examundo

CISSP 한국어 연습 문제

정답 포함 50문제. 가이드와 번역은 소프트웨어가 만들고 검토했어요. 아직 사람이 확인하지는 않았어요.

2026년 11월 25일 업데이트 · examundo.tech/ko/cissp/

보안 아키텍처 및 엔지니어링

1. 발신자가 메시지를 보냈다는 사실을 부인하지 못하게 하는 암호 개념은 무엇입니까?

Which cryptographic concept ensures that a sender cannot deny having sent a message?

A. 기밀성
B. 무결성
C. 부인 방지
D. 인증

---

2. 보안 아키텍트가 정부 기밀 데이터를 보호하는 시스템을 설계하고 있습니다. 높은 기밀 등급에서 낮은 등급으로 정보가 흘러가는 것을 막으려면 어떤 보안 모델을 적용해야 합니까?

A security architect is designing a system to protect classified government data. Which security model should be implemented to prevent information from flowing from higher classification levels to lower classification levels?

A. Bell-LaPadula(벨라파둘라) 모델
B. Clark-Wilson(클라크윌슨) 모델
C. Brewer-Nash(브루어내시) 모델
D. Biba(비바) 무결성 모델

---

3. 전자상거래 애플리케이션이 고객 브라우저와 대칭 암호화 키를 안전하게 교환해야 합니다. 어떤 프로토콜을 사용해야 합니까?

An e-commerce application needs to securely exchange symmetric encryption keys with customers' browsers. Which protocol should be used?

A. 디피-헬만 키 교환을 사용하는 TLS
B. 사전 공유 키를 사용하는 전송 모드 IPsec
C. 티켓 발급 티켓(TGT)을 사용하는 Kerberos
D. 인증서 기반 암호화를 사용하는 S/MIME

---

4. 보안 시설에서 서버실 출입에 2인 무결성(two-person integrity)을 요구합니다. 이 요구사항을 구현하는 물리적 접근 통제는 무엇입니까?

A secure facility requires two-person integrity for access to the server room. What type of physical access control implements this requirement?

A. 코드를 분기마다 변경하는 암호식 도어락
B. 모든 출입을 녹화하는 영상 감시가 있는 카드 리더
C. 다중 요소 인증용 PIN 패드가 있는 생체 인식 리더
D. 권한 있는 두 사람이 각각 인증해야 하는 맨트랩

---

5. 심층 방어(defense in depth)를 가장 잘 설명하는 보안 원칙은 다음 중 무엇입니까?

Defense in depth is BEST described as which of the following security principles?

A. 여러 겹의 보안 통제를 적용해 자산을 보호한다
B. 오류가 생기면 안전한 상태로 실패하도록 시스템을 설계한다
C. 사용자에게 업무에 필요한 최소한의 접근 권한만 부여한다
D. 불필요한 서비스와 기능을 제거해 시스템을 강화한다

---

6. 맨트랩(mantrap)은 어떤 유형의 물리적 보안 통제로 분류됩니까?

A mantrap is classified as which type of physical security control?

A. 예방 통제
B. 보완 통제
C. 탐지 통제
D. 교정 통제

---

7. 금융 시스템은 권한 없는 사용자가 거래 기록을 수정하지 못하게 하면서 감사를 위한 읽기 접근은 허용해야 합니다. 이 요구사항을 가장 잘 뒷받침하는 보안 모델은 무엇입니까?

A financial system must prevent unauthorized users from modifying transaction records while allowing read access for auditing. Which security model BEST supports this requirement?

A. Bell-LaPadula(벨라파둘라) 기밀성 모델
B. Brewer-Nash(Chinese Wall) 모델
C. Biba(비바) 무결성 모델
D. Graham-Denning(그레이엄데닝) 접근 통제 모델

---

8. 한 조직이 클라우드 환경의 저장 데이터를 보호하는 새 암호 시스템을 도입합니다. 이 시스템은 규정 준수를 위한 키 에스크로(key escrow)를 지원하면서 클라우드 제공업체로부터 운영상 독립성도 유지해야 합니다. 두 요구사항을 가장 잘 충족하는 방법은 무엇입니까?

An organization is implementing a new cryptographic system to protect data at rest in a cloud environment. The system must support regulatory compliance requirements for key escrow while maintaining operational independence from the cloud provider. Which approach BEST satisfies both requirements?

A. 온프레미스 HSM에서 키를 관리하는 클라이언트 측 암호화를 구현하고, 에스크로 사본을 제3자 키 에스크로 서비스에 제공한다
B. 클라우드 제공업체의 키 관리 서비스에 고객 관리 키를 저장하는 엔벨로프 암호화를 도입한다
C. 애플리케이션 설정에 키를 저장하는 데이터베이스 계층의 투명한 데이터 암호화(TDE)를 구현한다
D. 자동 키 교체와 다른 클라우드 리전으로의 백업이 있는 클라우드 제공업체의 기본 암호화 서비스를 사용한다

---

9. 보안 아키텍트가 여러 기밀 등급의 문서를 다루는 군 첩보 시스템(military intelligence system)에 적용할 정형 보안 모델(formal security model)을 선택해야 합니다. 가장 중요한 요구사항은 정보가 낮은 기밀 등급으로 흘러가는 것을 막는 것입니다. 어떤 모델이 가장 적합합니까?

A security architect must select a formal security model for a military intelligence system handling documents at multiple classification levels. The PRIMARY requirement is preventing information from flowing to lower classification levels. Which model is MOST appropriate?

A. Biba(비바) 무결성 모델
B. Clark-Wilson(클라크윌슨) 무결성 모델
C. Bell-LaPadula(벨라파둘라) 모델
D. Brewer-Nash(Chinese Wall) 모델

---

10. 데이터 센터에서 서버실 위의 수도관이 터졌습니다. 중요한 장비의 침수 피해를 가장 잘 막았을 환경 통제는 무엇입니까?

A data center experiences a water pipe burst above the server room. Which environmental control would have BEST prevented water damage to critical equipment?

A. 습기 유입을 막는 양압 시스템
B. 자동 차단 밸브가 있는 누수 감지 센서
C. 장비를 바닥보다 높이 올리는 이중 바닥
D. 습도 모니터링과 경보가 있는 HVAC 시스템

보안 운영

11. 운영 서버 구성의 무단 변경을 가장 잘 탐지하는 구성 관리 방법은 무엇입니까?

Which configuration management practice BEST detects unauthorized changes to production server configurations?

A. 실제 구성을 승인된 기준선과 정기적으로 비교한다
B. 권한 있는 관리자가 한 변경을 자동으로 승인한다
C. 서버 설정은 확인하지 않고 하드웨어 구매 기록만 검토한다
D. 스캔할 때마다 승인된 기준선을 현재 구성으로 교체한다

---

12. 사고 대응 팀에서 사고를 처음 식별하고 봉쇄하는 책임이 있는 역할은 무엇입니까?

Which role in an incident response team is responsible for initially identifying and containing the incident?

A. 사고 조정관
B. 포렌식 분석가
C. 최초 대응자
D. 커뮤니케이션 담당자

---

13. 비핵심 시스템에 경미한 장애가 생겼고 데이터 손실이 없는 사고는 일반적으로 어떤 심각도로 분류됩니까?

An incident that causes minor disruption to non-critical systems with no data loss would typically be classified as what severity level?

A. 치명적
B. 높음
C. 낮음
D. 비상

---

14. 사고 후 검토에서 공격자가 탐지되기 전까지 87일 동안 지속적으로 시스템에 머물렀다는 사실이 확인되었습니다. 앞으로 체류 시간(dwell time)을 줄이는 데 가장 효과적인 보안 운영 개선책은 무엇입니까?

During a post-incident review, the team identifies that the attacker maintained persistence for 87 days before detection. Which security operations improvement would MOST effectively reduce future dwell time?

A. 모든 직원에게 분기마다 보안 인식 교육을 의무화한다
B. 네트워크 분리 경계에 방화벽을 추가로 배치한다
C. 취약점 스캔 주기를 월 1회에서 주 1회로 늘린다
D. 행위 분석과 위협 헌팅을 포함한 지속적 보안 모니터링을 구현한다

---

15. 물리 보안의 심층 방어는 일반적으로 여러 계층으로 이루어집니다. 가장 바깥 계층에서 가장 안쪽 계층까지의 올바른 순서는 다음 중 무엇입니까?

Defense in depth for physical security typically includes multiple layers. Which of the following represents the CORRECT order from outermost to innermost layer?

A. 외곽 울타리, 건물 출입 통제, 방 출입 통제, 장비 잠금장치
B. 장비 잠금장치, 방 출입 통제, 건물 출입 통제, 외곽 울타리
C. 방 출입 통제, 장비 잠금장치, 외곽 울타리, 건물 출입 통제
D. 건물 출입 통제, 외곽 울타리, 장비 잠금장치, 방 출입 통제

---

16. 원본 증거의 사본이나 복제물로 이루어진 증거는 어떤 유형입니까?

Which type of evidence consists of copies or reproductions of original evidence?

A. 이차 증거
B. 최량 증거
C. 전문(傳聞) 증거
D. 보강 증거

---

17. 한 조직이 재해 복구 목표를 정하고 있습니다. 사업 부서는 재해 발생 후 4시간 이내에 핵심 시스템을 복구해야 한다고 요구합니다. 이 요구사항이 정의하는 복구 지표는 무엇입니까?

An organization is defining its disaster recovery objectives. The business requires that critical systems must be restored within 4 hours of a disaster. This requirement defines which recovery metric?

A. 평균 수리 시간(MTTR)
B. 최대 허용 중단 시간(MTD)
C. 복구 시간 목표(RTO)
D. 복구 시점 목표(RPO)

---

18. 한 조직의 재해 복구 계획은 고객 데이터베이스에 대해 복구 시간 목표(RTO) 4시간, 복구 시점 목표(RPO) 1시간을 요구합니다. 이 요구사항을 가장 잘 충족하는 백업 전략은 무엇입니까?

An organization's disaster recovery plan requires a recovery time objective (RTO) of 4 hours and a recovery point objective (RPO) of 1 hour for its customer database. Which backup strategy BEST meets these requirements?

A. 4시간마다 차등 백업을 하고 온프레미스에 보관한다
B. 6시간마다 증분 백업을 하고 테이프를 외부에 보관한다
C. 매주 전체 백업을 하고 매일 증분 백업을 한다
D. 매일 밤 전체 백업을 하고 웜 사이트로 데이터베이스를 연속 복제한다

---

19. 최초 대응자가 전원이 켜져 있고 거래를 처리 중인 침해된 운영 서버에 도착했습니다. RFC 3227 지침에 따르면 라이브 증거 수집 시 가장 먼저 수집해야 하는 데이터 소스는 무엇입니까?

A first responder arrives at a compromised production server that is still powered on and actively processing transactions. Per RFC 3227 guidelines, which data source should be collected FIRST during live evidence acquisition?

A. CPU 레지스터와 캐시 메모리
B. 시스템 RAM(주 메모리) 내용
C. ARP 캐시와 라우팅 테이블 항목
D. 임시 파일 시스템과 스왑 공간 데이터

---

20. 한 IT 부서가 공식 변경 관리 절차를 따르고 있습니다. 운영 시스템에 변경을 적용하기 전에 거쳐야 하는 승인 단계는 무엇입니까?

An IT department follows a formal change management process. Which authorization step should occur BEFORE implementing a change to production systems?

A. 비운영 환경에서 변경 테스트
B. 변경 자문 위원회(CAB) 승인
C. 구성 관리 데이터베이스에 변경 문서화
D. 영향을 받는 모든 이해관계자에게 공지

통신 및 네트워크 보안

21. 한 조직이 네트워크 접근 통제에 802.1X를 구현합니다. 서플리컨트(supplicant)와 인증 서버 사이에서 중개자 역할을 하는 구성 요소는 무엇입니까?

An organization implements 802.1X for network access control. Which component acts as the intermediary between the supplicant and the authentication server?

A. 인증 기관
B. 네트워크 컨트롤러
C. 인증자
D. RADIUS 프록시

---

22. 한 조직이 무선 보안에 WPA3-Enterprise를 도입합니다. WPA3-Enterprise는 어떤 인증 프레임워크를 사용합니까?

An organization implements WPA3-Enterprise for wireless security. What authentication framework does WPA3-Enterprise use?

A. EAP를 사용하는 802.1X
B. MAC 주소 필터링
C. 사전 공유 키(PSK)
D. LEAP

---

23. 한 조직이 인터넷 연결이 불안정한 여러 해외 지역에서 접속하는 현장 인력에게 안전한 원격 접속을 제공해야 합니다. 이 솔루션은 **TCP**와 **UDP** 트래픽을 모두 지원하고 대부분의 방화벽을 통과해야 합니다. 가장 적합한 **VPN** 프로토콜은 무엇입니까?

An organization needs to provide secure remote access for field personnel who connect from various international locations with unreliable internet connectivity. The solution must support both TCP and UDP traffic and work through most firewalls. Which VPN protocol is MOST appropriate?

A. PPTP
B. SSL/TLS VPN
C. L2TP/IPSec
D. 터널 모드 IPSec

---

24. 한 회사의 웹 애플리케이션에 여러 출처에서 트래픽이 급증해 서버가 응답하지 못하고 있습니다. 가장 가능성이 높은 공격은 무엇입니까?

A company's web application experiences a surge in traffic from multiple sources, overwhelming the server's ability to respond. Which attack is MOST likely occurring?

A. 중간자 공격(MitM)
B. 크로스 사이트 요청 위조(CSRF)
C. 세션 하이재킹
D. 분산 서비스 거부(DDoS)

---

25. 통신하는 호스트 사이의 종단 간 신뢰할 수 있는 데이터 전달, 흐름 제어, 오류 복구를 담당하는 **OSI** 모델 계층은 무엇입니까?

Which OSI model layer is responsible for end-to-end reliable data delivery, flow control, and error recovery between communicating hosts?

A. 2계층: 데이터 링크
B. 4계층: 전송
C. 3계층: 네트워크
D. 5계층: 세션

---

26. 한 조직의 웹 서버가 **SYN** 플러드 공격을 받고 있습니다. 가장 효과적인 방어 기법은 무엇입니까?

An organization is experiencing SYN flood attacks against its web server. Which defensive technique would be MOST effective?

A. TCP 타임스탬프 비활성화
B. MAC 주소 필터링 적용
C. ICMP 패킷 속도 제한
D. SYN 쿠키

---

27. 웹 애플리케이션에 **TLS**를 적용할 때, 신규 배포에서 최소한으로 허용되는 표준으로 보아야 하는 버전은 무엇입니까?

When implementing TLS for a web application, which version should be considered the MINIMUM acceptable standard for new deployments?

A. TLS 1.0
B. SSL 3.0
C. TLS 1.2
D. TLS 1.1

---

28. 한 금융 기관이 클라이언트와 서버 사이의 상호 인증을 요구합니다. 이를 가능하게 하는 **TLS** 기능은 무엇입니까?

A financial institution requires mutual authentication between clients and servers. Which TLS feature provides this capability?

A. 세션 재개
B. 클라이언트 인증서 인증
C. 완전 순방향 비밀성(PFS)
D. 서버 이름 표시(SNI)

---

29. 침입 탐지 시스템**(IDS)**이 정상 트래픽 패턴에 대해 경보를 많이 발생시키고 있습니다. 어떤 유형의 오류가 발생하고 있습니까?

An intrusion detection system (IDS) is generating numerous alerts for normal traffic patterns. What type of error is occurring?

A. 오탐(false positive)
B. 미탐(false negative)
C. 정상 판정(true negative)
D. 정탐(true positive)

---

30. 한 다국적 기업이 인터넷 라우팅 장애를 겪고 있습니다. 조사 결과 해외 ISP가 BGP로 이 회사의 IP 주소 공간을 광고하고 있었습니다. 어떤 공격이 일어났을 가능성이 가장 높으며, 라우트 포이즈닝(route poisoning)과의 가장 큰 차이는 무엇입니까?

A multinational corporation experiences Internet routing disruptions. Investigation reveals that a foreign ISP is advertising the company's IP address space via BGP. Which attack is MOST likely occurring, and what is the PRIMARY difference from route poisoning?

A. BGP 하이재킹이며, 라우트 메트릭이 아니라 프리픽스 소유권을 노린다는 점이 다르다

B. 라우트 포이즈닝이며, 내부 거리 벡터 프로토콜이 아니라 외부 라우팅에 영향을 준다는 점이 다르다

C. 라우트 플래핑이며, 트래픽을 지속적으로 다른 곳으로 돌리는 것이 아니라 간헐적 장애를 일으킨다는 점이 다르다

D. AS 경로 프리펜딩이며, 자율 시스템 번호를 조작해 라우팅 결정에 영향을 준다는 점이 다르다

자산 보안

31. 한 금융 서비스 회사의 기준 보안 표준은 모든 고객 데이터에 AES-256 암호화를 요구합니다. 위험 평가 결과 일부 레거시 시스템이 AES-256을 지원하지 못합니다. 보안 아키텍트는 이 제약을 해결하기 위해 어떤 프로세스를 적용해야 합니까?

A financial services firm's baseline security standard requires AES-256 encryption for all customer data. A risk assessment reveals that certain legacy systems cannot support AES-256. What process should the security architect apply to address this constraint?

A. 테일러링(tailoring)

B. 보완 통제

C. 범위 설정(scoping)

D. 위험 수용

32. 미국 정부의 분류 정책에서 무단 공개 시 국가 안보에 '심각한 피해(serious damage)'를 줄 것으로 합리적으로 예상되는 정보에 붙이는 등급은 무엇입니까?

Under U.S. government classification policy, which label applies to information whose unauthorized disclosure could reasonably be expected to cause 'serious damage' to national security?

A. Secret(비밀)

B. 통제된 비기밀 정보(CUI)

C. Confidential(기밀)

D. Top Secret(극비)

33. 조직 내 데이터의 분류 등급을 결정하는 최종 책임은 누구에게 있습니까?

Who is ultimately responsible for determining the classification level of data within an organization?

A. 데이터 수탁자(custodian)

B. 데이터 소유자(owner)

C. 보안 관리자

D. 최고 정보 보안 책임자(CISO)

34. 한 조직이 일부 HIPAA 준수 문서를 HIPAA에 따라 최소 6년, 적용되는 주법에 따라 최소 10년 보관해야 합니다. 보안 관리자는 이 문서에 어떤 보관 기간을 권고해야 합니까?

An organization must retain certain HIPAA compliance documentation for a minimum of 6 years under HIPAA and a minimum of 10 years under an applicable state law. What retention period should the security manager recommend for that documentation?

A. 두 요구사항의 절충안인 8년

B. 가장 엄격한 요구사항을 충족하는 10년

C. 규정 위반 위험을 피하기 위한 무기한 보관

D. 연방 HIPAA 요구사항에 맞춘 6년

35. 한 다국적 기업이 EU 고객 데이터를 클라우드 데이터 센터에 저장합니다. 프랑스 고객들은 EU 밖의 기관이 법을 근거로 자기 데이터의 제출을 강제할 수 있다는 점을 걱정합니다. 이 우려를 가장 잘 다루는 원칙은 무엇입니까?

A multinational corporation stores EU customer data in cloud data centers. French customers are concerned about their data being legally compelled from non-EU entities. Which principle BEST addresses this concern?

A. 데이터 주권(data sovereignty)
B. 데이터 현지화(data localization)
C. 지리적 이중화
D. 데이터 레지던시(data residency)

---

36. 한 조직의 데이터 보존 정책은 고객 거래 기록을 7년간 보관하도록 요구합니다. 이 기간이 끝났을 때 폐기 절차의 첫 번째 단계는 무엇입니까?

An organization's data retention policy requires keeping customer transaction records for seven years. At the end of this period, what is the FIRST step in the disposal process?

A. 법적 보존 요건이 적용되지 않는지 확인한다
B. DoD 5220.22-M을 준수하는 도구로 데이터를 덮어쓴다
C. 데이터가 든 모든 저장 매체를 물리적으로 파괴한다
D. 외부 보관소의 모든 백업 사본을 삭제한다

---

37. 조직의 데이터 자산에 부여할 분류 등급을 결정하는 일차적 책임이 있는 역할은 무엇입니까?

Which role is PRIMARILY responsible for determining the classification level assigned to an organizational data asset?

A. 데이터 스튜어드(steward)
B. 데이터 소유자(owner)
C. 데이터 수탁자(custodian)
D. 데이터 처리자(processor)

---

38. 한 의료 기관이 암호화되지 않은 환자 건강 기록이 저장되었던 노트북을 폐기합니다. 데이터 복구 불가능성을 가장 높은 수준으로 보장하는 완전 삭제(sanitization) 방법은 무엇입니까?

A healthcare organization is decommissioning laptops that stored unencrypted patient health records. Which sanitization method provides the HIGHEST assurance of data irrecoverability?

A. 파쇄나 소각을 통한 물리적 파괴
B. 암호화 키를 지우는 암호학적 삭제(cryptographic erasure)
C. 무작위 데이터로 7회 덮어쓰기
D. Type I 또는 Type II 디가우저를 사용한 디가우싱(degaussing)

---

39. 한 조직이 직원 성과 평가, 급여 정보, 개인 식별 정보(PII)가 담긴 새 데이터베이스를 분류하고 있습니다. 무단 공개 시 경쟁상 불이익과 법적 책임이 생길 수 있습니다. 가장 적절한 분류 등급은 무엇입니까?

An organization is classifying a new database containing employee performance reviews, salary information, and personally identifiable information (PII). The unauthorized disclosure could result in competitive disadvantage and potential legal liability. What classification level is MOST appropriate?

A. 비밀(Secret)
B. 기밀(Confidential)
C. 사내용(Internal Use Only)
D. 공개(Public)

---

40. 한 의료 기관이 환자 건강 기록의 올바른 분류, 규정에 따른 보존, 권한 있는 인원만의 접근을 보장할 책임이 누구에게 있는지 정해야 합니다. 이 결정들에 대한 일차적 책임은 누구에게 있습니까?

A healthcare organization must determine accountability for ensuring patient health records are properly classified, retained according to regulatory requirements, and accessible only to authorized personnel. Who has PRIMARY responsibility for these decisions?

A. 데이터 처리자
B. 최고 정보 보안 책임자(CISO)
C. 데이터 소유자
D. 데이터 수탁자

보안 및 위험 관리

41. 보안 분석가가 한 직원이 업무상 정당한 이유 없이 기밀 HR 파일에 접근해 왔다는 것을 발견했습니다. 이 직원의 직무에는 HR 데이터 접근이 필요하지 않습니다. 가장 위반되었을 가능성이 높은 보안 원칙은 무엇입니까?

A security analyst discovers an employee has been accessing confidential HR files without business justification. The employee's role does not require access to HR data. Which security principle was MOST likely violated?

A. 알 필요성
B. 심층 방어
C. 직무 분리
D. 최소 권한

---

42. 한 조직의 CISO가 보안 프로그램을 비즈니스 목표에 맞추려고 합니다. 이 목적에 가장 적합한 프레임워크는 무엇입니까?

An organization's CISO wants to align the security program with business objectives. Which framework is BEST suited for this purpose?

A. ISO 27002
B. COBIT
C. CIS Controls
D. NIST SP 800-53

---

43. 한 의료 기관이 환자 기록을 암호화하는 랜섬웨어 공격을 당했습니다. CISO는 이 사건을 이사회에 보고합니다. CISO가 보여주는 개념은 무엇입니까?

A healthcare organization suffers a ransomware attack that encrypts patient records. The CISO reports the incident to the board. Which concept is the CISO demonstrating?

A. 듀 딜리전스(due diligence)
B. 직무 분리
C. 신중한 사람 원칙(prudent man rule)
D. 듀 케어(due care)

---

44. CISO가 경영진에게 사업 연속성 계획(BCP)과 재해 복구 계획(DRP)의 관계를 설명하고 있습니다. 가장 정확한 설명은 무엇입니까?

A CISO is explaining the relationship between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) to the executive board. Which statement is MOST accurate?

A. BCP는 IT 시스템과 데이터만 다루고, DRP는 모든 비즈니스 운영을 다룬다
B. BCP와 DRP는 같은 계획 과정을 가리키는 바꿔 쓸 수 있는 용어다
C. DRP가 더 넓은 전략 계획이며 BCP를 구성 요소로 포함한다
D. BCP가 더 넓은 전략 계획이며, DRP는 IT 복구에 초점을 둔 전술적 하위 부분이다

---

45. 재해 복구 훈련 중 백업 테이프를 읽을 수 없다는 사실이 확인되었습니다. BCP/DRP 수명 주기의 어느 단계를 소홀히 했을 가능성이 가장 높습니까?

During a disaster recovery exercise, the backup tapes are found to be unreadable. Which phase of the BCP/DRP lifecycle was MOST likely neglected?

A. 위험 평가
B. 업무 영향 분석
C. 계획 개발
D. 테스트와 훈련

---

46. 위험 분석가가 파일 서버가 랜섬웨어에 침해될 연간 확률이 20%이고, 사고 1건당 예상 손실이 $50,000라고 판단했습니다. 연간 예상 손실액(ALE)은 얼마입니까?

A risk analyst determines that a file server has a 20% annual probability of being compromised by ransomware, with an estimated loss of $50,000 per incident. What is the Annualized Loss Expectancy (ALE)?

A. $10,000
B. $50,000
C. $40,000
D. $250,000

---

47. 한 조직의 보안 팀이 새 접근 통제 정책을 만들고 있습니다. 가장 엄격하고 구체적인 필수 조치를 제시해야 하는 문서 유형은 무엇입니까?

An organization's security team is developing a new access control policy. Which document type should be MOST restrictive and provide specific mandatory actions?

A. 절차(Procedure)
B. 표준(Standard)
C. 지침(Guideline)
D. 정책(Policy)

---

48. 한 회사가 새 고객 데이터 플랫폼에 개인정보 보호 중심 설계(Privacy by Design) 원칙을 적용하고 있습니다. 이 원칙을 가장 잘 보여주는 접근 방식은 무엇입니까?

A company is implementing Privacy by Design principles for a new customer data platform. Which approach BEST demonstrates this principle?

A. 운영 배포 전에 고객 데이터를 보호하는 암호화와 접근 통제를 추가한다
B. 데이터 최소화와 개인정보를 보호하는 기본 설정을 포함해, 처음 설계 단계부터 시스템 아키텍처에 개인정보 보호 통제를 내장한다
C. 개발자에게 개인정보 요구사항을 교육하고 개인정보 규정 준수를 위한 코드 리뷰를 한다
D. 시스템 개발이 끝난 뒤 개인정보 영향 평가를 실시해 위험을 찾아 해결한다

---

49. 한 회사가 데이터 유출과 관련된 재정적 위험을 이전하려고 합니다. 어떤 전략을 쓰고 있습니까?

A company wants to transfer financial risk associated with a data breach. Which strategy is being employed?

A. 위험 완화
B. 위험 이전
C. 위험 수용
D. 위험 회피

---

50. 금융 시스템에 대한 무단 접근 보안 사고가 발생했을 때, 법 집행 기관에 알릴지 결정하는 일차적 책임이 있는 역할은 무엇입니까?

During a security incident involving unauthorized access to financial systems, which role is PRIMARILY responsible for determining whether law enforcement should be notified?

A. 사고에 대한 최신 정보를 가장 많이 알고 있는 사고 대응 팀장
B. 모든 보안 문제에 책임이 있는 최고 정보 보안 책임자(CISO)
C. 이것이 규제적 영향이 있는 업무적, 법적 결정이므로 경영진 또는 법률 자문
D. 외부 기관과 관계를 유지하는 법 집행 기관 연락 담당자

정답

1. C 부인 방지(non-repudiation)는 어떤 행위를 한 당사자가 나중에 부인하지 못하게 하며, 보통 디지털 서명(digital signature)으로 구현합니다. 발신자의 개인 키로 서명하고 공개 키로 검증하면 출처를 증명할 수 있습니다. 인증은 신원을 확인할 뿐 부인할 수 없는 증거까지 만들지는 않습니다. 비밀번호를 여럿이 함께 쓰면 누가 한 일인지 증명할 수 없습니다. 기밀성은 노출을 막고, 무결성은 변조 여부를 확인할 뿐 누가 보냈는지 증명하지 않습니다.

2. A Bell-LaPadula는 단순 보안 속성(위로 읽기 금지)과 *-속성(아래로 쓰기 금지)으로 기밀성을 지키며, 높은 등급의 정보가 낮은 등급으로 새는 것을 막습니다. Biba는 기밀성이 아니라 무결성에 초점을 둡니다. Clark-Wilson도 무결성 모델이고, Brewer-Nash(Chinese Wall)는 상업 환경의 이해 충돌을 막는 모델입니다.

3. A TLS와 디피-헬만(Diffie-Hellman)을 쓰면 안전하지 않은 통신망에서도 두 당사자가 공유 비밀을 만들 수 있고, HTTPS가 이 방식을 씁니다. 임시 키 방식(DHE/ECDHE)은 완전 순방향 비밀성(perfect forward secrecy)을 제공합니다. IPsec은 주로 VPN용이며 사전 설정이 필요합니다. S/MIME은 이메일용이고, Kerberos는 KDC와 사전 신뢰가 필요한 기업 내부용입니다.

4. D 2인 무결성은 권한 있는 두 사람이 함께 있어야 출입할 수 있게 하여 한 사람의 단독 행동을 막습니다. 이런 맨트랩(mantrap)은 두 사람이 모두 인증해야 들어갈 수 있습니다. 생체 인식과 PIN은 한 사람의 다중 요소 인증일 뿐입니다. 영상 감시는 탐지 통제라 단독 출입을 막지 못하고, 도어락은 코드를 아는 사람이면 혼자서도 들어갈 수 있습니다.

5. A 심층 방어(계층 보안)는 독립적인 보안 통제를 여러 겹 배치해서 한 층이 뚫려도 다른 층이 계속 보호하게 하는 원칙입니다. 방화벽, IDS/IPS, 접근 통제, 암호화, 물리적 방벽이 함께 작동하는 것이 예입니다. 불필요한 기능 제거는 시스템 강화(hardening), 최소 권한 부여는 최소 권한 원칙, 안전한 실패는 fail-safe/fail-secure 설계입니다.

6. A 맨트랩(access control vestibule, 출입 통제 전실)은 연속된 두 문에서 인증하게 하고 한 번에 한 문만 열리게 하므로 무단 출입을 미리 막는 예방 통제(preventive control)입니다. 뒤따라 들어오기(tailgating, piggybacking)를 사전에 차단합니다. 탐지 통제는 사고 후 식별(CCTV 등), 교정 통제는 피해 복구(백업 복원 등), 보완 통제는 주 통제가 없을 때의 대체 보호입니다.

7. C Biba는 '위로 쓰기 금지'(낮은 무결성 주체가 높은 무결성 객체를 훼손하지 못함)와 '아래로 읽기 금지'로 무결성을 지킵니다. 그래서 거래 기록의 무단 수정을 막을 수 있습니다. Bell-LaPadula는 기밀성 모델이고, Chinese Wall은 이해 충돌을 막으며, Graham-Denning은 무결성 중심 모델이 아닙니다. 요구사항의 핵심은 무단 수정 방지, 즉 무결성입니다.

8. A 온프레미스 HSM으로 키를 관리하는 클라이언트 측 암호화는 암호화 작업을 클라우드 제공업체의 통제에서 분리해 독립성을 확보하고, 제3자를 통한 통제된 키 에스크로로 규정도 충족합니다. 제공업체 기본 서비스는 종속성을 만들고 독립성을 충족하지 못합니다. 클라우드 관리 키의 엔벨로프 암호화는 키 접근이 여전히 제공업체에 묶입니다. 앱 설정에 키를 저장하는 TDE는 키 보호가 부족하고 에스크로도 해결하지 못합니다.

9. C Bell-LaPadula는 기밀성을 위한 강제적 접근 통제(MAC)로, 단순 보안 속성(위로 읽기 금지)과 *-속성(아래로 쓰기 금지)을 적용해 높은 등급에서 낮은 등급으로 정보가 흐르는 것을 막습니다. Biba는 무결성 모델이고, Clark-Wilson은 상업용 무결성 모델이라 기밀 등급 격자 개념이 없습니다. Brewer-Nash는 경쟁 조직 간 이해 충돌을 막는 모델로 등급 기반 흐름 통제가 아닙니다.

10. B 자동 차단 밸브가 있는 누수 감지 센서는 누수를 감지해 경보를 울리고 급수를 자동으로 차단해 피해를 줄입니다. 센서는 탐지 통제이고 자동 차단은 추가 유출을 막는 교정 조치입니다. 이중 바닥은 아래에서 올라오는 침수에는 도움이 되지만 위에서 터진 배관은 막지 못합니다. 양압은 외부 오염 물질을 막고, HVAC 습도 모니터링은 주변 습도만 감지합니다.

11. A 실제 구성을 승인된 기준선 (baseline)과 정기적으로 비교하면 구성 드리프트(drift)를 찾아내고 승인 없는 변경을 조사할 수 있습니다. 관리자의 변경을 자동 승인하면 변경 승인 절차를 우회하게 됩니다. 스캔마다 기준선을 현재 구성으로 바꾸면 무단 변경이 정상으로 굳어질 수 있습니다. 구매 기록 검토로는 서버 설정 변경을 알 수 없습니다.

12. C 최초 대응자(first responder)는 처음 연락을 받아 사고를 식별하고, 피해가 커지지 않도록 즉시 봉쇄 조치를 하는 사람입니다. 사고 조정관은 전체 대응 과정을 관리하고 팀 활동을 조율합니다. 포렌식 분석가는 증거를 수집하고 분석하며, 휘발성 증거는 봉쇄 전이나 중에 보존해야 할 수 있습니다. 커뮤니케이션 담당자는 내외부 소통을 맡습니다.

13. C 낮음(Low) 등급 사고는 비핵심 시스템에 경미한 장애가 있고 데이터 손실이나 큰 업무 영향이 없는 경우입니다. 치명적 등급은 핵심 업무에 영향을 주는 대규모 시스템 장애나 데이터 유출입니다. 높음 등급은 중요하지만 핵심은 아닌 시스템에 영향을 주거나 제한적인 데이터 노출이 있는 경우입니다. 비상 등급은 생명, 안전, 핵심 기반 시설에 대한 즉각적인 위협입니다.

14. D 체류 시간은 예방 위주 통제가 아니라 적극적인 탐지로 줄입니다. 행위 분석과 위협 헌팅(threat hunting)은 침해를 암시하는 이상 활동을 먼저 찾아냅니다. 취약점 스캔은 약점을 찾을 뿐 진행 중인 위협을 탐지하지 못합니다. 보안 교육은 최초 침해 위험을 낮추고, 방화벽은 예방 통제입니다. 지속적 모니터링과 UEBA, 위협 헌팅은 평균 탐지 시간(MTTD)을 줄입니다.

15. A 물리 보안의 심층 방어는 바깥에서 안쪽으로 나아갑니다. 먼저 울타리, 출입문, 경비 같은 외곽 통제, 다음으로 배지 리더와 안내 데스크 같은 건물 출입 통제, 그다음 서버실 같은 방 출입 통제, 마지막으로 잠금 캐비닛과 케이블 잠금 같은 자산 단위 통제가 있습니다. 공격자가 넘어야 할 장벽이 여러 겹이 됩니다. 나머지 보기는 순서가 틀렸습니다.

16. A 이차 증거(secondary evidence)는 원본의 사본, 사진, 복제물이며, 법정에서는 원본인 최량 증거(best evidence)보다 덜 선호됩니다. 보강 증거는 다른 증거를 뒷받침하지만 반드시 사본은 아닙니다. 전문 증거는 다른 사람이 한 말에 대한 증언이며 대체로 증거로 인정되지 않습니다.

17. C 복구 시간 목표(RTO)는 장애 후 시스템이나 프로세스를 복구해야 하는 목표 시간이며, 4시간 목표가 전형적인 RTO입니다. RPO는 허용 가능한 데이터 손실을 시간으로 나타냅니다(예: 거래 손실 최대 2시간). MTD는 업무가 견딜 수 있는 최대 중단 시간이고 RTO는 그 안에서 업무를 복구할 시간을 남겨야 합니다. MTTR은 평균 수리 시간이라는 운영 지표입니다.

18. D RTO 4시간은 허용 가능한 중단 시간, RPO 1시간은 허용 가능한 데이터 손실입니다. 매일 밤 전체 백업과 웜 사이트(warm site)로의 연속 복제(continuous replication)가 가장 적합합니다. 연속 복제는 1시간 RPO를 뒷받침하고, 제대로 준비하고 테스트한 웜 사이트는 4시간 복구를 뒷받침합니다. 6시간 증분과 4시간 차등 백업은 RPO 1시간을 어기고 온프레미스 보관은 단일 장애점이 되며, 주간과 일간 백업은 최대 24시간 데이터를 잃을 수 있습니다.

19. A RFC 3227의 휘발성 순서(order of volatility) 예시는 레지스터와 캐시로 시작하고, 그다음 라우팅 테이블, ARP 캐시, 프로세스 테이블, 커널 통계, 메모리가 한 묶음으로 이어집니다. 임시 파일 시스템은 그 뒤이고, 이후 디스크, 원격 로그, 물리 구성, 보관 매체 순입니다. 따라서 보기 중 CPU 레지스터와 캐시가 가장 먼저입니다. RAM과 ARP 캐시는 같은 묶음이며 RFC 3227은 RAM을 먼저 수집하라고 정하지 않습니다.

20. B 변경 자문 위원회(CAB)의 승인은 적용 전에 거쳐야 하는 승인 단계로, 변경의 위험을 평가하고 업무 요구에 맞는지 확인하는 공식 관문입니다. 비운영 환경 테스트와 이해관계자 공지도 보통 적용 전에 끝내지만 승인 권한은 없습니다. 구성 관리 데이터베이스는 적용된 상태를 반영하도록 갱신합니다. CISSP는 기술적 준비와 함께 거버넌스 통제를 중시합니다.

21. C 802.1X 구조에서 인증자(authenticator)는 보통 스위치나 무선 액세스 포인트이며, 서플리컨트(클라이언트 기기)의 인증 요청을 인증 서버(보통 RADIUS)로 전달하는 중개자입니다. 서버의 결정에 따라 접근을 허용하거나 차단합니다. RADIUS 프록시는 경로에 있을 수 있지만 802.1X 용어의 중개자는 아닙니다. 인증 기관은 인증서를 발급할 뿐 실시간 인증에 참여하지 않으며, 네트워크 컨트롤러는 802.1X 표준 구성 요소가 아닙니다.

22. A WPA3-Enterprise는 EAP(확장 가능 인증 프로토콜, Extensible Authentication Protocol)를 쓰는 802.1X로 RADIUS 서버에서 사용자별로 인증하며, 개별 자격 증명으로 기업 수준의 보안을 제공합니다. WPA3-Personal은 SAE(동등 개체 동시 인증)를 사용하고 사전 공유 키는 Personal 모드용입니다. MAC 필터링은 주소를 쉽게 위조할 수 있어 약합니다. LEAP는 취약점이 알려진 시스코 독자 규격으로 WPA3에 포함되지 않습니다.

23. B SSL/TLS VPN은 방화벽과 NAT를 흔히 통과하는 TCP 443 포트로 동작할 수 있어 가장 적합합니다. 터널 방식 구현은 TCP와 UDP 애플리케이션 트래픽을 모두 실을 수 있고, 성능을 위해 UDP 채널을 쓰다가 필요할 때 TCP로 전환하는 제품도 많습니다. 터널 모드 IPSec과 L2TP/IPSec은 허용된 IPsec 트래픽(UDP 500, 4500 등)에 의존해 제한적인 방화벽에서 막힐 수 있습니다. PPTP는 알려진 취약점이 있고 GRE 트래픽도 방화벽과 NAT에서 문제가 됩니다.

24. D DDoS 공격은 여러 곳에 분산된 출처에서 대상에 트래픽을 쏟아부어 서버 자원을 소진시키고 정상 사용자의 서비스를 막습니다. 핵심 단서는 여러 출처에서의 트래픽 급증과 자원 고갈입니다. 중간자 공격은 통신을 가로챌 뿐 트래픽을 폭주시키지 않습니다. 세션 하이재킹은 인증된 세션을 가로채고, CSRF는 인증된 세션을 악용해 무단 작업을 하지만 둘 다 트래픽 폭주와는 무관합니다.

25. B 전송 계층(4계층)은 출발지와 목적지 프로세스 사이의 종단 간 통신 서비스를 제공합니다. TCP는 순서 번호, 확인 응답, 손실 세그먼트 재전송, 슬라이딩 윈도 흐름 제어로 신뢰성을 높입니다. UDP는 같은 계층에서 비연결형 최선 노력(best-effort) 전달을 합니다. 데이터 링크 계층은 MAC 주소로 같은 구간 내 노드 간 전달을, 네트워크 계층은 IP로 네트워크 간 라우팅을, 세션 계층은 대화 제어와 동기화를 맡으며 오류 복구는 하지 않습니다.

26. D SYN 쿠키는 연결이 확인되기 전까지 TCP 핸드셰이크 중에 서버가 자원을 할당하지 않게 하여 상태 고갈 취약점을 없앱니다. 서버는 반쯤 열린 연결 상태를 저장하는 대신 연결 정보를 시퀀스 번호에 담습니다. ICMP 속도 제한은 다른 공격 경로를 다루며 SYN 플러드에는 효과가 없습니다. MAC 필터링은 2계층 통제라 인터넷발 4계층 공격에 소용이 없고, TCP 타임스탬프를 끄는 것도 방어가 되지 않습니다.

27. C NIST와 PCI DSS 같은 업계 표준에 따르면 TLS 1.2가 신규 배포의 최소 허용 버전입니다. 강력한 암호 스위트, SHA-256 필수 지원, 알려진 공격에 대한 보호를 제공합니다. TLS 1.0과 1.1은 취약점과 약한 암호 지원 때문에 폐기 대상입니다. SSL 3.0은 POODLE 공격 같은 치명적 취약점이 있어 절대 쓰면 안 됩니다. TLS 1.3이 더 개선되었지만 규정 준수와 보안의 최소 기준은 TLS 1.2입니다.

28. B 클라이언트 인증서 인증은 TLS 핸드셰이크 중 클라이언트가 X.509 인증서를 제시하게 해, 양쪽이 서로의 신원을 확인하는 상호(양방향) 인증을 가능하게 합니다. 기본 TLS는 서버만 인증합니다. SNI는 한 IP에서 여러 TLS 사이트를 호스팅하게 할 뿐 인증 방향과 무관합니다. 세션 재개는 재연결을 빠르게 하고, PFS는 장기 키가 유출되어도 세션 키를 보호하지만 상호 인증은 제공하지 않습니다.

29. A 오탐은 IDS가 정상 트래픽을 악성으로 잘못 판단해 정상 활동에 경보를 내는 경우입니다. 경보 피로를 일으키고 분석가의 시간을 낭비합니다. 미탐은 악성 트래픽을 놓치는 반대 문제입니다. 정탐은 실제 공격을 올바르게 탐지한 것이고, 정상 판정은 정상 트래픽에 경보를 내지 않은 것입니다. 오탐은 시그니처, 임계값, 허용 목록을 조정해 해결하는 튜닝 문제입니다.

30. A BGP 하이재킹은 권한 없는 자율 시스템(AS)이 자기 것이 아닌 프리픽스를 광고해 다른 AS의 트래픽을 공격자 쪽으로 끌어오는 공격입니다. 라우트 포이즈닝은 RIP 같은 거리 벡터 프로토콜에서 실패한 경로를 무한대 메트릭으로 알려 제거하는 정상적인 수렴 기법이며 악의적 행위가 아닙니다. AS 경로 프리펜딩은 정상적인 트래픽 엔지니어링이고, 라우트 플래핑은 불안정한 광고로 상태가 반복 변하는 현상입니다.

31. A 테일러링은 기준 보안 통제를 조직의 제약, 시스템 특성, 운영 환경에 맞게 조정하는 과정으로, 기준 통제를 그대로 구현할 수 없을 때 바로 필요한 것입니다. 범위 설정은 기준이 어떤 시스템에 적용되는지를 정할 뿐 적용 대상인데 기술적으로 불가능한 통제를 조정하는 방법이 아닙니다. 보완 통제는 테일러링 과정에서 선택할 수 있습니다. 위험 수용은 잔여 위험에 대한 승인이 필요하며 자동 단계도, 요구사항 충족의 대체물도 아닙니다.

32. A 행정명령(Executive Order) 13526은 분류된(classified) 국가 안보 정보를 세 등급으로 정의합니다. Secret은 무단 공개 시 국가 안보에 '심각한 피해(serious damage)'를 줄 것으로 합리적으로 예상되는 정보입니다. Top Secret은 '예외적으로 중대한 피해(exceptionally grave damage)', Confidential은 '심각한'이라는 말 없이 '피해(damage)'를 줄 정보입니다. CUI는 이 세 등급에 들지 않으며, 민감하지만 비밀로 분류되지 않은 연방 정보를 NARA가 따로 관리하는 범주입니다. 낮은 순서로 Confidential, Secret, Top Secret입니다.

33. B 데이터 소유자(owner)는 보통 사업부 관리자나 임원으로, 데이터의 업무 가치와 민감도를 알고 관련 위험을 수용하므로 분류 등급을 결정할 최종 책임이 있습니다. 데이터 수탁자는 기술적 통제를 구현할 뿐 등급을 정하지 않습니다. 보안 관리자는 다른 사람이 정한 정책을 집행합니다. CISO는 전체 분류 체계와 정책을 정하지만 개별 데이터 자산을 분류하지는 않으며 그것은 소유자의 업무 결정입니다.

34. B 가장 엄격한 요구사항인 10년을 따르면 두 최소 보관 기간을 모두 충족합니다. 주법의 10년이 연방 의무를 대체하는 것이 아니라, 10년 보관으로 둘 다 만족하게 됩니다. 6년은 주법 위반이고, 절충안 8년은 주법 요건에 못 미칩니다. 무기한 보관은 불필요하고 비용이 들며 필요 이상으로 데이터를 가지고 있어 개인정보 위험을 높입니다.

35. A 데이터 주권은 데이터가 위치한 국가의 법과 관할권을 따른다는 원칙으로, 어느 정부가 접근을 강제할 수 있는지도 포함합니다. 비EU 정부가 EU 고객 데이터를 법적으로 요구하는 문제(예: 미국 CLOUD Act)를 직접 다룹니다. 데이터 레지던시는 물리적 저장 위치일 뿐 접근 권한의 관할은 다루지 않습니다. 데이터 현지화는 주권을 달성하는 정책 수단이고, 지리적 이중화는 가용성 개념입니다.

36. A 데이터를 폐기하기 전에 먼저 법적 보존 (legal hold), 진행 중인 소송, 규제 감사 등 계속 보관해야 할 의무가 없는지 확인해야 합니다. 법적 보존 대상 데이터를 파기하면 증거 인멸(spoliation) 제재와 사법 방해 혐의 같은 중대한 처벌을 받을 수 있습니다. 보존 의무가 없음을 확인한 뒤에야 기술적 파기를 진행합니다. 물리적 파괴, 덮어쓰기, 백업 삭제는 모두 이후 단계입니다. 관리자처럼 생각하면 법적 위험이 기술 실행보다 먼저입니다.

37. B 데이터 소유자는 보통 고위 관리자나 사업부 임원이며 데이터 자산의 분류 등급을 지정하고 주기적으로 검토합니다. 데이터 수탁자(주로 IT나 시스템 관리자)는 백업, 접근 제어 목록(ACL), 암호화처럼 소유자가 정한 통제를 구현할 뿐 분류를 결정하지 않습니다. 스튜어드는 데이터 품질, 계보, 거버넌스 업무를 맡고, 처리자는 컨트롤러(controller)나 소유자를 대신해 데이터를 다루며 분류 정책 권한이 없습니다. 소유자가 결정하고 수탁자가 구현합니다.

38. A 물리적 파괴는 매체를 완전히 쓸 수 없게 만들어 어떤 방법으로도 복구할 수 없으므로 가장 확실합니다. 암호학적 삭제는 원래 암호화된 데이터에만 쓸 수 있는데 이 경우는 암호화되지 않았으므로 해당되지 않습니다. 7회 덮어쓰기는 효과적이지만 펌웨어 영역, 불량 섹터, 오버프로비저닝(over-provisioning) 공간으로 복구될 이론적 가능성이 있고 SSD에서는 덜 확실합니다. 디가우싱은 자기 매체에만 통하며 NAND 플래시를 쓰는 SSD에는 효과가 없습니다.

39. B 기밀(Confidential)은 무단 공개 시 경쟁상 피해와 법적 책임처럼 조직에 심각한 피해를 줄 데이터에 쓰는 상업용 분류입니다. PII, 급여, 성과 평가의 조합은 분명히 이 기준에 해당합니다. 사내용은 법적 책임이 있는 데이터에는 너무 약합니다. 비밀은 정부 분류 등급이라 상업 환경에서는 보통 쓰지 않고, 공개는 민감한 직원 데이터에 분명히 부적절합니다. 기밀 등급은 엄격한 접근 통제가 필요합니다.

40. C 데이터 소유자(보통 사업부 관리자나 임원)는 분류, 보존 요건, 접근 승인에 대한 일차적 결정 책임이 있고 데이터의 업무 가치와 보호에 책임을 집니다. 데이터 수탁자는 소유자가 정한 기술적 통제를 구현할 뿐 정책을 결정하지 않습니다. 처리자는 컨트롤러를 대신해 데이터를 다루며 분류 결정권이 없습니다. CISO는 보안 지침과 거버넌스를 제공하지만 개별 데이터를 소유하지 않으며 그것은 업무 부서의 역할입니다.

41. A 알 필요성 (need-to-know)은 사용자에게 비밀 취급 인가(clearance)가 있더라도 특정 직무에 필요한 경우에만 접근을 허용한다는 원칙입니다. 이 직원은 시스템상 접근 권한이 있었을 수 있지만 업무상 필요가 없었습니다. 최소 권한은 이와 가깝지만 업무상 필요가 아니라 최소한의 권한 수준에 초점을 둡니다. 직무 분리는 부정을 막기 위해 업무를 여러 사람에게 나누는 것이고, 심층 방어는 계층 보안 전략입니다. 핵심 단서는 '업무상 정당한 이유 없이'입니다.

42. B COBIT은 IT 거버넌스를 비즈니스 목표에 맞추고 관리 체계를 제공하도록 설계되었습니다. ISO 27002는 정보 보안 통제의 실무 지침으로 기술과 운영 중심이며 거버넌스 중심이 아닙니다. NIST SP 800-53은 연방 시스템용 보안 및 개인정보 통제를 매우 상세히 다루지만 비즈니스 목표 정렬용이 아닙니다. CIS Controls는 우선순위가 매겨진 실행 항목으로 전략보다 전술에 가깝습니다. 먼저 거버넌스, 그다음 통제로 생각하세요.

43. D 듀 케어는 적절한 때에 올바른 일을 하는 것, 즉 합리적인 사람이 할 만한 행동을 취하는 것입니다. 침해를 이사회와, 필요하면 규제 기관에 보고하는 것이 듀 케어의 예입니다. 듀 딜리전스는 위험을 조사하고 보호 장치와 절차가 계속 효과적인지 확인하는 일입니다. 신중한 사람 원칙은 임원의 자산 보호 신인 의무(fiduciary duty)인데, 이 문제는 보고 행위가 보여주는 개념을 묻습니다. 직무 분리는 관련이 없습니다.

44. D BCP는 장애 중과 후에 모든 핵심 업무 기능의 연속성을 다루는 포괄적인 전략 체계로, 사람, 프로세스, 시설, 공급망, 통신, 기술을 포함합니다. DRP는 재해 후 IT 시스템, 데이터, 인프라를 복구하는 절차를 담은 더 좁은 전술 문서입니다. DRP가 BCP의 구성 요소이지 그 반대가 아닙니다. IT에만 초점을 두는 쪽은 DRP입니다. 두 계획은 서로 보완하지만 같지 않습니다.

45. D 정기적인 테스트와 훈련은 백업 무결성을 포함해 복구 절차가 실제로 작동하는지 검증합니다. 훈련에서 테이프를 읽을 수 없었다면 테스트가 부족했거나 없었다는 뜻입니다. 업무 영향 분석(BIA)은 핵심 시스템과 RTO를 식별하며 백업 매체를 검증하지 않습니다. 위험 평가는 위협과 취약점을 식별하지만 통제를 시험하지 않습니다. 계획 개발은 문서화된 절차를 만들 뿐이고 테스트 없이는 작동 여부를 알 수 없습니다.

46. A ALE = SLE × ARO입니다. SLE(단일 예상 손실액)는 한 번 발생할 때의 예상 손실로 $50,000이고, ARO(연간 발생률)는 연간 예상 빈도로 0.20(20%)입니다. 따라서 ALE = $50,000 × 0.20 = $10,000입니다. $50,000는 SLE일 뿐 연간 빈도를 반영하지 않았습니다. $250,000는 확률을 거꾸로 5배로 곱한 오류입니다. $40,000는 주어진 값으로 나올 수 없습니다. 통제 비용이 그 통제로 막는 ALE보다 크면 경제적으로 타당하지 않을 수 있습니다.

47. B 표준(standard)은 구체적인 구성, 설정, 요구사항을 의무로 정합니다(예: 비밀번호는 12자 이상). 표준은 전술적이며 강제할 수 있습니다. 정책은 경영진의 의도를 담은 상위 수준 문서라 덜 구체적입니다. 절차는 정책과 표준을 이행하는 단계별 작업 흐름을 설명하며 역시 의무일 수 있습니다. 지침은 의무가 아닌 권고입니다. 강제 가능한 요구사항을 구체적으로 정하므로 표준이 가장 적합합니다.

48. B Privacy by Design은 처음부터 시스템 아키텍처에 개인정보 보호를 내장하는 것으로, 데이터 최소화(필요한 데이터만 수집)와 개인정보 보호 기본값(privacy by default, 가장 강하게 보호하는 설정이 기본)을 포함합니다. 개발 후의 영향 평가는 사후 대응이지 선제적 설계가 아닙니다. 배포 전 암호화와 접근 통제는 보안을 다룰 뿐 수집 최소화 같은 전체 접근은 아닙니다. 개발자 교육은 도움이 되지만 설계에 내장되었음을 보장하지 않습니다.

49. B 위험 이전(risk transference)은 재정적 영향을 다른 당사자에게 넘기는 것으로, 보통 보험(사이버 배상 책임 보험)이나 계약(위약금이 있는 클라우드 제공업체 SLA)을 씁니다. 위험을 일으키는 활동을 없애는 회피가 아니고, 통제로 가능성이나 영향을 줄이는 완화도 아니며, 아무 조치 없이 인정하고 문서화하는 수용도 아닙니다. 이전해도 위험이 사라지지 않고 재정적 부담만 옮겨 갑니다. 보험, 보증, 책임 조항이 있는 외주를 떠올리세요.

50. C 법 집행 기관의 개입은 규제 의무, 소송 위험, 공개 영향이 얽혀 있어 경영진이나 법률 자문의 승인이 필요한 업무적, 법적 결정입니다. 사고 대응 팀은 기술 정보를 제공하지만 이런 전략적 결정을 내리지 않습니다. CISO는 보안 자문을 하지만 법적 노출, 침해 통지법 같은 규정 준수, 평판이 걸린 이 결정은 경영진 권한입니다. 연락 담당자는 접촉을 돕지 결정하지 않습니다. 기술 팀은 보고하고 경영진이 결정합니다.

핵심 영어 단어

due care	듀 케어(상당한 주의)	합리적인 사람이라면 할 보호 조치를 실행하는 것
due diligence	듀 딜리전스(상당한 노력)	위험을 조사하고 통제가 계속 유효한지 확인하는 것
risk acceptance	위험 수용	남은 위험을 알고 승인을 받아 받아들이는 것
risk transference	위험 이전	보험이나 계약으로 금전 부담을 다른 쪽에 넘기는 것
risk avoidance	위험 회피	위험을 만드는 활동을 그만두는 것
risk mitigation	위험 완화	통제로 발생 가능성이나 영향을 줄이는 것
residual risk	잔여 위험	통제를 적용한 뒤에도 남는 위험
single loss expectancy (SLE)	단일 예상 손실액	사고가 한 번 났을 때 예상되는 손실액
annualized rate of occurrence (ARO)	연간 발생률	사고가 1년에 일어날 것으로 예상되는 횟수
annualized loss expectancy (ALE)	연간 예상 손실액	SLE와 ARO를 곱한 1년 예상 손실액
business continuity planning (BCP)	사업 연속성 계획	중단 중에도 핵심 업무를 이어 가기 위한 전략 계획
disaster recovery planning (DRP)	재해 복구 계획	재해 뒤 IT 시스템과 데이터를 복구하는 전술 계획
business impact analysis (BIA)	업무 영향 분석	핵심 시스템과 필요한 복구 시간을 찾는 분석
recovery time objective (RTO)	복구 시간 목표	중단 뒤 시스템을 복구할 때까지의 목표 시간
recovery point objective (RPO)	복구 시점 목표	허용되는 데이터 손실을 시간으로 나타낸 값
maximum tolerable downtime (MTD)	최대 허용 중단 시간	업무가 견딜 수 있는 가장 긴 중단 시간
least privilege	최소 권한	업무에 필요한 만큼만 권한을 주는 원칙
need-to-know	알 필요성	업무상 필요할 때만 정보 접근을 허용하는 원칙
separation of duties	직무 분리	부정을 막으려고 업무를 여러 사람에게 나누는 것
policy	정책	경영진의 의도를 담은 상위 수준의 문서
standard	표준	반드시 지켜야 할 구체적인 요구 사항
procedure	절차	정책과 표준을 실행하는 단계별 방법

guideline	지침(가이드라인)	의무가 아닌 권고 사항
data owner	데이터 소유자	데이터의 등급, 보존, 접근 권한을 정하는 업무 책임자
data custodian	데이터 수탁자	소유자가 정한 기술 통제를 실행하는 사람
data sovereignty	데이터 주권	데이터가 있는 나라의 법과 관할을 따른다는 원칙
legal hold	법적 보존	소송이나 조사 때문에 데이터를 파기하지 못하게 하는 조치
tailoring	테일러링(조정)	기준선 통제를 조직과 시스템에 맞게 조정하는 것
scoping	범위 설정(스코핑)	기준선 통제를 적용할 시스템을 정하는 것
sanitization	데이터 완전 삭제	매체의 데이터를 복구할 수 없게 처리하는 것
degaussing	디가우싱(소자)	자기 매체의 데이터를 자기장으로 지우는 방법
non-repudiation	부인 방지	한 행동을 나중에 부인하지 못하게 하는 성질
key escrow	키 에스크로	암호 키의 사본을 제3자에게 맡기는 것
perfect forward secrecy (PFS)	완전 순방향 비밀성	장기 키가 유출돼도 세션 키는 안전한 성질
defense in depth	심층 방어	독립된 보안 통제를 여러 겹 두는 원칙
mantrap	맨트랩	두 문 중 하나만 열려 무단 출입을 막는 공간
compensating control	보완 통제(보상 통제)	기본 통제를 쓸 수 없을 때 대신하는 통제
false positive	오탐	정상 활동을 공격으로 잘못 판단하는 것
dwell time	체류 시간	공격자가 들키지 않고 시스템에 머문 시간
order of volatility	휘발성 순서	사라지기 쉬운 증거부터 수집하는 순서

Examundo는 독립 사이트입니다. 시험을 만드는 기관과 제휴 관계가 없으며 승인을 받지도 않았습니다. 문제는 자체 제작한 것이며 실제 시험 문제가 아닙니다.
examundo.tech/ko/cissp/