

ActualCollection

WELCOME TO ACTUALCOLLECTION

ActualCollection dumps, higher pass rate



ActualCollection is a website offering the latest and valid actual exam dump to make you go through the actual test with a high score.



Quality and Value

ActualCollection Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.



Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.



Easy to Pass

If you prepare for the exams using our ActualCollection testing engine, it is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.



Try Before Buy

ActualCollection offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

<http://www.actualcollection.com>

Actual dumps collection, higher pass rate

Exam : **CCSP-KR**

Title : **Certified Cloud Security
Professional (CCSP Korean
Version)**

Vendor : **ISC**

Version : **DEMO**

QUESTION NO: 1

SaaS 환경 내에서 다음 작업 중 클라우드 고객이 담당하지 않는 작업은 무엇입니까?

- A. 인증 메커니즘
- B. 브랜딩
- C. 훈련
- D. 사용자 액세스

Answer: A

Explanation:

The authentication mechanisms and implementations are the responsibility of the cloud provider because they are core components of the application platform and service. Within a SaaS implementation, the cloud customer will provision user access, deploy branding to the application interface (typically), and provide or procure training for its users.

QUESTION NO: 2

사용자 계정/액세스의 검토 및 유지 관리에는 누가 참여해야 합니까?

- A. 사용자의 관리자
- B. 보안 관리자
- C. 회계 부서
- D. 사고 대응팀

Answer: A

QUESTION NO: 3

다음 중 일반적으로 사용되는 위험 수용 범주가 아닌 것은 무엇입니까?

- A. 보통
- B. 심각
- C. 최소
- D. 승인됨

Answer: D

Explanation:

Accepted is not a risk acceptance category. The risk acceptance categories are minimal, low, moderate, high, and critical.

QUESTION NO: 4

미 국무부의 기술 수출 통제란 무엇입니까?

- A. DRM
- B. ITAR
- C. 귀
- D. EAL

Answer: B

Explanation:

ITAR is a Department of State program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Digital rights management tools are used for protecting electronic processing of intellectual property.

QUESTION NO: 5

클라우드 구성에서 공유 모니터링 및 테스트 책임을 해결하기 위해 공급자는 다음을 제외한 모든 항목을 클라우드 고객에게 제공할 수 있습니다.

- A. 감사 로그 및 성능 데이터에 대한 액세스
- B. DLP 솔루션 결과
- C. 보안 제어 관리
- D. SIM, SEIM. 및 SEM 로그

Answer: C

Explanation:

While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer. Security controls are the sole province of the provider.

QUESTION NO: 6

다음 중 시스템이나 애플리케이션이 준수해야 하는 규정을 뒷받침하는 주요 동인은 무엇입니까?

- A. 데이터 소스
- B. 지역
- C. 계약
- D. SLA

Answer: B

Explanation:

The locality--or physical location and jurisdiction where the system or data resides--is the dominant driver of regulations. This may be based on the type of data contained within the application or the way in which the data is used. The contract and SLA both articulate requirements for regulatory compliance and the responsibilities for the cloud provider and cloud customer, but neither artifact defines the actual requirements. Instead, the contract and SLA merely form the official documentation between the cloud provider and cloud customer. The source of the data may place contractual requirements or best practice guidelines on its usage, but ultimately jurisdiction has legal force and greater authority.

QUESTION NO: 7

파일 시스템 수준에서 암호화를 사용하는 것 외에 개체 스토리지 시스템에 저장된 데이터를 보호하는 데 가장 널리 사용되는 기술은 무엇입니까?

- A. TLS
- B. HTTPS
- C. VPN
- D. IRM

Answer: D

Explanation:

Information rights management (IRM) technologies allow security controls and policies to be enforced on a data object regardless of where it resides. They also allow for extended controls such as expirations and copying restrictions, which are not available through traditional control mechanisms. Hypertext Transfer Protocol Secure (HTTPS), virtual private

network (VPN), and Transport Layer Security (TLS) are all technologies and protocols that are widely used with cloud implementations for secure access to systems and services and likely will be used in conjunction with other object data protection strategies.

QUESTION NO: 8

클라우드 시스템은 조직의 BCDR 솔루션에 점점 더 많이 사용되고 있습니다. 클라우드 컴퓨팅의 어떤 측면이 BCDR 사용을 가장 매력적으로 만드는가?

- A. 주문형 셀프 서비스
- B. 측정된 서비스
- C. 이식성
- D. 광범위한 네트워크 액세스

Answer: B

Explanation:

Business continuity and disaster recovery (BCDR) solutions largely sit idle until they are actually needed.

This traditionally has led to increased costs for an organization because physical hardware must be purchased and operational but is not used. By using a cloud system, an organization will only pay for systems when they are being used and only for the duration of use, thus eliminating the need for extra hardware and costs. Portability is the ability to easily move services among different cloud providers.

Broad network access allows access to users and staff from anywhere and from different clients, and although this would be important for a BCDR situation, it is not the best answer in this case.

On-demand self-service allows users to provision services automatically and when needed, and although this too would be important for BCDR situations, it is not the best answer because it does not address costs or the biggest benefits to an organization.

QUESTION NO: 9

다음 스토리지 유형 중 기존 파일 시스템 및 트리 구조와 가장 밀접하게 연관되어 있는 것은 무엇입니까?

- A. 볼륨
- B. 구조화되지 않음
- C. 개체
- D. 구조적

Answer: A

Explanation:

Volume storage works as a virtual hard drive that is attached to a virtual machine. The operating system sees the volume the same as how a traditional drive on a physical server would be seen.

QUESTION NO: 10

다음 중 애플리케이션이나 시스템에 대한 요구 사항 수집에 대한 입력으로 포함되지 않는 것은 무엇입니까?

- A. 사용자
- B. 관리

- C. 조정기
- D. 감사자

Answer: D

QUESTION NO: 11

감사 범위 설명은 감사의 한계와 결과를 정의합니다. 다음 중 감사 범위 기술서의 일부로 포함되지 않는 것은 무엇입니까?

- A. 보고서
- B. 인증
- C. 청구
- D. 제외

Answer: C

Explanation:

Billing for an audit, or other cost-related items, would not be part of an audit scope statement and would instead be handled prior to the actual audit as part of the contract between the organization and auditors.

Reports, exclusions to the scope of the audit, and required certifications on behalf of the systems or auditors are all crucial elements of an audit scope statement.

QUESTION NO: 12

다음 보안 측면 중 전적으로 클라우드 제공업체의 책임은 무엇입니까?

- A. 규정 준수
- B. 물리적 보안
- C. 운영 체제 감사
- D. 개발자의 개인 보안

Answer: B

Explanation:

Regardless of the particular cloud service used, physical security of hardware and facilities is always the sole responsibility of the cloud provider. The cloud provider may release information about their physical security policies and procedures to ensure any particular requirements of potential customers will meet their regulatory obligations. Personal security of developers and regulatory compliance are always the responsibility of the cloud customer. Responsibility for operating systems, and the auditing of them, will differ based on the cloud service category used.

QUESTION NO: 13

다양한 인증과 표준은 데이터 센터 설계 및 운영에 대해 서로 다른 접근 방식을 취합니다. 많은 기존 접근 방식이 계층형 방법론을 사용하지만 다음 중 데이터 센터 설계에 거시적 수준 접근 방식을 활용하는 것은 무엇입니까?

- A. IDCA
- B. BICSI
- C. 가동 시간 연구소
- D. NFPA

Answer: A

Explanation:

The Infinity Paradigm of the International Data Center Authority (IDCA) takes a macro-level approach to data center design. The IDCA does not use a specific, focused approach on specific components to achieve tier status. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities.

The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers.

QUESTION NO: 14

TLS가 사용하는 두 가지 프로토콜은 무엇입니까?

- A. 핸드셰이크 및 녹음
- B. 이동 및 개시
- C. 핸드셰이크 및 전송
- D. 녹음 및 전송

Answer: A

Explanation:

TLS uses the handshake protocol to establish and negotiate the TLS connection, and it uses the record protocol for the secure transmission of data.

QUESTION NO: 15

SLA에는 클라우드 공급자와 클라우드 고객 간의 계약 성과 및 만족도에 대한 공식 요구 사항이 포함되어 있습니다.

다음 중 SLA의 일부로 측정 가능한 지표와 요구 사항이 포함된 구성 요소가 아닌 것은 무엇입니까?

- A. 네트워크
- B. 사용자
- C. 메모리
- D. CPU

Answer: B

Explanation:

Dealing with users or user access would not be an appropriate item for inclusion in an SLA specifically.

However, user access and user experience would be covered indirectly through other metrics.

Memory, CPU, and network resources are all typically included within an SLA for availability and response times when dealing with any incidents.

QUESTION NO: 16

조직에는 업계 전체에서 BCDR 상황을 활성화하는 데 공통적인 여러 가지 이유가 있을 수 있습니다. 다음 중 BCDR 계획을 활성화하는 일반적인 이유가 아닌 것은 무엇입니까?

- A. 자연재해
- B. 유틸리티 중단

- C. 직원 손실
- D. 테러 공격

Answer: C

QUESTION NO: 17

다음 중 어떤 클라우드 모델을 사용하든 관계없이 클라우드 고객의 단독 책임은 무엇입니까?

- A. 인프라
- B. 플랫폼
- C. 애플리케이션
- D. 데이터

Answer: D

Explanation:

Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

QUESTION NO: 18

일반적으로 클라우드 BC/DR 활동에 사용할 수 있는 다양한 모델에는 다음을 제외한 모든 모델이 포함됩니다.

- A. 프라이빗 아키텍처, 클라우드 백업
- B. 클라우드 제공자, 다른 클라우드 제공자로부터 백업
- C. 클라우드 공급자, 동일한 공급자의 백업
- D. 클라우드 공급자, 개인 공급자로부터 백업

Answer: D

Explanation:

This is not a normal configuration and would not likely provide genuine benefit.

QUESTION NO: 19

당신은 정부 연구 시설에서 일합니다. 귀하의 조직은 종종 다른 정부 연구 기관과 데이터를 공유합니다.

각 조직의 사용자가 해당 조직에서 발급한 사용자 ID/인증으로 로그인한 다음 다른 모든 조직의 연구 데이터에 액세스할 수 있는 조직 전반에 걸쳐 Single Sign-On 환경을 만들고 싶습니다.

각 조직의 데이터 저장소를 다른 모든 조직에 복제하는 대신(이 목표를 달성하는 한 가지 방법) 모든 사용자가 각 조직의 특정 스토리지 리소스에 액세스할 수 있기를 원합니다.

조직 간에 각 사용자의 사용자 ID와 인증 자격 증명을 전달하기 위해 어떤 프로토콜/언어/모티프를 활용할 가능성이 가장 높습니까?

응답:

- A. 표현 상태 전송(REST)
- B. SAML(보안 보장 마크업 언어)
- C. SOAP(단순 개체 액세스 프로토콜)
- D. 하이퍼텍스트 마크업 언어(HTML)

Answer: B

QUESTION NO: 20

클라우드 환경에 있는 클라우드 고객은 데이터가 저장되고 시스템이 배포되는 방식에 대한 많은 통찰력과 지식을 잃습니다.

ISO/IEC 클라우드 표준의 어떤 개념이 클라우드 공급자가 클라우드 고객에게 이러한 문제를 알려야 하는 필요성과 관련이 있습니까?

- A. 공개
- B. 투명성
- C. 개방성
- D. 문서

Answer: B

Explanation:

Transparency is the official process by which a cloud provider discloses insight and information into its configurations or operations to the appropriate audiences. Disclosure, openness, and documentation are all terms that sound similar to the correct answer, but none of them is the correct term in this case.

QUESTION NO: 21

귀하는 감사 범위 기술서를 작성하고 프로젝트 개요를 작성하는 임무를 맡았습니다. 다음 중 일반적으로 감사 범위 기술서에 포함되지 않는 것은 무엇입니까?

- A. 목적 설명
- B. 결과물
- C. 분류
- D. 비용

Answer: D

QUESTION NO: 22

다음 중 Cloud Security Alliance에서 게시한 Cloud Controls Matrix 내에서 정의된 보안 제어 도메인 중 하나가 아닌 것은 무엇입니까?

- A. 금융
- B. 인적 자원
- C. 모바일 보안
- D. ID 및 액세스 관리

Answer: A

QUESTION NO: 23

TLS의 일부로서 실제 보안 통신 및 데이터 전송을 처리하는 프로토콜은 무엇입니까?

- A. 협상
- B. 악수
- C. 전송
- D. 기록

Answer: D

Explanation:

The TLS record protocol is the actual secure communications method for transmitting data; it's responsible for encrypting and authenticating packets throughout their transmission between the parties, and in some cases it also performs compression. The TLS handshake

protocol is what negotiates and establishes the TLS connection between two parties and enables the secure communications channel to then handle data transmissions. Negotiation and transfer are not protocols under TLS.

QUESTION NO: 24

다음 중 IaaS(Infrastructure as a Service) 솔루션과 함께 사용되는 스토리지 유형은 무엇입니까?

- A. 볼륨 및 블록
- B. 구조화 및 객체
- C. 구조화되지 않고 일시적입니다.
- D. 볼륨 및 개체

Answer: D

QUESTION NO: 25

다음은 모두 공급업체 종속 가능성을 최소화하기 위해 클라우드 데이터의 이동성을 향상시키는 기술입니다.

- A. 이동에 물리적 제한이 없는지 확인하세요.
- B. 클라우드 운영 전반에 걸쳐 DRM 및 DLP 솔루션을 광범위하게 사용합니다.
- C. 이식성을 지원하기 위해 유리한 계약 조건을 보장합니다.
- D. 독점 데이터 형식을 피하세요

Answer: B

Explanation:

DRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

QUESTION NO: 26

정기적으로 BCDR 테스트를 수행하는 것이 프로세스와 문서의 관련성과 효율성을 보장하는 모범 사례이지만, 다음 중 정기적인 간격이 아닌 BCDR 검토를 수행하는 이유는 무엇입니까?

- A. 직원 변경
- B. 애플리케이션 변경
- C. 규정 변경
- D. 관리 변경

Answer: B

QUESTION NO: 27

다음 중 클라우드 고객이 클라우드 환경 내에서 사용하는 리소스 및 제품에 대해서만, 그리고 이를 소비하는 기간 동안만 비용을 지불한다는 개념은 무엇입니까?

- A. 소모성 서비스
- B. 측정된 서비스
- C. 청구 가능한 서비스
- D. 측정 서비스

Answer: B

Explanation:

Measured service is where cloud services are delivered and billed in a metered way, where

the cloud customer only pays for those that they actually use, and for the duration of time that they use them.

QUESTION NO: 28

클라우드 데이터 센터 캠퍼스의 물리적 레이아웃에는 _____을(를) 제외하고 다음 모든 항목의 중복이 포함되어야 합니다.

- A. 물리적 경계 보안 제어(울타리, 조명, 벽 등)
- B. 관리/지원 직원 건물
- C. 전기 유틸리티 라인
- D. 통신 연결 라인

Answer: B

QUESTION NO: 29

온프레미스 환경에서 호스팅된 클라우드 서비스로 마이그레이션하는 옵션을 고려할 때 조직은 _____에 대한 협업 목적으로 외부 엔터티가 클라우드 데이터에 액세스하도록 허용하는 데 따른 위험을 고려해야 합니다.

- A. 레거시 환경에서 데이터를 보호하지 않음
- B. 데이터를 공개적으로 공개합니다.
- C. 협업을 강화하기 위해 기존 작업공간에 외부 인력을 초대합니다.
- D. 협업 목적으로 레거시 환경 외부로 데이터 전송

Answer: D

QUESTION NO: 30

클라우드 교차 측면 중 작업, 작업, 역할 할당 및 이러한 작업이 성공적이고 적절하게 수행되도록 보장하는 것과 관련된 측면은 무엇입니까?

- A. 서비스 수준 계약
- B. 거버넌스
- C. 규제 요구 사항
- D. 감사 가능성

Answer: B

Explanation:

Governance at its core is the idea of assigning jobs, takes, roles, and responsibilities and ensuring they are satisfactory performed.

QUESTION NO: 31

비즈니스 연속성과 재해 복구는 어떤 보안 개념에 속합니까?

- A. 기밀성
- B. 가용성
- C. 내결함성
- D. 무결성

Answer: B

Explanation:

Disaster recovery and business continuity are vital concerns with availability. If data is destroyed or compromised, having regular backup systems in place as well as being able to

perform disaster recovery in the event of a major or widespread problem allows operations to continue with an acceptable loss of time and data to management. This also ensures that sensitive data is protected and persisted in the event of the loss or corruption of data systems or physical storage systems.

QUESTION NO: 32

DAST(동적 애플리케이션 보안 테스트)는 일반적으로 _____ 형태의 테스트로 간주됩니다.

응답:

화이트박스

- A. 바깥 마른 들판
- B. 블랙박스
- C. 회색 상자
- D. 바깥 마른 들판

Answer: B

QUESTION NO: 33

TLS는 _____ 통신을 위해 _____ 을(를) 제공합니다.

- A. 개인 정보 보호, 보안
- B. 보안, 최적화
- C. 개인 정보 보호, 무결성
- D. 향상, 개인 정보 보호

Answer: C

QUESTION NO: 34

SOC Type 2 보고서는 5가지 원칙으로 구분됩니다.

다른 네 가지 원칙 중 하나를 감사할 때 다섯 가지 원칙 중 어떤 원칙도 포함되어야 합니까?

- A. 기밀성
- B. 개인정보 보호
- C. 보안
- D. 가용성

Answer: C

Explanation:

Under the SOC guidelines, when any of the four principles other than security are being audited, which includes availability, confidentiality, processing integrity, and privacy, the security principle must also be included with the audit.

QUESTION NO: 35

Cloud Security Alliance CCM(클라우드 제어 매트릭스)이란 무엇입니까?

- A. 클라우드 서비스 제공업체를 위한 소프트웨어 개발 수명 주기 요구 사항 집합
- B. 보안 도메인 계층 구조로 정렬된 클라우드 서비스 보안 제어 목록입니다.
- C. 별도의 보안 도메인으로 정렬된 클라우드 서비스 보안 제어 목록
- D. 클라우드 서비스 제공업체에 대한 규제 요구 사항 집합

Answer: C

Explanation:

The CSA CCM is an inventory of cloud service security controls that are arranged into separate security domains, not a hierarchy.