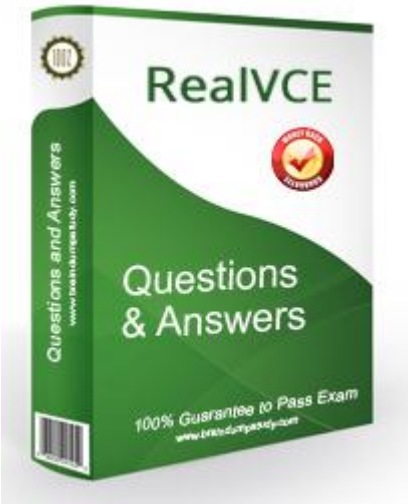
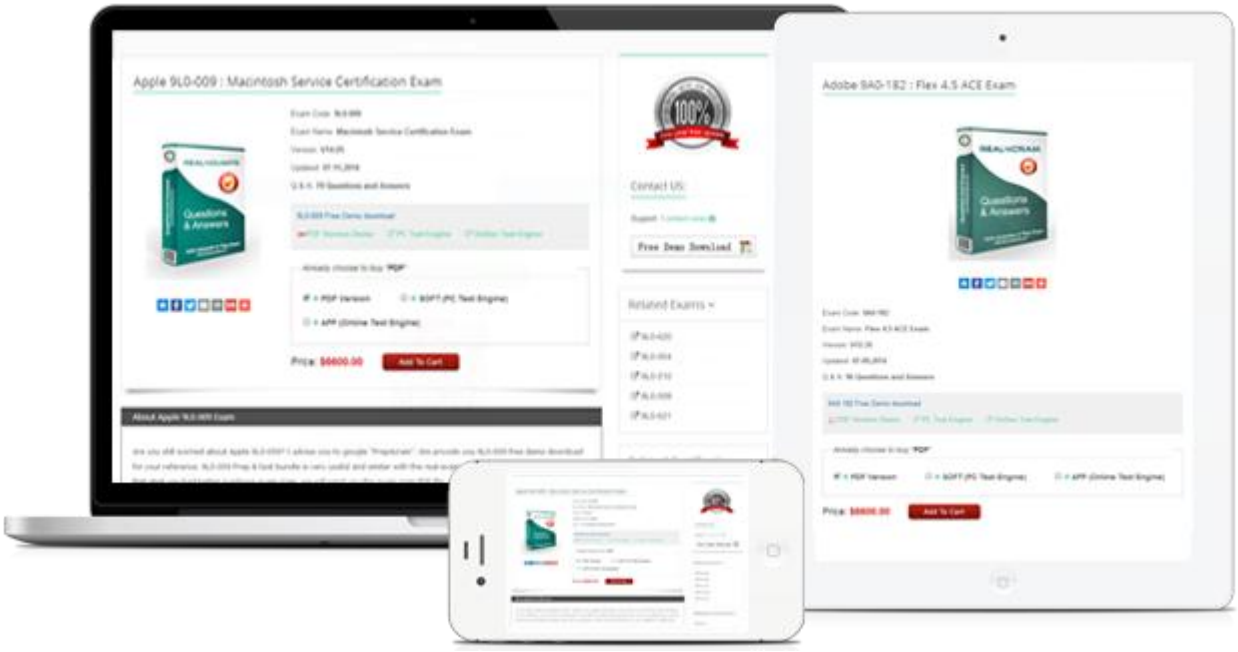
RealVCE





http://www.realvce.com

Free VCE Exam Simulator, Real Exam Dumps File Download

Exam : **CCSK-JPN**

Title : Certificate of Cloud Security Knowledge (v4.0) Exam (CCSK日本語版)

Vendor : Cloud Security Alliance

Version : DEMO

QUESTION NO: 1
クラウド環境内でオーケストレーションによって何が自動化されるのでしょうか?
A. アプリケーションのパフォーマンスを監視する
B. セキュリティポリシーの手動設定
C. オペレーティングシステムのインストール
D. VM、ネットワーク、その他のリソースのプロビジョニング
Answer: D
Explanation:
In a cloud environment, orchestration automates the provisioning and management of various cloud resources, including virtual machines (VMs), networking, storage, and other infrastructure components. Cloud orchestration involves the use of software to coordinate and automate tasks that would otherwise require manual intervention, improving efficiency, scalability, and consistency across the environment.
Monitoring application performance is typically handled by monitoring tools, not orchestration. Manual configuration of security policies is something that can be automated through policy management but is not the focus of orchestration. Installation of operating systems is part of provisioning resources, but orchestration primarily focuses on automating the overall management of infrastructure and services, not just the installation of operating systems.

QUESTION NO: 2
FaaS において、サードパーティのサービス/API
を使用する際の主なセキュリティ上の懸念事項は何ですか?
A. サーバー管理を直接制御する
B. 簡素化されたIAMと権限管理
C. 不正アクセスによる攻撃対象領域の拡大
D. 実行のステートレスな性質によりリスクが軽減される
Answer: C
Explanation:
"When integrating third-party APIs with FaaS, each connection potentially increases the attack surface by exposing additional authentication, authorization, and data access points." - CSA Security Guidance v4.0 - Domain 14: Serverless Security

QUESTION NO: 3
クラウドのコンテキストでは、ユーザーの権限に関してエンタイトルメントとは何を指しますか?
A. ユーザーがクラウド環境にアクセスする際に使用する必要がある認証方法。
B. ユーザーがクラウド サービス プロバイダーから受けられるテクニカル
サポートのレベル。
C. クラウド環境でユーザーがアクセスする権限を付与されるリソースまたはサービス。
D. ユーザーがクラウド環境内の他のユーザーにアクセス権限を付与する機能。
Answer: C
Explanation:
In a cloud context, entitlement refers to the specific resources or services a user is granted permission to access based on their roles or permissions. This includes access to

applications, data, or cloud services, and is typically managed through Identity and Access Management (IAM) systems, which define what users can do and what they can access within the cloud environment.

QUESTION NO: 4
物理インフラストラクチャと仮想化プラットフォームのセキュリティは誰が担当していますか?
A. クラウド コンシューマ
B. 大部分が消費者負担
C. 契約による
D. 責任は均等に分割されます
E. クラウド プロバイダー
Answer: E

QUESTION NO: 5
新しいワークロード タイプにサーバーレス
コンピューティングを使用する利点は次のどれですか。
A. 短期的なコミットメントが必要であり、初期費用を延期する
B. 自動スケーリングと運用オーバーヘッドの削減
C. 大規模な初期設定は必要ありません
D. 基盤となるサーバー環境を完全に制御
Answer: B
Explanation:
Serverless computing (Function as a Service - FaaS) is designed for auto-scaling, high availability, and reduced management overhead. It enables developers to focus on writing code without managing the underlying infrastructure. This makes it an ideal solution for new or unpredictable workloads.
As explained in CSA Security Guidance v4.0 - Domain 1: Cloud Computing Concepts and Architectures:
"Serverless computing abstracts infrastructure management and allows automatic scaling of application functions in response to demand. This reduces operational overhead and enables teams to deploy scalable solutions rapidly." (CSA Security Guidance v4.0, Domain 1: Cloud Computing Concepts and Architectures) Why not the others?
A . While cost benefits exist, it's not the core benefit of serverless.
C . Configuration may be minimal, but not exclusive to serverless.
D . Serverless removes control over the underlying server environment.

QUESTION NO: 6
システムまたは環境がテンプレートから自動的に構築されるとはどういう意味ですか?
A. 何もありません。
B. 自動化の構成によって異なります。
C.
本番環境で行われた変更は、次のコードまたはテンプレートの変更によって上書きされます。

D.
テストで行われた変更は、次のコードまたはテンプレートの変更によって上書きされます。
E.
本番環境で行われた変更は、次のコードまたはテンプレートの変更によって変更されません。
Answer: D

QUESTION NO: 7
可能な場合はエラスティック
サーバーを使用し、ワークロードを新しいインスタンスに移動します。
A. いいえ
B. 真
Answer: B

QUESTION NO: 8
事業継続性を継続的にテストするために、クラウドの一部を選択的に劣化させるツールの使用を説明するために使用される用語はどれですか?
A. 計画停電
B. 回復力の計画
C. 期待されるエンジニアリング
D. カオスエンジニアリング
E. 組織的なダウンタイム
Answer: D

QUESTION NO: 9
クラウド リソースの管理と構成に使用され、クラウド セキュリティ
プログラムの最優先事項となるのは次のどれですか。
A. 管理コンソール
B. 管理プレーン
C. オーケストレーター
D. 抽象化レイヤー
Answer: B
Explanation:
The management plane is used for governing and configuring cloud resources and is considered a top priority in cloud security programs. It provides the tools and interfaces for administrators to manage, configure, and control cloud resources, such as virtual machines, storage, and networking. It is critical to secure the management plane because it often has access to sensitive configurations and the ability to modify cloud environments, making it a prime target for attacks.
Management Console is an interface that interacts with the management plane, but it is not the underlying system for governance and configuration. Orchestrators are used to automate the management and deployment of cloud resources but are not the primary component for governing andsecuring cloud environments. Abstraction layer refers to the layer that hides the complexity of underlying infrastructure, but it does not directly govern or configure cloud

resources.

QUESTION NO: 10
基本的にインスタンス化された仮想ハード ドライブまたは VM の仮想ハード ドライブであるクラウド ストレージ テクノロジはどれですか?
A. ボリューム ストレージ
B. プラットフォーム
C. データベース
D. アプリケーション
E. オブジェクトストレージ
Answer: A

QUESTION NO: 11
クラウド セキュリティの実装に役立つ一般化されたテンプレートを提供するクラウド セキュリティ モデル タイプはどれですか?
A. 概念モデルまたはフレームワーク
B. デザインパターン
C. モデルまたはフレームワークを制御します
D. 参照アーキテクチャ
E. クラウド コントロール マトリックス (CCM)
Answer: D

QUESTION NO: 12
キーに対する ID およびアクセス管理 (IAM) ポリシーによって、最小権限の原則の遵守をどのように確保できますか?
A. 定期的にキーをローテーションすることで
B. すべてのキーにデフォルトのポリシーを使用する
C. きめ細かな権限を指定することで
D. 管理者にルートアクセスを許可することで
Answer: C
Explanation:
Fine-grained permissions enable specific control over who can access certain resources, thus enforcing the least privilege principle. Reference: [Security Guidance v5, Domain 5 - IAM]

QUESTION NO: 13
クラウド環境では、共有セキュリティ責任モデルは主に何を定義することを目指していますか?
A. クラウドプロバイダーと顧客間のセキュリティ責任の分担
B. IaaS、PaaS、SaaSプロバイダー間の関係
C. 地理的データの所在地と主権の遵守
D. クラウドコンプライアンスフレームワークのガイダンス
Answer: A
Explanation:

The Shared Security Responsibility Model clarifies which security responsibilities are managed by the CSP and which by the CSC, based on the service model. Reference: [CCSK Study Guide, Domain 1 - Cloud Security Models][16source].

QUESTION NO: 14
ルート/コア
アクセスを最小限に抑え、デプロイメントの作成を制限することでセキュリティ
リスクを軽減するのに最も役立つプラクティスはどれですか?
A. 信頼の原則を強制し、最終的には要求に応じて実行します。
B. スタッフの多要素認証を無効にし、意思決定者のアカウントに焦点を当てる
C. 完全なアクセス権を持つアプリケーションを展開し、必要に応じて制限を適用する
D. 最小権限の原則の実施
Answer: D
Explanation:
Enforcing the principle of least privilege is the practice of granting users and systems the minimum level of access necessary to perform their tasks. By limiting root or core access and restricting the creation of deployments to onlythose who absolutely need it, the risk of unauthorized access, misuse, or damage is minimized. This helps ensure that critical systems and sensitive data are protected by reducing the number of people or services with high-level access.
Trust and verify on demand is not a standard security practice and could create security gaps. Disabling multi-factor authentication is a poor security practice, as multi-factor authentication (MFA) enhances security by adding an additional layer of verification.
Deploying applications with full access) contradicts the principle of least privilege and could expose the system to unnecessary risks.

QUESTION NO: 15
クラウド プロバイダーを評価する上で、どの側面が最も大きな課題となるでしょうか?
A. 一貫性のないポリシー標準とプロバイダー要件の増加。
B. 内部の運用とテクノロジーに対する可視性が限られています。
C. クラウド
プロバイダーによって共有される詳細情報が多すぎるため、情報過多になります。
D. プロバイダーのドキュメントが不十分で、プールされた監査に過度に依存しています。
Answer: B
Explanation:
One of the biggest challenges incloud security risk assessmentisthe lack of transparencyregardingcloud provider operations and security controls.
Key Issues with Limited Visibility:
Cloud providers manage infrastructure at a global scale:
Customerscannot directly inspectsecurity implementations.
Rely onthird-party attestationslikeSOC 2, ISO 27001, CSA STARinstead of direct assessments.
Multi-tenancy complexities:
Cloud customersshare infrastructurewith other tenants.
Data isolation mechanisms (e.g., virtual private clouds, encryption)must be trustedwithout

direct verification.
Regulatory compliance challenges:
Organizations handling sensitive data (e.g., healthcare, finance)requirestrict controls.
Cloud providers may not offer sufficient audit logsor control overdata residency and processing.
Incident response limitations:
In traditional IT, organizations controllog access, forensic analysis, and recovery.
In the cloud,incident investigation depends on the provider's logging and notification practices.
Thisvisibility issueis extensively covered in:
CCSK v5 - Security Guidance v4.0, Domain 4 (Compliance and Audit Management) ENISA's Cloud Computing Risk Assessment (Limited visibility into cloud provider security policies)

QUESTION NO: 16
Software Defined Perimeter (SDP) にはどのコンポーネントが含まれていますか?
A. クライアント、コントローラー、およびゲートウェイ
B. クライアント、コントローラー、ファイアウォール、およびゲートウェイ
C. クライアント、ファイアウォール、およびゲートウェイ
D. コントローラー、ファイアウォール、およびゲートウェイ
E. クライアント、コントローラー、およびファイアウォール
Answer: A

QUESTION NO: 17
Zero Trust Network Access (ZTNA)
は、アプリケーションへのアクセスを制御するために主に何を使用しますか?
A. 位置情報データのみ
B. ユーザー名とパスワード
C. IPアドレスとポート番号
D. アイデンティティ、デバイス、コンテキスト要因
Answer: D
Explanation:
Zero Trust Network Access (ZTNA) enforces the principle of "never trust, always verify." Unlike traditional perimeter-based security, ZTNA continuously evaluates access requests using dynamic factors. These include:
User identity (authenticated via SSO or MFA)
Device posture (device compliance, health status)
Contextual information (time of access, location, behavior patterns)
This layered decision-making process ensures that access is tightly controlled and highly contextual, minimizing attack surfaces and mitigating lateral movement within networks.
ZTNA aligns with cloud-native security practices discussed in Domain 7: Infrastructure Security, emphasizing the transition from static access control lists to dynamic, identity-centric enforcement models.
Reference:
CSA Security Guidance v4.0 - Domain 7: Infrastructure Security

CSA Cloud Controls Matrix v3.0.1 - IVS-09: Segmentation & Zoning

QUESTION NO: 18
コンピューティングの仮想化におけるクラウド
プロバイダーの主なセキュリティ責任は何ですか?
A. 分離を実施し、安全な仮想化インフラストラクチャを維持します
B. ワークロードを監視してログに記録し、セキュリティ設定を構成する
C. 分離を強制し、セキュリティ設定を構成します
D. 安全な仮想化インフラストラクチャを維持し、セキュリティ設定を構成する
E. 分離を実施し、ワークロードを監視してログに記録する
Answer: A

QUESTION NO: 19
ENISA: 買収されるクラウド プロバイダーのリスク懸念の理由は次のとおりです。
A.買収企業による任意の契約解除
B. リソースの分離に失敗する可能性があります
C. プロバイダーは物理的な場所を変更する可能性があります
D. 大量解雇の可能性
E. 拘束力のない契約が危険にさらされる
Answer: E

QUESTION NO: 20
セキュリティのコンテキストで Infrastructure as Code (IaC)
を使用する主な利点は次のどれですか?
A. 手動パッチ管理
B. アドホックセキュリティポリシー
C. 静的リソース割り当て
D. 自動化されたコンプライアンスチェック
Answer: D
Explanation:
The correct answer isD. Automated compliance checks.
Infrastructure as Code (IaC)is a key DevSecOps practice where infrastructure configurations are defined and managed through code. In a security context, the primary benefit of using IaC is the ability toautomate compliance checksand enforce security best practices consistently across environments.
Key Benefits of IaC in Security:
Automated Compliance:IaC allows for the embedding ofsecurity policies directly into configuration scripts. This means that when infrastructure is deployed, it automatically adheres to compliance requirements (like NIST, CIS benchmarks).
Consistency and Repeatability:Since IaC scripts are version-controlled, any configuration changes are tracked, minimizing the risk ofconfiguration drift.
Security by Design:By coding security configurations (like IAM roles, network ACLs, encryption settings), organizations ensure that every deployment meets security standards.
Reduced Human Error:Automating infrastructure provisioning reduces manual errors that can

lead to vulnerabilities.
Why Other Options Are Incorrect:
A . Manual patch management:IaC promotes automated and repeatable configurations, reducing the need for manual patching.
B . Ad hoc security policies:IaC encouragesstandardized and consistentpolicies rather than ad hoc management.
C . Static resource allocation:IaC is dynamic and scalable, allowing for automatic scaling and configuration management rather than static resource setups.
Real-World Example:
Using tools likeTerraformorAWS CloudFormation, organizations can defineIAM policies, security group rules, and data encryption settingsas part of the infrastructure code. These configurations are then automatically checked for compliance against established policies during deployment.
Security and Compliance in IaC:
Organizations can integrate tools likeTerraform ComplianceorAWS Config Rulesto automatically verify that infrastructure settings align withregulatory requirementsandinternal security policies.
Reference:
CSA Security Guidance v4.0, Domain 10: Application Security
Cloud Computing Security Risk Assessment (ENISA) - Infrastructure as Code Best Practices
Cloud Controls Matrix (CCM) v3.0.1 - Configuration and Change Management Domain

QUESTION NO: 21
一般的なアプリケーション セキュリティの問題を軽減するのに役立つ機会はどれですか?
A. エラスティック インフラストラクチャ
B. デフォルトの拒否
C. マイクロサービスの利用の減少
D. デフォルトで分離
E. サーバーレス構成が少ない
Answer: A

QUESTION NO: 22
ドライブに障害が発生した場合、仮想化ストレージはどのようにデータ損失を回避するのに役立ちますか?
A. 異なる場所にある複数のコピー
B. ドライブは常にバックアップ、交換、およびアーカイブされます
C. 毎週のフル バックアップ
D. ドライブの故障によるデータ損失は避けられない
E. 毎日の増分バックアップ
Answer: A

QUESTION NO: 23
次の項目のうち、Security as a Service (SecaaS) の例ではないものはどれですか?
A. 迷惑メールフィルタリング

B. 認証
C. プロビジョニング
D. Web フィルタリング
E. 侵入検知
Answer: C

QUESTION NO: 24
ロール、ペルソナ、属性などの ID から承認へのマッピングの概念はどれですか?
A. アクセス制御
B. フェデレーテッド ID 管理
C. 信頼できる情報源
D. 資格
E. 認証
Answer: D

QUESTION NO: 25
CCM:
「Health4Sure」という架空の会社は米国にあり、患者の健康を追跡するためのクラウドベースのサービスを提供しています。同社は、他の業界標準の中でも HIPAA/HITECH Act に準拠しています。Health4Sure は、クラウド サービスの全体的なセキュリティを CCM ツールキットに照らして評価し、このドキュメントを潜在的なクライアントに提示できるようにすることにしました。
次のアプローチのうち、Health4Sure のクラウド
サービスの全体的なセキュリティ体制を評価するのに最も適しているのはどれですか?
A. CCM 列は HIPAA/HITECH 法にマッピングされているため、Health4Sure は、HIPPA/HITECH 法への準拠の結果として、CCM コントロールが既にカバーされていることを確認できます。その後、残りのコントロールを評価できます。このアプローチは時間を節約します。
B. CCM ドメイン コントロールは HIPAA/HITECH Act にマッピングされているため、Health4Sure は HIPPA/HITECH Act への準拠の結果として既にカバーされている CCM コントロールを検証できます。その後、残りのコントロールを徹底的に評価できます。このアプローチにより、企業の全体的なセキュリティ体制を効率的に評価できるため、時間を節約できます。
C. CCM ドメインは HIPAA/HITECH Act にマッピングされていません。したがって、Health4Sure は、CCM のすべてのコントロールに対してクラウド
サービスのセキュリティ体制を評価する必要があります。このアプローチにより、セキュリティ体制を徹底的に評価できます。
Answer: C

QUESTION NO: 26
セキュリティ コンポーネントと技術的制御を定義する際のプログラム
フレームワークの役割を最もよく説明しているのは次のうちどれですか。

A.
プログラムフレームワークは、個々のセキュリティツールのパフォーマンスを評価します。
B. プログラムフレームワークは、特定のセキュリティ技術の実装に重点を置いています。
C.
プログラムフレームワークは、包括的なセキュリティポリシーと目標を整理するのに役立ちます。
D. プログラムフレームワークは主に規制のコンプライアンス要件を定義します
Answer: C
Explanation:
Program frameworksplay a critical role in cloud security by helping toorganize overarching security policies and objectives. Frameworks suchas NIST CSF, ISO 27001, or the CSA Cloud Controls Matrix (CCM) provide structured guidance for defining security components, aligning technical controls with business objectives, and ensuring a comprehensive security program.
From theCCSK v5.0 Study Guide, Domain 3 (Governance and Enterprise Risk Management), Section 3.2:
"Program frameworks, such as the CSA CCM or NIST Cybersecurity Framework, provide a structured approach to organizing security policies, objectives, and technical controls. These frameworks help organizations align their security programs with business goals and ensure comprehensive coverage of security requirements." Option C (Program frameworks help organize overarching security policies and objectives) is the correct answer.
Option A (Evaluate the performance of individual security tools) is incorrect because frameworks focus on strategy, not tool performance.
Option B (Focus on implementing specific security technologies) is incorrect because frameworks guide policy, not technology implementation.
Option D (Primarily define compliance requirements) is incorrect because compliance is a subset of framework objectives, not the primary role.
Reference:
CCSK v5.0 Study Guide, Domain 3, Section 3.2: Security Program Frameworks.

QUESTION NO: 27
さまざまなクラウド サービス プロバイダー (CSP)
を比較する場合、サイバーセキュリティの専門家は組織構造に関してどのような点に留意する必要がありますか?
A. すべてのCSPは同じ組織構造と用語を使用します
B. 異なるCSPは同様の構造を持ちますが、異なる用語を使用します。
C. CSP は組織構造が大きく異なり、用語も同一である
D. CSP における用語の違いは、サイバーセキュリティの実践には影響しません。
Answer: B
Explanation:
When comparing different Cloud Service Providers (CSPs), it is important to recognize that while they may have similar organizational structures - such as divisions for security, compliance, and support - they often use varying terminology to describe their services, roles, and responsibilities. Understanding these differences is crucial for cybersecurity

professionals to ensure proper alignment of security practices, controls, and policies across different cloud platforms.
CSPs typically have variations in organizational structure and terminology. While the structure can vary, it is not usually "vastly" different in terms of core functions. Differences in terminology can have implications for understanding security roles, policies, and practices, affecting how cybersecurity tasks are performed.

QUESTION NO: 28
サイバーセキュリティの観点から、ネットワーク間のトラフィックフローを制御することが重要なのはなぜですか?
A. データ転送速度を上げる
B. 攻撃の爆発範囲を縮小する
C. ネットワークアーキテクチャを簡素化する
D. 保存されるデータの量を減らす
Answer: B
Explanation:
Controlling traffic flows between networks is critical in a cybersecurity context toreduce the blast radius of attacks. By segmenting networks and implementing controls such as firewalls, organizations can limit the lateral movement of attackers, containing breaches and minimizing their impact.
From theCCSK v5.0 Study Guide, Domain 9 (Network Security), Section 9.2:
"Controlling traffic flows between networks is a fundamental cybersecurity practice to reduce the blast radius of attacks. Network segmentation and micro-segmentation limit an attacker's ability to move laterally within the environment, containing breaches and protecting critical assets." Option B (To reduce the blast radius of attacks) is the correct answer.
Option A (To increase the speed of data transmission) is incorrect because traffic control focuses on security, not speed.
Option C (To simplify network architecture) is incorrect because segmentation may increase complexity.
Option D (To reduce the amount of data stored) is incorrect because traffic control does not directly affect data storage.
Reference:
CCSK v5.0 Study Guide, Domain 9, Section 9.2: Network Segmentation and Traffic Control.

QUESTION NO: 29
サイバーセキュリティ
プロジェクトにおいて、導入前テストの早期統合が重要なのはなぜですか?
A. 完全な展開前に問題を特定し、時間とリソースを節約します。
B. 全体的なテスト時間とコストが増加します。
C. 最終検証テストをスキップできます。
D. 継続的インテグレーションの必要性がなくなります。
Answer: A
Explanation:
Integrating testing early helps identify security vulnerabilities and configuration issues before they reach production, reducing remediation costs and time. Reference: [Security Guidance

v5, Domain 10 - Application Security]

QUESTION NO: 30
CCM: ある企業が、一部の CSP の IaaS サービスを使用したいと考えています。CCM を使用するための次のオプションのうち、クラウドの顧客である会社に適していないものはどれですか?
A. CSP に代わって CCM を CSA Security, Trust & Assurance Registry (STAR) に提出します。STAR は、CSP によって提供されるセキュリティ管理を文書化した、無料で公開されているレジストリです。
B. CCM を使用して、CSP に実装してほしい要件とコントロールの詳細なリストを作成します。
C. CCM を使用して、CSP に関連するリスクを評価する
D. 上記のいずれでもない
Answer: D

QUESTION NO: 31
クラウドベースのリソースへのアクセス レベルを決定するために使用される、トランザクション内のエンティティのクレームと属性で構成される一連の定義ルールは何と呼ばれますか?
A. 資格マトリックス
B.サポートテーブル
C. エントリーログ
D. 検証プロセス
E. アクセスログ
Answer: D

QUESTION NO: 32
Dynamic Application Security Testing (DAST) は、制限されているか、プロバイダーからの事前テストの許可が必要な場合があります。
A. いいえ
B. 真
Answer: B

QUESTION NO: 33
リソース プールに必要な抽象化を提供する概念はどれですか?
A. 仮想化
B. アプリストラクチャー
C. ハイパーバイザー
D. メタストラクチャー
E. オーケストレーション
Answer: A

QUESTION NO: 34

クラウドに依存しないコンテナ戦略の使用に関連する主な運用上の課題は何ですか?
A. 単一のクラウド サービスへの展開を制限する
B. アイデンティティとアクセス管理プロトコルの確立
C. クラウドストレージの使用量の削減
D. 管理プレーンの互換性と一貫した制御
Answer: D
Explanation:
One of the primary operational challenges associated with using cloud-agnostic container strategies is ensuring management plane compatibility and consistent controls across multiple cloud environments. Cloud-agnostic strategies aim to make containers portable between different cloud providers. However, each cloud provider has its own management tools, APIs, and security controls, which can lead to complexities in maintaining consistent policies, monitoring, and management practices across different cloud environments. Limiting deployment to a single cloud service is contrary to the goal of a cloud-agnostic strategy, which seeks to avoid reliance on a single cloud provider. Establishing identity and access management protocols is important but not unique to cloud-agnostic strategies; IAM challenges exist regardless of cloud approach. Reducing the amount of cloud storage used is a general optimization concern, not specifically related to cloud-agnostic containers.