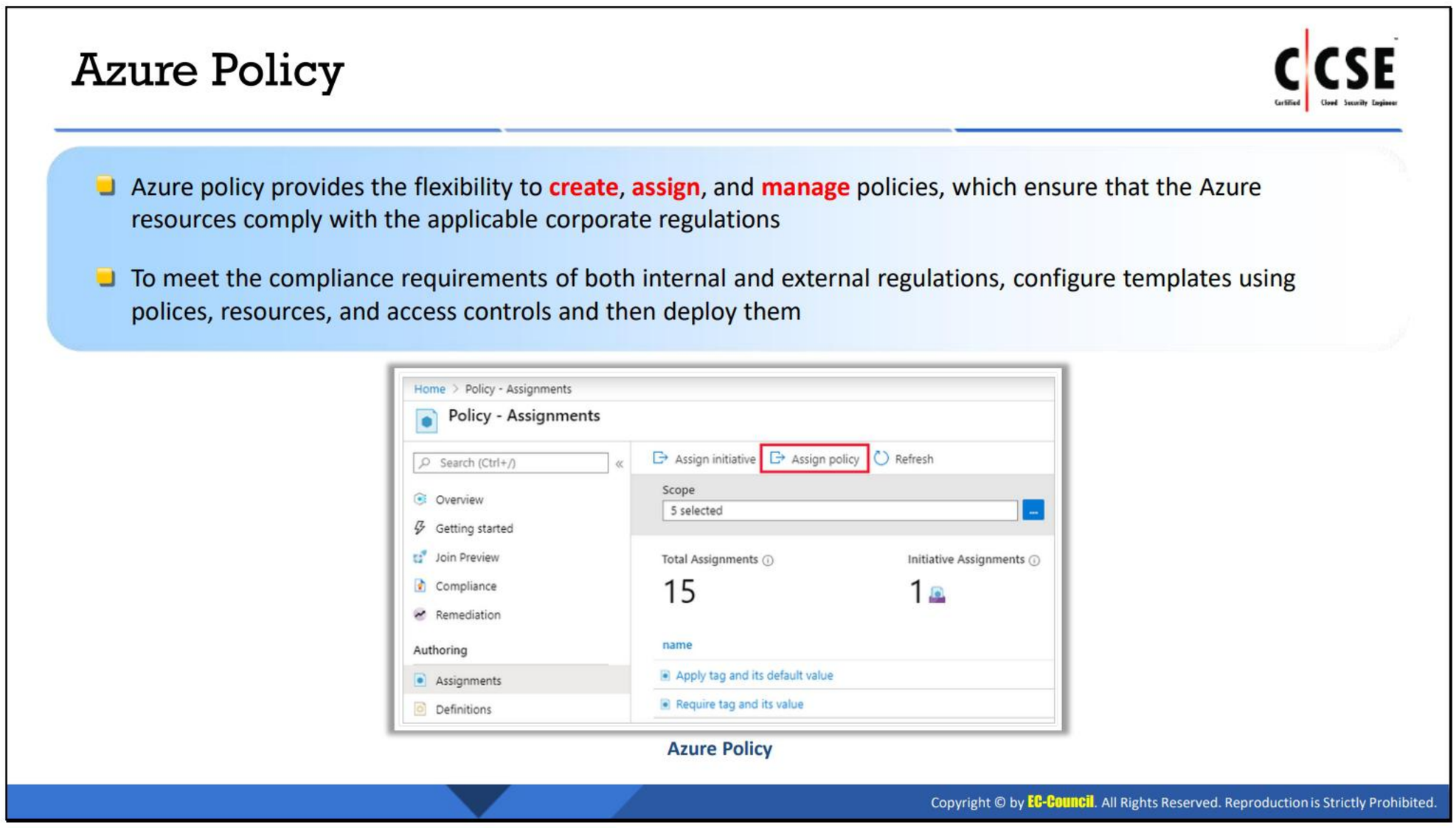
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Guidance to the root management group:

- **Plan Carefully:** Enterprise-wide elements that have requirements should be selected to the root management group so that they can be applied to all the resources.
- **Test First:** Before applying the Azure RBAC model, tags, and policy the enterprise-wide changes should be cautiously tested on the root management group.
- **Validate Changes:** All the changes applied should be validated to confirm whether the required effects took place or not.

hide01.ir

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



Azure Policy

Azure Policy provides the flexibility to create, manage, and assign policies. These policies ensure that the Azure resources comply with the required corporate regulations. The predefined policies evaluate the resources if they are compliant with them or not. For example, if a policy is created such that it should accept virtual machines of certain SKU (Stock-Keeping-Unit) size, then it evaluates existing, updating, and resources at the time of creation.

Assign a Policy: Assigning policy definition is the basic action to enforce compliance with Azure policy. The policy definition indicates the condition of the policy. For example, To add a tag for the new or updated resource from the parent resources group, assign a built-in policy "Inherit a tag from resource group if missing".

Source: https://www.microsoft.com

Steps to Assign a Policy:

- Sign in to the Azure portal.
- Search **Policy** and select it.

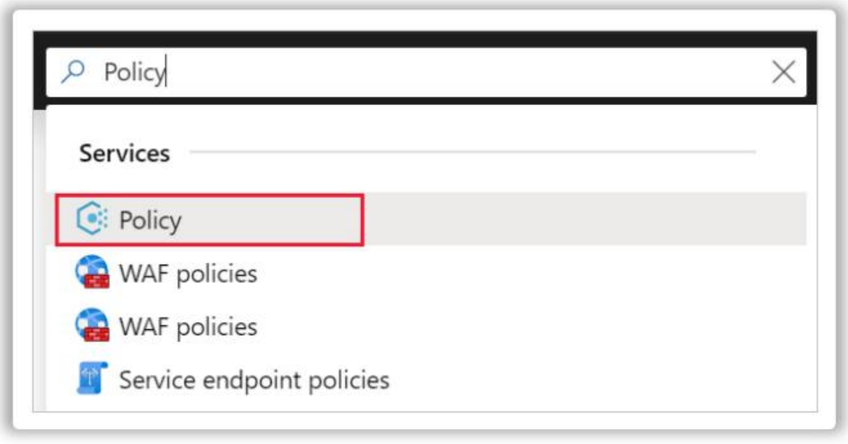


Figure 10.32: Selecting Policy

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

- From the left navigation panel select **Assignments**.

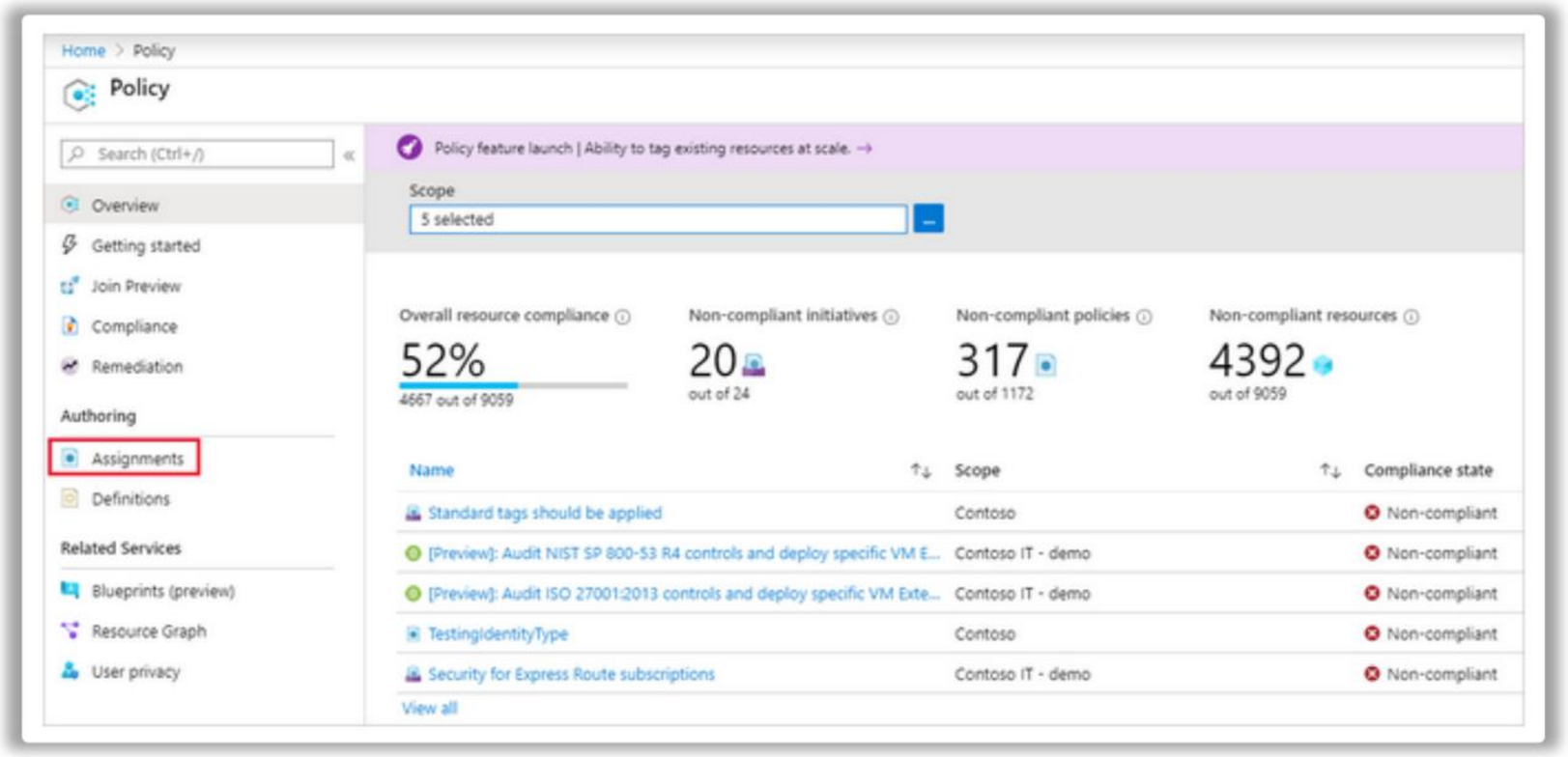


Figure 10.33: Selecting Assignments

- Click on **Assign policy** from the right-side panel.

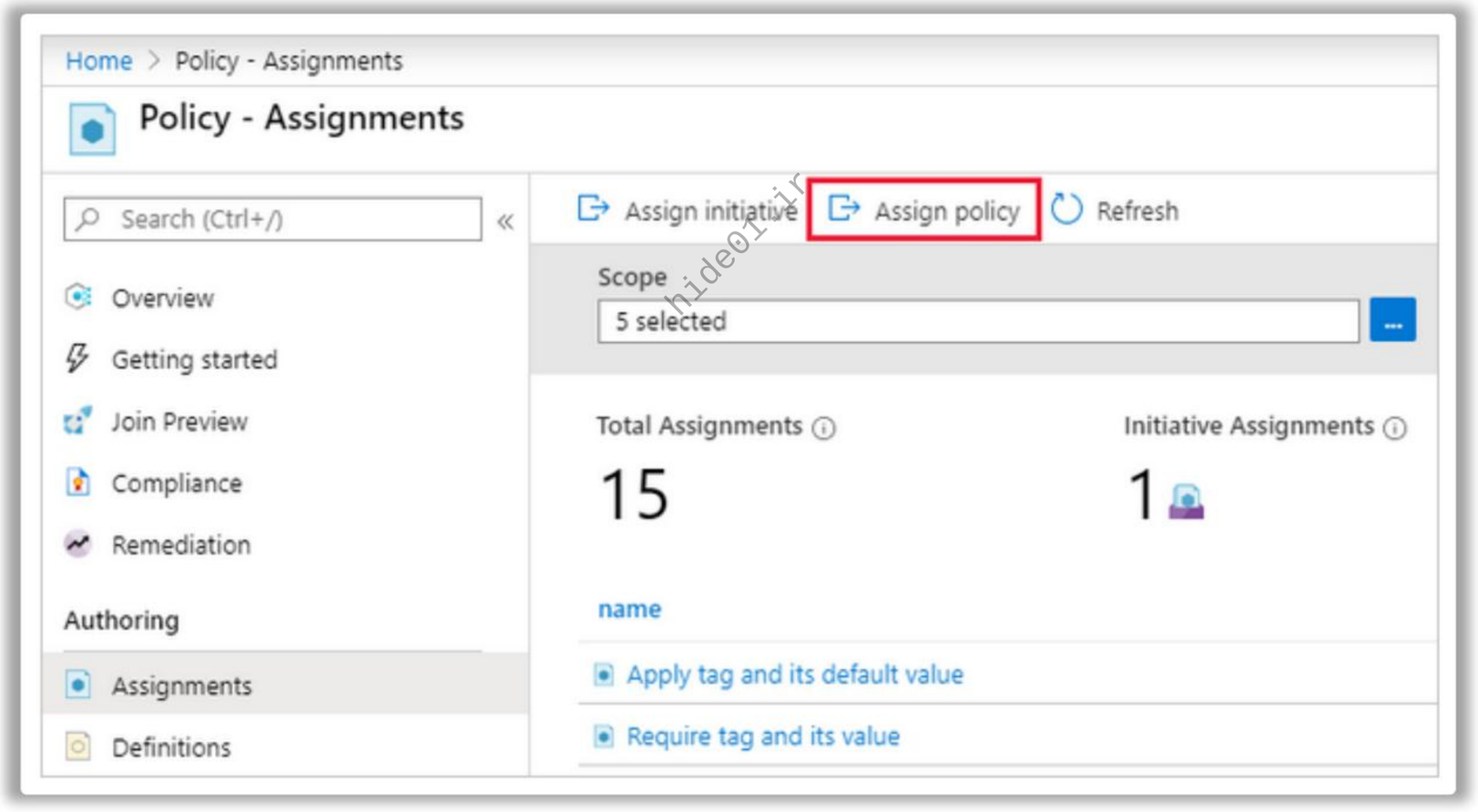


Figure 10.34: Selecting Assign Policy Option

- In the **Basics** tab, ellipsis should be selected in **Scope**, then either a management group or subscription should be selected.
- Select the resource group for what policy should be enforced, Click on the **Select** on **Scope** page.
- Depending on the scope the resources can be excluded and it is optional. The staring of **Exclusions** will be one level lower than **Scope**.
- From the list of available definitions, the **Policy definition** should be selected. To view and read descriptions the **Type** of policy definition can be set to **Built-in**.

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

- Search by typing **inherit a tag** and select **Inherit a tag from the resource group if missing**.
- From the **Available Definitions** page click on **Select** that is present at page bottom after selecting policy definition.

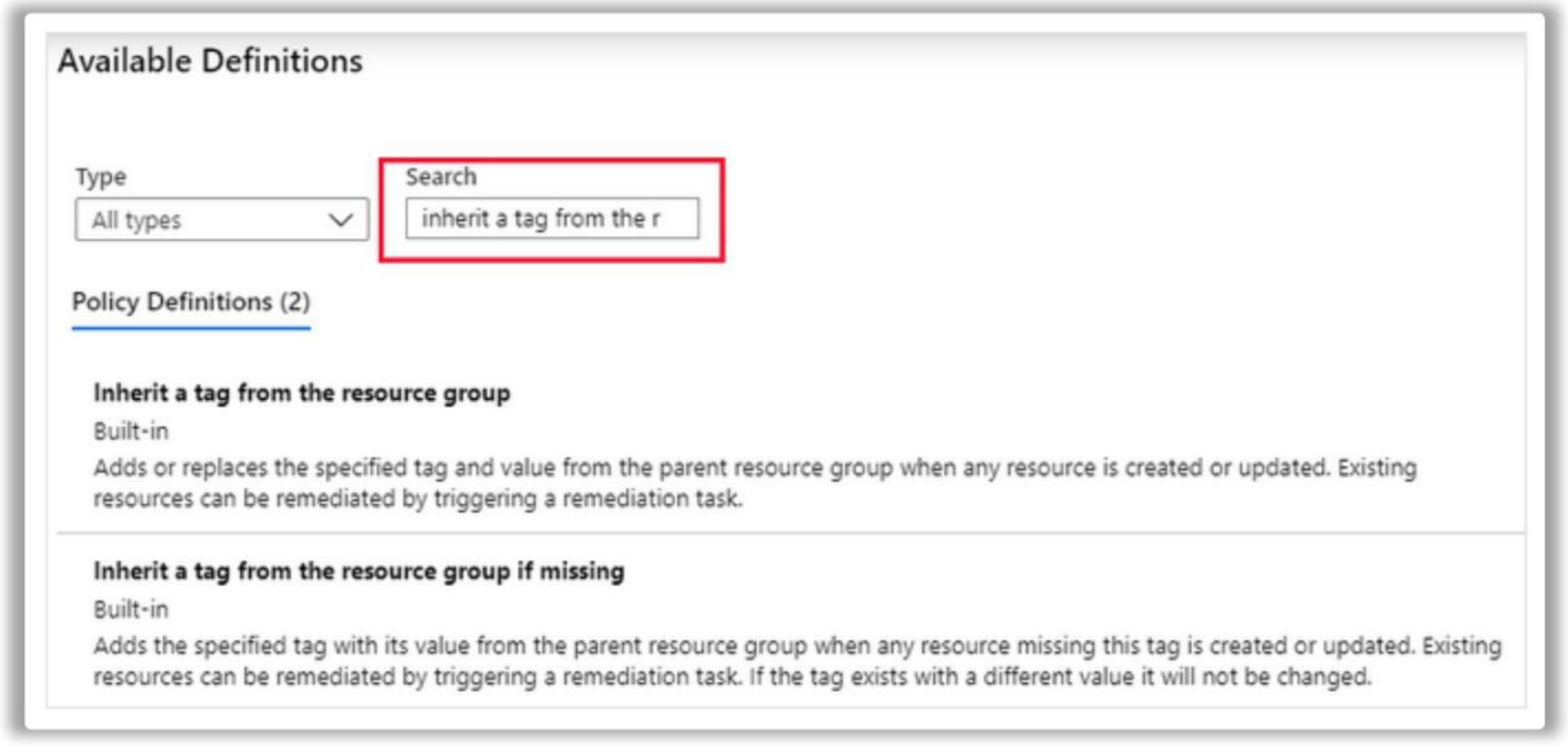
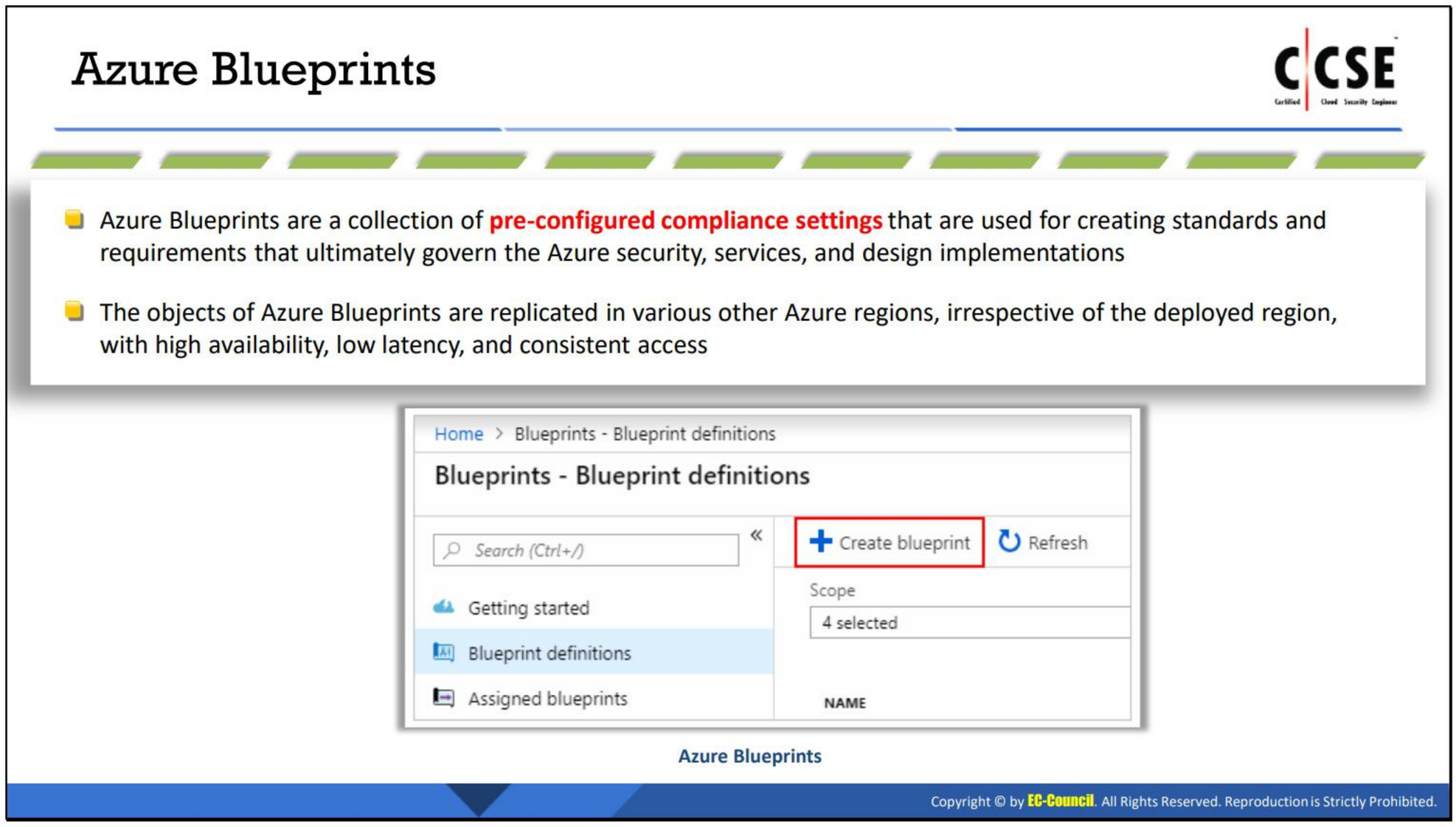


Figure 10.35: Selecting an Available Defintion

- **Assignment name** can be changed or else you can leave with automated selection.
- The **Description** is optional and if required provide policy assignment details.
- **Policy enforcement** should be left as **Enabled**.
- Depending on the user signed-in the **Assigned by** is automatically selected.
- Now go to the **Parameters** tab.
- Input **Environment** as the **Tag Name**.
- Then go to the **Remediation** tab.
- **Create a remediation task** should be left unchecked.
- As the policy definition uses modify effect the **Create a Managed Identity** is checked automatically.
- Contributor is automatically set in the **Permissions** filed.
- Go to the **Non-compliance** tab from the top options.
- The **Non-compliance message** should be set to “This resource doesn’t have the required tag.”
- Click on the **Review + create** tab from the top options.
- Finally, the selections should be reviewed and proceeded to **Create**.

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



Azure Blueprints

Azure Blueprints are a collection of pre-configured compliance settings that are used for creating particular standards and requirements that ultimately govern the Azure security, services, and design implementations. These Azure Blueprints are reused and it is consistent and compliant with required regulations. It is one of the Azure governance services. Cloud architects and other IT teams use Azure Blueprints to deploy Azure resources that bind to patterns, standards, and requirements of the organization. The deployment of various resource templates including artifacts like Role Assignments, Azure Resouce Manager templates, Policy Assignments, and Resource Groups are coordinated by the Blueprints. Azure Cosmos DB provides the finance for Azure Blueprints. The objects of the Azure Blueprints are replicated to various other Azure regions irrespective of the deployed region, with high availability, low latency, and consistent access.

Source: https://www.microsoft.com

Steps to Create a Blueprint:

- Sign in to the Azure portal.
- From the left navigation panel click on **All services**.
- Search for **Blueprints** and select it.
- On the left navigation panel select **Blueprint definition**. Click on + **Create blueprint** button.

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

- Alternatively, On the **Getting started** page you can click on **Create**.

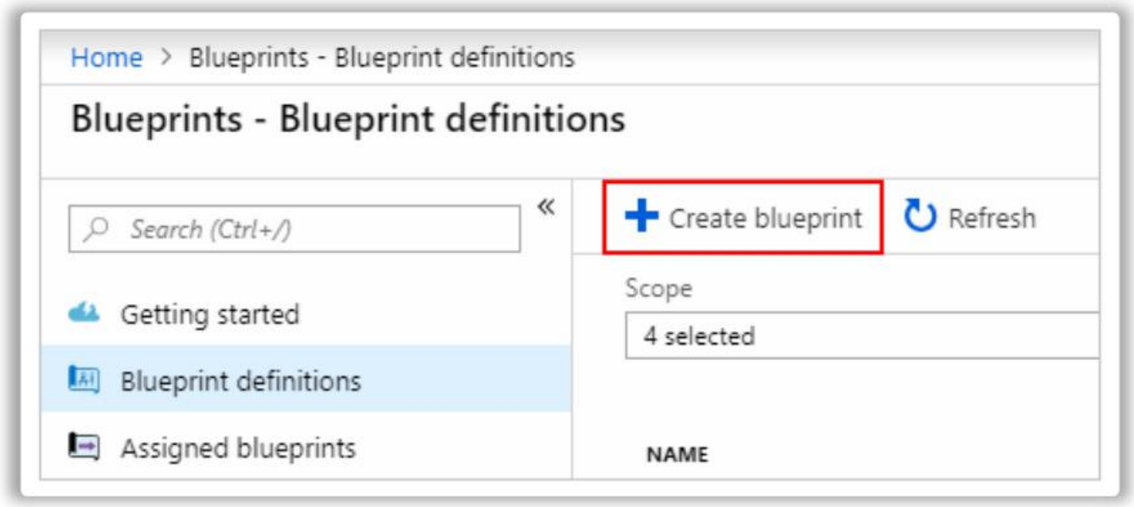


Figure 10.36: Creating a Blueprint

- From the list of built-in blueprints available at the top, select the **Start with blank blueprint** option.
- Input the **Blueprint name** as "**MyBlueprint**."
- **"Blueprint description"** can be left blank.
- Select ellipsis in the **Definition location** field.
- Choose the management group or subscription and click on **Select**.
- Ensure that the selected information is appropriate as the fields **Blueprint name** and **Definition location** cannot be changed at later stages.
- To add a role assignment implement the below steps (this change is subscription level):
    - Under **Subscription,** click on **+ Add artifact**.
    - For the **Artifact type**, select the **Role assignment**.
    - Under **Role,** choose **Contributor**.
    - **Add user, app, or group** field can be left with the checkbox indicating dynamic parameter.
    - Finally, click on **Add**. The artifact will be successfully added to the blueprint.

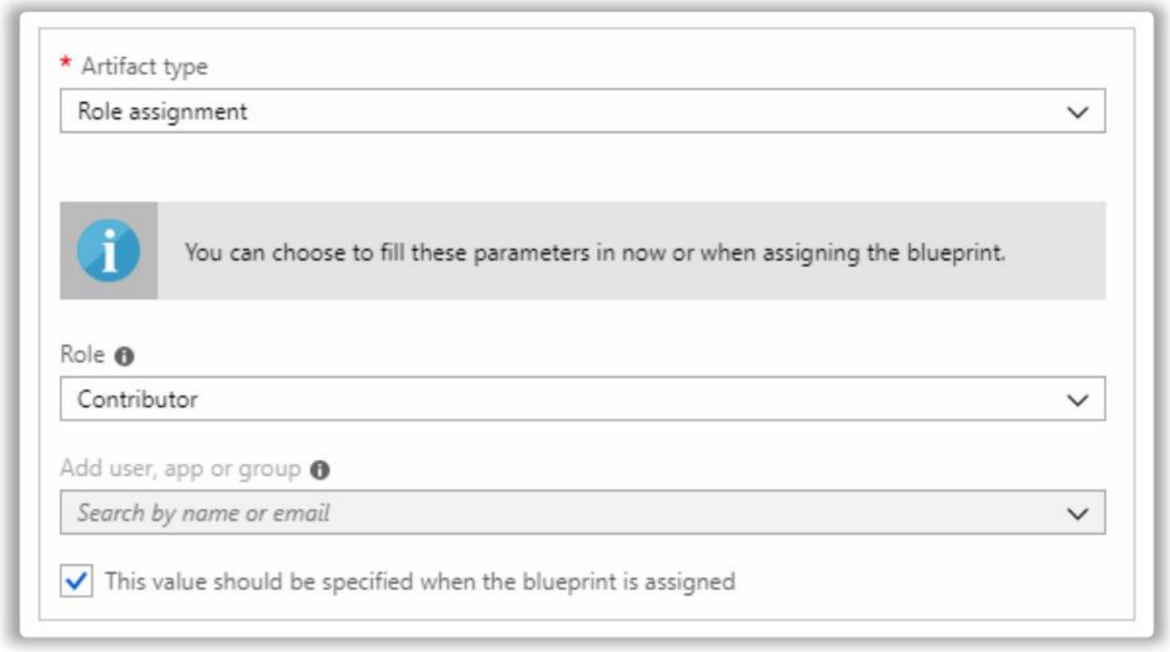


Figure 10.37: Adding a Role Assignment

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

- To add policy assignment follow the below steps (this is a subscription level change):
  - Under the role assignment artifact, click on **+ Add artifact**.
  - In **Artifact type,** choose **Policy assignment**.
  - The **Type** should be changed to **Built-in** and in **Search** enter a **tag**.
  - Select **Append tag and its default value to resource groups.**
  - Click on **Add**. The artifact is added to the blueprint.
- For the policy assignment, select the **Append tag and its default value to resource groups**.
- Next click on **Cancel**.
- Now add resource group:
  - Under **Subscription** click on **+Add artifact**.
  - For "**Artifact type"** select the required **Resource group**.
  - The **Artifact display name, Location, and Resource Group Name** should be left blank, and then enable the check box.
  - Click on **Add**.
- Next, under the resource group add a template:
  - Under resource group, click on **+ Add artifact**.
  - For **"Artifact type"** choose the **Azure Resource Manager template,** enter **StorageAccount** in **Artifact display name**.
  - Paste the following ARM template on the **Template** tab.
  - Select the **Parameters** tab and verify that **location** and **"storageAccountType"** are detected.

JSON Script:

```
{
"$schema":        "https://schema.management.azure.com/schemas/2015-01-
01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
"storageAccountType": {
"type": "string",
"defaultValue": "Standard_LRS",
"allowedValues": [
"Standard_LRS",
"Standard_GRS",
```


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

```
"Standard_ZRS",
"Premium_LRS"
],
"metadata": {
"description": "Storage Account type"
}
},
        "location": {
            "type": "string",
            "defaultValue": "[resourceGroup().location]",
            "metadata": {
                "description": "Location for all resources."
            }
        }
    },
    "variables": {
        "storageAccountName":                    "[concat('store',
uniquestring(resourceGroup().id))]"
    },
    "resources": [{
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[variables('storageAccountName')]",
        "location": "[parameters('location')]",
        "apiVersion": "2018-07-01",
        "sku": {
            "name": "[parameters('storageAccountType')]"
        },
        "kind": "StorageV2",
        "properties": {}
    }],
    "outputs": {
        "storageAccountName": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
        }
```

hide01.ir

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

```
        }
}
```

- **"storageAccountType"** should be unchecked. Under "**allowedValues"** it lists only values that are available in the ARM template.
- Click on **Add**. Observe **x out of y parameters populated** in the **Parameters** column

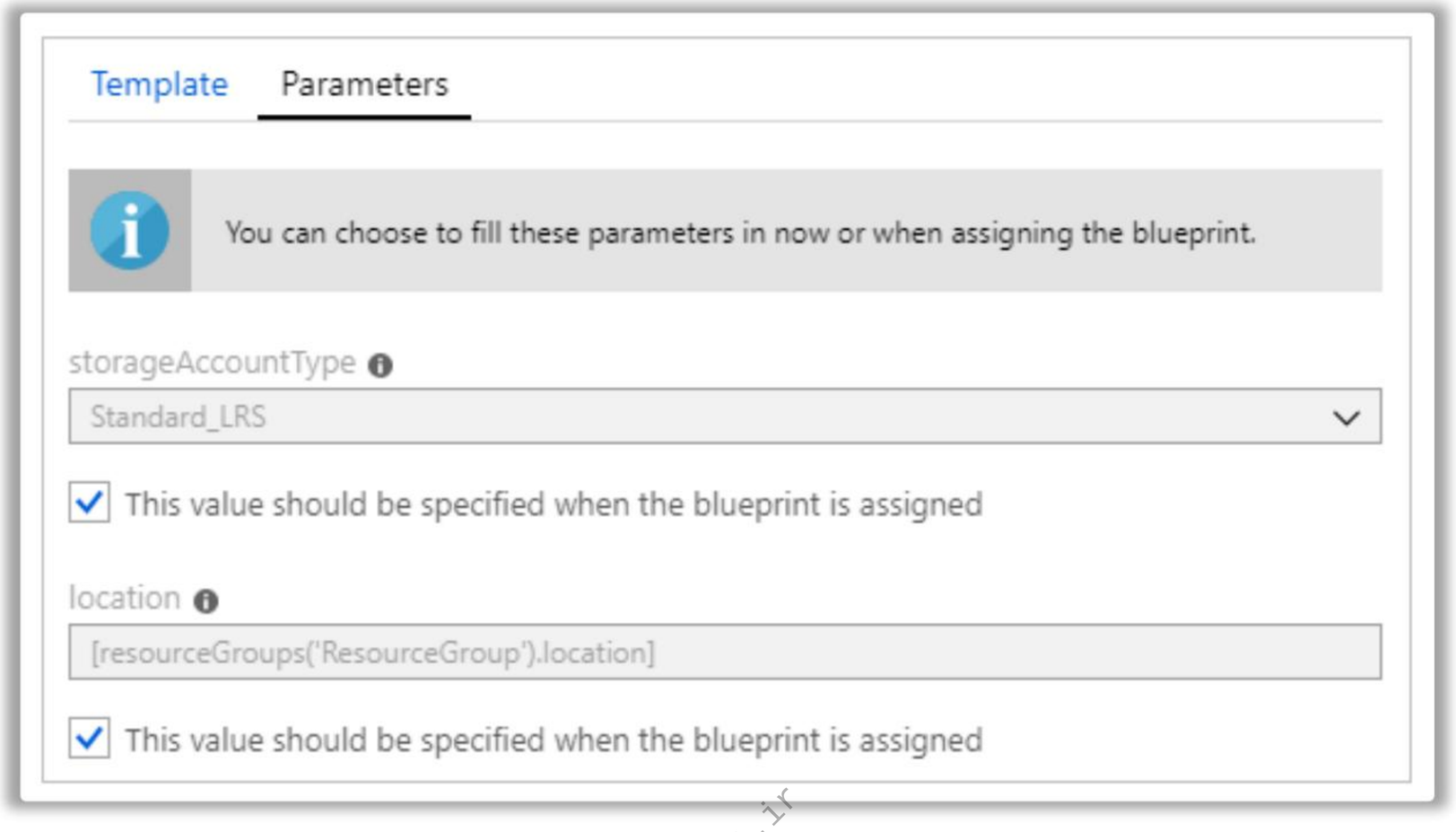


Figure 10.38: Parameters Column

- Finally, the addition of all the artifacts is done. Now click on **Save Draft**.

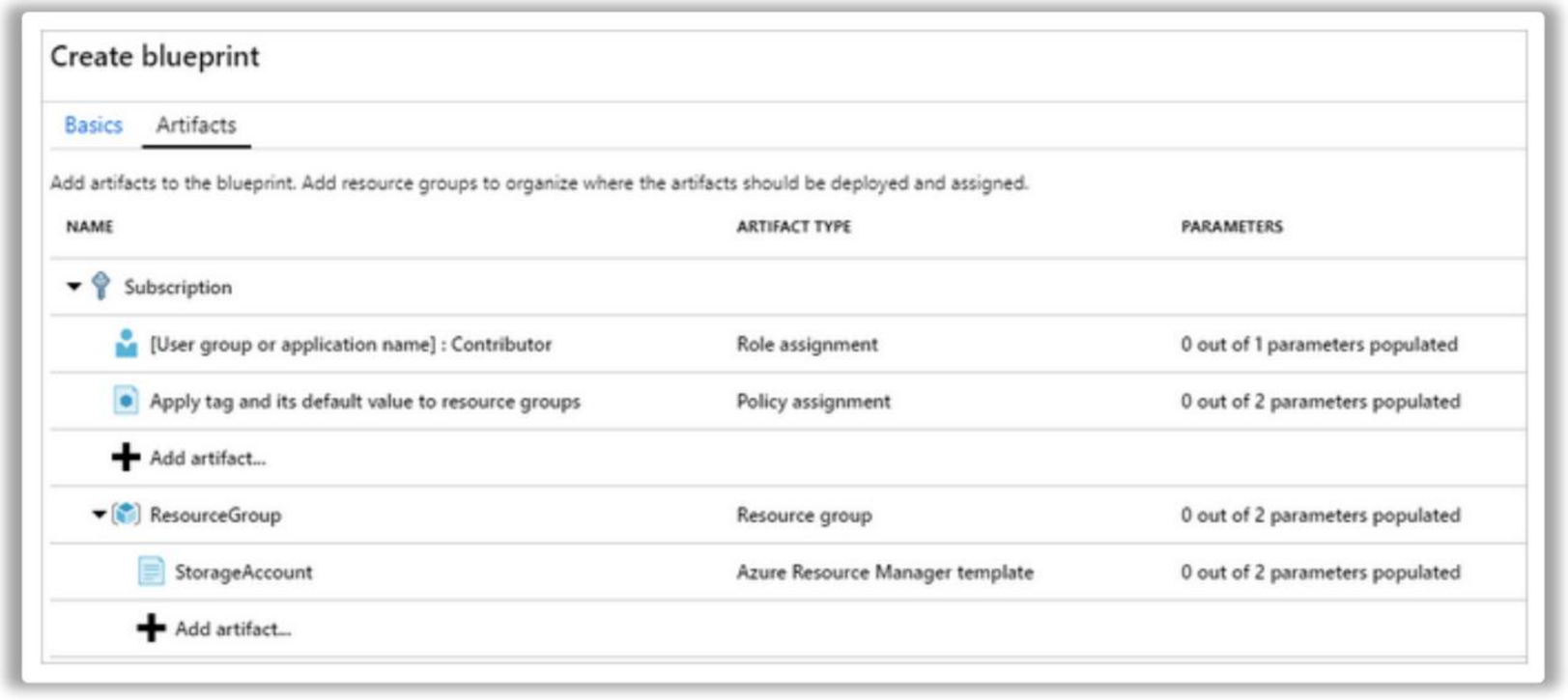


Figure 10.39: Adding Additional Details of All Artifacts

Azure Blueprints for Automation

Azure Blueprints are a collection of pre-configured compliance settings that are used for creating particular standards and requirements that govern the Azure security, services, and design implementations. These Azure Blueprints are reused and it is consistent and compliant with required regulations.

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

For the improved workload speed of consistency, deployment, and compliance, Azure's built-in automation features can be used. To avoid human errors from manual tasks and reduce the risk of security and compliance, automation of deployment and maintenance is required. This automation helps security and IT Operations teams to concentrate on higher tasks like protecting information, and business initiatives. Azure Blueprint facility enables organizations to deploy application environments consistently and quickly, these environments comply with both external and organizational regulations. It automates deployments of environment, which include policies, Azure roles, and resources. Among built-in configurations, Resource Manager scripts, or own configurations anyone can be used in Azure Blueprints. Resource Manager scripts are usually used for small scopes. An initial template can be used from the collection of Security and Compliance Blueprints samples.

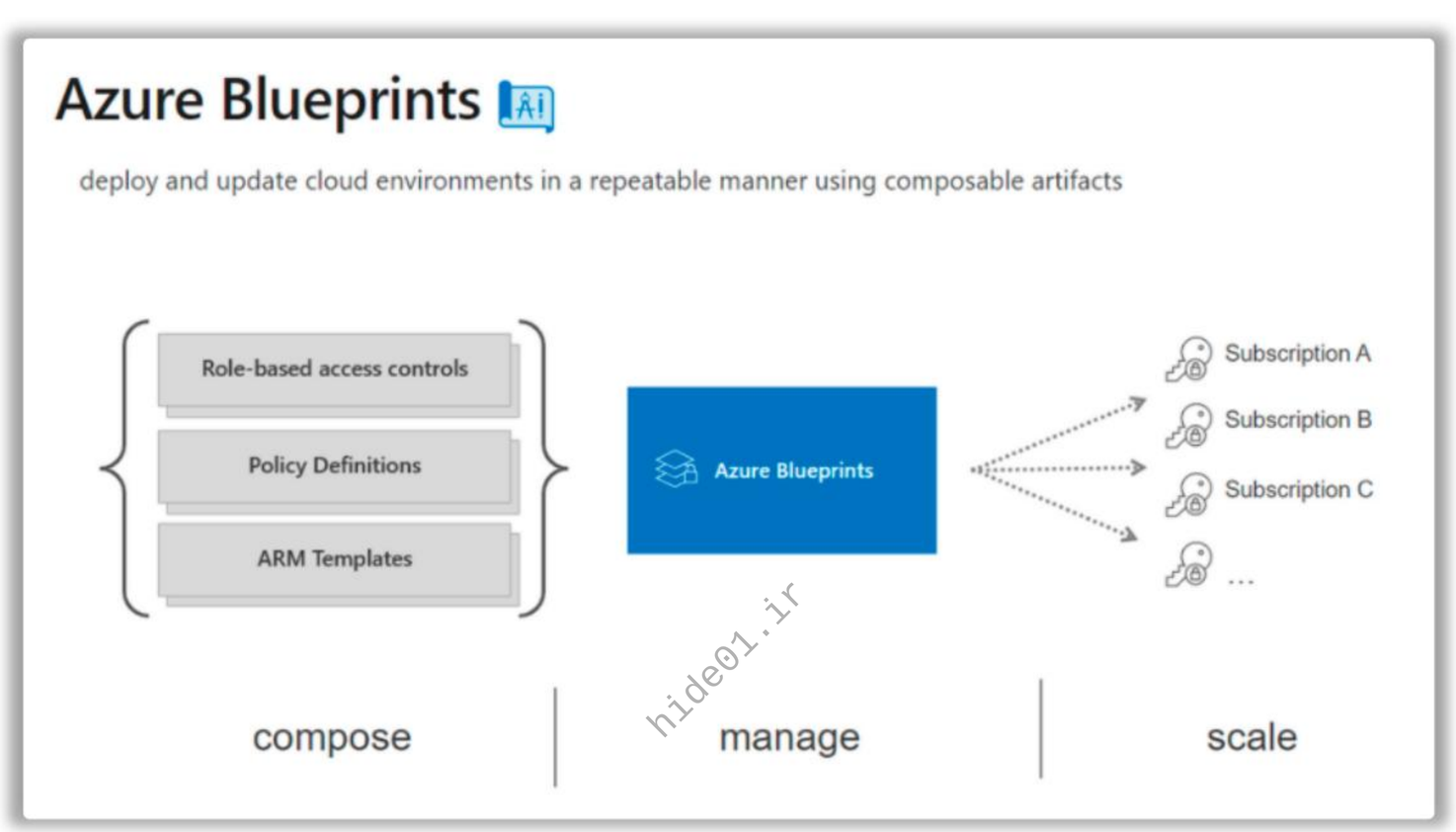
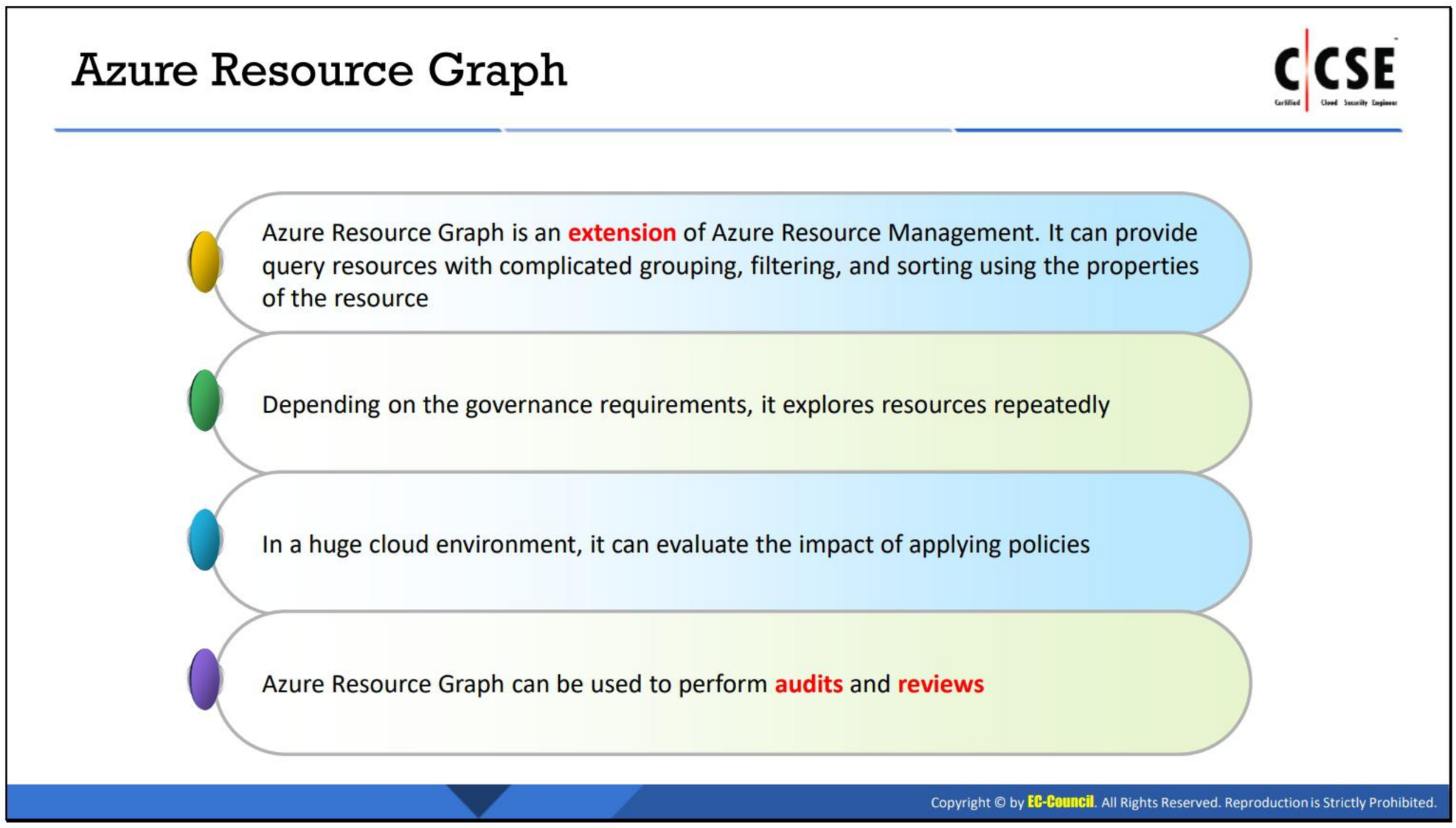


Figure 10.40: Azure Blueprints for Automation

Source: https://www.microsoft.com

Initially, the Azure Blueprints should be created which can be done using various ways like PowerShell, Azure portal, or REST API. It can be created from a blank Blueprint, existing samples, or custom scripts. Select the subscriptions in which this Blueprint has to be deployed. If required, Blueprints can be updated according to the compliance regulations like ISO 27001, PCI-DSS, and NIST.

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



Azure Resource Graph

Azure Resource Graph is an extension of Azure Resource Management. It is efficient with high-performance ability and governs the environment effectively. Azure resource graph has the following features:

hide01.ir

- It has the capability of providing query resources with complicated grouping, filtering, and sorting using properties of the resource.
- Depending on the governance requirements, it explores resources repeatedly.
- In a huge cloud environment, it can evaluate the impact of applying policies.
- It can detail changes made to the resource properties. This is a preview feature.

Steps to Run Resource Graph Query:

- Sign in to the Azure portal.
- From the left navigation panel. Click on **All services.**
- Search for **Resource Graph Explorer** and click on it.
- Enter the below query in **Query 1** and select **Run query**.

```
Resources | project name, type | limit 5
```

- The response can be viewed in the **Results** tab.
- To get the details of the query like duration and result count select the **Messages** tab, this also provides details of errors if available.

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

- Update the query as mentioned below and select **Run query**.

```
order by the Name property: Resources | project name, type |
limit 5 | order by name asc
```

- Again update the query as mentioned below and click on **Run query**.

```
order by the Name property and then limit to the top five
results: Resources | project name, type | order by name asc |
limit 5
```

If there is no change in the environment and the final query is executed multiple times, then the results obtained will maintain consistency and sequence depending on the Name property. However, the results are limited to five as mentioned in the query.

The Azure Resource Graph can be used to perform audits and reviews. For example, to verify the storage accounts in which HTTPS or encryption is not enforced. To review this, the below script should be executed in Azure CLI or PowerShell.

```
resources
| where type == "microsoft.storage/storageaccounts"
|                                                                  where
aliases["Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly"]
== "false"
       or
aliases["Microsoft.Storage/storageAccounts/enableFileEncryption"]    ==
"false"
       or
aliases["Microsoft.Storage/storageAccounts/enableBlobEncryption"]    ==
"false"
| project name, kind,  resourceGroup, subscriptionId
```

hide01.ir

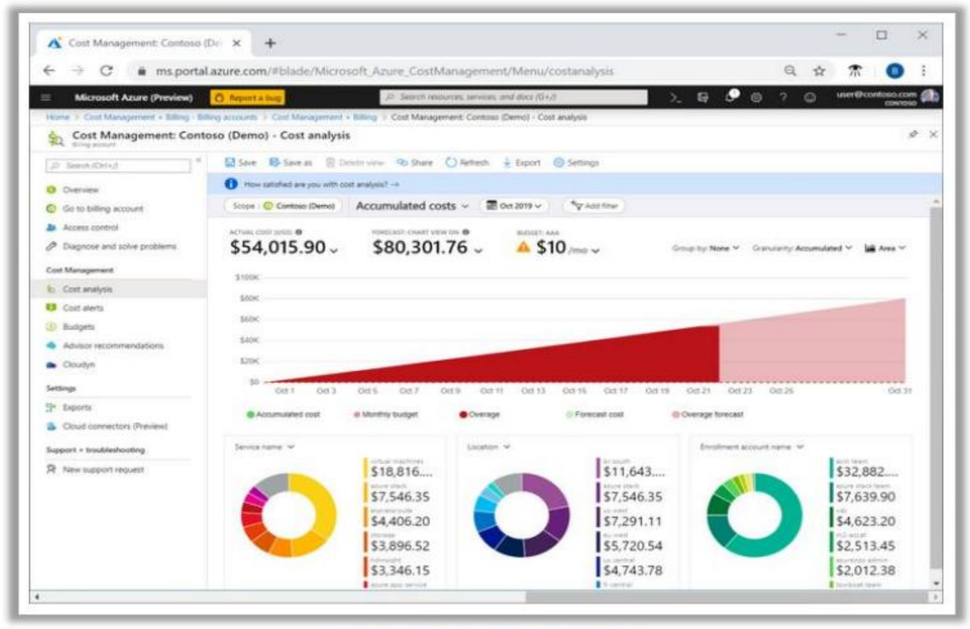
If there is a requirement of running the quries that should result resources based on the particular subscription irrespective of the geolocation, then the following script should be executed in Azure CLI or PowerShell.

```
Resources
| where subscriptionId == 'YOUR SUBSCRIPTION GUID'
```


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

Azure Cost Management

- Azure Cost Management is a SaaS solution provided by Microsoft as a **governance service** that allows organizations to allocate, monitor, and optimize the cost in a multi-cloud environment



Azure Cost Management

Source: https://www.microsoft.com

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

Azure Cost Management

Azure Cost Management is a SaaS solution provided by Microsoft as a governance service that allows organizations to allocate, monitor, and optimize the multi-cloud environment cost. It provides optimization, the end-to-end cost management, which is a cost-cutting benefit for the organizations. The features of Azure Cost Management is extended to the following:

- Perform Administrative events like payment of the bill.
- Data analysis over the costs incurred.
- Setting up of threshold limits.
- Detect changes in workload that result in optimization.
- Downloading the data usage and costs that provide monthly invoice generation.

Most organizations prefer moving their services to the cloud, as this is a cost-saving compared to on-premises, but cloud accounts can end up billing very huge if proper care is not taken.

Cloudyn is a SaaS cost management which is a multi-cloud monitoring tool collaborated by Microsoft. After the migration of Cloudyn features into the Azure value Management portal, it became available for all the Azure users who are paying for Microsoft cloud services. This helps organizations in key components like monitoring the cloud spends, increase the accountability of structure, and optimization of cloud strength.

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

Monitoring Cloud Spends: Azure Cost Management allows administrators to fetch and view the billing history and facilitates viewing of estimated future billings. Organizations can analyze the cost performance using yearly, monthly, or daily history and develop changes in the usage of required. This provides breaking of charges depending on resources and time frame.

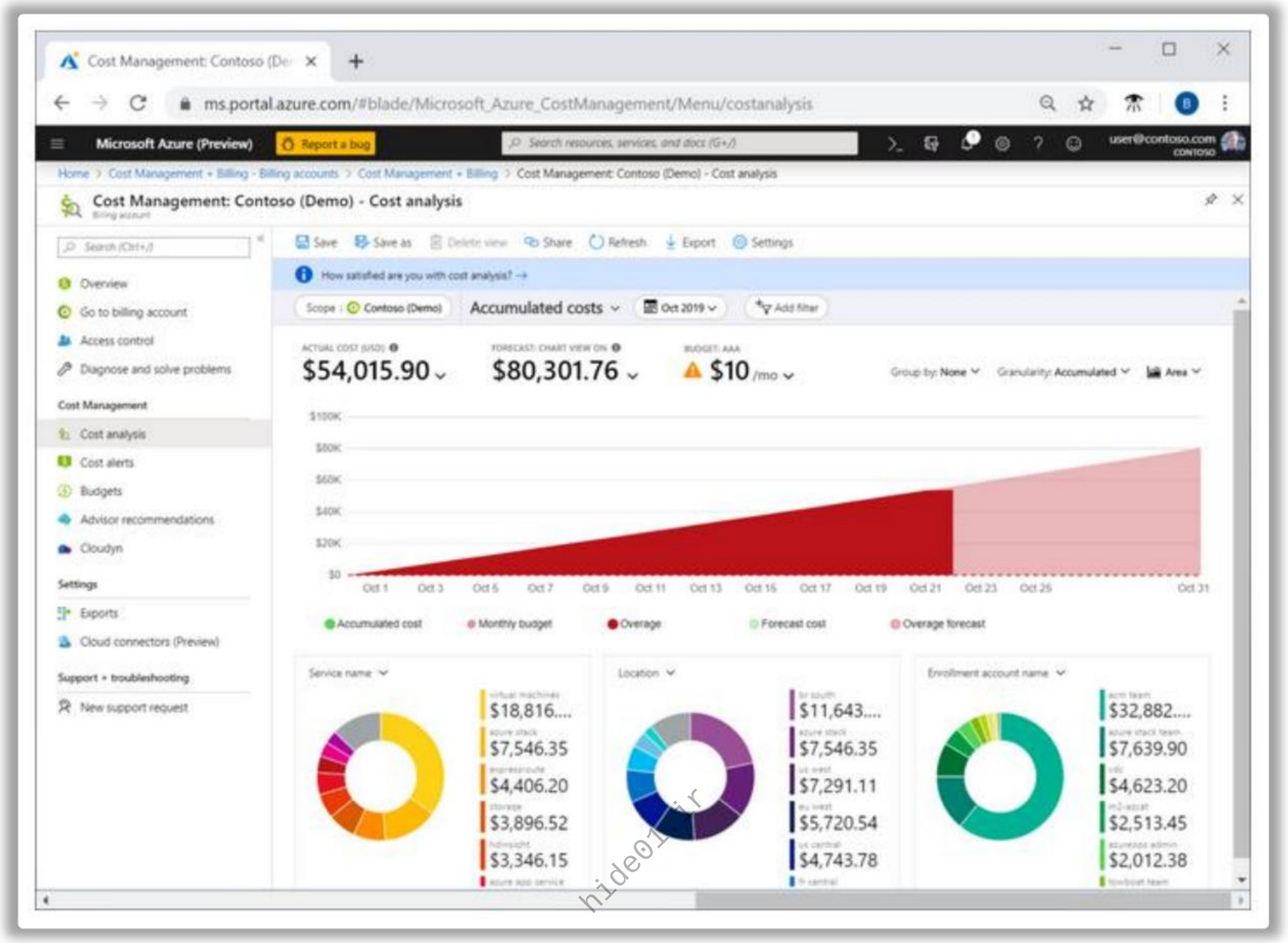


Figure 10.41: Dashboard of Azure Cost Management

Source: https://www.microsoft.com

Enhancement of Organizational Accountability: Microsoft Azure Cost Management provides the reports by splitting the cost incurred by resources into different buckets. As different resources are handled by different teams in the organization, accountability derives from user logs present in Azure Cost Management after the implementation of cost models. Azure provides a facility to set up alerts to avoid overspending either by teams or individuals.

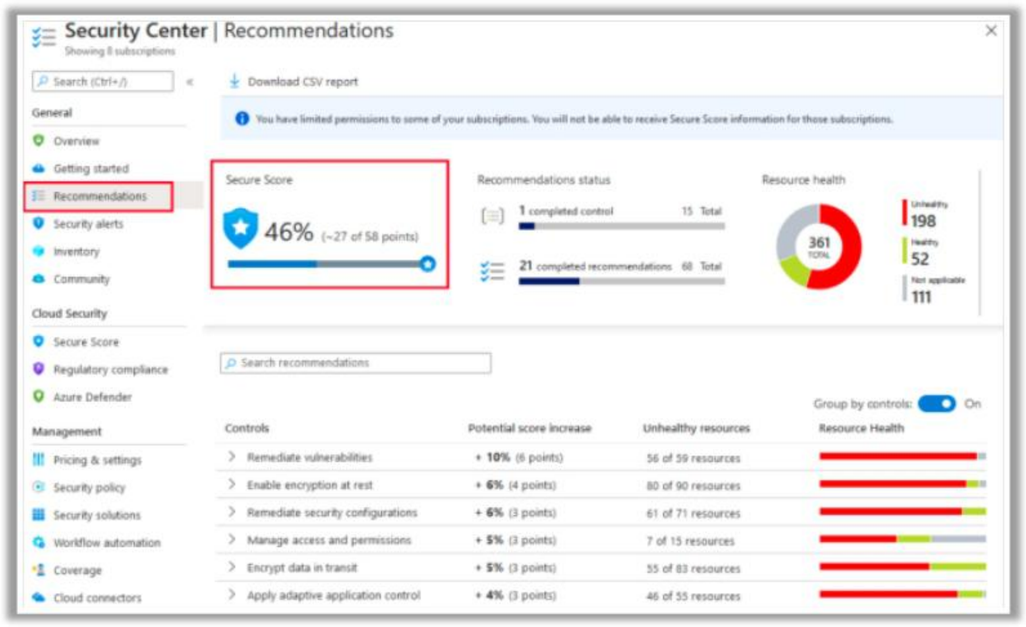
Optimization of Cloud Efficiency: In Microsoft Azure value Management the cloud optimization is a core tenant, but among all possible ways this is the least effective component. In this method, the surplus is eradicated manually where this is not feasible to perform over reach resource.

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

Operationalizing Azure Secure Score

- To monitor and improve the **security posture**, stakeholders should be assigned to use Secure Score in Azure Security Center

- This helps in improving the security posture by quickly finding and remediating common security risks, which ultimately reduces the risk of the organization



Azure Secure Score

Source: https://www.microsoft.com

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

Operationalizing Azure Secure Score

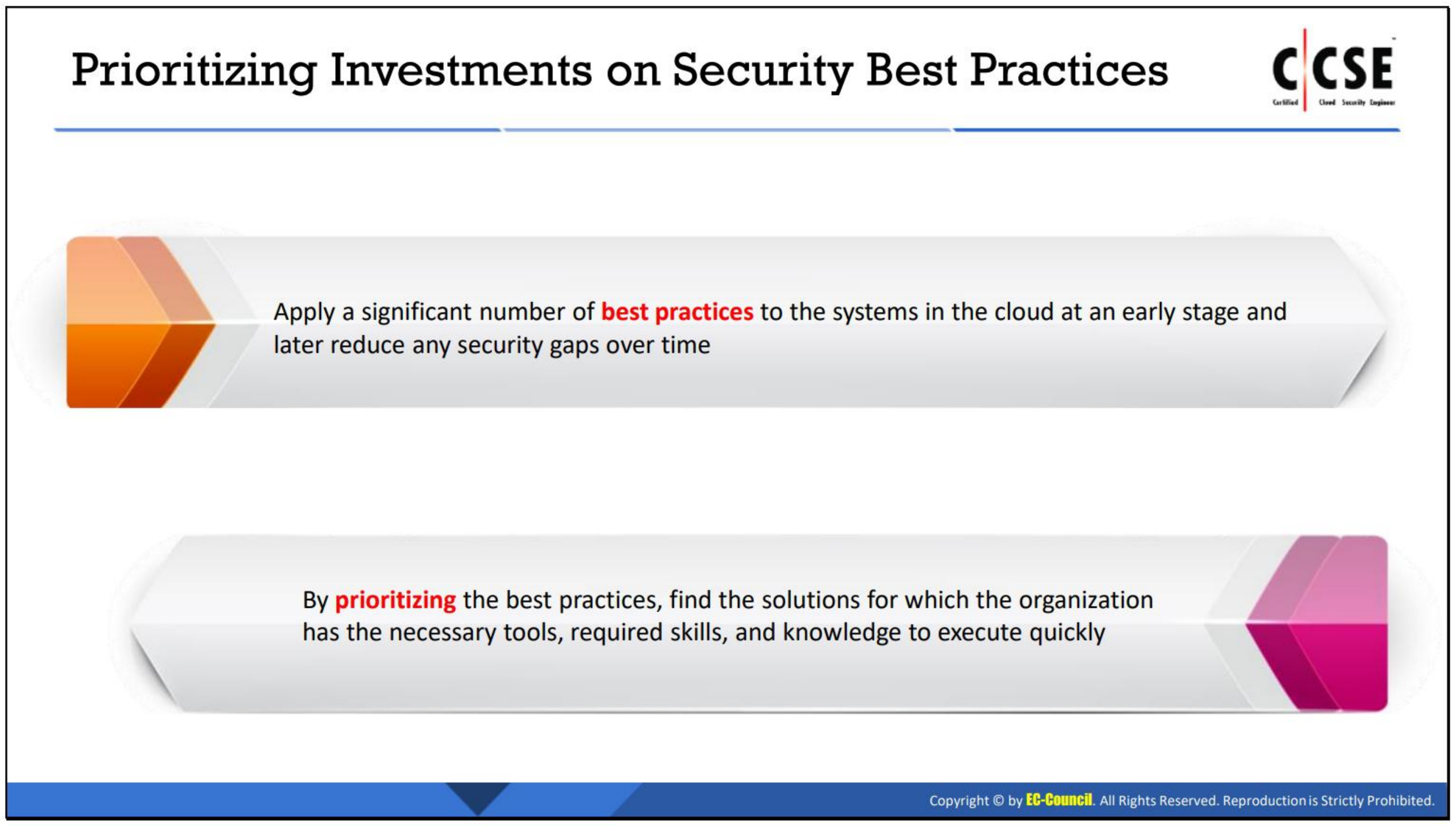
Azure Secure Score is a measurement of the security posture of the organization. This helps the organization by protecting from various threats vectors, Common Vulnerabilities Exposures (CVEs) with the use of improved security configuration and modification. The two key primary objectives of Azure Security Center are (a) Creating awareness of the current security situation to the users and (b) Helping the users to improve overall security efficiently. To satisfy these objectives Azure Secure Score is used.

To monitor and improve security posture, stakeholders should be assigned to use Secure Score that is available in Azure Security Center. This helps in security posture improvement by quickly finding and remediating common security risks, which ultimately reduces the risk of the organization. A regular pace should be set up for Azure secure score review, if possible, it should be set to monthly, and initiatives should be planned accordingly for the improvement.

Note: Security posture management is an emerging function, some organizations may have this as a dedicated team and some others may have this as a responsibility that is taken by one or more existing teams.

The Secure Score of different resources is handled by different teams. For example, App Services should be reviewed by Application Development or Security teams, Containers should be reviewed either solely or combinedly by Application Development, IT Operations, and Infrastructure teams.

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



Prioritizing Investments on Security Best Practices

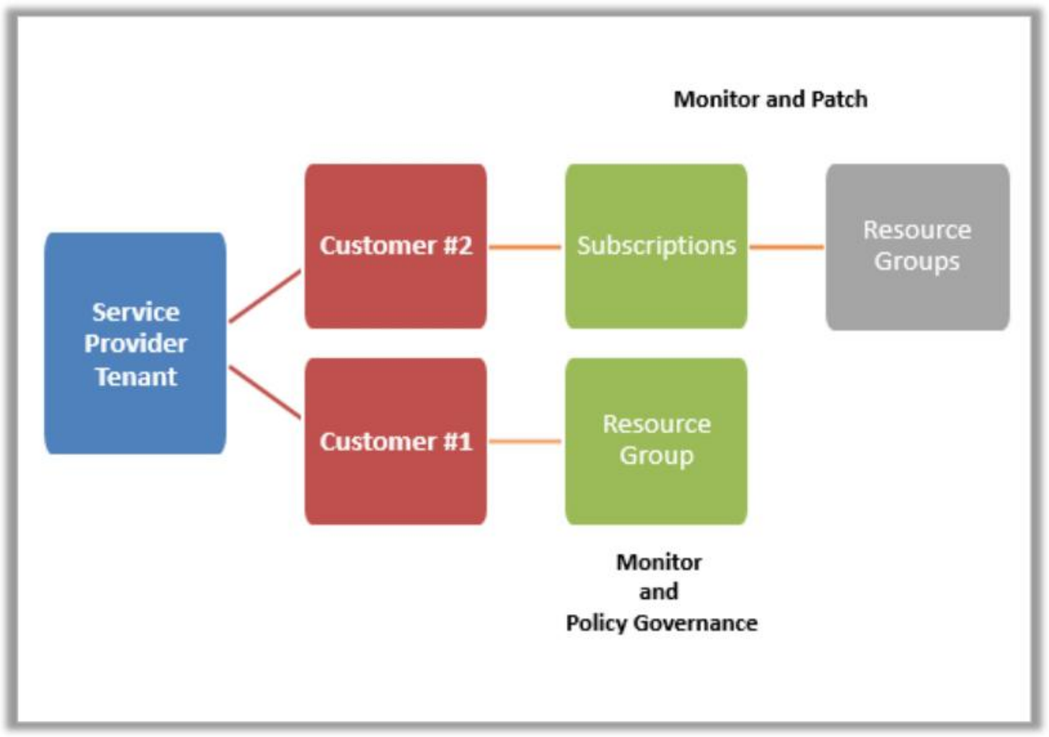
Generally, security best practices should be applied before any damage takes place to the systems in the cloud, but most enterprise organizations are not implementing this. Some factors like project constraints, business goals, and other factors cause organizations to balance security risks. It is recommended to apply a significant number of best practices at an early stage and later reduce any security gaps over time. Evaluation of the following considerations is recommended when prioritizing what to follow first:

- **Highly Exposed Systems and High Business Impact:** These include systems with direct intrinsic values and also systems that provide different ways for attackers.
- **Implementing Mitigations is Easy:** By prioritizing the best practices, find the solutions that can be executed quickly since the organization has the necessary tools, required skills, and knowledge. For example, implementing a Web Application Firewall (WAF) for the protection of the legacy application. This short-term prioritizing method should not be used excessively or exclusively as it may increase the level of risk by exposing critical risks for prolonged periods.

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

Managing Connected Tenants

- A tenant is a representation of an organization that maintains and administers instances of **Microsoft cloud services** such as Active Directory and Office 365
- It provides cloud administrators to manage groups, users, and their permissions from a single point
- Use **Azure Lighthouse** to handle multiple customers in different tenants without different logins



Managing Tenants with Azure Lighthouse

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

Managing Connected Tenants

A tenant is a representation of an organization that maintains and administers Microsoft cloud services instances. It is used to refer to Microsoft services like Active Directory and Office 365. An Azure tenant is a single instance of Azure Active Directory which is a part of Microsoft's cloud platform. It provides cloud administrators to manage groups, users, and their permissions in a single place. Azure AD's tenants are unique and are separate from each other.

Ensure your security organization is well-acquainted with all enrollments and associated subscriptions connected to your existing environment (via Site-Site VPN or ExpressRoute) and supervising as a part of the enterprise. Security organizations require visibility of the Azure resources that are part of the organization's enterprise environment. Access to security organizations is required for the evaluation of risk and identification of organizational policies and applicable regulatory requirements, which should be followed. Make sure that the Azure environments that are connected to the production environment should be enforced with the organizational IT governance controls and policy for security.

All the existing connected tenants should be discovered using the tool provided by Microsoft. Service providers are required to log in to the Azure portal that is related to the customer's tenant to manage Azure resources for customers. To avoid this Azure Lighthouse can be used, this allows the service providers to handle multiple customers in different tenants without different logins. The below image shows that the service provider has two customers where they hold different access levels and responsibilities. All these resources could be accessed by logging in to the service providers tenants through Azure Lighthouse.

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

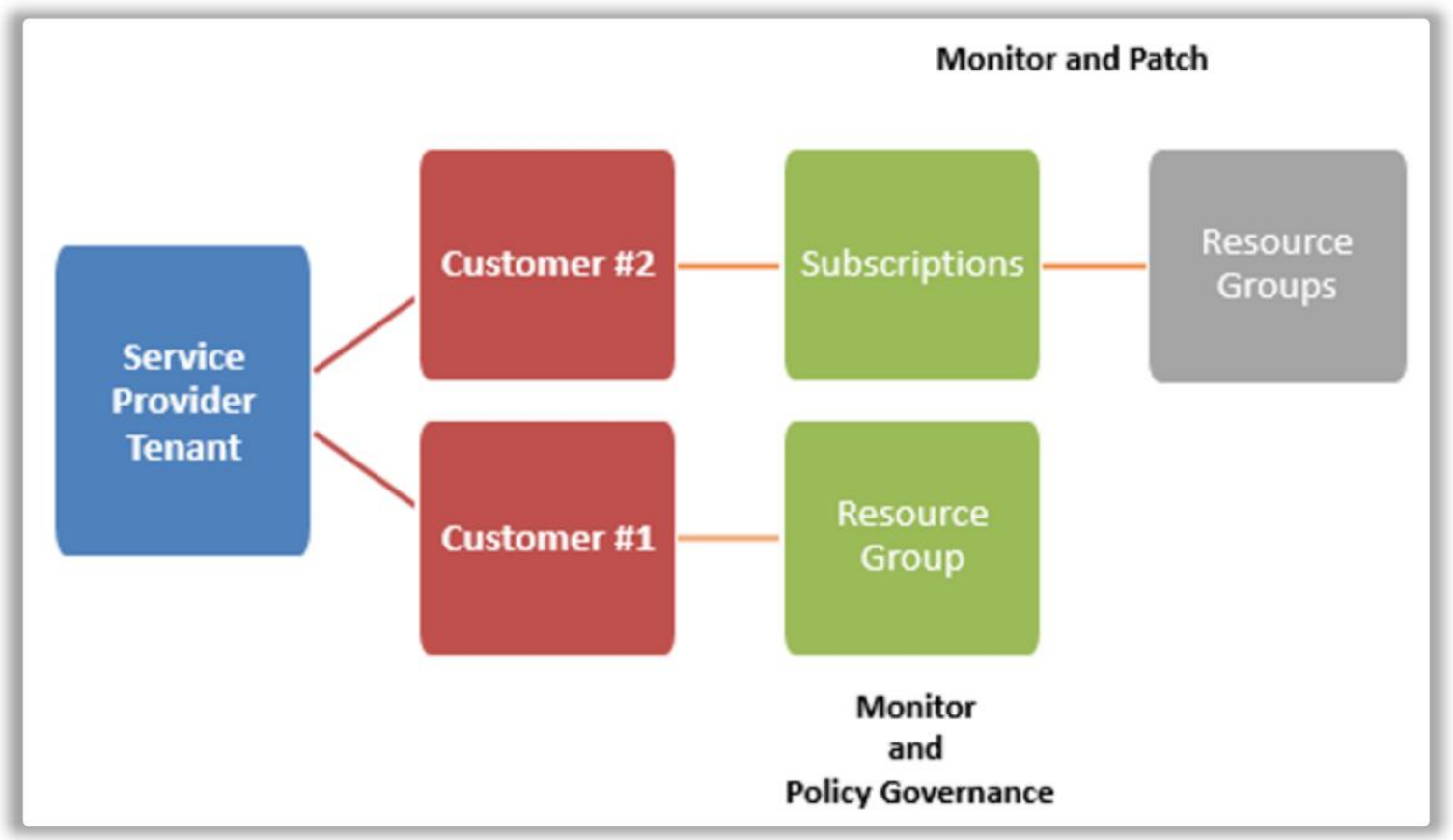
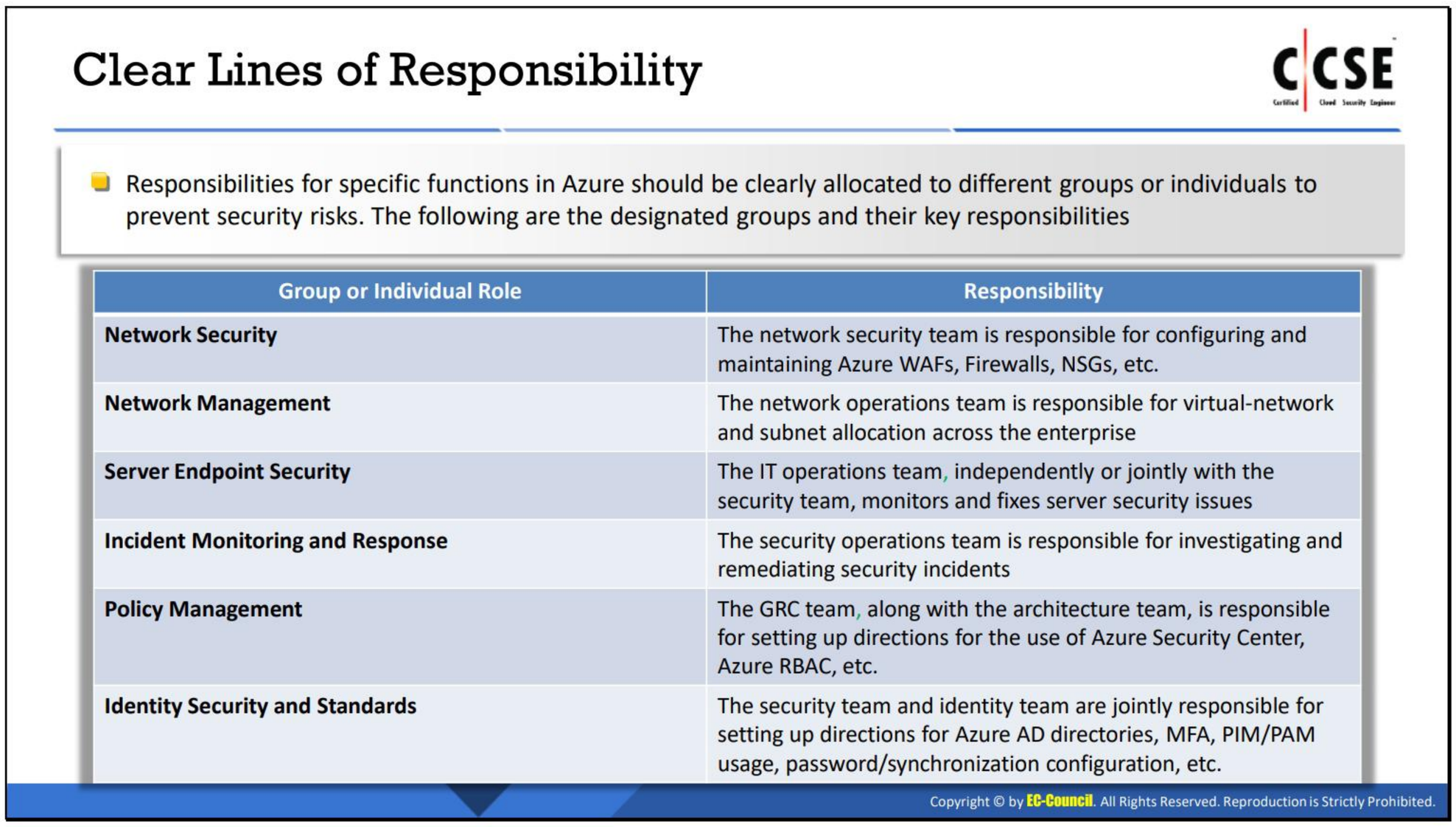


Figure 10.42: Managing Tenants with Azure Lighthouse

hide01.ir

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



Clear Lines of Responsibility

Responsible person should be designated for specific functions in Azure. It is important to document and share the contacts of responsible persons of different functions, this creates consistency and provides a way for communication. This avoids any confusion that could lead to human and automation errors, which creates a security risk.

The following are the designated groups with their responsible key functions:

Network Security: The responsibility of network security is usually the existing network security team. The functions of network security include Azure Firewall configuration and maintenance, Network Virtual Appliances, Network Security Groups (NSGs), Application Security Group (ASGs), and Web Application Firewalls (WAFs), etc.

Network Management: It is handled by the network operations team. The key functional is enterprise-wide virtual network and subnet allocation.

Server Endpoint Security: IT Operations team, security team, or jointly takes care of this group. Monitoring and remediating server security is the function of this group. For example, configuration, patching, endpoint security, etc.

Incident Monitoring and Response: This group is handled by the security operation team. The key function of this group is to investigate and remediate security incidents that are in Security Information and Event Management (SIEM) or source dashboard.

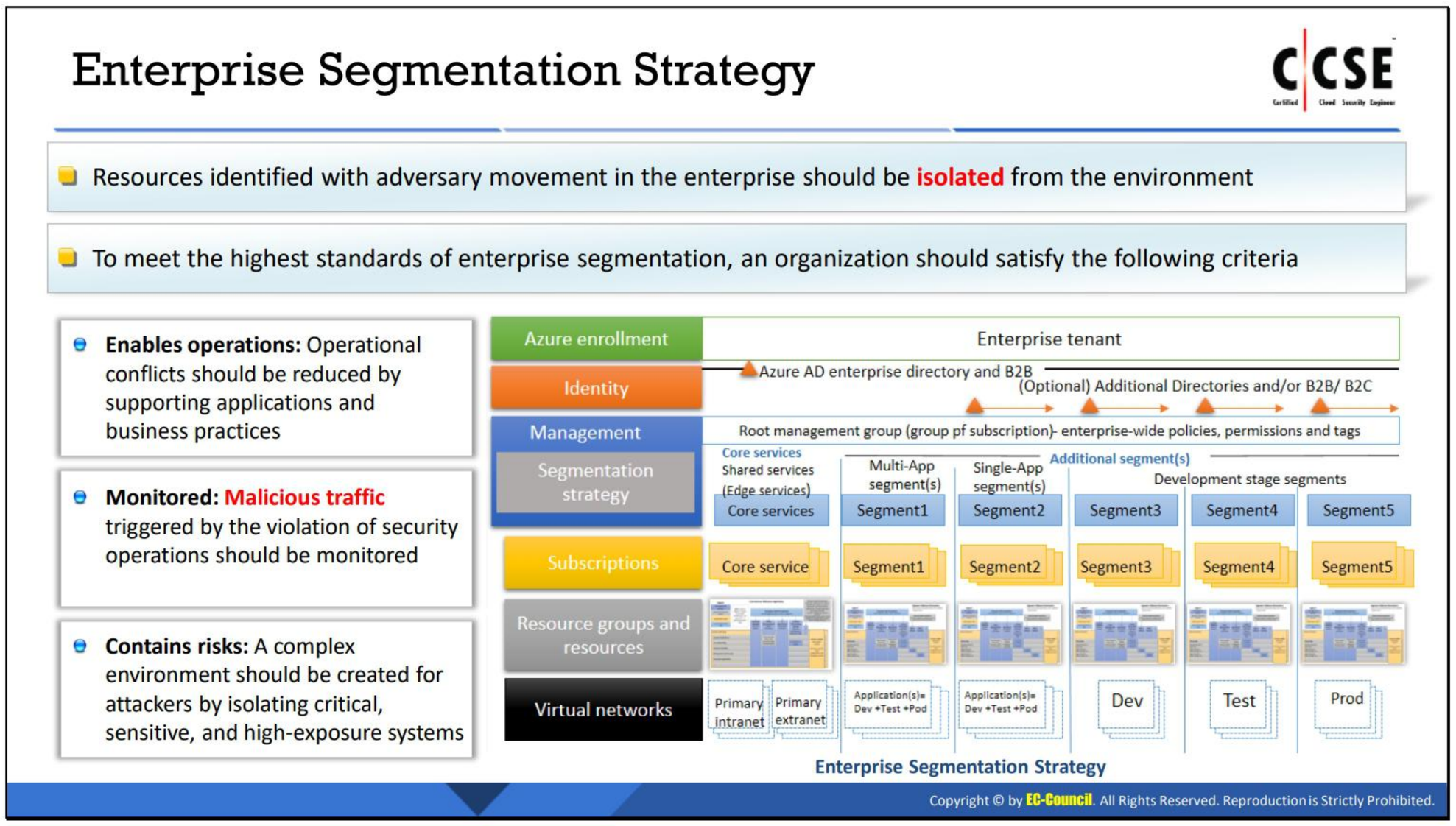
Policy Management: This group responsibility is generally a combination of two teams i.e, the Governance Risk and Compiance (GRC) team and Architecture team. The key functions for this group are setting up directions for use of Azure role-based access control (RBAC), administrator protection strategy, Azure Security Center, and Azure policy to govern Azure resources.

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

Identity Security and Standard: This group is usually handled by two teams and they are the Security team and the Identity team. The key functions of this group include "Set direction for Azure AD directories", Privileged Identity Management (PIM) and Privileged Access Management (PAM) usage, Multi-Factor Authentication, and Application Identity Standards.

hide01.ir

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



Enterprise Segmentation Strategy

The identified resources with adversary movement in the enterprise should be isolated from the environment. It helps technical teams in guiding consistent segmentation, this process is done by applications, networking, identity, etc. Comparing to network segmentation the enterprise segmentation is considered a higher factor. The traditional segmentations other than this method has a high failure rate due to the involvement of multiple technical teams without focusing on business use cases. This process creates multiple firewall exceptions due to support issues. An integrated enterprise segmentation helps the required technical teams like Application, IT, and Security teams in guiding security containment assurances. This clear guidance avoids the risk of automation failures and human errors that may end up in operational downtime or security vulnerabilities. Concerning Zero Trust Principles, Microsoft recommends the following:

- Make sure that the technical teams form a single enterprise segmentation strategy is formed.
- Considering applications, devices, and identity, care should be taken in expanding containment using a modern perimeter that depends on the zero-trust principle.

If the organization needs to meet the best enterprise segmentation, it should meet the following criteria:

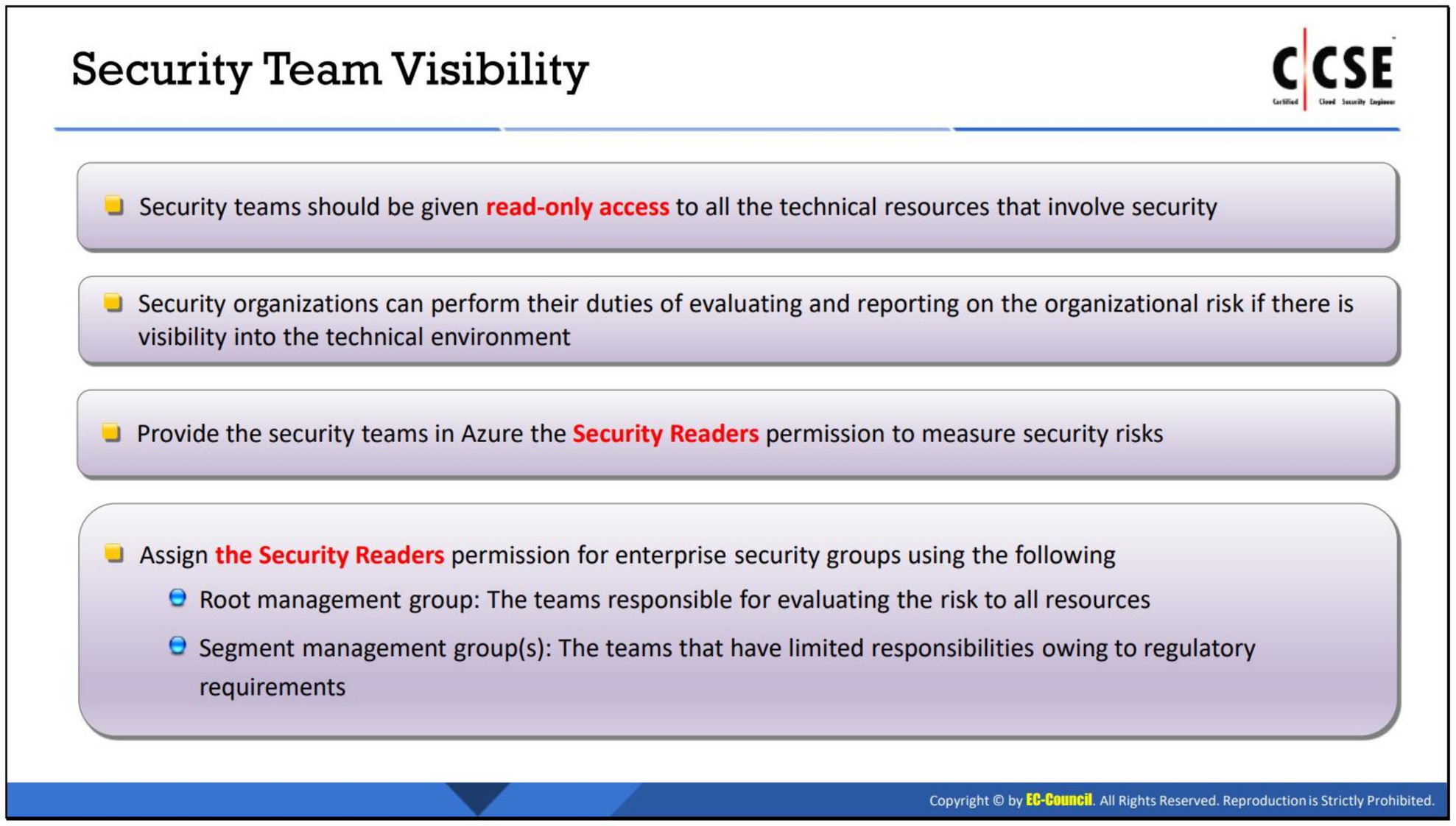
- **Enables Operations:** The operation conflicts should be reduced by supporting applications and business practices.
- **Contains Risks:** Creates a complex environment for attackers by isolating critical, sensitive, and high exposure systems.

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

- **Monitored:** Malicious traffic that is triggered due to the violation of the security operations should be monitored.

hide01.ir

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



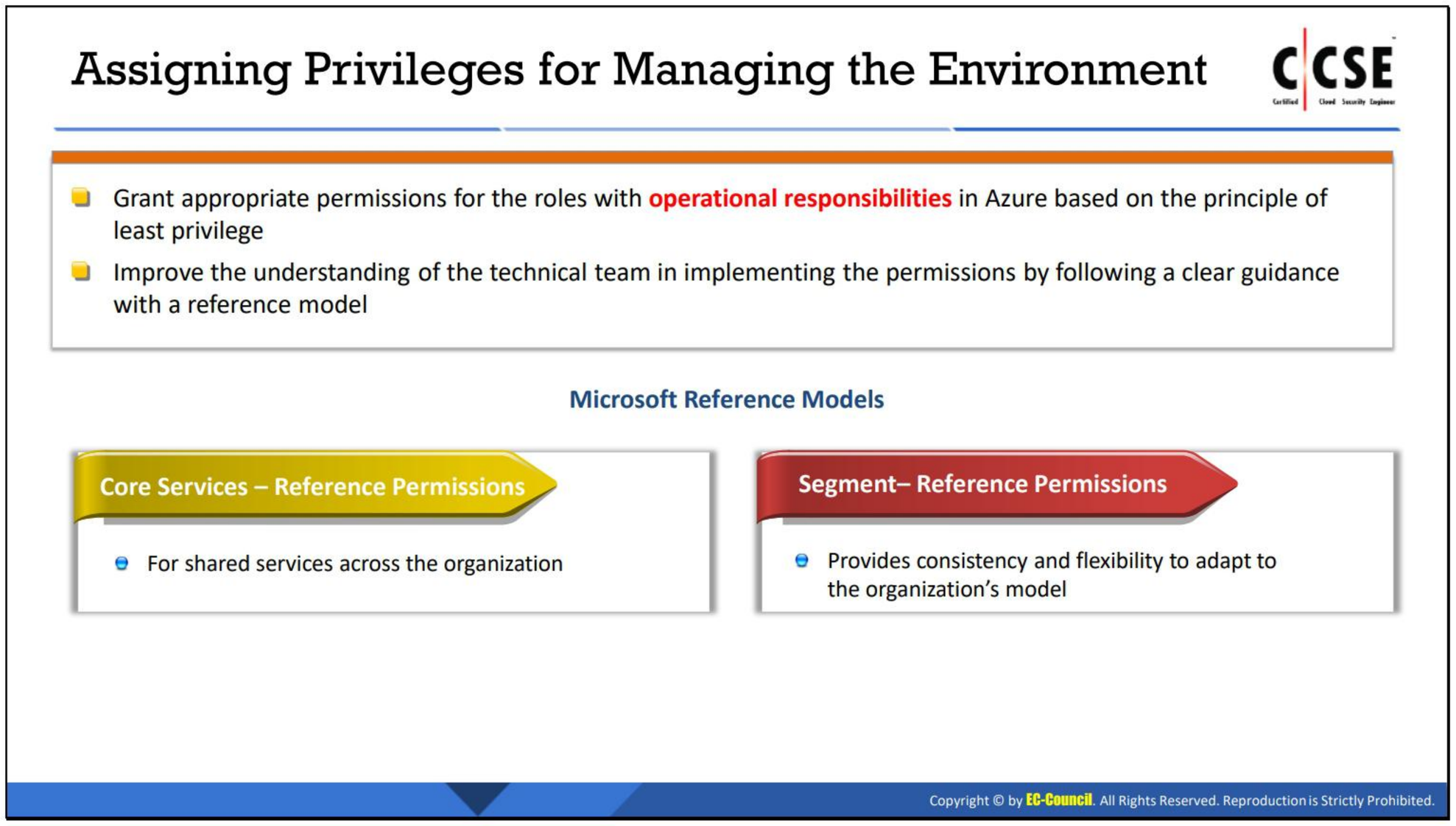
Security Team Visibility

Security teams should be given read-only access to all the technical resources that have security involvement. The security organizations can perform their duties of evaluating and reporting on the organizational risk if there is visibility in the technical environment. Due to the non-visibility of the technical environment, the security teams might need the help of information that is provided from groups, personnel operating the particular environment, and those who have a potential conflict of interest. If the security team has any requirement of operation or enforcing policies on Azure resources, then they are granted additional privileges. For example, when the "Security Readers" permission in Azure is given then they get access to measure security risk, but that does not provide any access to the data for what it is measuring the security risk. For enterprise security groups with extensive concern over Azure security, this permission can be assigned using:

- Root management group: This is for the teams that are responsible for reviewing and reporting risk on any resource.
- Segment management groups: This is for the teams that have limited responsibility scope.

As the security perspective has very wide access to the environment, they should be considered as critical impact accounts, and the protection applied should be the same as administrators.

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



Assigning Privileges for Managing the Environment

Secure the Azure environment from unauthorized access by assigning the appropriate privileges to users. The appropriate permissions for the different roles with operational responsibilities should be granted by following the principle of least privilege. The users should be granted only the required access controls. The technical teams should be trained to follow clear guidance with the Microsoft reference models in implementing the permissions. The Microsoft Reference Models are

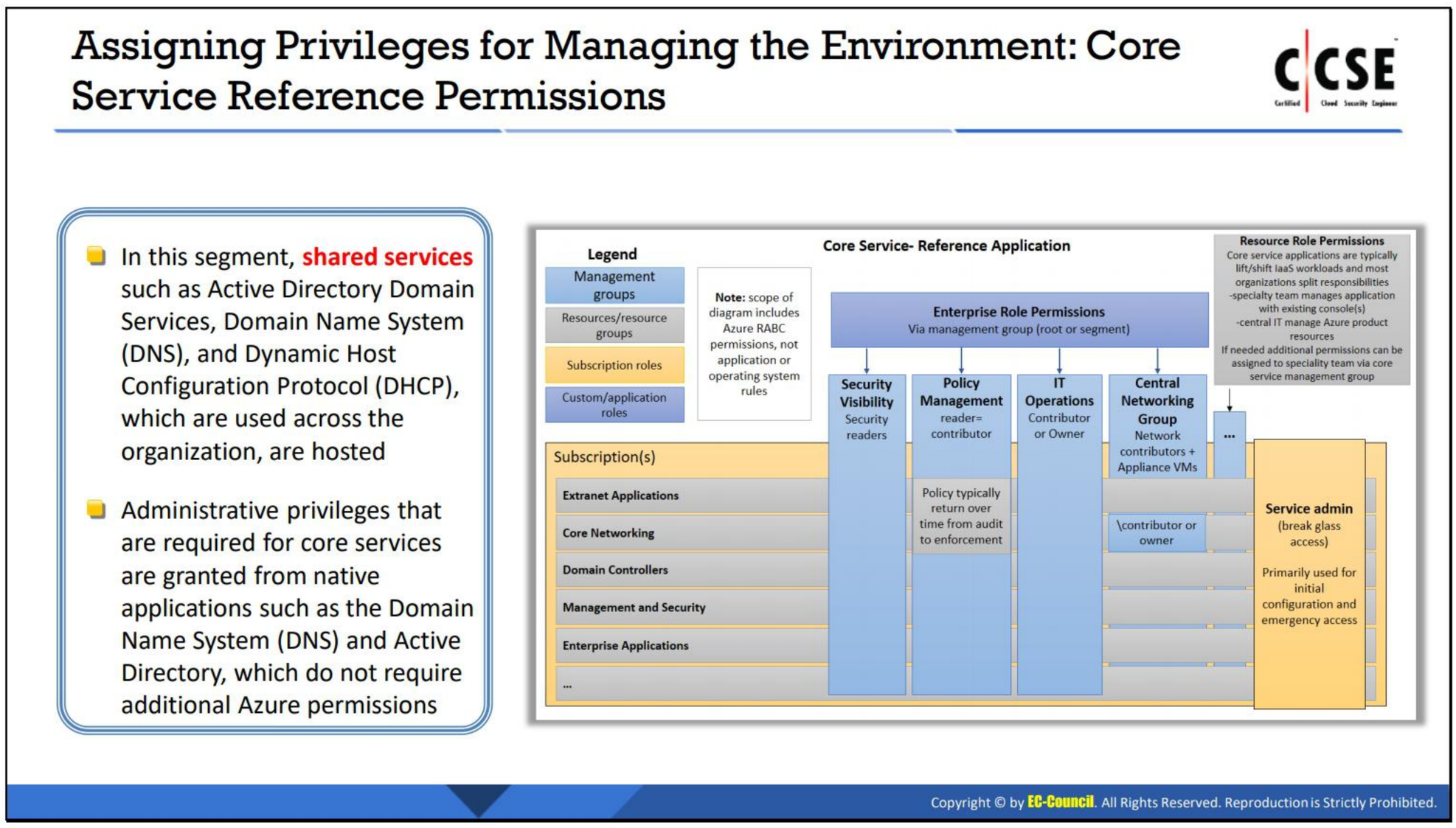
- **Core Services- Reference Permissions**

  The core service reference model should be followed for shared services across the organization.

- **Segment- Reference Permissions**

  The segment reference model provides consistency and flexibility to adapt to the organization's security model.

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



Assigning Privileges for Managing the Environment: Core Service Reference Permissions

In this segment, shared services are hosted that are used across the organization. Usually, shared services include Active Directory Domain Services, System Management Tools that are hosted on Azure Infrastructure as a Service virtual machines, Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP).

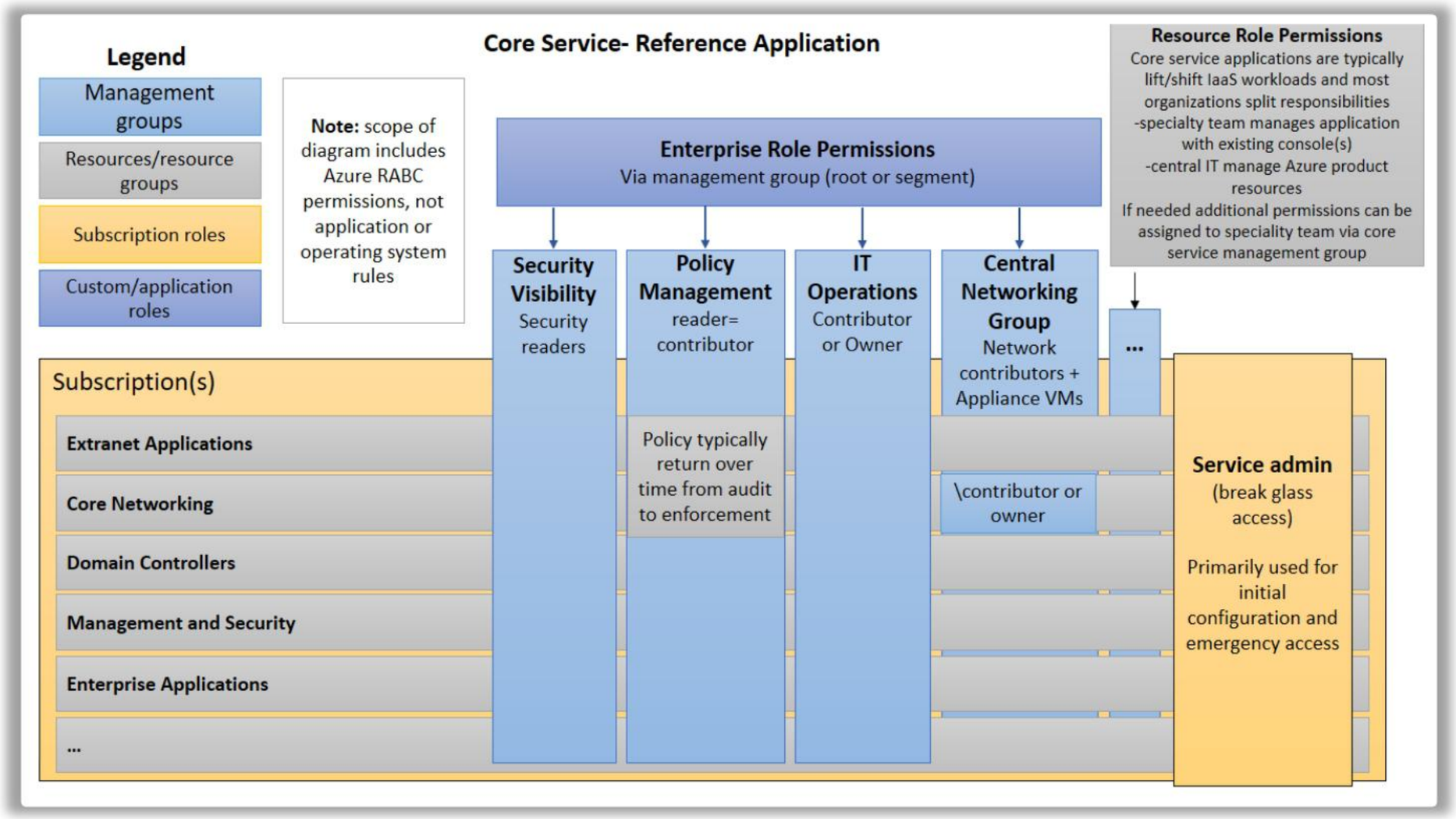


Figure 10.43: Core Services Reference Permissions

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

Security Visibility Across All Resources: For all the technical environments the security teams should be granted read-only access. This level of access is required for the assessment of risk factors, advice organizational stakeholders, and identify potential mitigations.

Policy Management Across Required Resources: Appropriate permissions should be granted for designated roles to monitor and implement compliance satisfying internal and external regulations, security policies, and standards. The selected roles and permissions vary based on the policy program expectations and culture of the organization.

Central IT Operations Across All Resources: To create, delete, and modify the resources like storage and virtual machines the central IT department should be given permissions. The central IT department is often the infrastructure team in most organizations.

Central Networking Group Across Network Resource: The network resource responsibilities should be assigned to the central networking organization so that it maintains consistency and prevents any technical conflicts. Some of the included resources are subnets, virtual networks, virtual machines with virtual network appliances, and Network Security Groups (NSG).

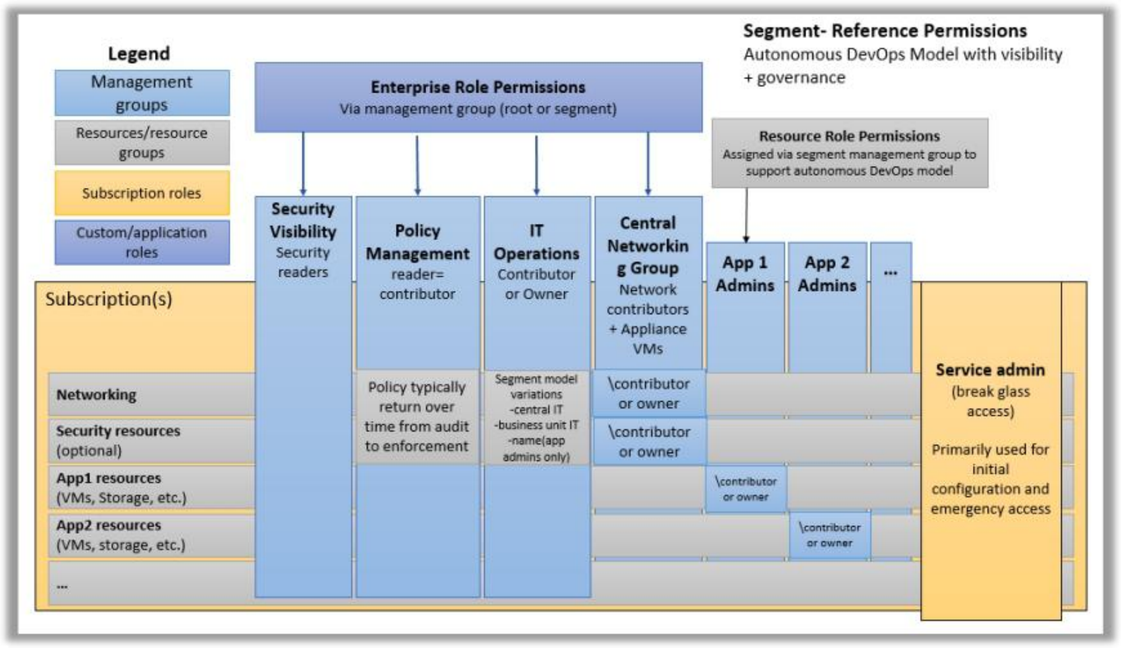
Resource Role Permissions: Administrative privileges that are required for core services are usually granted through the native application. For example, Domain Name System (DNS)/ Dynamic Host Configuration Protocol (DHCP), Active Directory, and System Management Tools.), therefore there is no requirement of additional Azure resource permission. If there is any requirement for the organization that their storages, virtual machines, or any other Azure resources have to be managed by them then the permissions to these roles can be assigned.

Service Admin (Break Glass Account): A Break Glass Account or emergency access account is a highly privileged account. It is highly recommended to use for only emergency purposes rather than regular usage and it should not be assigned to any individual. A rare situation with lockout of all administrative accounts makes it impossible to perform any operations that require higher privileges as well as creating another user, so to avoid this situation an emergency access account is used. For any organization, it is recommended to have two or more emergency access accounts. Different authentication mechanisms should be used for this account i.e if general administrative accounts have on-premises Multi-Factor authentication then the emergency access account has to use Azure AD Multi-Factor authentication or vice versa.

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

Assigning Privileges for Managing the Environment: Segment Reference Permissions

- The design of segment reference permissions delivers **consistency** and **flexibility** to adapt to the organizational model from the centralized IT group to independent DevOps and IT teams
- The resources that are associated with each application will be managed by the **autonomous DevOps teams**



Segment Reference Permissions

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

Assigning Privileges for Managing the Environment: Segment Reference Permissions

Segment Reference Permissions

hide01.ir

Consistency is obtained by using the design of segment permission and it allows flexibility to adapt the organizational model's range i.e from centralized IT group to DevOps and IT teams.

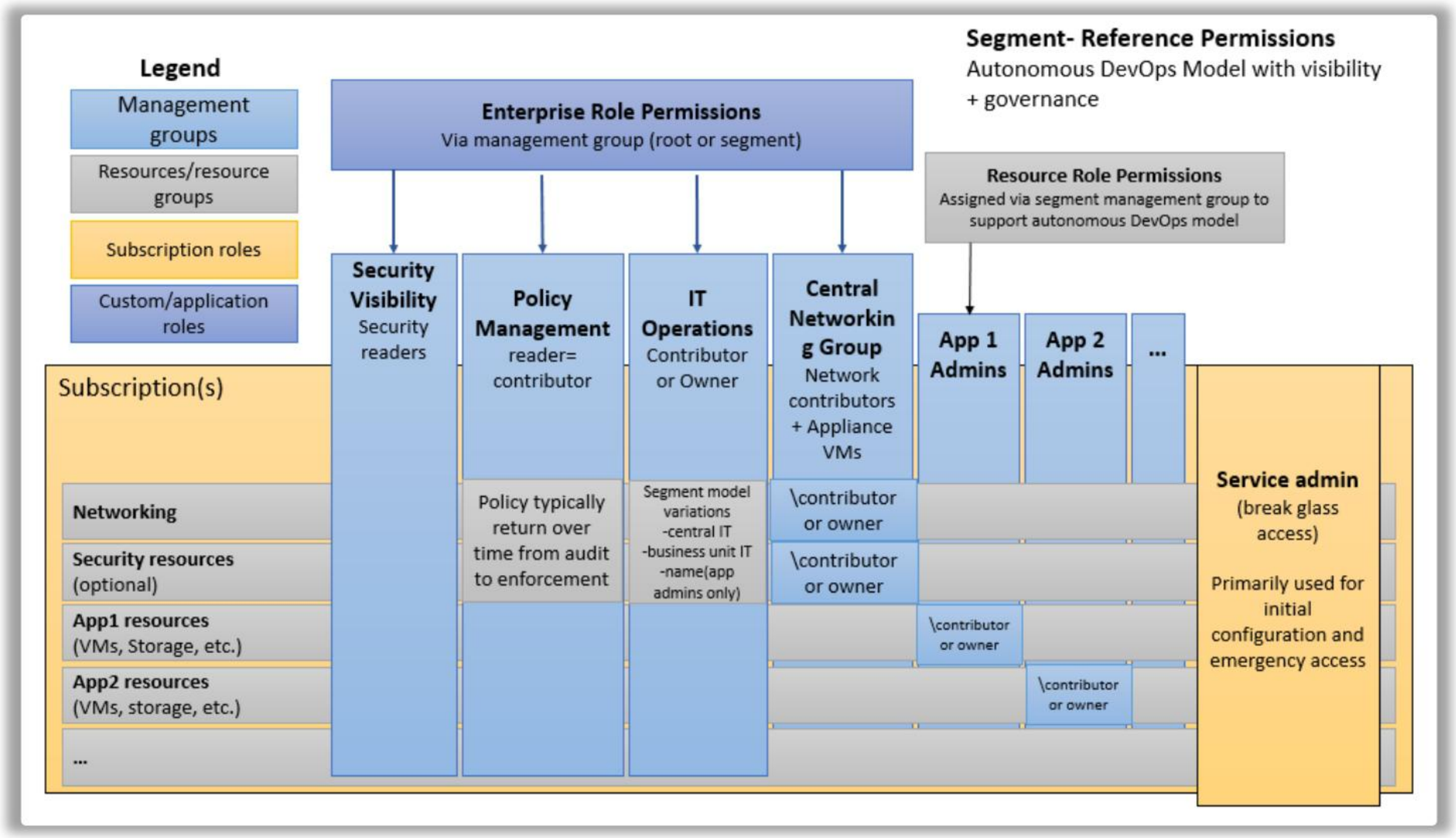


Figure 10.44: Segment Reference Permissions

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

Security Visibility Across All Resources: For all the technical environments the security teams should be granted read-only access. This level of access is required for the assessment of risk factors, advice organizational stakeholders, and identify potential mitigations.

Policy Management Across Required Resources: Appropriate permissions should be granted for designated roles to monitor and implement compliance satisfying internal and external regulations, security policies, and standards. The selected roles and permissions vary based on the policy program expectations and culture of the organization.

IT Operations Across All Resources: Depending on the structure of the organization the segment purpose varies. Permission to modify, create, and delete should be granted.

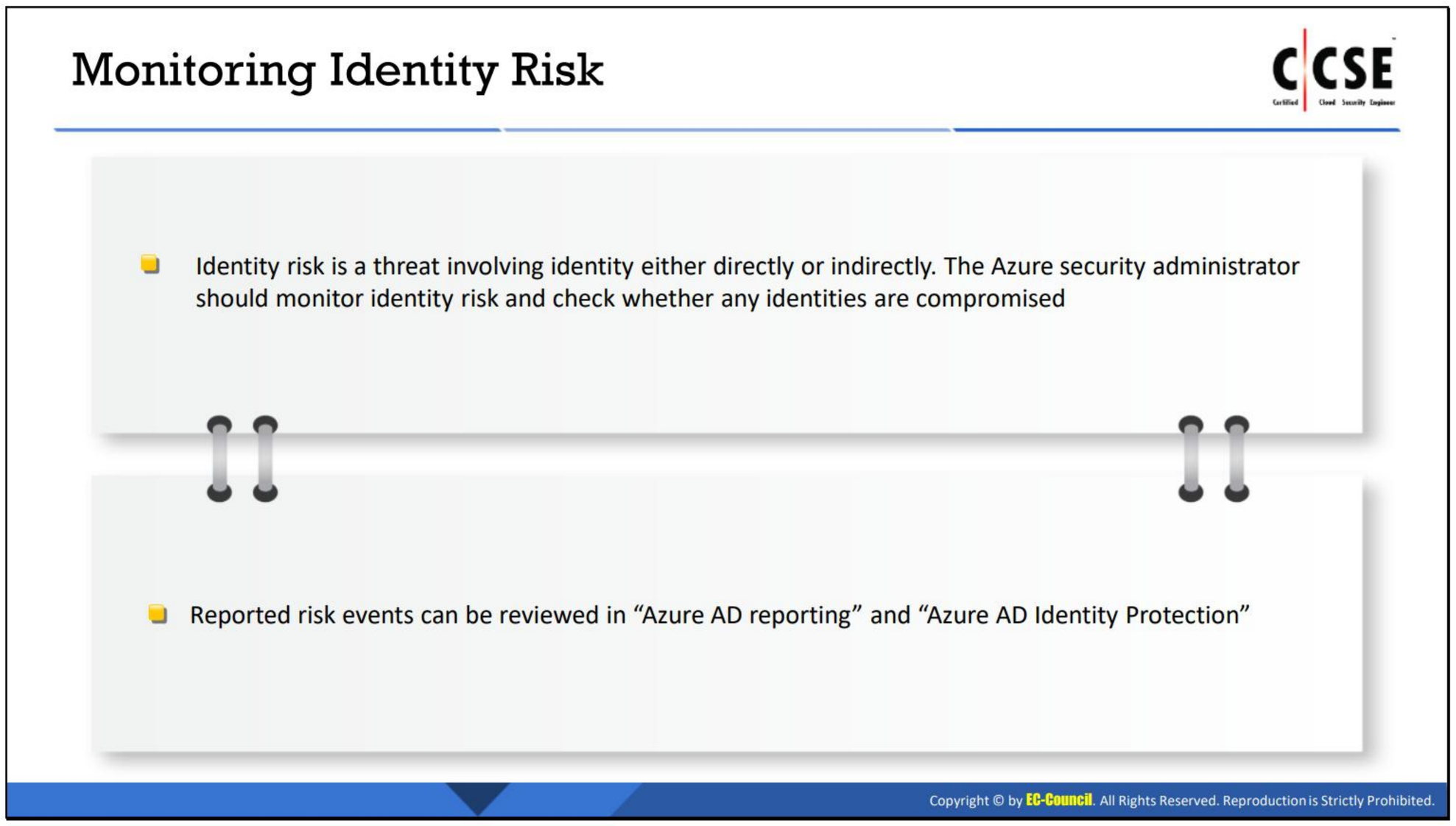
- Segments containing resources that are managed by a centralized IT organization can provide permissions to the central IT department (generally considered as the infrastructure team) for modification of the resources.
- Teams like the Human Resources IT team that manages the segment can provide permissions of those teams to the resources that are available in the segment.
- There is no requirement to grant permissions for the segments with autonomous DevOps, as the permissions for these resource roles are granted to the application teams.

Central Networking Group Across Network Resource: The network resource responsibilities should be assigned to the central networking organization so that it maintains consistency and prevents any technical conflicts. Some of the included resources are subnets, virtual networks, virtual machines with virtual network appliances, and Network Security Groups (NSG).

Resource Role Permissions: Resources related to applications can be managed by segments with autonomous DevOps teams. The permissions and actual roles depend on many factors like size and complexity of application and application team size, and organization culture and application team culture.

Service Admin (Break Glass Account): A Break Glass Account or emergency access account is a highly privileged account. It is highly recommended to use for only emergency purposes rather than regular usage and it should not be assigned to any individual. A rare situation with lockout of all administrative accounts makes it impossible to perform any operations that require higher privileges as well as creating another user, so to avoid this situation an emergency access account is used. For any organization, it is recommended to have two or more emergency access accounts. Different authentication mechanisms should be used for this account i.e if general administrative accounts have on-premises Multi-Factor authentication then the emergency access account has to use Azure AD Multi-Factor authentication or vice versa.

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



Monitoring Identity Risk

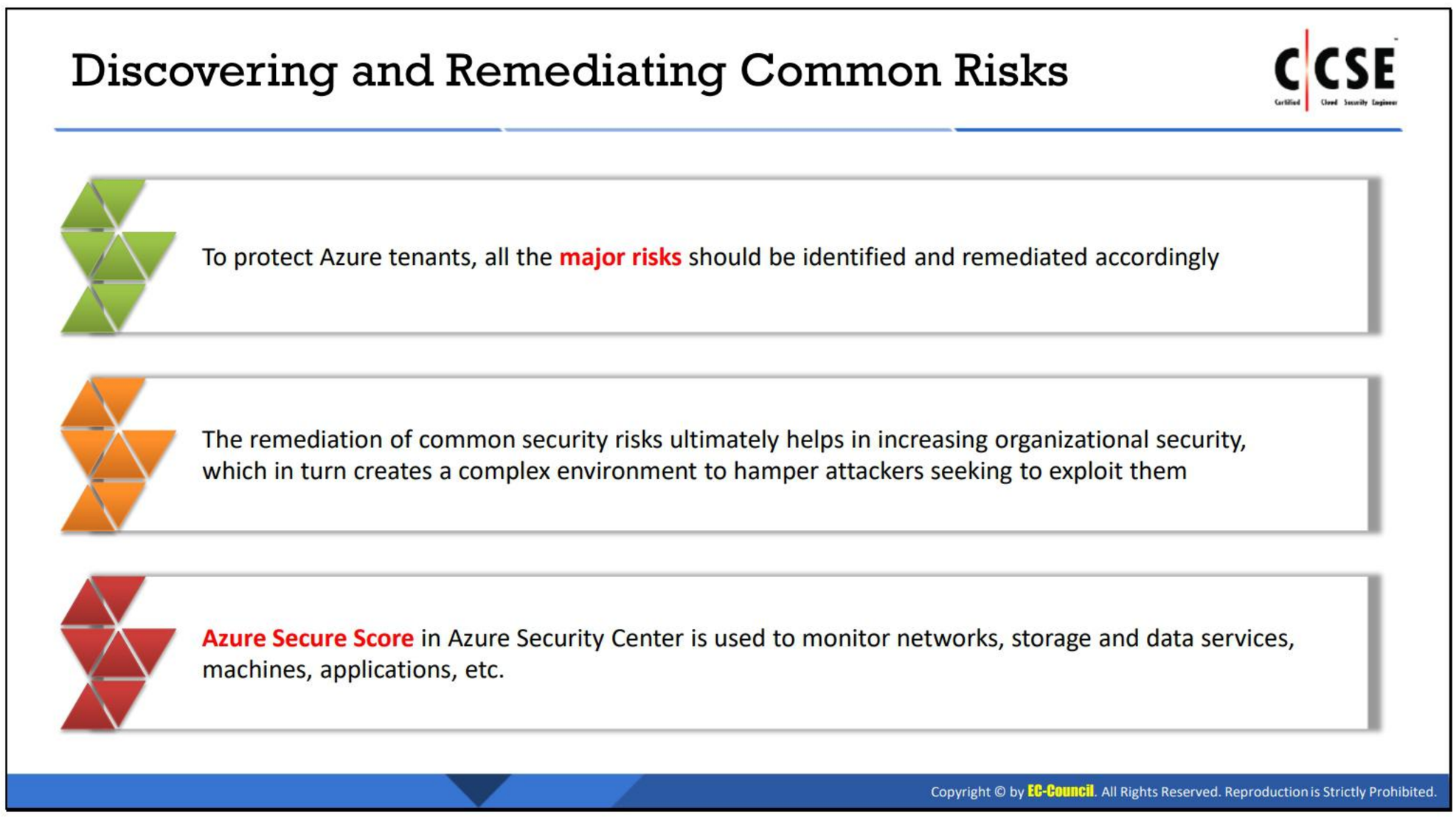
Identity Risk is a threat involving identity either directly or indirectly. For example, user accounts are one of the identities in organizations. It is highly recommended for cloud administrators to monitor identity risk and verify if any identities are compromised. This kind of risks should be immediately remediated.

Initially, an attacker compromises one of the identities in an organization, so that it becomes easier to perform malicious actions in the organizational environment. Most of the attackers try to gain the highest privilege account so that they perform any type of action. In reality, the attacker may not get the highest privileged account during identity compromise, but can get access later. This finally provides access to the target system or data.

For the detection of suspicious actions in the organization's user accounts, different technologies and methodologies like heuristics, machine learning algorithms, and compromised credentials are used by Microsoft Azure Active Directory. As a part of detection development, these compromised credentials are obtained from various sources like surface web (data found using regular search engines) and dark web (unauthorized data found via advanced techniques). This collaboration also includes law enforcement, security researchers, and security teams from Microsoft.

Reported risk events can be reviewed in “Azure AD reporting” and “Azure AD Identity Protection.” Security events can also be detected using programmatic access via “Identity Protection risk events API.” These detected user accounts should be manually remediated or passwords for those accounts should be changed using the user risk policy.

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



Discovering and Remediating Common Risks

To protect Azure tenants all the renowned risks should be identified, then they should be remediated accordingly. Secure Score helps to keep track of this progress. Remediation of common security risks ultimately helps in increasing organizational security which in turn creates a complex environment for attackers to exploit. If all the low and popularly know attack vectors are closed then the attackers will have to use unconventional attack methods as the regular attack methods will not work. In Azure Security Center the security posture is monitored by the Azure Secure Score. For the discovery of security issues, the various aspects monitored by the Azure Secure Score are storage and data services, networks, machines, and applications. Security issues include missing security updates, VMs that are connected to the internet, encryption or endpoint protection, missing Web Application Firewall, etc. This feature can be enabled in Azure Security Center, it helps in examining security discoveries and recommends remediating the issues. It is recommended to remediate the highest priority issues first.

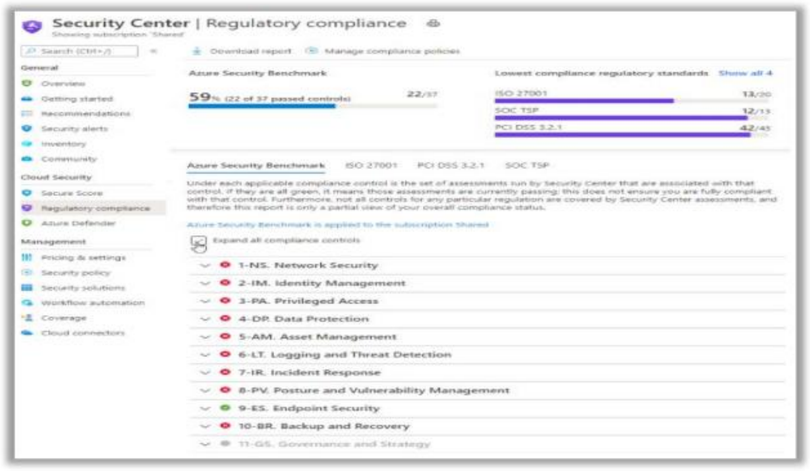
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Improving Regulatory Compliance with Azure Security Center

- The regulatory compliance dashboard in Azure Security Center simplifies the process of meeting regulatory compliance requirements
- The risk factors can be reduced, and compliance can be improved by acting on the recommendations provided in the regulatory compliance dashboard

Improve regulatory compliance with Azure Security Center by performing the following tasks:

- **Assess the regulatory compliance from the regulatory compliance dashboard**: The regulatory compliance dashboard helps identify gaps in compliance with the selected compliance standards



Azure Security Center Dashboard

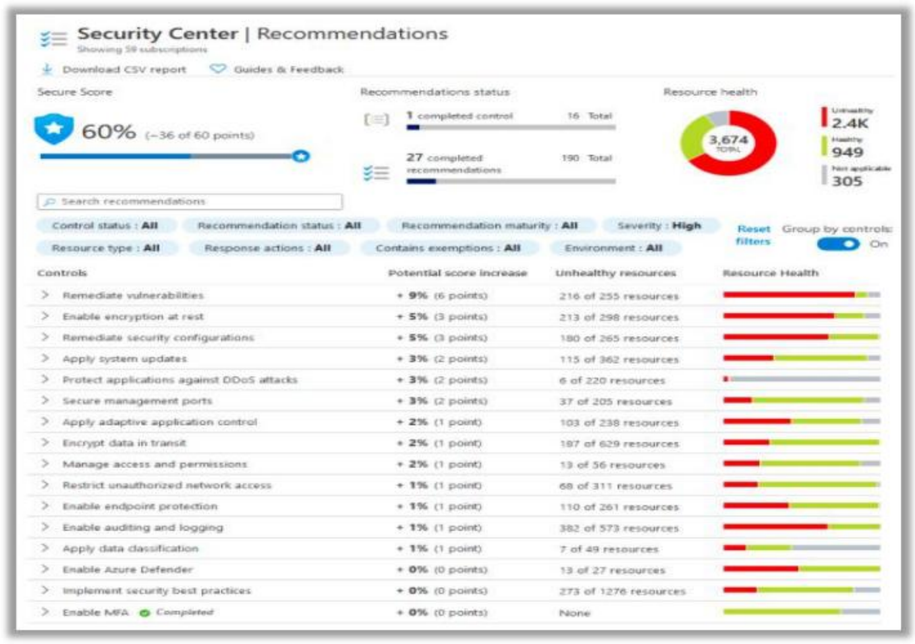
Source: https://www.microsoft.com

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

Improving Regulatory Compliance with Azure Security Center (Cont'd)

hide01.ir

- **Improve the compliance posture with Azure Security Center**: The compliance posture of the cloud environment can be improved by resolving the **security center recommendations** in the dashboard



Azure Security Center Recommendations

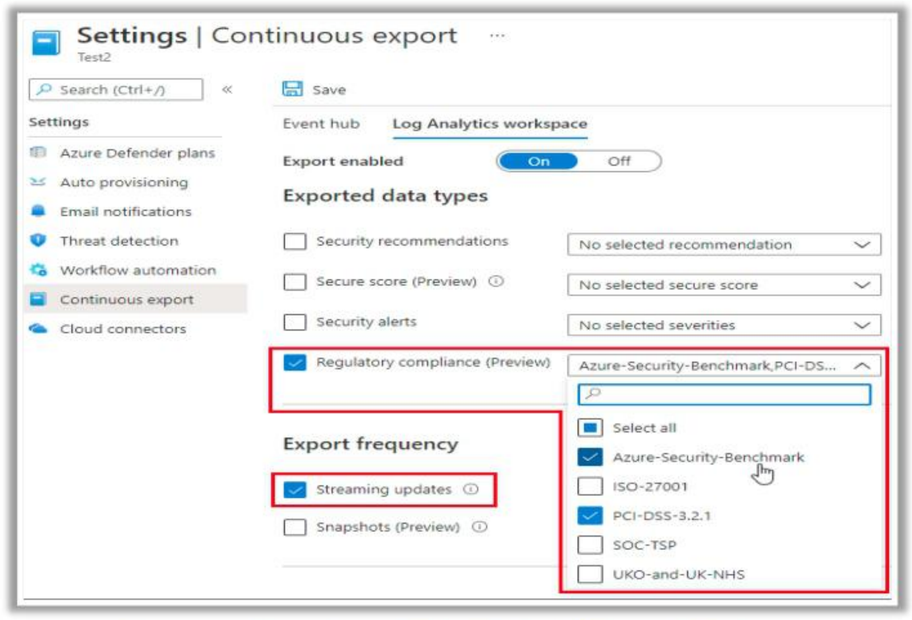
Source: https://www.microsoft.com

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.

Improving Regulatory Compliance with Azure Security Center (Cont'd)

- **Export the compliance status data:** Azure Security Center includes an **export mechanism** that helps track compliance status with other monitoring tools directly



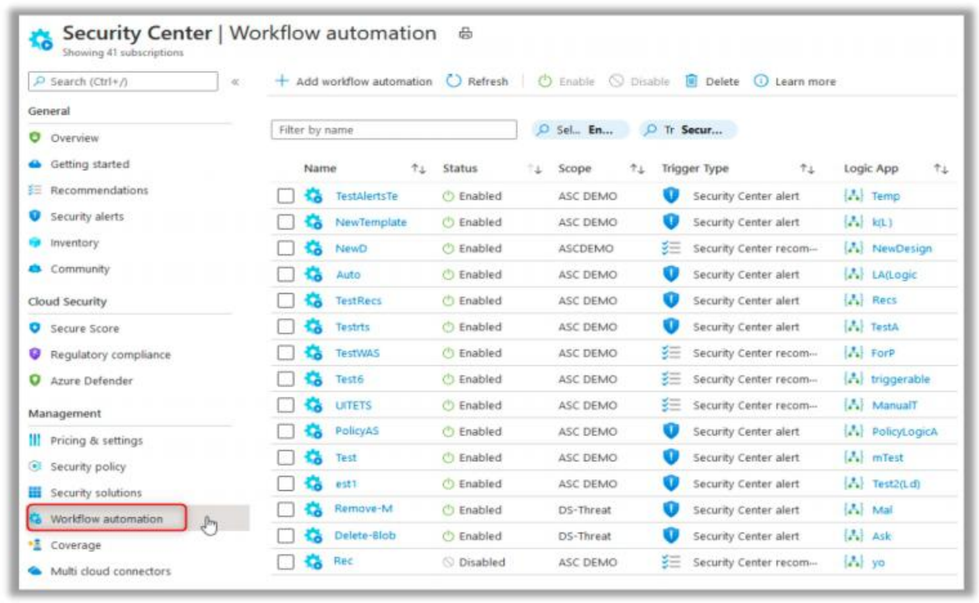
Exporting Compliance Status Data with Security Center

Source: https://www.microsoft.com

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

Improving Regulatory Compliance with Azure Security Center (Cont'd)

- **Run workflow automation during changes in compliance:** The workflow automation feature in Azure Security Center triggers **Logic Apps** if any of the regulatory compliance assessments change state



Workflow Automation in Azure Security Center

Source: https://www.microsoft.com

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

Improving Regulatory Compliance with Azure Security Center

The regulatory compliance dashboard in Azure Security Center simplifies the process of meeting regulatory compliance requirements. Security Center analyses the hybrid cloud environment to determine the risks associated with the environment based on the controls and best practices for the standards implemented. The regulatory compliance dashboard provides an insight into the status of the compliance with these standards. The risk factors can be

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

reduced, and the compliance can be improved by acting on the recommendations provided in the regulatory compliance dashboard. Azure Security Center regulatory compliance dashboard helps to,

- Get insights regarding the standards and regulations that are important.
- Resolve the security recommendations and improving the compliance status.

Source: https://www.microsoft.com

Improve Regulatory Compliance With Azure Security Center By

Assessing the Regulatory Compliance

The regulatory compliance dashboard helps to identify the gaps in compliance with the selected compliance standards. The regulatory compliance dashboard shows all the compliance standards, and the supported requirements are aligned with applicable security assessments. Compliance with the standards is determined by the status of these assessments.

To Assess the Regulatory Compliance from Regulatory Compliance Dashboard

- Navigate to Security Center and select **Regulatory Compliance**

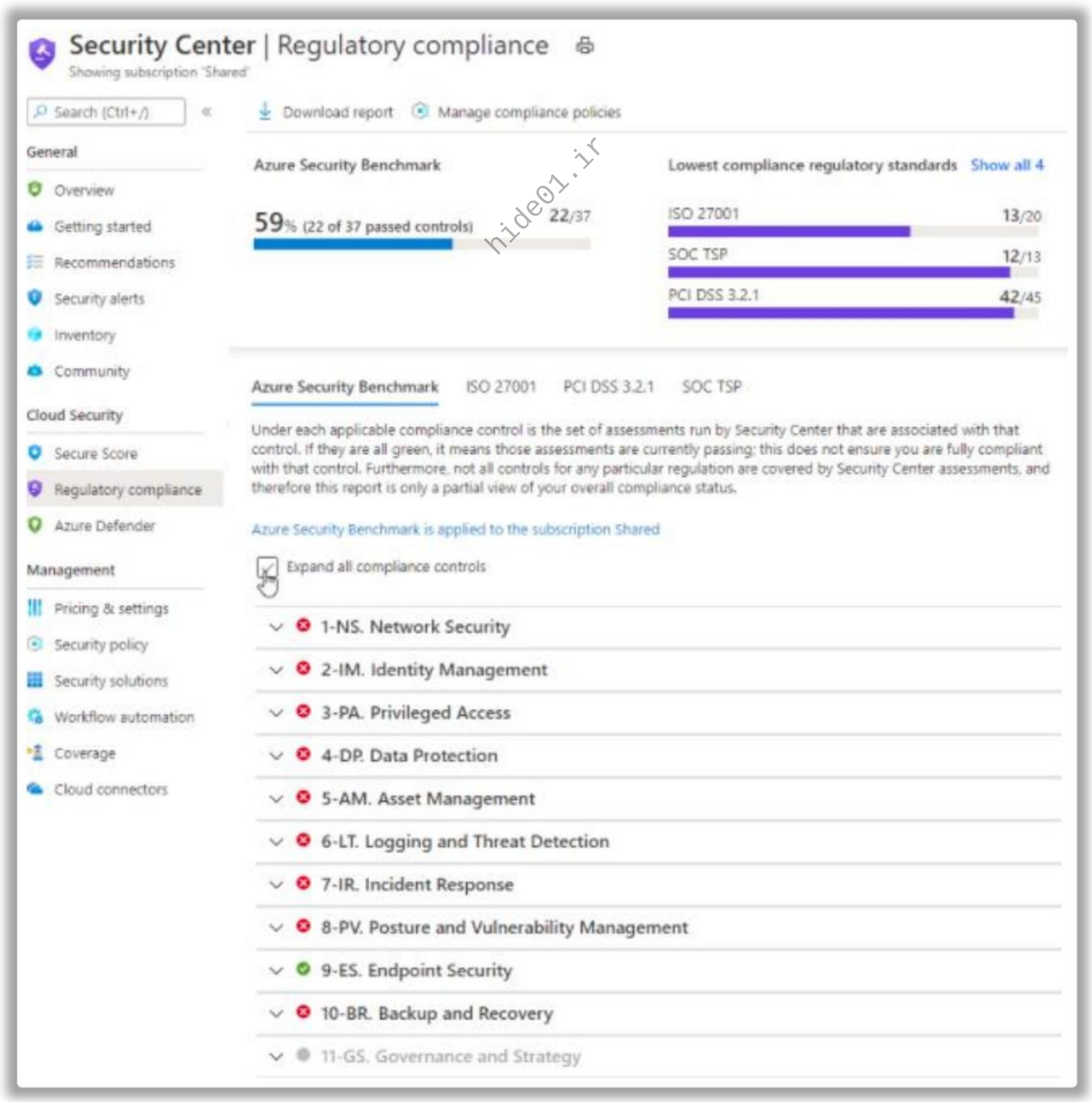


Figure 10.45: Regulatory Compliance

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

- Analyze the top of the screen to get insight into the compliance status with the supported compliance regulations, compliance score, passing and failing assessments associated with each standard.
- Click on the tab of a particular compliance standard.
- It shows,
    - The subscriptions to which the standard is applied.
    - All the controls for that particular standard.
    - The details of passing and failing assessments with the appropriate controls.
    - The affected resources.
- Click on **Download Report** to download the PDF report containing the high-level summary of the particular standard's current compliance status, which can be shared with relevant stakeholders.

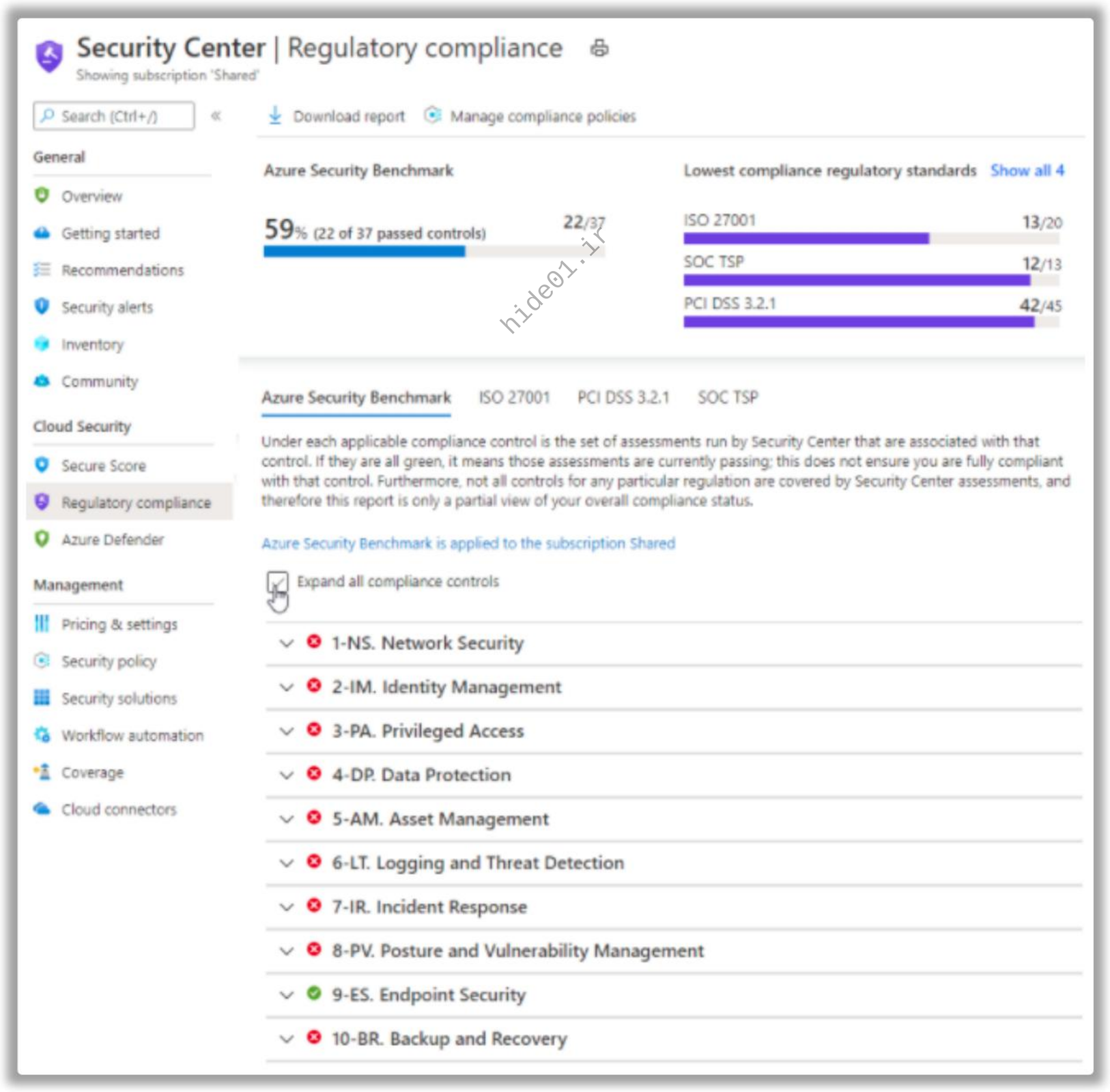


Figure 10.46: Downloading a Standard’s Compliance Status Report

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

Improve the Compliance Posture with Azure Security Center

The compliance posture of the cloud environment gets improved by resolving the security center recommendations in the dashboard. The recommendations also include remediation steps to resolve the issue.

To Improve the Compliance Posture By Responding to Recommendations in the Security center

- Click on **Recommendations** in Azure Security Center Dashboard.

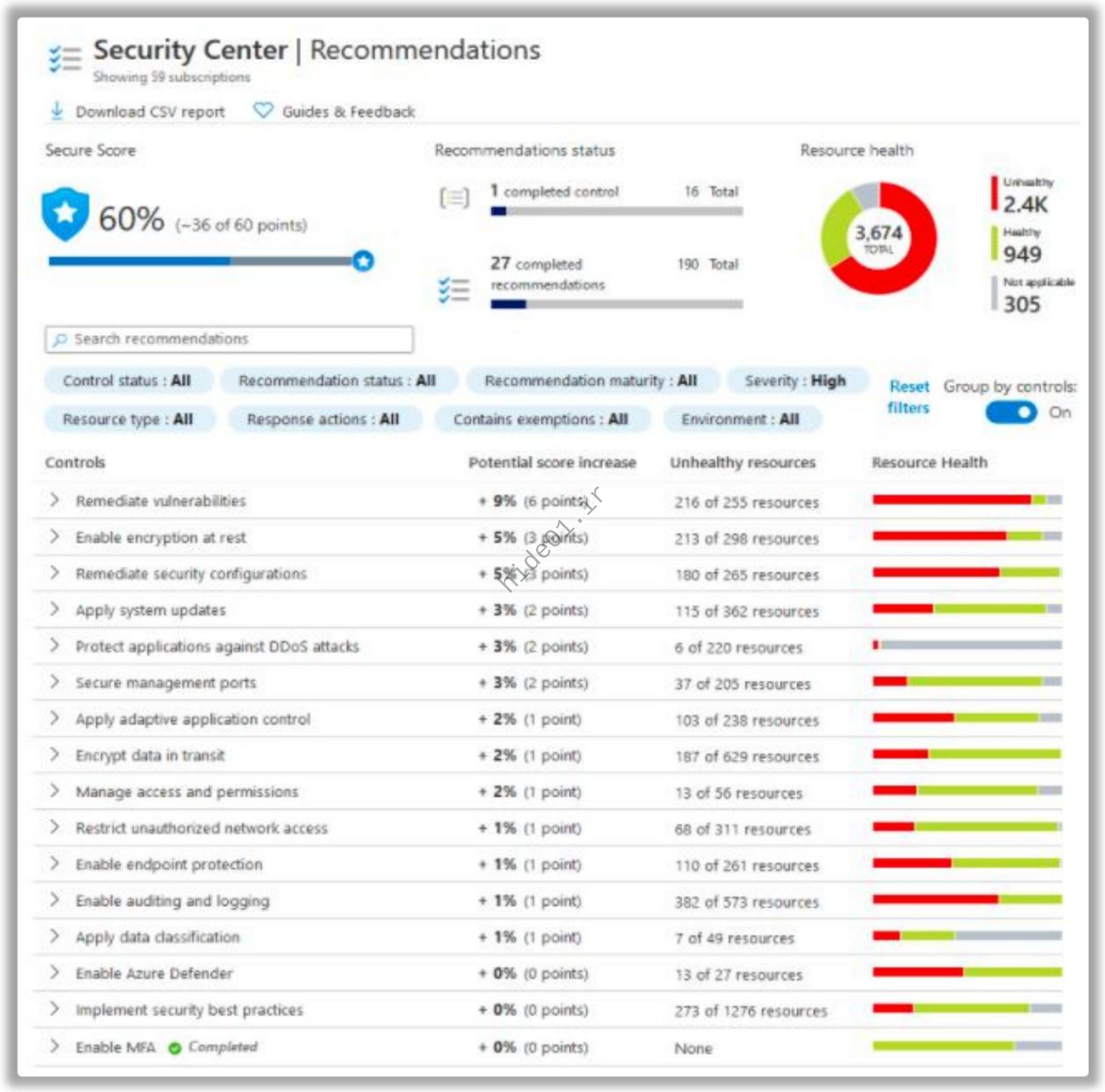


Figure 10.47: Azure Security Center Dashboard

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

- Expand any of the controls to get details regarding the recommendation and the remediation steps.

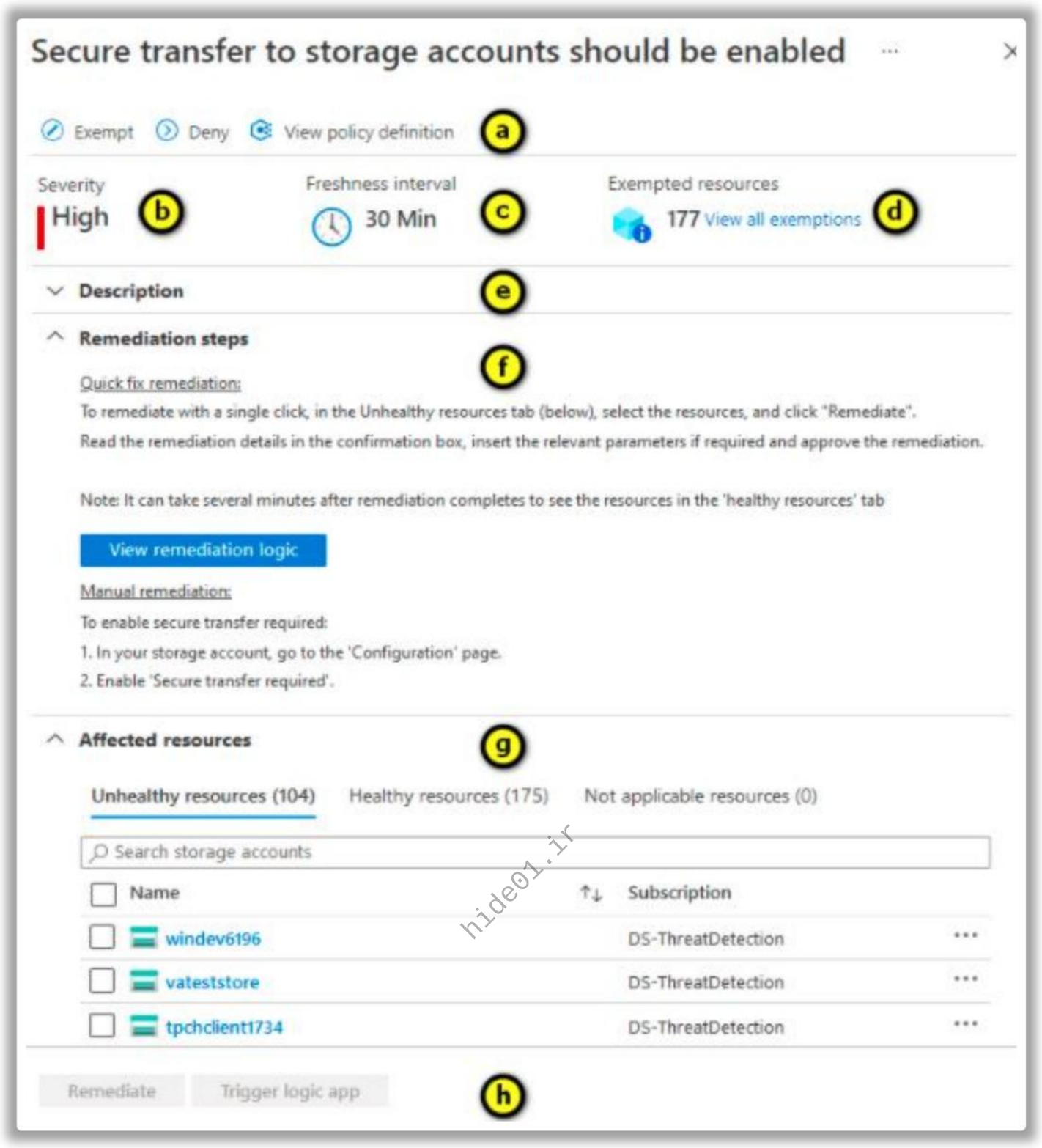


Figure 10.48: Recommendation and its Remediation Steps

- The recommendation details page contains,
  - The severity of the vulnerability.
  - Freshness Interval.
  - The number of exempted resources.
  - Description of the issue.
  - Remediation steps for a manual fix of the issue.
  - The different types of affected resources like,
    - Healthy Resources: The resources which are not impacted or already remediated.
    - Unhealthy Resources: Resources still impacted by the issue.

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

- Not Applicable Resources: The affected resources for which there is no proper remediation.

- Action buttons to remediate the recommendation.

- Verify the compliance score in the compliance dashboard after the issue gets remediated.

Exporting the Compliance Status Data

Azure Security Center includes an export mechanism that helps to track compliance status with other monitoring tools directly. Continuous export must be configured to send data to Azure Event Hub or Log Analytics workspace.

Using Continuous Export to Send Data to Azure Event Hub or Log Analytics Workspace

- Navigate to Azure Security Center.
- Click on **Pricing and Settings**.
- Select the specific subscription for which the data export is to be configured.
- Click on **Continuous Export** on the left side.

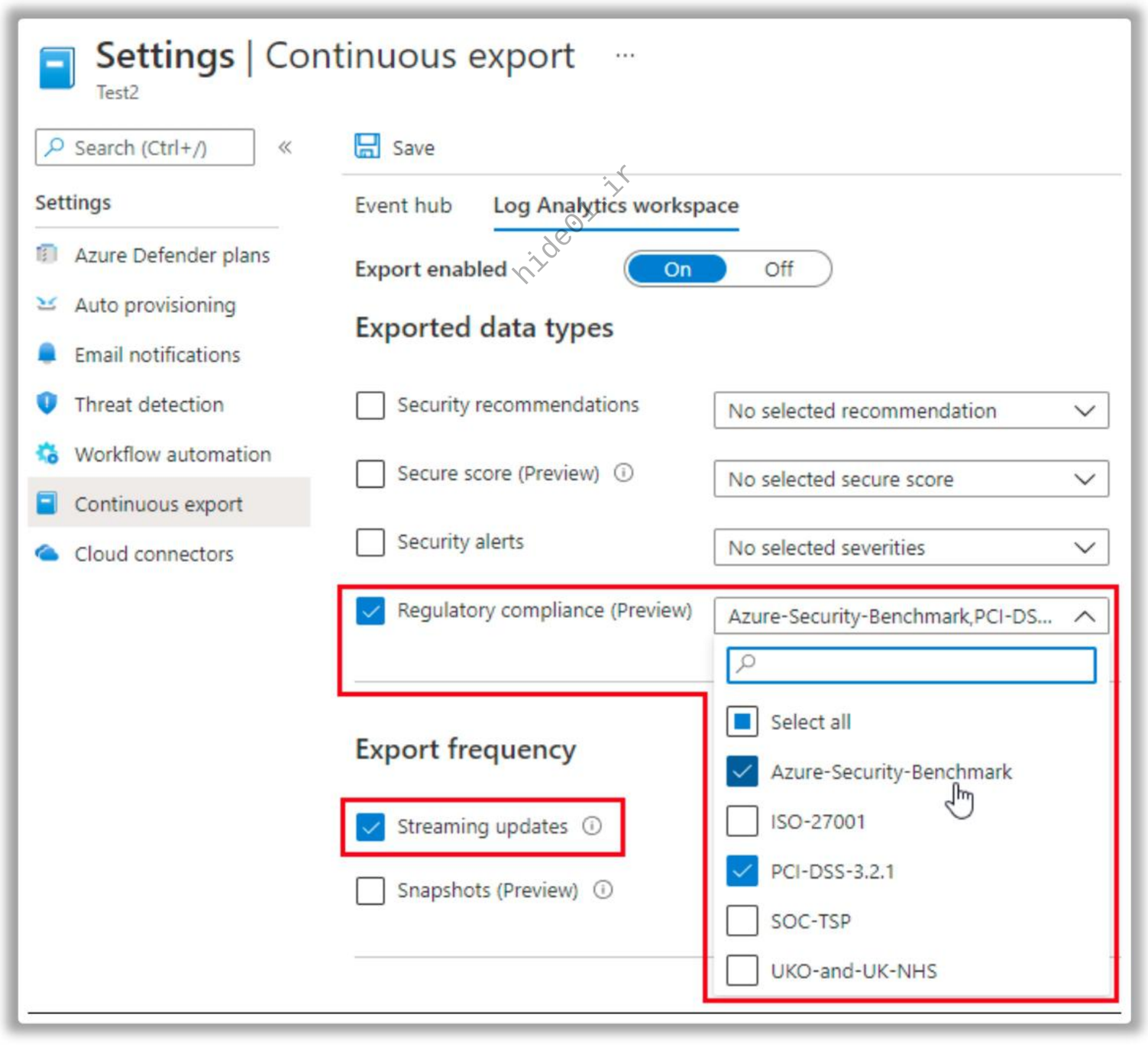


Figure 10.49: Continuous Export

- Select the checkbox for regulatory compliance.
- Select the checkbox for the different regulatory compliances.

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

- Select the checkbox for **Snapshots** under Export Frequency to export weekly snapshots.

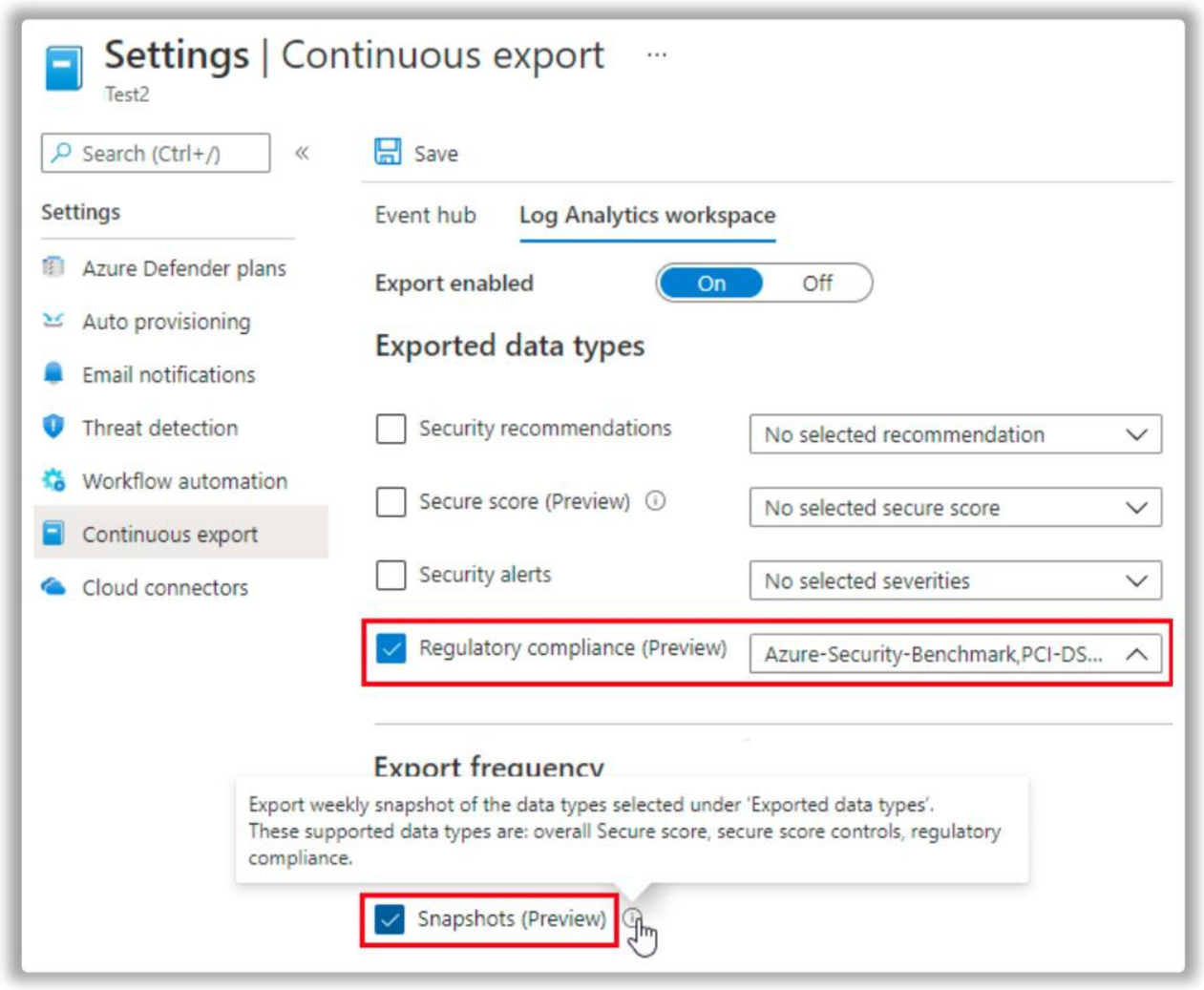


Figure 10.50: Exporting Weekly Sanpshots

- Navigate to the regulatory compliance dashboard in Azure Security Center.
- Click on **Download Report** to export compliance data in PDF/CSV format.

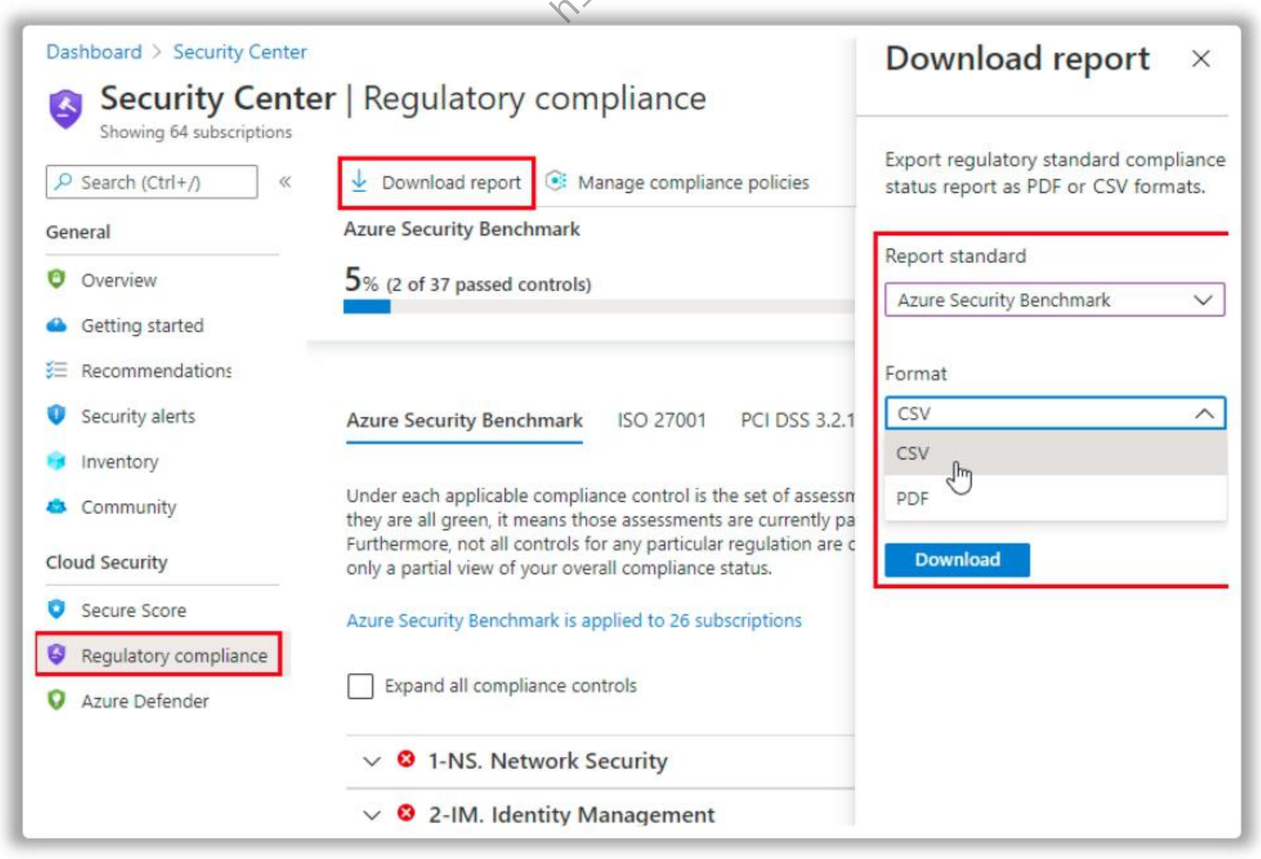


Figure 10.51: Downloading Report to Export Compliance Data

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

Running Workflow Automation During Changes in Compliance

The workflow automation feature in Azure Security Center triggers Logic Apps if any of the regulatory compliance assessments change state. For implementing this, create a logic app first and configure a trigger in the new workflow automation.

- **Step 1: Creating a Logic App**
  - Navigate to Azure Security Center.
  - Click on **Workflow Automation** on the left.

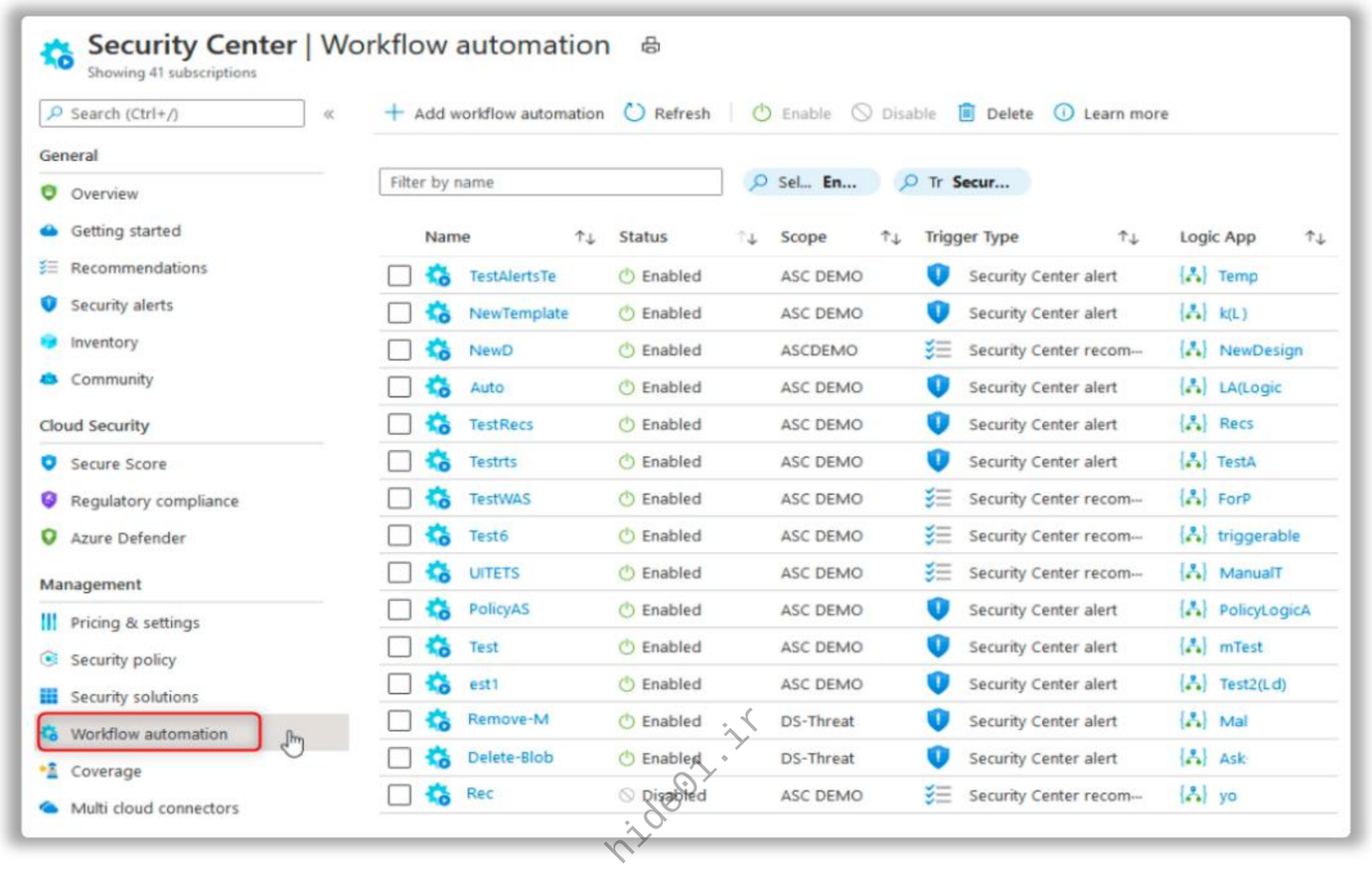


Figure 10.52: Navigating to Workflow Automation

  - Click on **Add Workflow Automation.**
  - Enter the Name and Description for the automation in the pane that appears.
  - Under **Trigger Conditions,**
    - Select **Regulatory compliance standards** under Select Security Center Data types.
    - Select the required compliance standard under Compliance Standards.
    - Select the required Compliance control state.

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

- Under **Actions,** click **Create a new one.**

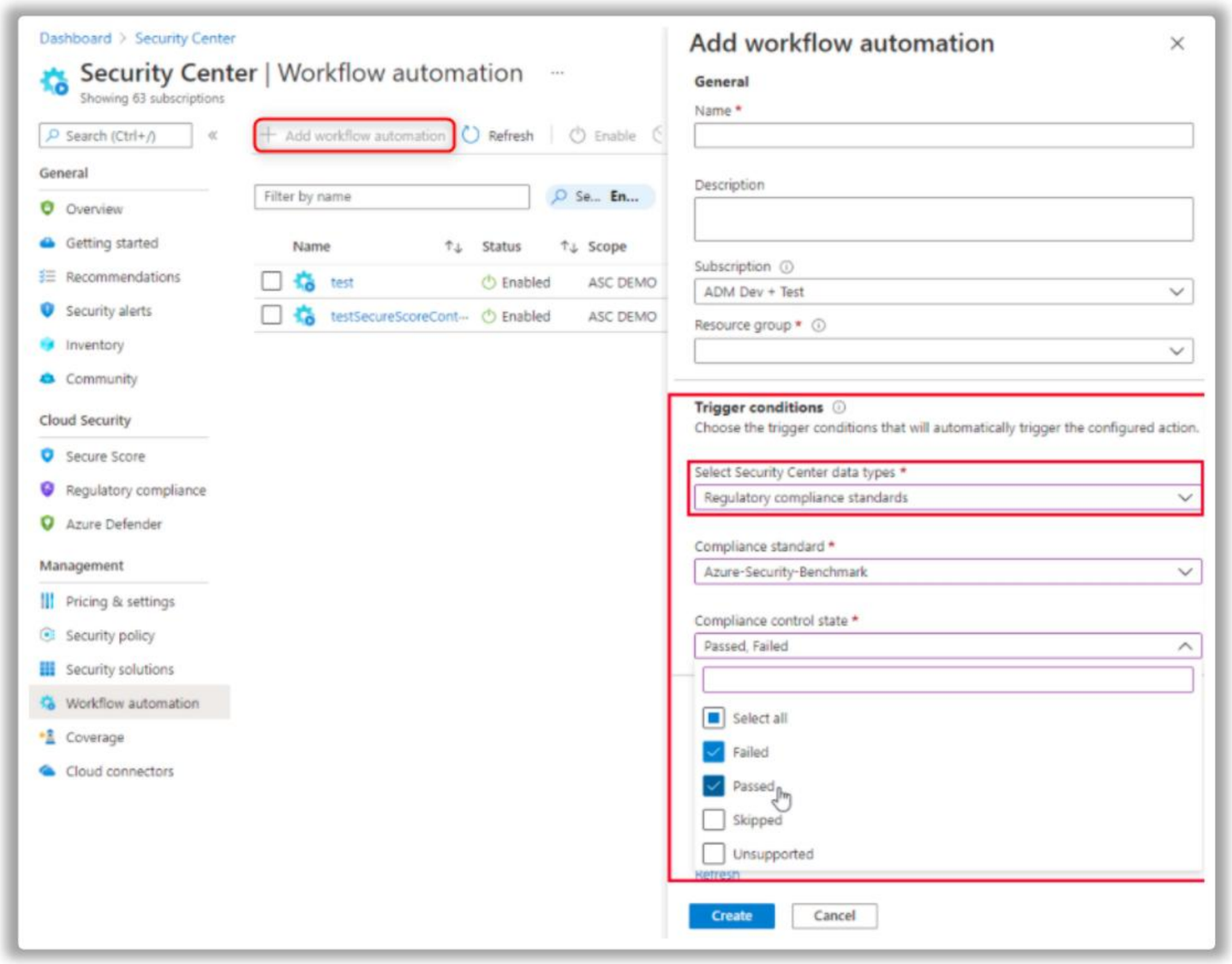


Figure 10.53:Adding a Workflow Automation

- In the Azure Logic Apps window that appears,
  - Enter the **Name**, **Resource group,** and **Location**.
  - Click on **Create**.

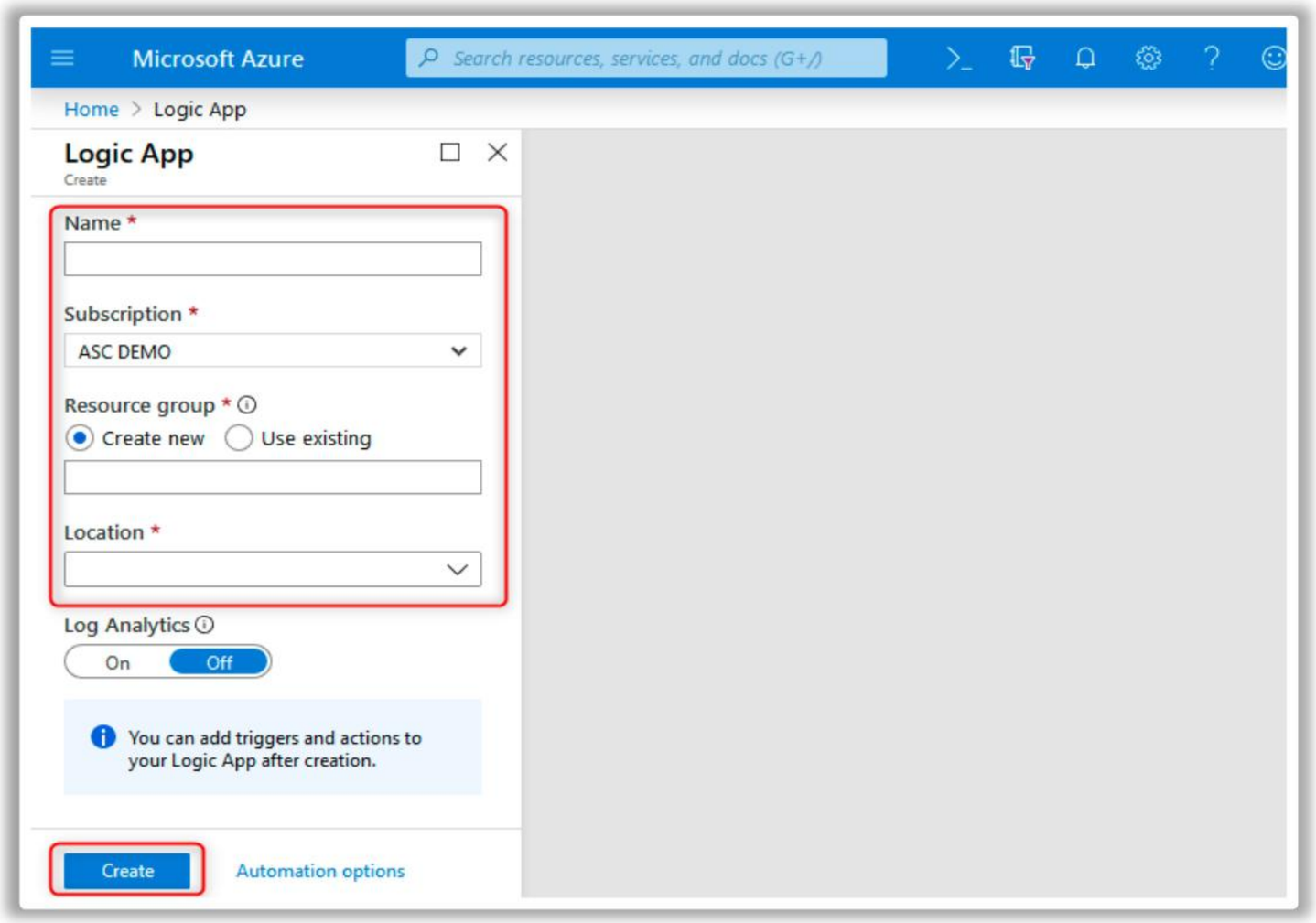


Figure 10.54: Azure Logic Apps Window

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

- **Step 2: Setting Up Trigger in New Workflow automation**
  - Define the built-in trigger in logic app designer "**When a Security Center regulatory compliance assessment is created or triggered**."
  - Navigate back to the Workflow Automation definition pane in Security Center.
  - Click on **Refresh.**

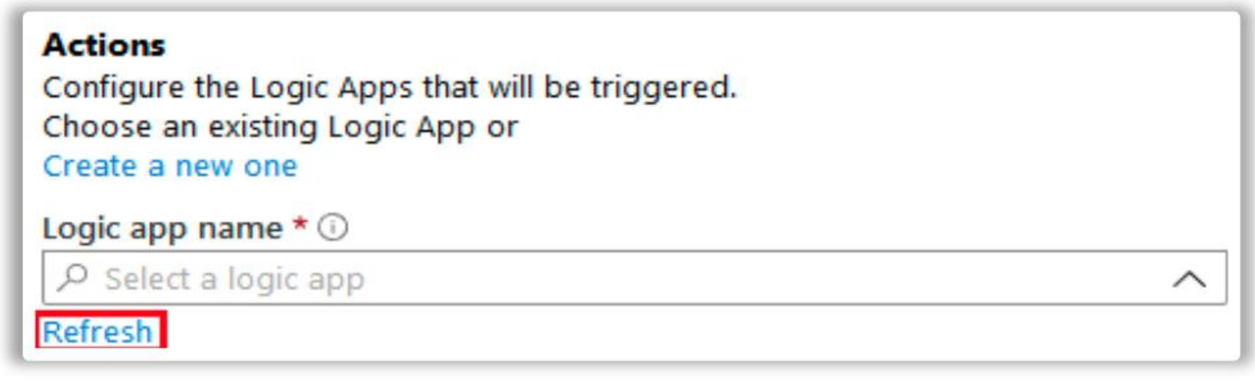
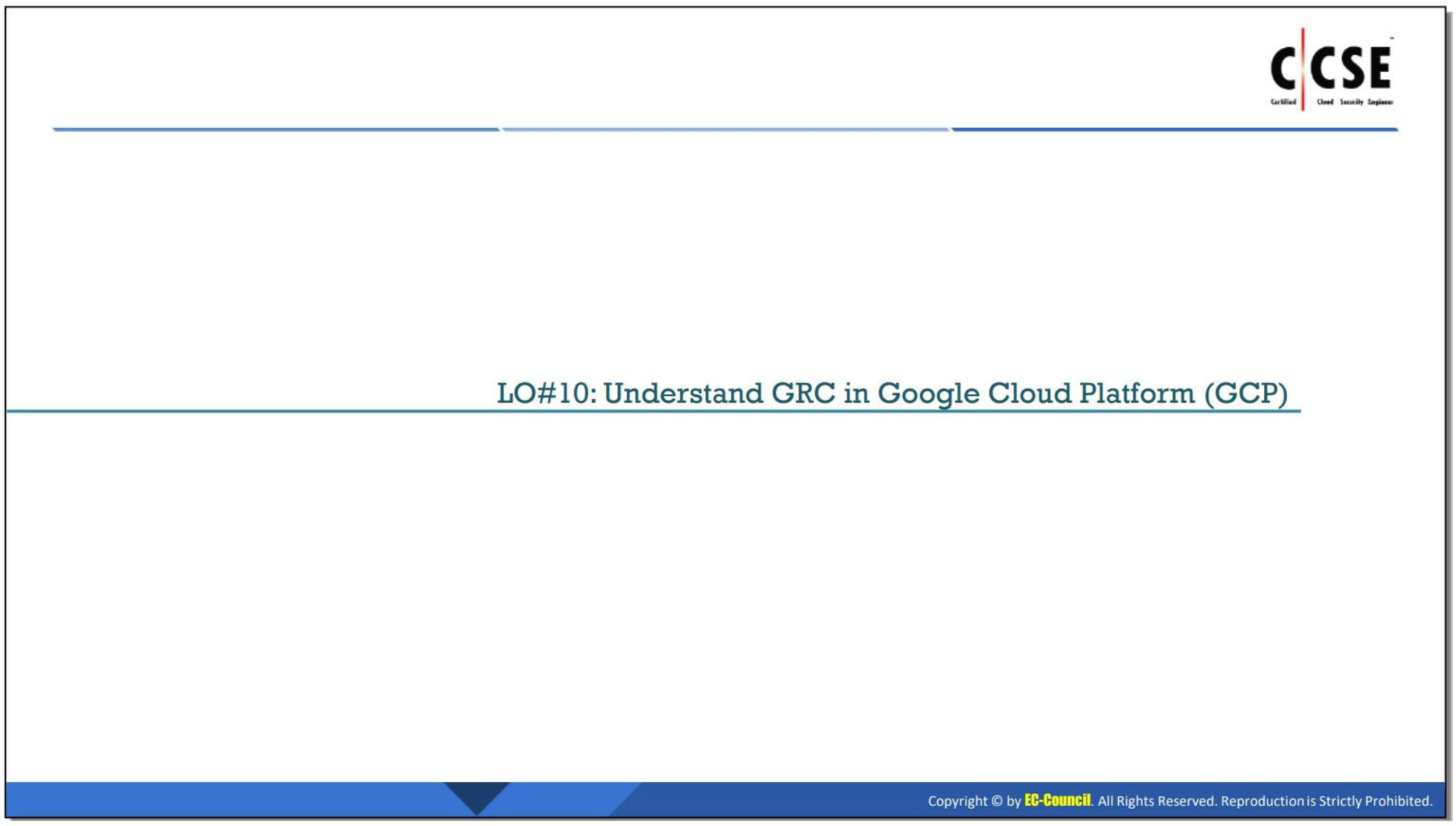


Figure 10.55: Setting Up a Trigger

hide01.ir

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



LO#10: Understand GRC in Google Cloud Platform (GCP)

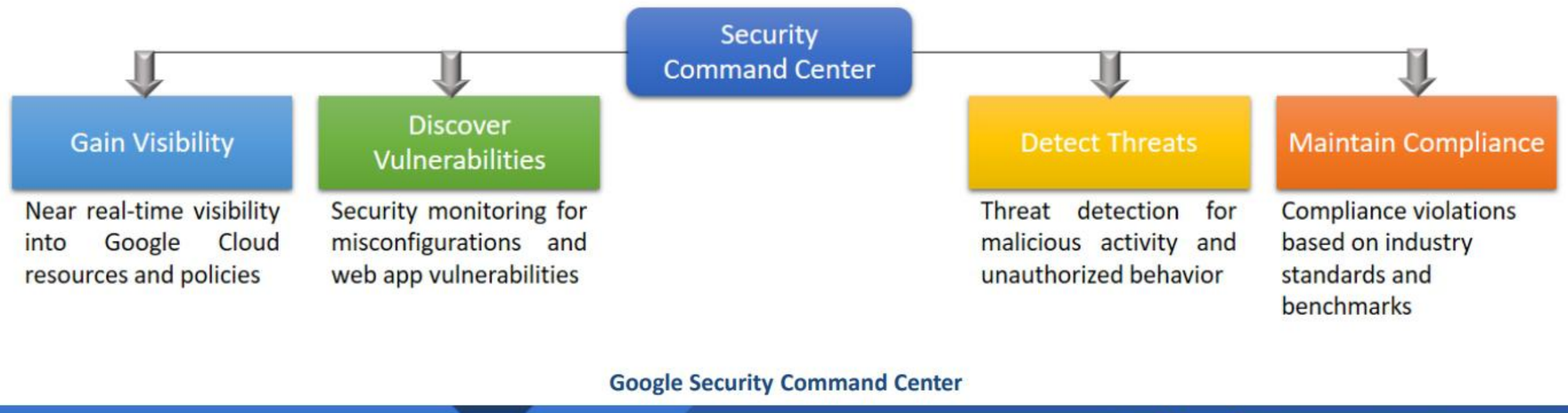
The objective of this section is to introduce the various GRC features provided in Google Cloud It shows how to implement the Google tools and the best practices to maintain compliance.

hide01.ir

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

Inbuilt Features for Governance and Risk Management in GCP

- Google Cloud Platform (GCP) offers various **inbuilt features** for the verification of security, privacy, compliance controls, etc. The inbuilt features of GCP for governance and risk management are as follows
  - **Security and risk management using the Cloud Security Command Centre:** Google Cloud Security Command Center provides real-time visibility into cloud resources; helps in detecting vulnerabilities, threats, and malicious activities; and thereby maintains compliance standards



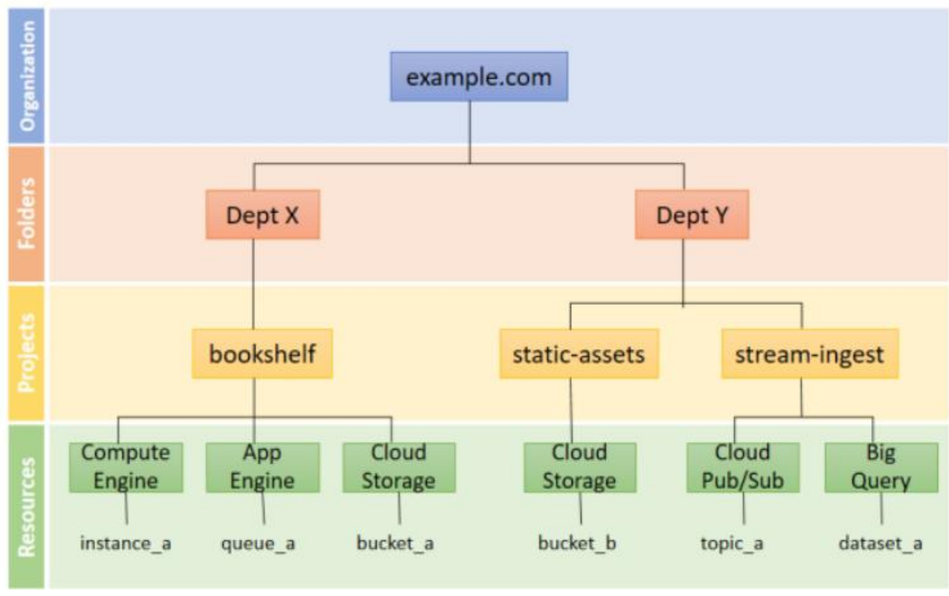
Google Security Command Center

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

Inbuilt Features for Governance and Risk Management in GCP (Cont'd)

hide01.ir

- **Google Security and Trust Centre:** Google Cloud Security and Trust Center has **secure design infrastructure** with built-in protection and helps in protecting user applications and data
- **Identity Platform:** Identity Platform in GCP is a **customer identity and access management** (CIAM) service that can add IAM into applications to help the organization coordinate security policies with internal and external partners and manage risks
- **Cloud Identity and Access Management (IAM):** The cloud IAM service can be used for the **central management of resources** in the cloud and for implementing access to cloud resources by enforcing the principle of least privilege and separation of duties



Google Cloud IAM Resource Hierarchy

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

Inbuilt Features for Governance and Risk Management in GCP

The inbuilt features of GCP for governance and risk management are as follows:

- **Security & Risk Management by Cloud Security Command Centre**

  Security Command Centre is the security and risk management service for GCP. Security Command Centre helps in ensuring the complete security of the organization by centralized asset inventory, vulnerability, and anomaly detection with live notifications.

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

With Security Command Centre Organizational policies can be established and communicated.

- **Google Security and Trust Centre**

  Google Cloud Security Model has a secure design infrastructure with built-in protection that helps in protecting the user applications and data. Google ensures that only authorized personnel can access the resources by providing default encryption at rest and at transit. Google performs independent verification of security compliance for fulfilling the regulatory and policy objectives of the organizations.

- **Identity Platform**

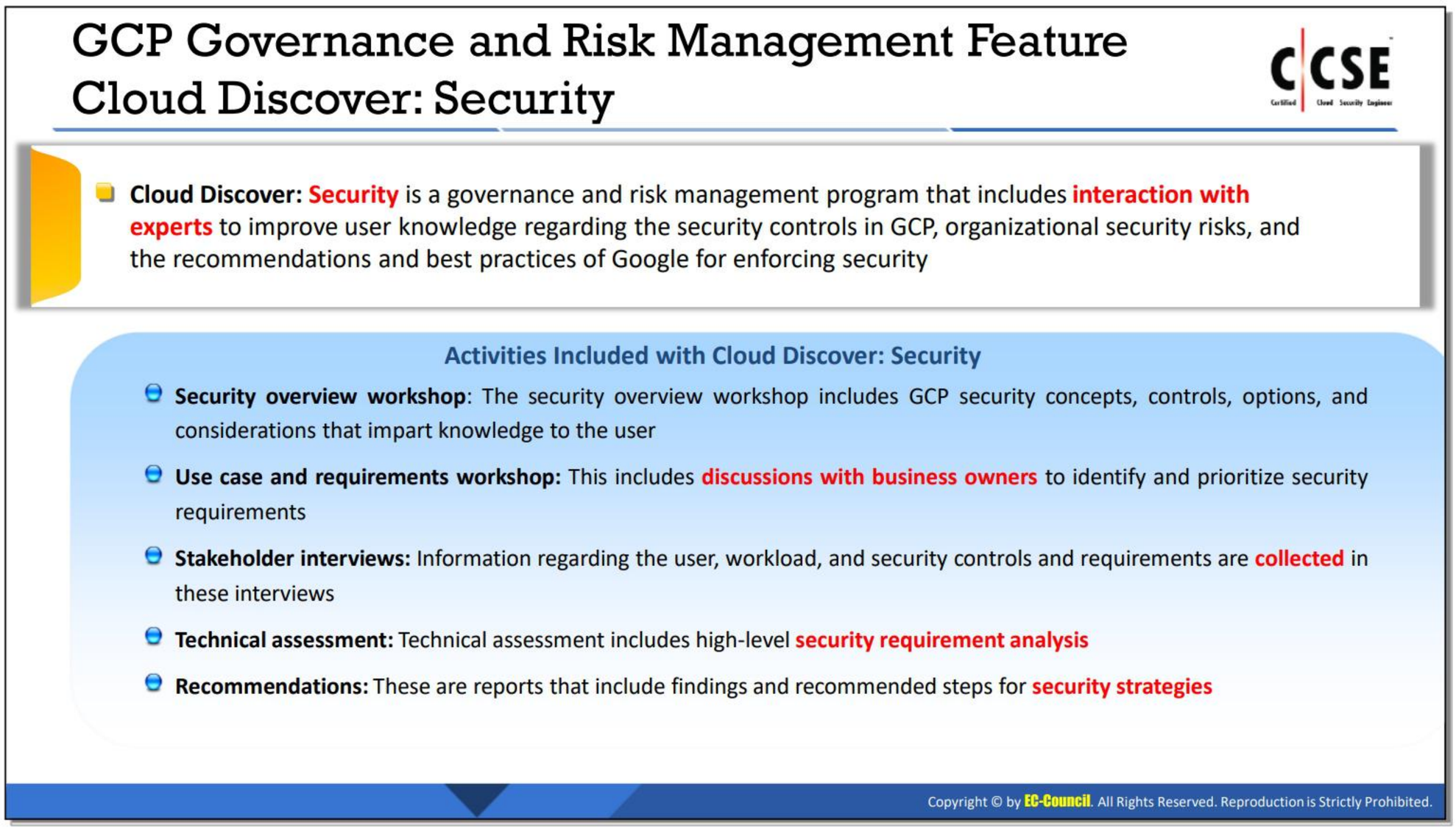
  Identity Platform in GCP is a Customer Identity and Access Management (CIAM) service which helps the organization to implement IAM into the applications. Identity Platform also helps in coordination of the roles and responsibilities, then associate them with internal roles and external parties.

- **Cloud Identity and Access Management (IAM)**

  Cloud Identity and Access Management service can be used for central management of resources in the cloud and implementing access to cloud resources enforcing the principle of least privilege and separation of duties. With Cloud IAM organizational security policies can be established efficiently. Cloud IAM also helps in coordination of the roles and responsibilities, then associate them with internal roles and external parties.

hide01.ir

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

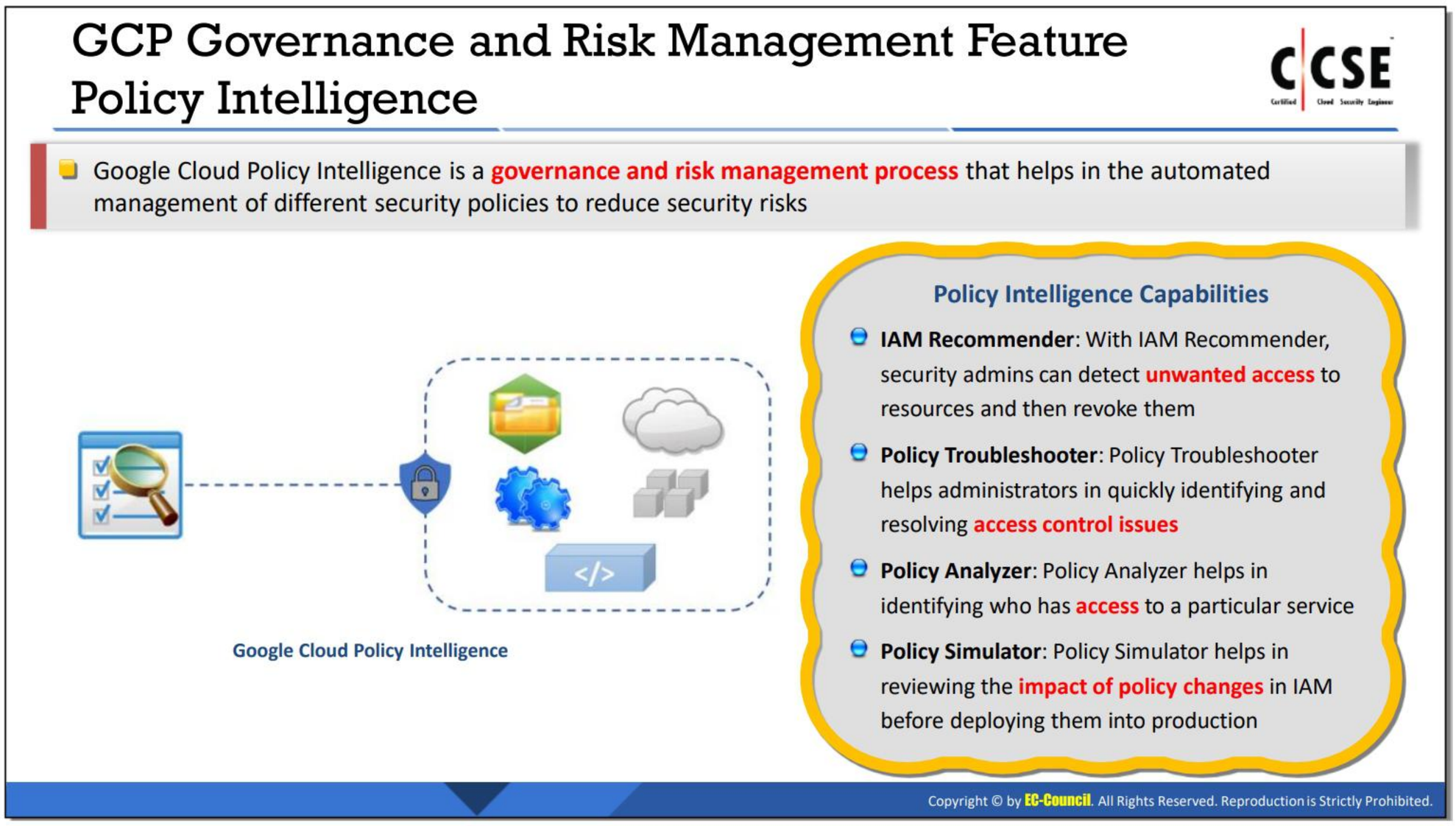


GCP Governance and Risk Management Feature Cloud Discover: Security

Cloud Discover Security helps in improving user's knowledge regarding the security controls in GCP, organization security risks, recommendations, and best practices by Google for enforcing security. It also includes discussions with Google consultants and a summary report. The activities included with Cloud Discover Security are as follows:

- **Security Overview Workshop**: The security overview workshop includes GCP security concepts, controls, options, and considerations that impart knowledge to the user.
- **Use Case and Requirements Workshop**: This includes discussions with business owners to identify and prioritize security requirements
- **Stakeholder Interviews**: The information regarding the user, workload, and the security controls and requirements are collected.
- **Technical Assessment**: Technical assessment includes high-level security requirement analysis.
- **Recommendations**: A report which includes findings and recommended steps for security strategies are developed

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



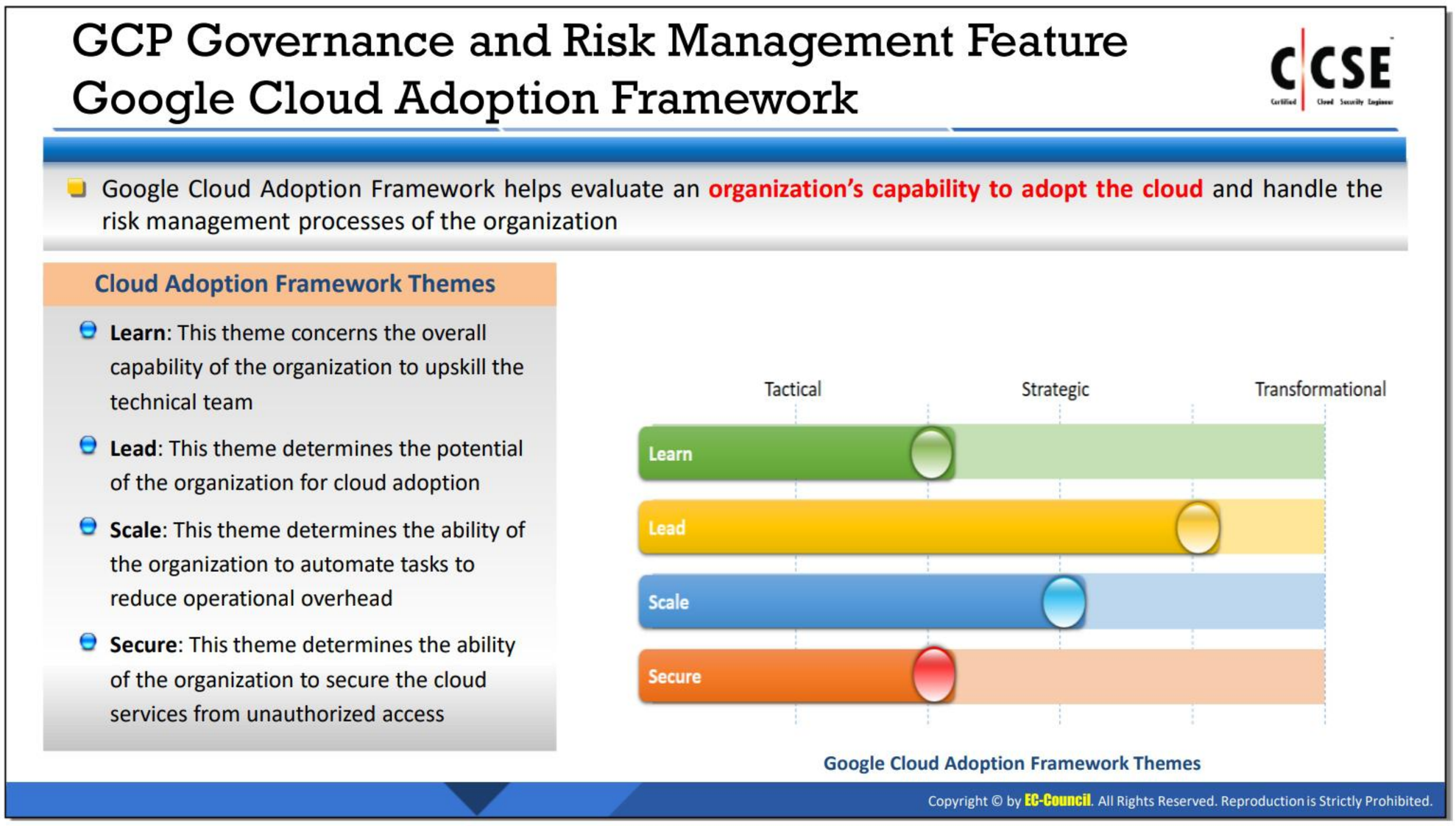
GCP Governance and Risk Management Feature: Policy Intelligence

Google Cloud Policy Intelligence helps in the automated management of policies that reduce security risks. The different capabilities included with Google Cloud Policy Intelligence are as follows:

hide01.ir

- **IAM Recommender**: IAM Recommender uses machine learning to implement smart access control. It helps in enforcing the principle of least privilege. With IAM Recommender the security admins can detect unwanted access to resources and then revoke them. IAM Recommender also gives recommendations regarding the necessary access controls to be granted and revoked.
- **Policy Troubleshooter**: Policy Troubleshooter helps the administrators to quickly identify and resolve access control issues. It helps in analyzing the reasons why the particular user was denied access and the access control policies can be modified to grant appropriate access.
- **Policy Analyzer**: Policy Analyzer helps in identifying who has access to a particular service.
- **Policy Simulator**: The changes made to the user accounts cause risks to the resources. Policy Simulator helps in reviewing the impact of policy changes in IAM before deploying them into production.

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



GCP Governance and Risk Management Feature: Google Cloud Adoption Framework

Google Cloud Adoption Framework can be used to evaluate how much the organization is prepared for cloud adoption, the changes to be made, and the development of new capabilities. It helps to determine the organization's capability to adopt the cloud and handle the risk management processes of the organization. Cloud Adoption Framework helps the organization to develop the strategies required for cloud adoption. The organization can be better prepared for cloud adoption by considering four themes i.e., learn, lead, scale, and secure.

The four themes related to cloud adoption are as follows:

- **Learn:** This theme is concerned with the overall capability of the organization to upskill the technical team. The lead theme includes upskilling and external experience.
- **Lead:** The lead theme determines the potential of the organization for cloud adoption which includes the direction from top to bottom level from sponsors and the motivation gathered from the bottom to up level of the organization. The objectives, decisions can be executed by the collaboration of these two. In short, the lead theme includes sponsorship and teamwork.
- **Scale:** The scale theme determines the ability of the organization to automate tasks to reduce operational overhead. It determines the extent to which the organization use managed and serverless cloud services, continuous integration and delivery (CI & CD), and the infrastructure code.

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

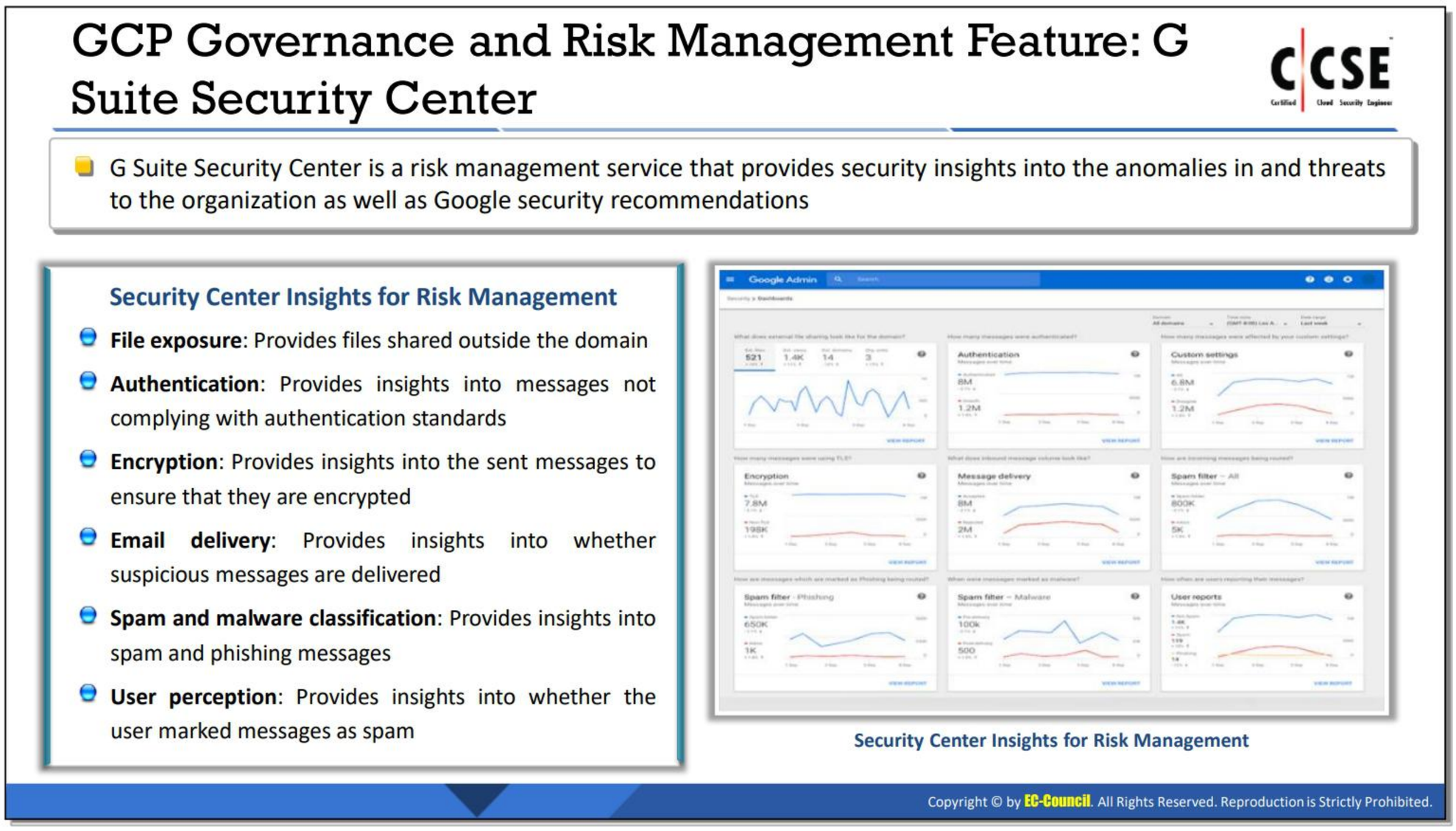
- **Secure:** Secure theme determines the ability of the organization to secure the cloud services from unauthorized access and understanding of the organization regarding the data which needs to be protected, encrypted, and to be guarded against exfiltration.

The success of the organization in the cloud is determined by the ongoing business practices of the organization under these themes which falls under three phases that are as follows:

- **Tactical**: A systematic plan which includes all the individual workloads for future cloud adoption. The organization must be able to migrate to the cloud without any disruption.
- **Strategic**: The strategic phase is based on the management of individual workloads which are designed to meet future needs.
- **Transformational**: This phase is related to transformation where the data and insights can be integrated with the cloud environment.

hide01.ir

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



GCP Governance and Risk Management Feature: G Suite Security Center

G Suite Security Center provides security insights for Google Workspace. G Suite Security Center can protect the organization with security analytics and it also provides security recommendations. Security Center Provides a single dashboard to monitor external file sharing, spam, malware targeting the users in the organization. It also provides the functionalities for detecting and mitigating security issues in the organization. The security center provides insights into the following.

- File Exposure: Analyse the files shared outside the domain
- Authentication: Analyse the messages which do not meet authentication standards
- Encryption: Ensure the messages are TLS encrypted
- Email Delivery: The incoming messages accepted
- Spam and Malware Classification: The messages which are spam, phishing, or contains malware are analyzed
- User Perception: The whitelists are evaluated to check whether the users marked the messages as spam.

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

Certifications, Audits, and Assessments in GCP

- Google Cloud undergoes **third-party audits** of the security, privacy, and compliance controls of data centers, infrastructure, and operations to achieve certifications that demonstrate security compliance with various standards

GCP Information Security Management Standard: ISO 27001

- GCP is ISO/IEC 27001 certified for systems, technology, processes, and data centers that run G Suite
- GCP security controls that comply with ISO 27001 include the following:
  - Policies for information security
  - Physical, logical, and environmental security
  - Cryptography
  - Operations security and incident management
  - Asset management and access control

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

Certifications, Audits, and Assessments in GCP (Cont'd)

- Google Cloud is audited by third parties to validate individual products with SOC 2 and SOC 3 compliance, which ensures the security, integrity, availability, and confidentiality of organizational systems

hndec1.ir

Controls Covered by SOC 2 and SOC 3 in GCP

- Logical security controls
- Data-center physical security controls
- Change management controls to track, test, validate, and approve changes
- Organizational and administrative controls to monitor security compliances and security training
- Availability controls for disaster recovery sites

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.

Certifications, Audits, and Assessments in GCP (Cont'd)

Cloud-specific Compliance: ISO 27017

- GCP is compliant with ISO 27017, which is an information security compliance standard specific to cloud services

International Privacy Compliance for GCP: ISO 27018

- ISO/IEC 27018:2014 compliance in GCP ensures that Google follows **international privacy** and **data protection** standards
- ISO 27018 compliance has the following benefits:
  - Ensures that the data will not be used for advertisements
  - Provides tools to export and delete the data
  - Protects against requests for data from third parties
  - Provides a clear picture about where the user data are stored

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

Certifications, Audits, and Assessments in GCP (Cont'd)

h1001.ir

FedRAMP

- Google Cloud complies with the Federal Risk & Authorization Management Program (FedRAMP), which authorizes the use of moderate-impact-level data by federal agencies and offers authorization to handle official information

PCI DSS

- GCP users can comply with the Payment Card Industry Data Security Standard (PCI DSS) for securing payment card information by configuring a data loss prevention (DLP) policy to block payment card emails from GCP

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

Certifications, Audits and Assessments in GCP

The Google Cloud provides information, best practices, and documentation to help its customers with compliance and offerings. The Google products undergo verification of security, compliance controls, and privacy on regular basis. These verifications helped in achieving certifications for global standards that make customers trust GCP. GCP still focuses on expanding its coverage. Google Cloud provides independent verification of security, privacy,

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

and compliance controls by undergoing third-party audits. The certifications, aduits, and assessments in GCP are as follows:

ISO/IEC 27001

The International Organization for Standardization/International Electrotechnical Commission (ISO)/IEC 27001 standard helps an organization to secure its data and information assets. This standard offers requirements for an Information Security Management System (ISMS). ISO/IEC 27001 provides details about the security controls that can be used to handle information risks.

GCP is certified to be compliant with ISO/IEC 27001. It is not mandatory to use specific information security controls mentioned in this standard. But the list of security controls and the framework laid out helps Google to have a comprehensive model for security management. The ISO/IEC 27001 certificates of GCP, Google Workspace, and Apigee can be requested from Compliance Reports Manager.

ISO/IEC 27017

ISO/IEC 27017 is a security standard developed for GCP and other cloud service providers (CSPs). It provides cloud customers with guidelines to reduce security issues and to make the cloud environment safe and secure. It is a part of the ISO/IEC 27000 family of standards and is developed from ISO/IEC 27002 standard. ISO/IEC 27017 suggests security controls for the cloud which are not defined in ISO/IEC 27002.

The ISO/IEC 27017 provides guidelines for information security controls that can be used for cloud services. It provides guidance for seven new cloud security controls along with the 37 ISO/IEC 27002 controls.

hide01.ir

Google Cloud Platform, Google Workspace, Chrome, and Apigee are certified to be compliant with ISO/IEC 27017.

ISO/IEC 27018

ISO/IEC 27018 standard deals with the protection of personally identifiable information (PII), which is a critical component of GCP privacy. It ensures that the GCP has required information security controls to protect the privacy of its customers. It focuses on security controls for processing PII by adding specific items for cloud privacy on the existing ISO/IEC 27002. It also offers additional security controls for processing personal data in the cloud.

This standard mainly ensures that the user data is not used for advertising and remains with the owner. Google Cloud Platform, Google Workspace, Chrome, and Apigee are compliant with this standard to ensure that it follows international data protection and privacy standards.

ISO/IEC 27701

ISO/IEC 27701 is a global privacy standard. It focuses on collecting and processing personally identifiable information (PII). It helps the organization to be complaint with the international privacy frameworks and laws. It includes the guidance of implementing, maintaining a Privacy Information Management System (PIMS).

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

The Google Cloud is the first cloud provider to receive an accredited ISO/IEC 27701 certification as a PII data processor. GCP has undergone a third-party audit to receive this certification. GCP received an accredited certificate of registration for ISO/IEC 27701. This ensures that PIMS for GCP complies with ISO/IEC 27701 requirements. It also shows that the audit and certificate issued by a body have performed according to the International Accreditation Forum (IAF)/ANSI National Accreditation Board (ANAB) requirements. The accredited certificate of GCP shows its commitment to privacy.

SOC 2 and SOC 3

SOC (Service Organization Controls) 2 and SOC 3 are developed by the Auditing Standards Board of American Institute of Certified Public Accountants (AICPA) based on Trust Service Criteria. The SOC 2 report examines the information security of an organization in terms of security, availability, confidentiality, and privacy. Whereas SOC3 is a public report that includes internal controls on security, confidentiality, and availability.

The individual products of GCP undergo regular third-party audits to certify for SOC 2 and SOC 3. The SOC 2 report of GCP includes the principles of security, confidentiality, processing integrity, and availability in the AICPA's Trust Services Principles and Criteria.

C5:2020

The Cloud Computing Compliance Criteria Catalogue (C5:2020) is developed by the German Federal Office for Information Security (BSI). It is a method for assessing the cloud services information security that handles internationally recognized security standards. This sets an audit baseline to establish trust between customers and cloud providers.

hide01.ir

Google has received the BSI's Cloud Computing Compliance Controls Catalog ("C5") attestation previously. In 2020, BSI revised it as C5:2020. Google Cloud has gained attestation for C5:2020 requirements through an independent third-party audit. As a part of the assessment for using Google Cloud services, GCP customers can use C5:2020 attestation as verification of compliance.

MTCS Tier 3

The Multi-Tier Cloud Security is a cloud security certification handled by Singapore. The MTCS Tier 3 certifies the cloud service providers (CSPs) at various operational security levels with the most strict requirements.

GCP received MTCS Tier 3 certificate through an audit conducted by an independent MTCS certifying body.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a standardized approach to authorization, security assessment, and continuous monitoring for cloud services and products. Cloud deployments of all federal agencies should meet FedRAMP at the required risk impact level.

The Google Cloud has received FedRAMP High Authorization to Operate (ATO) for 17 products in 5 different cloud regions. It also received FedRAMP Moderate ATO for its 64 products in 17

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

cloud regions. This shows that the GCP can run compliant workloads at the highest level of civilian classification.

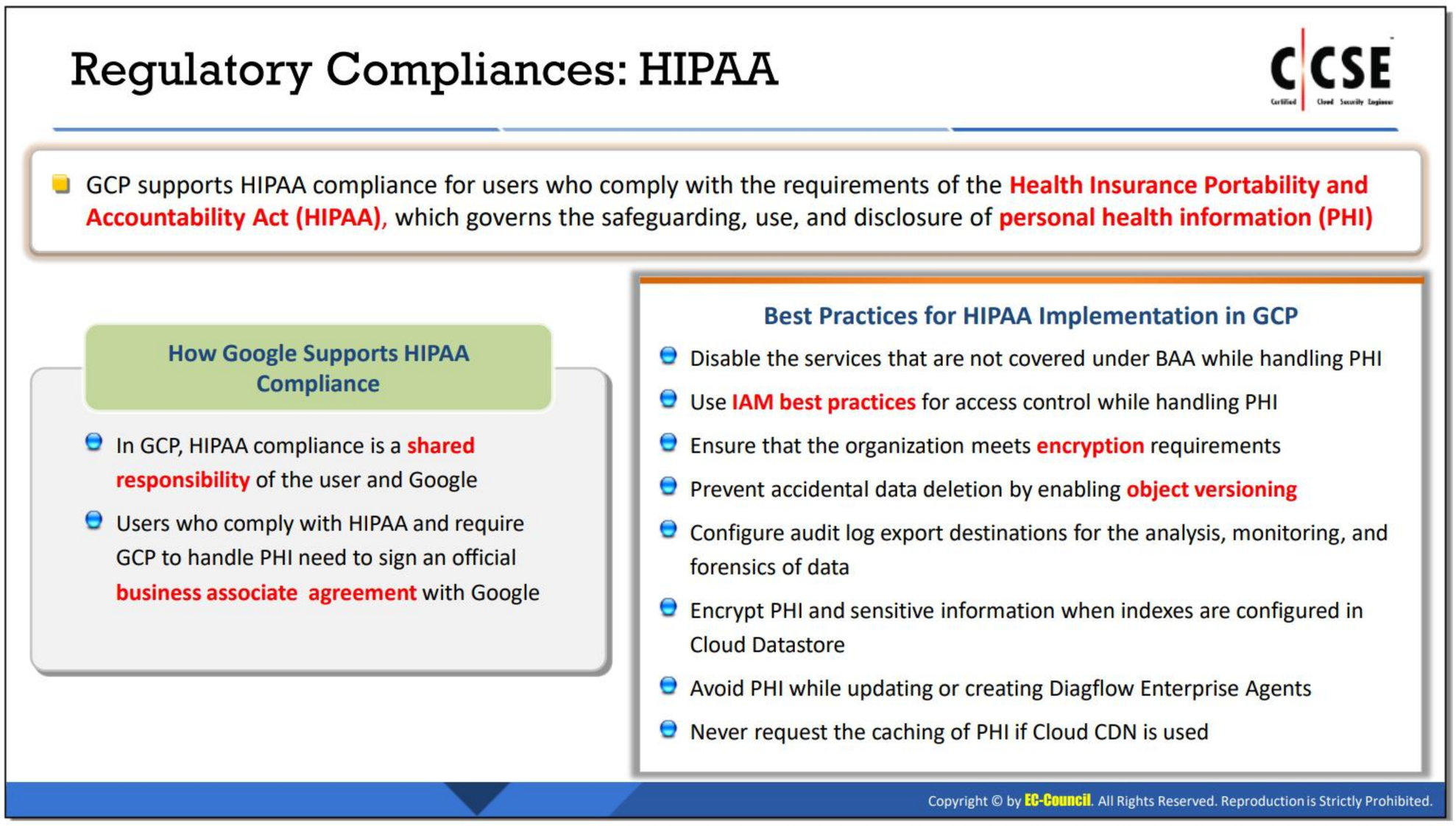
PCI DSS

Payment Card Industry (PCI) Data Security Standards (DSS) is developed by the PCI Security Standards Council. It is an information security standard for organizations that handle credit and debit card information. PCI DSS has classifications for different merchant types.

The Google Cloud undergoes third-party audits every year to certify its products for PCI DSS. This shows that the Google Cloud has an infrastructure where customers can build applications that process, store, and transmit card details. It is still the customer's responsibility to ensure that their applications are compliant with PCI DSS.

hide01.ir

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



Regulatory Compliances: HIPAA

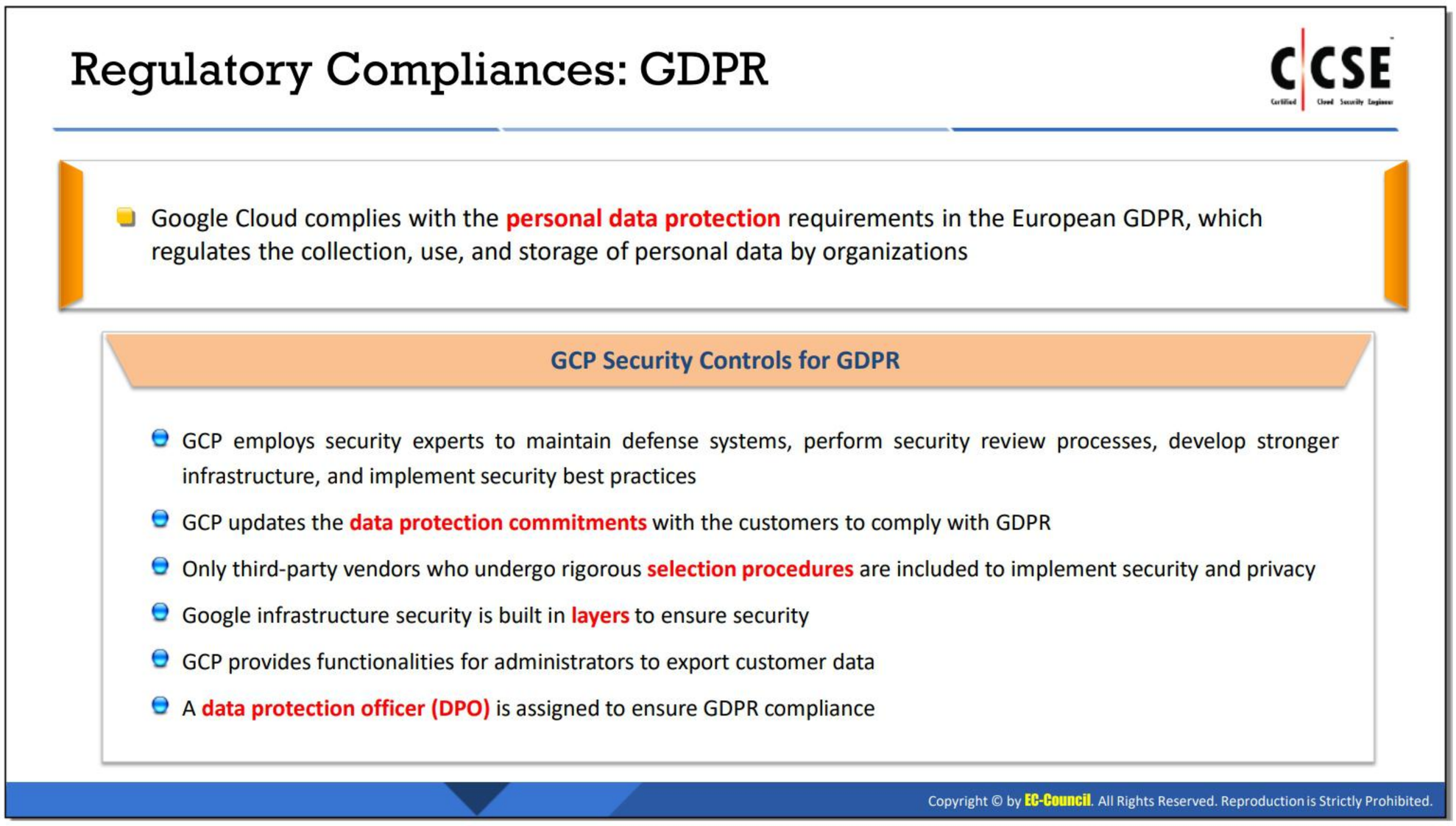
GCP supports user compliance with HIPAA, which is the US Health Insurance Portability and Accountability Act. HIPAA governs the safeguarding, use, and disclosure of personal health information. In GCP HIPAA compliance acts as a shared responsibility between the user and Google. Users with HIPAA compliance can use Google Cloud for storage and data processing by signing a business associate amendment with Google.

Users who comply with HIPAA requires GCP to handle Personal Health Information (PHI) must sign a Business Associate Agreement (BAA) with Google

Best Practices for HIPAA Implementation

- Disable the services that are not covered under BAA while handling PHI
- IAM best practices can be used for access control while handling PHI
- Ensure that the organization has encryption requirements
- To prevent accidental data deletion, enable object versioning
- For analysis, monitoring, and forensics of the data, configure audit log export destinations
- Encrypt PHI, sensitive information when indexes are configured in Cloud Datastore
- Avoid PHI while updating or creating Diagflow Enterprise Agents
- Never request caching of PHI if Cloud CDN is used

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



Regulatory Compliances: GDPR

Google Cloud is compliant with the personal data protection compliance in Europe GDPR which regulates the organizations in collecting, using, and storing personal data

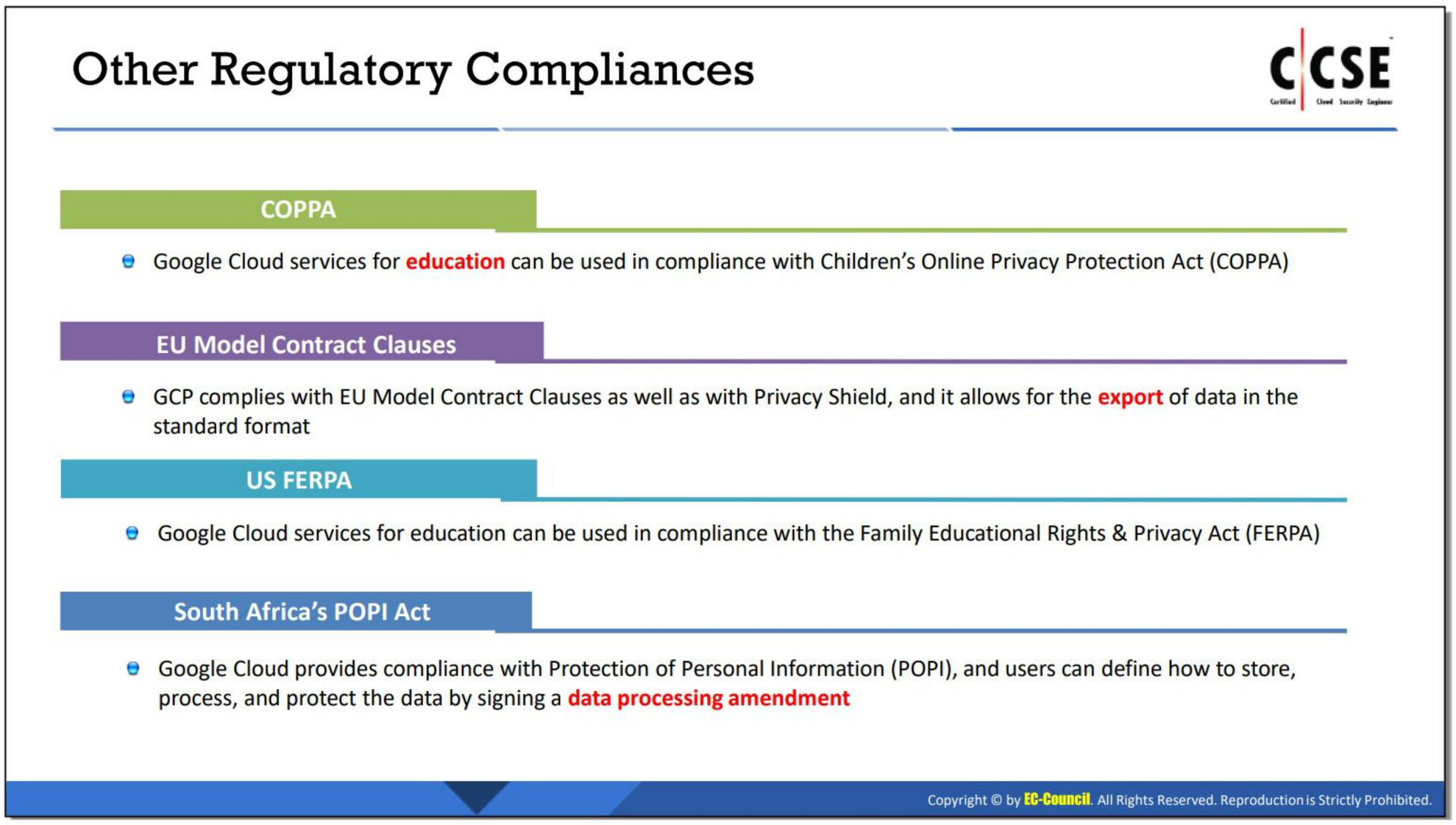
hide01.ir

GCP Security Controls for GDPR

GCP security controls that comply with GDPR are

- GCP employs experts in security to maintain the defense systems, security review processes, stronger infrastructure, and implementing security best policies
- Updates the data protection commitments with the customers to comply with GDPR
- Include third-party vendors who undergo rigorous selection procedures to implement security and privacy
- Google infrastructure security is built in layers to ensure security
- Provides functionalities for administrators to export customer data
- A data protection officer (DPO) is assigned to ensure GDPR compliance of data

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

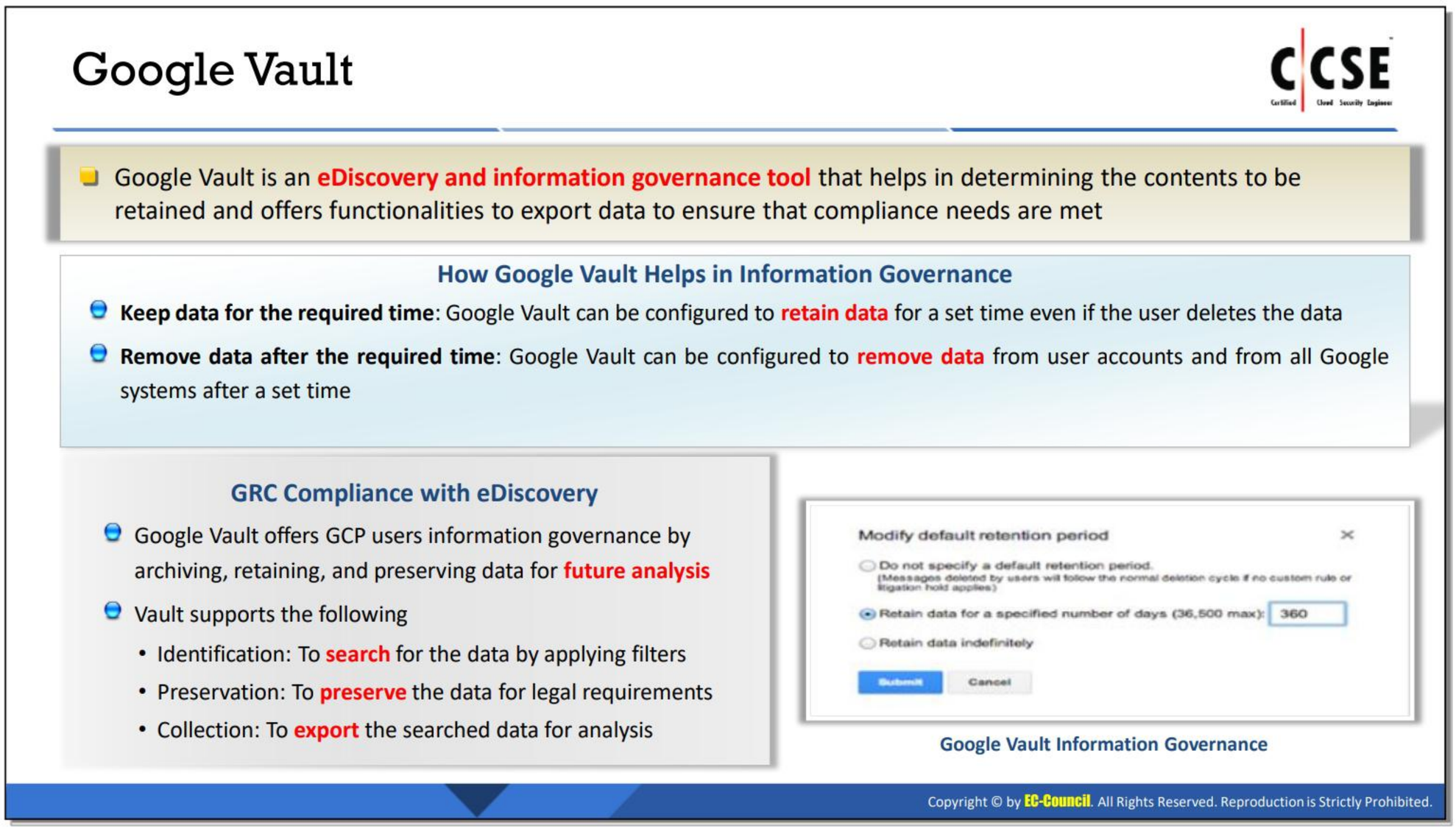


Other Regulatory Compliances

- **COPPA:** GCP is compliant with COPPA which is the Children's Online Privacy Protection Act. Google Cloud Service for education can be used in compliance with COPPA.
- **EU Model Contract Clauses:** GCP is compliant with EU Model Contract Clauses and it is also compliant with Privacy Shield and allows for export of data in the standard format.
- **US FERPA:** GCP is compliant with FERPA which is Family Educational Rights & Privacy Act. Google Cloud Services for Education can be used in compliance with FERPA.
- **South Africa's POPI Act:** Google Cloud provides capabilities for user compliance with POPI which is Protection of Personal Information. Users can define how to store, process, and protect the data by signing a Data Processing Amendment.

hole01.ir

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



Google Vault

Google Vault is an eDiscovery and information governance tool for Google workspace. Google vault helps in determining the contents to be retained and it offers functionalities to export data and ensures that it meets the compliance needs. It helps to retain, hold, search, and export Google Workspace's data to support an organization's eDiscovery and archiving needs.

The Google Vault supports the following:

- Email messages
- Google Drive and Team Drive files
- Google Hangout chats with history turned on
- Messages of Google Groups
- Google Meet recordings

To search and retain the data using Vault, users should have a Google Workspace license and Google license.

The Vault can be used for:

- **Archiving Data:** Administrators can create retention rules to determine how long the data should be stored before deleting it from user accounts and Google systems.
- **Legal Holds:** Administrators can set the hold on data from certain Workspace applications to retain the data as long as required for legal activities.

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

- **Search:** Using search parameters such as user, file name, file type, etc can be used to find the required data. The powerful search capability of Google can be used for all the data in the organization's domain.
- **Export:** For further processing and external use, the data from Google Vault can be exported in different formats. The data can be exported in PST, XML, MBox format, and CSV format.
- **Audit Reports:** With Vault, users can control who can access and perform actions on Vault. Only specific users who have access to Vault can create retention rules and can perform other actions. To know the activity of a particular user, an audit report can be created. An audit report helps to discover the rules created by users and which users have removed certain data. The audit report also includes when a user performs search or exports data.

- **How Google Vault Helps in Information Governance By Retaining and Deleting Data**
  - **Keep the Data for the Required Time**: Google Vault can be configured to retain the data for a set time. Even if the user deletes the data it will remain with Google Vault for the configured time.
  - **Remove the Data After the Required Time:** Google Vault can be configured to remove the data from user accounts and from all Google Systems after a set time. The data after deletion by vault cannot be retrieved by administrators or users.

hide01.ir

GRC Compliance with e-Discovery

Google vault offers GCP users information governance by archiving, retaining, and preserving data for future analysis. Vault supports the following

Identification: To search for the data applying filters

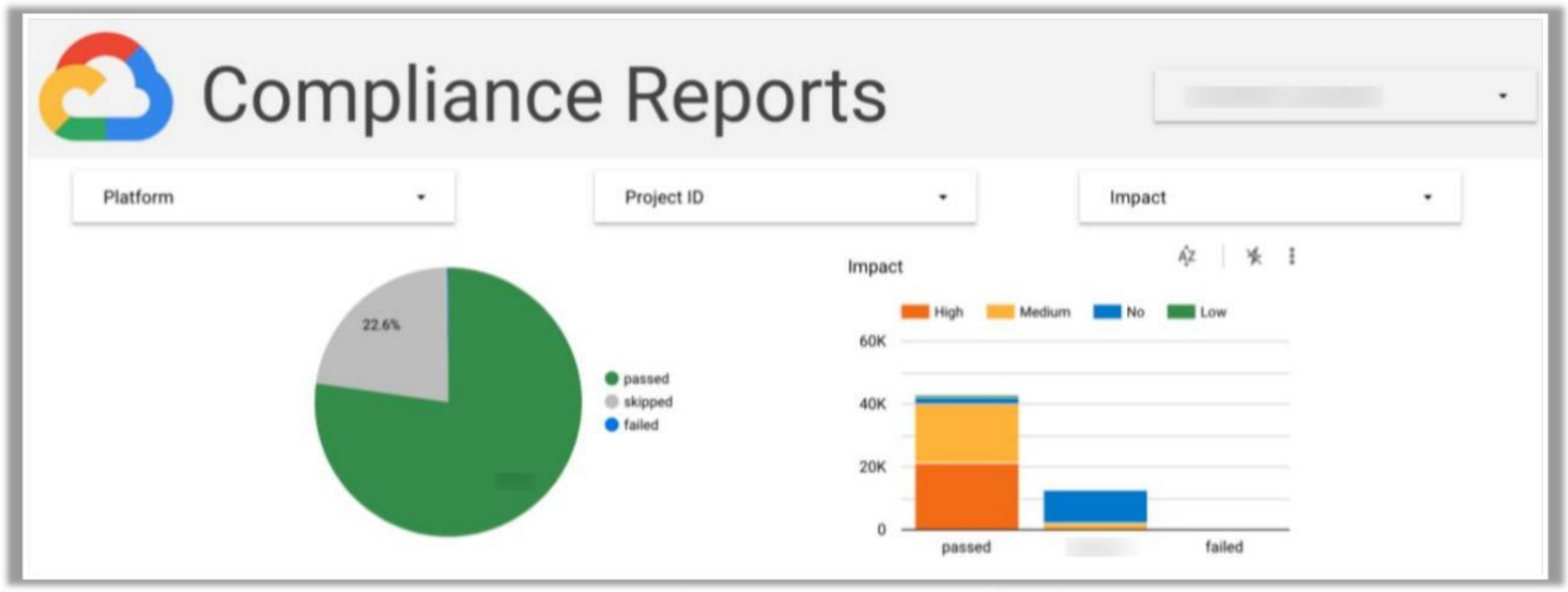
Preservation: To preserve the data for legal requirements

Collection: The searched data can be exported for analysis

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

Compliance Reports Manager

- Compliance Reports Manager in Google Cloud provides **access** to the security third-party audits, certifications, and documentation that support compliance



Compliance Reports Manager Dashboard

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

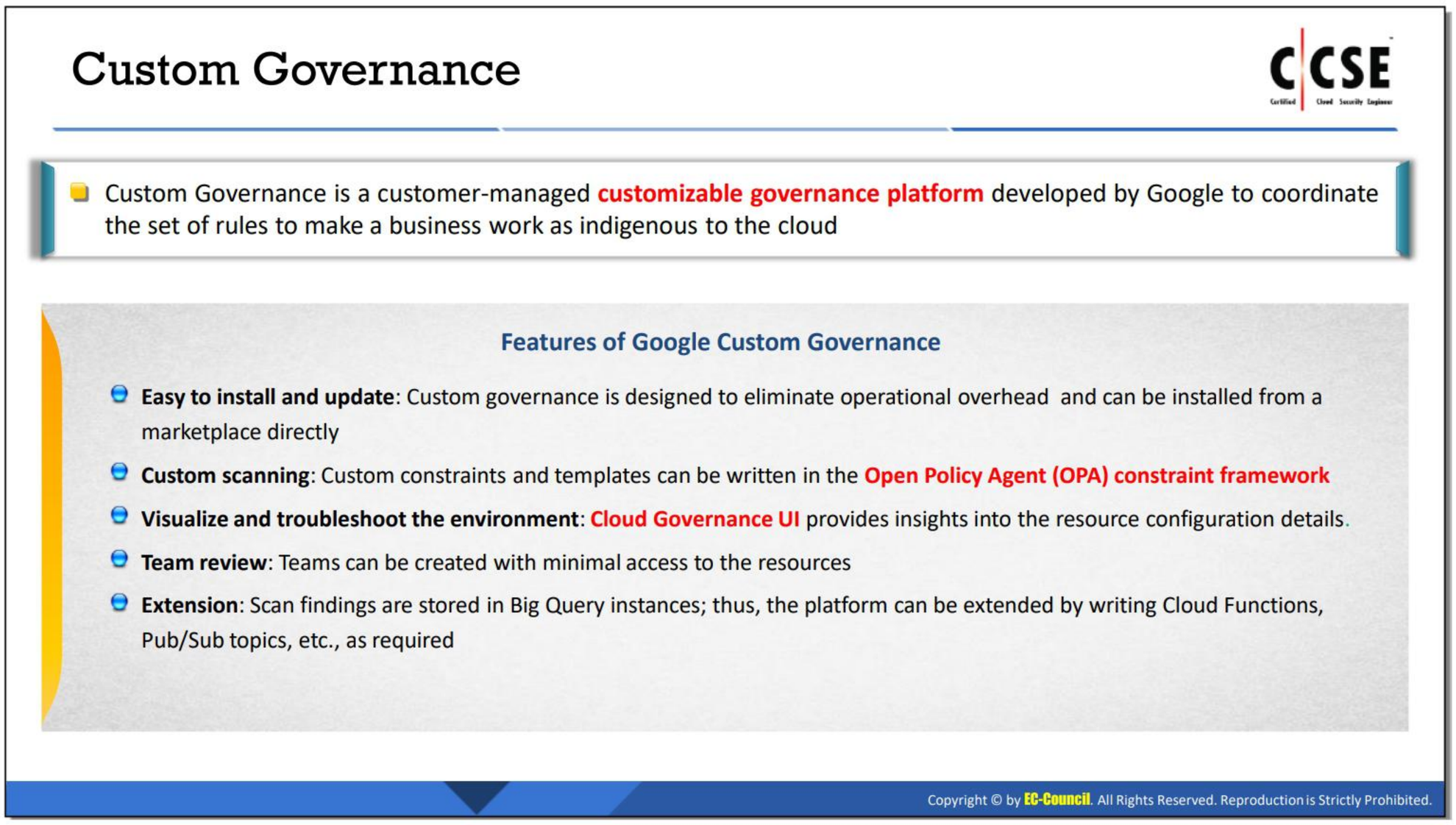
Compliance Reports Manager

The industry-leading security, third-party audits and certifications, documentation, and contract commitments of Google Cloud helps to support compliance for its customers. Compliance Reports Manager in Google Cloud provides access to the security third party audits, certifications, documentation which supports compliance.

Using Compliance Reports Manager, users can quickly and easily access the compliance resources without any additional costs. The key compliance resources include the latest ISO/IEC certificates, SOC reports, and self-assessments.

To select specific resources, the users need to sign in to the Google Workspace or Google Cloud account.

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



Custom Governance

Custom Governance is a customer-managed customizable governance platform developed by Google to coordinate the set of rules to make the business work as indigenous to the cloud. Using this software, cloud customers can build a unique set of rules to make their business work as a part of the cloud environment.

The features of Google Custom Governance include:

- **Easy Installation and Update:** The CG is designed in such a way that it is flexible and easily extensible. It is also designed to reduce the labour and overhead by providing an easily managed experience. For greater simplicity, it can be easily installed from Marketplace.
- **Custom Scanning:** The cloud users can write custom constraints and templates in the Open Policy Agent (OPA) constraint framework. The library of constraints can be managed in the CG's web UI (User Interface), or in a git repository. The CG also allows using the Forseti Policy Library to start quickly and easily. The users can also use their existing Forseti install.
- **Visualization and Troubleshooting the Environment:** The resource hierarchy backed by Cloud Asset Inventory (CAI) data can be visualized from the CG's web UI. The visualization also provides a filter and search option to quickly know the configuration details of a resource. It also lets to see the resources that belong to the same label, folder, or project.
- **Team Review:** The organization can create teams and set limited access to resources and the results can be scanned. To maintain the integrity of the cloud environment, teams other than the compliance team can also be engaged.

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

- **Extension:** The GCP customers own the data and resources it lives on as the CG runs on the GCP environment. The scan findings can be stored in a BigQuery instance. With this, the platform can be easily extended by writing Cloud Functions, Data Studio Dashboards, Pub/Sub topics, etc.

  The basic Custom Governance does not need any software license or software tier requirement.

hide01.ir

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



Module Summary

This module describes the governance, risk, and compliance of Cloud along with the explanation about the cloud governance, risk management and cloud compliances. It highlights the importance and need of GRC in cloud for establishing an agile, secure and cost-efficient organizational environment. It discussed the security features provided by the Amazon Cloud, Microsoft Azure Cloud, and Google Cloud Platform in detail. The key points discussed in this module are:

- GRC provides an organizational strategy to manage governance and risk to meet government and industry compliance.
- GRC tools increase organizational productivity and efficiency of governance, risk, and compliance.
- Cloud governance is a set of rules used to control cost, enhance efficiency and remove security risks in a cloud environment.
- Cloud governance framework offers financial, operational, data, security, and compliance management for optimizing the cloud services and controls.
- Risk management framework offers a well-defined process to detect threats or risks and determine a strategy for eliminating the risk impact on the organizations.
- Cloud compliance ensures the implementation of laws and regulation applied to cloud.
- GRC implementation offers an efficiently planned strategy that provides effective governance, risk, and compliance.
- Google Cloud Security Command Center provides real time visibility into cloud resources.

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

This page is intentionally left blank.

hide01.ir