examundo

Đề thi thử CISSP tiếng Việt

50 câu hỏi kèm đáp án. Hướng dẫn và bản dịch do phần mềm làm và kiểm tra.
Chưa có người nào kiểm tra lại.

Cập nhật ngày 25 tháng 11 năm 2026 · examundo.tech/vi/cissp/

Domain 3: Kiến trúc và kỹ thuật bảo mật

1. Khái niệm mật mã nào bảo đảm người gửi không thể chối bỏ việc đã gửi một thông điệp?

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

A. Tính bí mật (Confidentiality)
B. Tính toàn vẹn (Integrity)
C. Chống chối bỏ (Non-repudiation)
D. Xác thực (Authentication)

---

2. Một kiến trúc sư bảo mật đang thiết kế hệ thống bảo vệ dữ liệu mật của chính phủ. Nên áp dụng mô hình bảo mật nào để ngăn thông tin chảy từ mức phân loại cao xuống mức phân loại thấp?

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. Mô hình Bell-LaPadula
B. Mô hình Clark-Wilson
C. Mô hình Brewer-Nash
D. Mô hình toàn vẹn Biba

---

3. Một ứng dụng thương mại điện tử cần trao đổi khóa mã hóa đối xứng với trình duyệt của khách hàng một cách an toàn. Nên dùng giao thức nào?

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

A. TLS với trao đổi khóa Diffie-Hellman
B. IPsec ở chế độ transport với khóa chia sẻ trước (pre-shared key)
C. Kerberos với vé cấp vé (ticket-granting ticket)
D. S/MIME với mã hóa dựa trên chứng thư số

---

4. Một cơ sở cần an ninh cao yêu cầu nguyên tắc hai người (two-person integrity) khi vào phòng máy chủ. Biện pháp kiểm soát truy cập vật lý nào thực hiện yêu cầu này?

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

A. Khóa số, đổi mã hằng quý
B. Đầu đọc thẻ kèm camera ghi lại mọi lượt ra vào
C. Đầu đọc sinh trắc học kèm bàn phím PIN để xác thực nhiều yếu tố
D. Mantrap xác thực kép, yêu cầu hai người được ủy quyền

---

5. Phòng thủ nhiều lớp (defense in depth) được mô tả ĐÚNG NHẤT là nguyên tắc bảo mật nào sau đây?

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

A. Triển khai nhiều lớp biện pháp kiểm soát bảo mật để bảo vệ tài sản

B. Thiết kế hệ thống để khi có lỗi thì chuyển về trạng thái an toàn

C. Chỉ cấp cho người dùng quyền truy cập tối thiểu cần để làm việc

D. Gia cố hệ thống (hardening) bằng cách gỡ các dịch vụ và tính năng không cần thiết

---

6. Mantrap được xếp vào loại biện pháp kiểm soát an ninh vật lý nào?

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

A. Kiểm soát phòng ngừa (Preventive)

B. Kiểm soát bù đắp (Compensating)

C. Kiểm soát phát hiện (Detective)

D. Kiểm soát khắc phục (Corrective)

---

7. Một hệ thống tài chính phải ngăn người dùng không được phép sửa các bản ghi giao dịch, nhưng vẫn cho phép đọc để kiểm toán. Mô hình bảo mật nào hỗ trợ yêu cầu này TỐT NHẤT?

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. Mô hình bảo vệ tính bí mật Bell-LaPadula

B. Mô hình Brewer-Nash (Chinese Wall)

C. Mô hình toàn vẹn Biba

D. Mô hình kiểm soát truy cập Graham-Denning

---

8. Một tổ chức triển khai hệ thống mật mã mới để bảo vệ dữ liệu lưu trữ (data at rest) trên đám mây. Hệ thống phải đáp ứng yêu cầu tuân thủ về ký gửi khóa (key escrow) và vẫn giữ được sự độc lập vận hành với nhà cung cấp đám mây. Cách tiếp cận nào đáp ứng cả hai yêu cầu TỐT NHẤT?

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. Mã hóa phía máy khách, khóa do HSM tại chỗ quản lý, và gửi bản sao khóa cho một dịch vụ ký gửi khóa (key escrow) của bên thứ ba

B. Dùng mã hóa phong bì (envelope encryption) với khóa do khách hàng quản lý, lưu trong dịch vụ quản lý khóa của nhà cung cấp đám mây

C. Dùng mã hóa dữ liệu trong suốt (TDE) ở tầng cơ sở dữ liệu, khóa lưu trong cấu hình ứng dụng

D. Dùng dịch vụ mã hóa có sẵn của nhà cung cấp đám mây, tự động xoay vòng khóa và sao lưu sang một vùng đám mây khác

---

9. Một kiến trúc sư bảo mật phải chọn mô hình bảo mật hình thức cho hệ thống tình báo quân sự xử lý tài liệu ở nhiều mức phân loại. Yêu cầu CHÍNH là ngăn thông tin chảy xuống mức phân loại thấp hơn. Mô hình nào phù hợp NHẤT?

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. Mô hình toàn vẹn Biba

B. Mô hình toàn vẹn Clark-Wilson

C. Mô hình Bell-LaPadula

D. Mô hình Brewer-Nash (Chinese Wall)

---

10. Một đường ống nước phía trên phòng máy chủ của trung tâm dữ liệu bị vỡ. Biện pháp kiểm soát môi trường nào đáng lẽ đã ngăn TỐT NHẤT thiệt hại do nước cho thiết bị quan trọng?

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. Hệ thống áp suất không khí dương để chặn hơi ẩm xâm nhập
B. Cảm biến phát hiện nước kèm van khóa tự động
C. Sàn nâng để đặt thiết bị cao hơn mặt sàn
D. Hệ thống HVAC có giám sát độ ẩm và cảnh báo

Domain 7: Vận hành bảo mật

11. Cách quản lý cấu hình nào phát hiện TỐT NHẤT các thay đổi trái phép trên cấu hình máy chủ đang vận hành (production)?

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

A. Thường xuyên so sánh cấu hình thực tế với đường cơ sở đã được phê duyệt
B. Tự động phê duyệt các thay đổi do quản trị viên có đặc quyền thực hiện
C. Xem lại hồ sơ mua phần cứng mà không kiểm tra cài đặt máy chủ
D. Thay đường cơ sở đã phê duyệt bằng cấu hình hiện tại sau mỗi lần quét

12. Vai trò nào trong đội ứng phó sự cố chịu trách nhiệm nhận diện và khoanh vùng (containment) sự cố lúc ban đầu?

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

A. Điều phối viên sự cố (Incident coordinator)
B. Chuyên viên điều tra số (Forensic analyst)
C. Người ứng cứu đầu tiên (First responder)
D. Trưởng nhóm truyền thông (Communications lead)

13. Một sự cố gây gián đoạn nhỏ cho các hệ thống không quan trọng và không mất dữ liệu thường được phân loại ở mức độ nghiêm trọng nào?

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

A. Rất nghiêm trọng (Critical)
B. Cao (High)
C. Thấp (Low)
D. Khẩn cấp (Emergency)

14. Khi rà soát sau sự cố, nhóm phát hiện kẻ tấn công đã duy trì sự hiện diện (persistence) 87 ngày trước khi bị phát hiện. Cải tiến vận hành bảo mật nào giúp giảm HIỆU QUẢ NHẤT thời gian ẩn náu (dwell time) trong tương lai?

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. Bắt buộc đào tạo nhận thức bảo mật cho mọi nhân viên hằng quý
B. Triển khai thêm tường lửa ở các ranh giới phân đoạn mạng
C. Tăng tần suất quét lỗ hổng từ hằng tháng lên hằng tuần
D. Triển khai giám sát bảo mật liên tục với phân tích hành vi và săn tìm mối đe dọa

15. Phòng thủ nhiều lớp cho an ninh vật lý thường gồm nhiều lớp. Thứ tự nào sau đây ĐÚNG, từ lớp ngoài cùng đến lớp trong cùng?

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

A. Hàng rào chu vi, kiểm soát ra vào tòa nhà, kiểm soát ra vào phòng, khóa thiết bị

B. Khóa thiết bị, kiểm soát ra vào phòng, kiểm soát ra vào tòa nhà, hàng rào chu vi

C. Kiểm soát ra vào phòng, khóa thiết bị, hàng rào chu vi, kiểm soát ra vào tòa nhà

D. Kiểm soát ra vào tòa nhà, hàng rào chu vi, khóa thiết bị, kiểm soát ra vào phòng

---

16. Loại bằng chứng nào gồm các bản sao hoặc bản tái tạo của bằng chứng gốc?

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

A. Bằng chứng thứ cấp (Secondary evidence)

B. Bằng chứng tốt nhất (Best evidence)

C. Bằng chứng nghe nói lại (Hearsay evidence)

D. Bằng chứng bổ trợ (Corroborative evidence)

---

17. Một tổ chức đang xác định mục tiêu khôi phục sau thảm họa. Doanh nghiệp yêu cầu các hệ thống quan trọng phải được khôi phục trong vòng 4 giờ sau thảm họa. Yêu cầu này xác định chỉ số khôi phục nào?

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. Thời gian sửa chữa trung bình (Mean Time to Repair, MTTR)

B. Thời gian gián đoạn tối đa chấp nhận được (Maximum Tolerable Downtime, MTD)

C. Mục tiêu thời gian khôi phục (Recovery Time Objective, RTO)

D. Mục tiêu điểm khôi phục (Recovery Point Objective, RPO)

---

18. Kế hoạch khôi phục sau thảm họa của một tổ chức yêu cầu RTO là 4 giờ và RPO là 1 giờ cho cơ sở dữ liệu khách hàng. Chiến lược sao lưu nào đáp ứng yêu cầu TỐT NHẤT?

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. Sao lưu chênh lệch (differential) mỗi 4 giờ, lưu tại chỗ

B. Sao lưu tăng dần (incremental) mỗi 6 giờ, lưu băng từ ở nơi khác

C. Sao lưu đầy đủ hằng tuần kèm sao lưu tăng dần hằng ngày

D. Sao lưu đầy đủ mỗi đêm cùng sao chép cơ sở dữ liệu liên tục sang địa điểm dự phòng ấm (warm site)

---

19. Người ứng cứu đầu tiên (first responder) tiếp cận một máy chủ production đã bị xâm nhập, vẫn đang bật và đang xử lý giao dịch. Theo hướng dẫn RFC 3227, nguồn dữ liệu nào nên được thu thập TRƯỚC TIÊN khi lấy bằng chứng trên máy đang chạy (live acquisition)?

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. Thanh ghi CPU và bộ nhớ đệm

B. Nội dung RAM của hệ thống (bộ nhớ chính)

C. Bộ nhớ đệm ARP và bảng định tuyến

D. Hệ thống tệp tạm và dữ liệu swap

---

20. Một bộ phận CNTT tuân theo quy trình quản lý thay đổi chính thức. Bước cấp phép (authorization) nào nên diễn ra TRƯỚC KHI triển khai thay đổi lên hệ thống đang vận hành (production)?

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

A. Kiểm thử thay đổi trong môi trường thử nghiệm (non-production)
B. Phê duyệt từ Hội đồng tư vấn thay đổi (Change Advisory Board, CAB)
C. Ghi nhận thay đổi vào cơ sở dữ liệu quản lý cấu hình (CMDB)
D. Thông báo cho tất cả các bên bị ảnh hưởng

Domain 4: Bảo mật truyền thông và mạng

21. Một tổ chức triển khai 802.1X để kiểm soát truy cập mạng. Thành phần nào đóng vai trò trung gian giữa supplicant và máy chủ xác thực?

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

A. Tổ chức cấp chứng thư số (Certificate authority)
B. Bộ điều khiển mạng (Network controller)
C. Authenticator
D. RADIUS proxy

---

22. Một tổ chức triển khai WPA3-Enterprise cho mạng không dây. WPA3-Enterprise dùng khung xác thực nào?

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

A. 802.1X với EAP
B. Lọc địa chỉ MAC
C. Khóa chia sẻ trước (PSK)
D. LEAP

---

23. Một tổ chức cần cung cấp truy cập từ xa an toàn cho nhân viên hiện trường kết nối từ nhiều địa điểm quốc tế với đường truyền internet không ổn định. Giải pháp phải hỗ trợ cả lưu lượng TCP và UDP và đi qua được hầu hết tường lửa. Giao thức VPN nào phù hợp NHẤT?

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. VPN SSL/TLS
C. L2TP/IPSec
D. IPSec ở chế độ tunnel

---

24. Ứng dụng web của một công ty có lưu lượng tăng vọt từ nhiều nguồn, làm máy chủ không đáp ứng được. Cuộc tấn công nào NHIỀU KHẢ NĂNG NHẤT đang xảy ra?

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. Man-in-the-Middle (MitM)
B. Cross-Site Request Forgery (CSRF)
C. Chiếm phiên (Session hijacking)
D. Từ chối dịch vụ phân tán (Distributed Denial of Service, DDoS)

---

25. Tầng nào của mô hình OSI chịu trách nhiệm truyền dữ liệu tin cậy từ đầu cuối đến đầu cuối (end-to-end), kiểm soát luồng và khôi phục lỗi giữa các máy (host) đang giao tiếp?

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

A. Tầng 2, Liên kết dữ liệu (Data Link)
B. Tầng 4, Giao vận (Transport)
C. Tầng 3, Mạng (Network)
D. Tầng 5, Phiên (Session)

---

26. Một tổ chức đang bị tấn công SYN flood vào máy chủ web. Kỹ thuật phòng thủ nào HIỆU QUẢ NHẤT?

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

A. Tắt TCP timestamps
B. Triển khai lọc địa chỉ MAC
C. Giới hạn tốc độ gói ICMP
D. SYN cookies

---

27. Khi triển khai TLS cho một ứng dụng web, phiên bản nào nên được coi là chuẩn TỐI THIỂU chấp nhận được cho hệ thống triển khai mới?

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. Một tổ chức tài chính yêu cầu xác thực hai chiều (mutual authentication) giữa máy khách và máy chủ. Tính năng TLS nào cung cấp khả năng này?

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

A. Tiếp tục phiên (Session resumption)
B. Xác thực bằng chứng thư số máy khách
C. Perfect Forward Secrecy (PFS)
D. Server Name Indication (SNI)

---

29. Một hệ thống phát hiện xâm nhập (IDS) tạo ra nhiều cảnh báo cho lưu lượng bình thường. Đây là loại lỗi nào?

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

A. Dương tính giả (False positive)
B. Âm tính giả (False negative)
C. Âm tính thật (True negative)
D. Dương tính thật (True positive)

---

30. Một tập đoàn đa quốc gia gặp gián đoạn định tuyến internet. Điều tra cho thấy một ISP nước ngoài đang quảng bá dải địa chỉ IP của công ty qua BGP. Cuộc tấn công nào NHIỀU KHẢ NĂNG NHẤT đang xảy ra, và điểm khác biệt CHÍNH so với route poisoning là gì?

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 hijacking; nhắm vào quyền sở hữu dải địa chỉ chứ không phải metric của tuyến
B. Route poisoning; ảnh hưởng định tuyến bên ngoài chứ không phải các giao thức distance-vector bên trong
C. Route flapping; gây gián đoạn từng lúc chứ không chuyển hướng lưu lượng liên tục
D. AS path prepending; thao túng số hiệu hệ thống tự trị để ảnh hưởng quyết định định tuyến

---

Domain 2: Bảo mật tài sản

31. Tiêu chuẩn bảo mật nền (baseline) của một công ty dịch vụ tài chính yêu cầu mã hóa AES-256 cho mọi dữ liệu khách hàng. Đánh giá rủi ro cho thấy một số hệ thống cũ không hỗ trợ AES-256. Kiến trúc sư bảo mật nên áp dụng quy trình nào để xử lý hạn chế này?

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. Điều chỉnh biện pháp (Tailoring)
B. Biện pháp bù đắp (Compensating controls)
C. Xác định phạm vi (Scoping)
D. Chấp nhận rủi ro (Risk acceptance)

---

32. Theo chính sách phân loại của chính phủ Hoa Kỳ, nhãn nào áp dụng cho thông tin mà việc tiết lộ trái phép có thể được dự đoán một cách hợp lý là sẽ gây "thiệt hại nghiêm trọng" (serious damage) cho an ninh quốc gia?

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
B. Thông tin không mật được kiểm soát (Controlled Unclassified Information, CUI)
C. Confidential
D. Top Secret

---

33. Ai chịu trách nhiệm cuối cùng về việc xác định mức phân loại của dữ liệu trong một tổ chức?

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

A. Người bảo quản dữ liệu (Data custodian)
B. Chủ sở hữu dữ liệu (Data owner)
C. Quản trị viên bảo mật (Security administrator)
D. Giám đốc an ninh thông tin (CISO)

---

34. Một tổ chức phải lưu giữ một số tài liệu tuân thủ HIPAA tối thiểu 6 năm theo HIPAA và tối thiểu 10 năm theo một luật tiểu bang có áp dụng. Người quản lý bảo mật nên đề xuất thời hạn lưu giữ nào cho các tài liệu đó?

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. 8 năm như một mức dung hòa giữa các yêu cầu
B. 10 năm để đáp ứng yêu cầu nghiêm ngặt nhất
C. Lưu giữ vô thời hạn để tránh rủi ro tuân thủ
D. 6 năm để tuân thủ yêu cầu HIPAA liên bang

---

35. Một tập đoàn đa quốc gia lưu dữ liệu khách hàng EU trong các trung tâm dữ liệu đám mây. Khách hàng Pháp lo ngại dữ liệu của họ có thể bị các bên ngoài EU dùng pháp luật buộc phải cung cấp. Nguyên tắc nào giải quyết mối lo này TỐT NHẤT?

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. Chủ quyền dữ liệu (Data sovereignty)
B. Nội địa hóa dữ liệu (Data localization)
C. Dự phòng địa lý (Geographic redundancy)
D. Nơi lưu trữ dữ liệu (Data residency)

---

36. Chính sách lưu giữ dữ liệu của một tổ chức yêu cầu giữ hồ sơ giao dịch khách hàng bảy năm. Khi hết thời hạn này, bước ĐẦU TIÊN trong quy trình hủy dữ liệu là gì?

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. Xác minh rằng không có lệnh giữ dữ liệu nào áp dụng
B. Ghi đè dữ liệu bằng công cụ tuân thủ DoD 5220.22-M
C. Hủy vật lý toàn bộ phương tiện lưu trữ chứa dữ liệu
D. Xóa mọi bản sao lưu khỏi kho lưu trữ ở nơi khác

---

37. Vai trò nào chịu trách nhiệm CHÍNH về việc xác định mức phân loại gán cho một tài sản dữ liệu của tổ chức?

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

A. Người quản trị dữ liệu (Data steward)
B. Chủ sở hữu dữ liệu (Data owner)
C. Người bảo quản dữ liệu (Data custodian)
D. Bên xử lý dữ liệu (Data processor)

---

38. Một tổ chức y tế đang ngừng sử dụng các máy tính xách tay từng lưu hồ sơ sức khỏe bệnh nhân chưa mã hóa. Phương pháp xóa sạch dữ liệu (sanitization) nào cho mức bảo đảm CAO NHẤT rằng dữ liệu không thể khôi phục?

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

A. Hủy vật lý bằng cách nghiền hoặc đốt
B. Xóa bằng mật mã (cryptographic erasure) bằng cách hủy khóa mã hóa
C. Ghi đè bảy lần bằng dữ liệu ngẫu nhiên
D. Khử từ bằng thiết bị degausser loại I hoặc loại II

---

39. Một tổ chức đang phân loại một cơ sở dữ liệu mới chứa đánh giá hiệu suất nhân viên, thông tin lương và thông tin nhận dạng cá nhân (PII). Việc tiết lộ trái phép có thể gây bất lợi cạnh tranh và trách nhiệm pháp lý. Mức phân loại nào phù hợp NHẤT?

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. Secret
B. Confidential
C. Internal Use Only
D. Public

---

40. Một tổ chức y tế phải xác định ai chịu trách nhiệm bảo đảm hồ sơ sức khỏe bệnh nhân được phân loại đúng, được lưu giữ theo quy định và chỉ người được phép mới truy cập được. Ai có trách nhiệm CHÍNH về các quyết định này?

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. Bên xử lý dữ liệu (Data Processor)
B. Giám đốc an ninh thông tin (CISO)
C. Chủ sở hữu dữ liệu (Data Owner)
D. Người bảo quản dữ liệu (Data Custodian)

Domain 1: Bảo mật và quản lý rủi ro

41. Một chuyên viên phân tích bảo mật phát hiện một nhân viên đã truy cập các tệp nhân sự (HR) mật mà không có lý do công việc. Vai trò của nhân viên này không cần truy cập dữ liệu HR. Nguyên tắc bảo mật nào NHIỀU KHẢ NĂNG NHẤT đã bị vi phạm?

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. Cần biết (Need-to-know)
B. Phòng thủ nhiều lớp (Defense in depth)
C. Phân tách nhiệm vụ (Separation of duties)
D. Đặc quyền tối thiểu (Least privilege)

---

42. CISO của một tổ chức muốn gắn chương trình bảo mật với mục tiêu kinh doanh. Khung (framework) nào phù hợp NHẤT cho mục đích này?

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. Một tổ chức y tế bị tấn công ransomware mã hóa hồ sơ bệnh nhân. CISO báo cáo sự cố cho hội đồng quản trị. CISO đang thể hiện khái niệm nào?

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. Thẩm định (Due diligence)
B. Phân tách nhiệm vụ (Separation of duties)
C. Quy tắc người thận trọng (Prudent man rule)
D. Cẩn trọng hợp lý (Due care)

---

44. Một CISO đang giải thích mối quan hệ giữa kế hoạch duy trì hoạt động kinh doanh (BCP) và kế hoạch khôi phục sau thảm họa (DRP) cho ban lãnh đạo. Phát biểu nào CHÍNH XÁC NHẤT?

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. BCP chỉ lo hệ thống và dữ liệu CNTT, còn DRP bao quát mọi hoạt động kinh doanh
B. BCP và DRP là hai thuật ngữ thay thế nhau, mô tả cùng một quy trình lập kế hoạch
C. DRP là kế hoạch chiến lược rộng hơn và chứa BCP như một thành phần
D. BCP là kế hoạch chiến lược rộng hơn, còn DRP là phần chiến thuật tập trung vào khôi phục CNTT

---

45. Trong một cuộc diễn tập khôi phục sau thảm họa, các băng từ sao lưu không đọc được. Giai đoạn nào của vòng đời BCP/DRP NHIỀU KHẢ NĂNG NHẤT đã bị lơ là?

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. Đánh giá rủi ro (Risk assessment)
B. Phân tích tác động kinh doanh (Business impact analysis)
C. Xây dựng kế hoạch (Plan development)
D. Kiểm thử và diễn tập (Testing and exercises)

---

46. Một chuyên viên phân tích rủi ro xác định một máy chủ tệp có xác suất bị ransomware xâm nhập là 20% mỗi năm, với thiệt hại ước tính 50.000 đô la mỗi sự cố. Tổn thất dự kiến hằng năm (Annualized Loss Expectancy, ALE) là bao nhiêu?

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. Nhóm bảo mật của một tổ chức đang xây dựng chính sách kiểm soát truy cập mới. Loại tài liệu nào nên NGHIÊM NGẶT NHẤT và đưa ra các hành động bắt buộc cụ thể?

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. Quy trình (Procedure)
B. Tiêu chuẩn (Standard)
C. Hướng dẫn (Guideline)
D. Chính sách (Policy)

---

48. Một công ty đang áp dụng nguyên tắc Quyền riêng tư ngay từ thiết kế (Privacy by Design) cho nền tảng dữ liệu khách hàng mới. Cách tiếp cận nào thể hiện nguyên tắc này TỐT NHẤT?

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

A. Thêm mã hóa và kiểm soát truy cập để bảo vệ dữ liệu khách hàng trước khi đưa hệ thống vào vận hành (production)
B. Xây dựng các biện pháp quyền riêng tư vào kiến trúc hệ thống ngay từ thiết kế ban đầu, gồm tối thiểu hóa dữ liệu và thiết lập riêng tư mặc định
C. Đào tạo lập trình viên về yêu cầu quyền riêng tư và rà soát mã nguồn để kiểm tra tuân thủ
D. Thực hiện đánh giá tác động quyền riêng tư sau khi phát triển hệ thống để xác định và khắc phục rủi ro

---

49. Một công ty muốn chuyển giao rủi ro tài chính liên quan đến một vụ rò rỉ dữ liệu. Chiến lược nào đang được áp dụng?

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

A. Giảm thiểu rủi ro (Risk mitigation)
B. Chuyển giao rủi ro (Risk transference)
C. Chấp nhận rủi ro (Risk acceptance)
D. Né tránh rủi ro (Risk avoidance)

---

50. Trong một sự cố bảo mật liên quan đến truy cập trái phép vào hệ thống tài chính, vai trò nào chịu trách nhiệm CHÍNH trong việc quyết định có báo cho cơ quan thực thi pháp luật hay không?

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

A. Trưởng nhóm ứng phó sự cố, vì họ có thông tin cập nhật nhất về sự cố
B. Giám đốc an ninh thông tin (CISO), vì họ chịu trách nhiệm về mọi vấn đề bảo mật
C. Lãnh đạo cấp cao hoặc cố vấn pháp lý, vì đây là quyết định kinh doanh và pháp lý có hệ quả về quy định
D. Cán bộ liên lạc với cơ quan thực thi pháp luật, vì họ giữ quan hệ với các cơ quan bên ngoài

---

Đáp án đúng

1. C Chống chối bỏ (non-repudiation) khiến một bên không thể phủ nhận việc mình đã làm, thường nhờ chữ ký số. Khóa riêng của người gửi tạo chữ ký, khóa công khai của họ dùng để kiểm tra, nên có bằng chứng về nguồn gốc. Xác thực chỉ kiểm tra danh tính, chưa chắc tạo được bằng chứng không thể chối, ví dụ mật khẩu dùng chung không chứng minh được ai đã hành động. Tính bí mật chống lộ thông tin, tính toàn vẹn chống sửa dữ liệu, cả hai đều không chứng minh ai là người gửi.

2. A Bell-LaPadula bảo vệ tính bí mật bằng hai quy tắc: không đọc lên (simple security property) và không ghi xuống (*-property). Nhờ đó thông tin không rò từ mức cao xuống mức thấp. Biba và Clark-Wilson lo về tính toàn vẹn, không phải tính bí mật. Brewer-Nash (Chinese Wall) ngăn xung đột lợi ích trong môi trường thương mại, không kiểm soát truy cập theo mức mật.

3. A TLS (Transport Layer Security) với Diffie-Hellman cho phép hai bên tạo ra một bí mật chung qua kênh không an toàn, và là cách chuẩn cho HTTPS. Diffie-Hellman tạm thời (DHE/ECDHE) còn cho perfect forward secrecy. IPsec thường dùng cho VPN và cần cấu hình trước, không hợp với khách bất kỳ trên web. S/MIME dùng cho email. Kerberos cần quan hệ tin cậy có sẵn và máy chủ KDC, không phù hợp với thương mại điện tử công cộng.

4. D Nguyên tắc hai người đòi hỏi hai người được ủy quyền cùng có mặt khi vào, để không ai hành động một mình. Mantrap xác thực kép buộc cả hai người xác thực trước khi cho vào. Sinh trắc học kèm PIN chỉ là xác thực nhiều yếu tố cho một người. Camera chỉ là biện pháp phát hiện, không ngăn một người vào. Khóa số cho bất kỳ ai biết mã vào một mình, và khi mã bị chia sẻ thì không quy được trách nhiệm cho ai.

5. A Phòng thủ nhiều lớp (defense in depth) là triển khai nhiều lớp kiểm soát độc lập, để nếu một lớp hỏng thì các lớp khác vẫn bảo vệ. Ví dụ: tường lửa, IDS/IPS, kiểm soát truy cập, mã hóa và rào chắn vật lý phối hợp với nhau. Gia cố hệ thống (hardening) là giảm bề mặt tấn công. Chỉ cấp quyền vừa đủ là nguyên tắc đặc quyền tối thiểu (least privilege). Chuyển về trạng thái an toàn khi có lỗi là thiết kế fail-safe/fail-secure.

6. A Mantrap (còn gọi là access control vestibule) là biện pháp phòng ngừa. Nó chặn người không được phép bằng cách buộc xác thực ở hai cửa liên tiếp, và chỉ một cửa mở tại một thời điểm. Nhờ đó nó chặn việc bám theo người khác vào cửa (tailgating, piggybacking) trước khi xảy ra. Biện pháp phát hiện (CCTV, cảm biến chuyển động, nhật ký) nhận ra sự cố sau đó. Biện pháp khắc phục sửa thiệt hại, còn biện pháp bù đắp dùng thay khi biện pháp chính không dùng được.

7. C Biba bảo vệ tính toàn vẹn bằng hai quy tắc: không ghi lên (chủ thể có mức toàn vẹn thấp không được làm hỏng đối tượng có mức cao) và không đọc xuống (chủ thể có mức cao không đọc dữ liệu mức thấp). Nhờ đó bản ghi giao dịch không bị sửa trái phép. Bell-LaPadula lo về tính bí mật, không phải toàn vẹn. Chinese Wall ngăn xung đột lợi ích. Graham-Denning định nghĩa các thao tác giữa chủ thể và đối tượng, không tập trung vào toàn vẹn.

8. A Mã hóa phía máy khách với khóa trong HSM tại chỗ giúp độc lập với nhà cung cấp đám mây, và vẫn ký gửi khóa có kiểm soát qua bên thứ ba để tuân thủ. Dịch vụ có sẵn của nhà cung cấp gây phụ thuộc, không đạt tính độc lập. Mã hóa phong bì với khóa nằm trong dịch vụ quản lý khóa trên đám mây vẫn khiến việc truy cập khóa phụ thuộc vào nhà cung cấp. TDE với khóa trong cấu hình ứng dụng bảo vệ khóa kém và không giải quyết việc ký gửi.

9. C Bell-LaPadula áp dụng kiểm soát truy cập bắt buộc (mandatory access control) để giữ tính bí mật, với hai quy tắc: không đọc lên và không ghi xuống. Nhờ đó thông tin không chảy từ mức cao xuống mức thấp, đúng yêu cầu đề bài. Biba lo về tính toàn vẹn, ngăn chủ thể kém tin cậy làm hỏng dữ liệu ở mức cao hơn. Clark-Wilson dùng giao dịch đúng chuẩn và phân tách nhiệm vụ, không có khái niệm cấp mật. Brewer-Nash ngăn xung đột lợi ích giữa các tổ chức cạnh tranh.

10. B Cảm biến phát hiện nước kèm van khóa tự động sẽ phát hiện rò rỉ, báo động và tự cắt nguồn nước để giảm thiệt hại. Cảm biến là biện pháp phát hiện, còn van tự khóa là biện pháp khắc phục vì hạn chế lượng nước tiếp tục chảy. Sàn nâng chỉ giúp khi nước ngập từ dưới, không giúp khi ống vỡ phía trên. Áp suất dương chỉ chặn bụi và chất bẩn từ ngoài vào. HVAC giám sát độ ẩm không dừng được nước từ ống vỡ.

11. A So sánh định kỳ cấu hình thực tế với baseline đã duyệt sẽ phát hiện cấu hình bị lệch (configuration drift) và hỗ trợ điều tra các thay đổi không có phê duyệt. Tự động duyệt thay đổi của quản trị viên bỏ qua bước phê duyệt. Thay baseline bằng cấu hình hiện tại sau mỗi lần quét có thể biến thay đổi trái phép thành bình thường. Xem hồ sơ mua phần cứng không phát hiện được thay đổi cấu hình máy chủ.

12. C Người ứng cứu đầu tiên (first responder) là đầu mối liên hệ ban đầu: họ nhận diện sự cố và khoanh vùng ngay để hạn chế thiệt hại thêm. Điều phối viên quản lý toàn bộ quá trình ứng phó và phối hợp đội. Chuyên viên điều tra số thu thập và phân tích bằng chứng, kể cả bằng chứng dễ mất cần giữ lại trước hoặc trong lúc khoanh vùng. Trưởng nhóm truyền thông lo thông tin nội bộ và bên ngoài về sự cố.

13. C Sự cố mức thấp (Low) chỉ gây gián đoạn nhỏ cho hệ thống không quan trọng, không mất dữ liệu và không ảnh hưởng đáng kể đến kinh doanh. Mức Critical là hỏng hệ thống lớn hoặc lộ dữ liệu ảnh hưởng hoạt động cốt lõi. Mức High ảnh hưởng hệ thống quan trọng nhưng chưa sống còn, hoặc lộ dữ liệu hạn chế. Mức Emergency là mối đe dọa tức thời đến tính mạng, an toàn hoặc hạ tầng trọng yếu.

14. D Muốn giảm dwell time (thời gian kẻ tấn công ở trong hệ thống) phải phát hiện chủ động, không thể chỉ ngăn chặn. Phân tích hành vi và threat hunting tìm ra hoạt động bất thường cho thấy đã bị xâm nhập. Quét lỗ hổng tìm điểm yếu, không tìm ra kẻ tấn công đang hoạt động. Đào tạo và thêm tường lửa là phòng ngừa, không bù được phần thiếu về phát hiện. Giám sát liên tục giúp giảm MTTD (Mean Time to Detect) từ nhiều tháng xuống vài ngày hoặc vài giờ.

15. A Phòng thủ nhiều lớp đi từ ngoài vào trong: kiểm soát chu vi (hàng rào, cổng, bảo vệ), kiểm soát lối vào tòa nhà (đầu đọc thẻ, lễ tân), kiểm soát phòng bên trong (phòng máy chủ), rồi kiểm soát ở cấp tài sản (tủ khóa, khóa cáp). Như vậy kẻ tấn công phải vượt qua nhiều rào cản. Các đáp án còn lại xếp sai thứ tự các lớp.

16. A Bằng chứng thứ cấp gồm bản sao, ảnh chụp hoặc bản tái tạo của bằng chứng gốc, thường kém giá trị trước tòa hơn bằng chứng tốt nhất (best evidence, tức bản gốc). Bằng chứng bổ trợ hỗ trợ hoặc xác nhận bằng chứng khác nhưng không nhất thiết là bản sao. Bằng chứng nghe nói lại (hearsay) là lời khai về điều người khác đã nói, và thường không được tòa chấp nhận.

17. C RTO là thời gian mục tiêu để khôi phục một hệ thống hoặc quy trình sau gián đoạn, và mốc 4 giờ là ví dụ điển hình. RPO là mức mất dữ liệu chấp nhận được, tính theo thời gian (ví dụ tối đa 2 giờ giao dịch). MTD là thời gian gián đoạn tối đa trước khi tác động trở nên không chấp nhận được, và RTO phải nằm trong MTD và chừa đủ thời gian để hoạt động kinh doanh phục hồi. MTTR là chỉ số vận hành về thời gian sửa trung bình, không phải yêu cầu của doanh nghiệp.

18. D RTO (4 giờ) là thời gian ngừng chấp nhận được, RPO (1 giờ) là mức mất dữ liệu chấp nhận được. Sao chép liên tục có thể đạt RPO 1 giờ, và warm site được chuẩn bị đầy đủ có thể khôi phục trong 4 giờ, nhưng phải diễn tập để chắc chắn. Sao lưu mỗi 4 giờ hoặc mỗi 6 giờ đều vi phạm RPO, và chỉ lưu tại chỗ tạo điểm lỗi duy nhất. Sao lưu hằng tuần và hằng ngày có thể mất tới 24 giờ dữ liệu.

19. A RFC 3227 nêu một ví dụ về thứ tự dễ mất (order of volatility): đầu tiên là thanh ghi và cache, rồi đến nhóm gồm bảng định tuyến, ARP cache, bảng tiến trình, thống kê kernel và bộ nhớ. Sau đó là hệ thống tệp tạm, rồi đĩa và các nguồn khó mất hơn. Vì vậy thanh ghi CPU và cache được thu trước. RAM và bảng ARP, bảng định tuyến cùng một nhóm, RFC 3227 không quy định thu RAM trước các bảng mạng.

20. B Phê duyệt từ CAB là bước cấp phép phải có trước khi triển khai trong quy trình chính thức này. Nó bảo đảm thay đổi được đánh giá rủi ro và phù hợp nhu cầu kinh doanh. Kiểm thử ngoài môi trường production và thông báo cho các bên liên quan cũng thường làm trước khi triển khai, nhưng không phải là sự cho phép. CMDB được cập nhật để phản ánh trạng thái sau khi đã triển khai.

21. C Trong 802.1X, authenticator (thường là switch hoặc điểm truy cập không dây) là trung gian: nó chuyển yêu cầu xác thực từ supplicant (thiết bị máy khách) đến máy chủ xác thực, thường qua RADIUS, rồi cho hoặc chặn truy cập theo quyết định của máy chủ. RADIUS proxy có thể nằm trên đường đi nhưng không phải trung gian theo định nghĩa 802.1X. CA chỉ cấp chứng thư số. Network controller không phải thành phần chuẩn của 802.1X.

22. A WPA3-Enterprise dùng 802.1X với EAP (Extensible Authentication Protocol) để xác thực từng người dùng với máy chủ RADIUS, mỗi người có thông tin đăng nhập riêng. Còn WPA3-Personal dùng SAE (Simultaneous Authentication of Equals). PSK dùng ở chế độ Personal, không phải Enterprise. Lọc MAC bảo mật yếu vì địa chỉ dễ bị giả mạo. LEAP là giao thức độc quyền cũ của Cisco, có lỗ hổng đã biết và không thuộc WPA3.

23. B VPN SSL/TLS là lựa chọn tốt nhất vì chạy được trên cổng TCP 443, thường đi qua được tường lửa và NAT. Loại dạng đường hầm chở được cả lưu lượng TCP và UDP của ứng dụng. IPSec chế độ tunnel hỗ trợ NAT traversal nhưng có thể bị tường lửa chặt chẽ chặn. L2TP/IPSec cũng phụ thuộc vào việc lưu lượng IPsec được phép, thường là UDP 500 và 4500. PPTP không an toàn vì lỗ hổng đã biết, và lưu lượng GRE của nó cũng dễ bị chặn.

24. D DDoS dùng nhiều nguồn phân tán để làm ngập mục tiêu bằng lưu lượng, làm cạn tài nguyên máy chủ và khiến người dùng hợp lệ không dùng được dịch vụ. Dấu hiệu chính ở đây là lưu lượng tăng vọt từ nhiều nguồn và tài nguyên bị cạn. MitM nghe lén giữa hai bên. Chiếm phiên là cướp phiên đã xác thực, không tạo lưu lượng đột biến. CSRF lợi dụng phiên đã xác thực để thực hiện hành động trái phép, không làm quá tải bằng lưu lượng.

25. B Tầng Giao vận (tầng 4) lo giao tiếp từ đầu cuối đến đầu cuối giữa tiến trình nguồn và đích. TCP ở tầng này bảo đảm tin cậy bằng số thứ tự, xác nhận, gửi lại segment bị mất và kiểm soát luồng bằng cửa sổ trượt. UDP cùng tầng nhưng không kết nối và không bảo đảm. Tầng 2 chuyển dữ liệu giữa các nút trong một đoạn mạng bằng địa chỉ MAC. Tầng 3 định tuyến gói bằng địa chỉ IP. Tầng 5 quản lý hội thoại, không lo khôi phục lỗi.

26. D SYN cookies giúp máy chủ chưa phải cấp tài nguyên trong bước bắt tay TCP cho đến khi kết nối được xác minh, nên SYN flood không làm cạn bảng trạng thái được. Máy chủ đưa thông tin kết nối vào số thứ tự thay vì giữ trạng thái kết nối nửa mở. Giới hạn ICMP xử lý kiểu tấn công khác. Lọc MAC là biện pháp tầng 2, không hiệu quả với tấn công tầng 4 từ internet. Tắt TCP timestamps chỉ bỏ một tính năng, không chống được việc cạn tài nguyên.

27. C TLS 1.2 là phiên bản tối thiểu chấp nhận được cho hệ thống mới theo các chuẩn ngành của NIST và PCI DSS. Nó có bộ mật mã (cipher suite) mạnh, bắt buộc hỗ trợ SHA-256 và chống được các tấn công đã biết. TLS 1.0 và 1.1 đã lỗi thời vì có lỗ hổng và bộ mật mã yếu. SSL 3.0 có lỗ hổng nghiêm trọng (tấn công POODLE) và không bao giờ nên dùng. TLS 1.3 tốt hơn, nhưng TLS 1.2 vẫn là mức tối thiểu để tuân thủ và bảo mật.

28. B Xác thực bằng chứng thư số máy khách buộc máy khách trình chứng thư X.509 khi bắt tay TLS, nên cả hai bên cùng kiểm tra danh tính của nhau (xác thực hai chiều). TLS thông thường chỉ xác thực máy chủ. SNI cho phép nhiều trang TLS dùng chung một IP, không liên quan đến chiều xác thực. Session resumption chỉ giúp kết nối lại nhanh hơn. PFS bảo đảm khóa phiên không bị lộ khi khóa dài hạn bị lộ, nhưng không tạo xác thực hai chiều.

29. A Dương tính giả xảy ra khi IDS nhận nhầm lưu lượng hợp lệ là độc hại và cảnh báo cho hoạt động bình thường. Hậu quả là quá tải cảnh báo (alert fatigue) và mất thời gian của nhân viên phân tích. Âm tính giả là ngược lại: lưu lượng độc hại không bị phát hiện. Dương tính thật nhận đúng một cuộc tấn công thật, âm tính thật nhận đúng lưu lượng hợp lệ mà không cảnh báo. Cách xử lý là chỉnh lại mẫu nhận diện (signature), ngưỡng hoặc danh sách cho phép.

30. A BGP hijacking là khi một hệ thống tự trị (AS) trái phép quảng bá các prefix mà nó không sở hữu, khiến các AS khác chuyển lưu lượng đến kẻ tấn công. Route poisoning là kỹ thuật hội tụ hợp lệ của giao thức distance-vector như RIP, quảng bá metric vô cực để loại tuyến hỏng. AS path prepending là cách điều phối lưu lượng hợp lệ để làm tuyến kém ưu tiên. Route flapping là tuyến được quảng bá không ổn định, không phải chuyển hướng có chủ đích.

31. A Tailoring là điều chỉnh các biện pháp của baseline cho hợp với ràng buộc của tổ chức, đặc điểm hệ thống và môi trường vận hành, đúng với tình huống này. Scoping chỉ xác định baseline áp dụng cho hệ thống nào. Biện pháp bù đắp (compensating control) có thể được chọn trong quá trình tailoring khi không làm được biện pháp quy định. Chấp nhận rủi ro cần người có thẩm quyền phê duyệt rủi ro còn lại, không phải bước cuối tự động và không thay cho việc đáp ứng yêu cầu.

32. A Sắc lệnh hành pháp 13526 (Executive Order 13526) định ra ba cấp mật. Secret dùng khi tiết lộ trái phép có thể gây thiệt hại nghiêm trọng (serious damage) cho an ninh quốc gia. Top Secret là thiệt hại đặc biệt nghiêm trọng (exceptionally grave damage). Confidential là thiệt hại, không có chữ nghiêm trọng. CUI không phải cấp mật, mà là loại riêng do NARA quản lý cho thông tin liên bang nhạy cảm nhưng không mật. Thứ tự tăng dần: Confidential, Secret, Top Secret.

33. B Chủ sở hữu dữ liệu (data owner), thường là quản lý đơn vị kinh doanh hoặc lãnh đạo, chịu trách nhiệm cuối cùng về mức phân loại vì họ hiểu giá trị và độ nhạy cảm của dữ liệu và chấp nhận rủi ro đi kèm. Người bảo quản dữ liệu triển khai biện pháp kỹ thuật nhưng không đặt mức phân loại. Quản trị viên bảo mật thực thi chính sách do người khác định ra. CISO đặt khung và chính sách phân loại chung, không phân loại từng bộ dữ liệu.

34. B 10 năm đáp ứng yêu cầu nghiêm ngặt nhất và thỏa cả hai mức tối thiểu. Yêu cầu 10 năm của tiểu bang không thay thế nghĩa vụ liên bang, nhưng lưu 10 năm thì thỏa cả hai. 6 năm vi phạm luật tiểu bang. 8 năm dung hòa vẫn không đạt yêu cầu của tiểu bang. Lưu vô thời hạn là không cần thiết, tốn kém và tạo rủi ro về quyền riêng tư vì giữ dữ liệu lâu hơn mức yêu cầu.

35. A Chủ quyền dữ liệu (data sovereignty) nghĩa là dữ liệu chịu luật và quyền tài phán của quốc gia nơi nó được lưu, kể cả việc chính phủ nào có thể buộc cung cấp. Điều này đúng với lo ngại về yêu cầu pháp lý từ ngoài EU (ví dụ U.S. CLOUD Act). Data residency chỉ là nơi lưu vật lý: dữ liệu ở Pháp vẫn có thể do công ty mẹ ở Mỹ sở hữu và truy cập hợp pháp. Data localization là chính sách giữ dữ liệu trong biên giới, một công cụ để đạt chủ quyền. Dự phòng địa lý thuộc về tính sẵn sàng.

36. A Trước khi hủy dữ liệu, phải xác nhận không có lệnh giữ dữ liệu (legal hold), vụ kiện, cuộc kiểm toán hay nghĩa vụ nào buộc tiếp tục lưu. Hủy dữ liệu đang bị legal hold có thể bị phạt nặng, kể cả chế tài vì hủy chứng cứ (spoliation) và cáo buộc cản trở tư pháp. Hủy vật lý, ghi đè và xóa bản sao lưu đều là bước hợp lệ về sau. Đây là câu hỏi kiểu nghĩ như người quản lý: rủi ro pháp lý xét trước, kỹ thuật làm sau.

37. B Chủ sở hữu dữ liệu (thường là quản lý cấp cao hoặc lãnh đạo đơn vị kinh doanh) gán mức phân loại và định kỳ xem xét lại. Người bảo quản dữ liệu (thường là nhân viên CNTT) làm các biện pháp mà chủ sở hữu yêu cầu, như sao lưu, kiểm soát truy cập và mã hóa. Data steward lo chất lượng và quản trị dữ liệu. Data processor xử lý dữ liệu thay cho bên khác và không có quyền về phân loại. Tóm lại: chủ sở hữu quyết định, người bảo quản thực hiện.

38. A Hủy vật lý cho mức bảo đảm cao nhất vì phương tiện không còn dùng được và không thể khôi phục bằng bất kỳ cách nào. Xóa bằng mật mã chỉ dùng được nếu dữ liệu vốn đã mã hóa, mà đề bài nói rõ là chưa. Ghi đè bảy lần về lý thuyết vẫn có thể để sót dữ liệu ở vùng firmware, bad sector và vùng over-provisioned, và kém tin cậy hơn trên SSD. Khử từ chỉ có tác dụng với phương tiện từ tính, không có tác dụng với SSD vì SSD dùng bộ nhớ flash NAND.

39. B Confidential là mức phân loại thương mại phù hợp cho dữ liệu mà nếu bị lộ trái phép sẽ gây thiệt hại nghiêm trọng cho tổ chức, kể cả bất lợi cạnh tranh và trách nhiệm pháp lý. PII, lương và đánh giá hiệu suất rõ ràng đạt ngưỡng này. Internal Use Only quá yếu cho dữ liệu có hệ quả pháp lý. Secret là cấp mật của chính phủ, thường không dùng trong doanh nghiệp. Public rõ ràng không phù hợp với dữ liệu nhân viên nhạy cảm.

40. C Chủ sở hữu dữ liệu (thường là quản lý hoặc lãnh đạo kinh doanh) có trách nhiệm chính về phân loại, thời hạn lưu giữ và việc cho phép ai truy cập. Người bảo quản dữ liệu làm các biện pháp kỹ thuật mà chủ sở hữu yêu cầu, không quyết định chính sách. Data processor xử lý dữ liệu thay cho bên kiểm soát và không quyết định phân loại. CISO hướng dẫn và quản trị bảo mật nhưng không sở hữu từng tài sản dữ liệu, vì đó là chức năng kinh doanh.

41. A Need-to-know nghĩa là chỉ cho truy cập khi một công việc cụ thể cần đến, kể cả khi người đó đã có cấp độ an ninh (clearance) phù hợp. Nhân viên này có thể được hệ thống cho quyền nhưng không có nhu cầu công việc. Đặc quyền tối thiểu (least privilege) rất gần nhưng nói về mức quyền thấp nhất. Phân tách nhiệm vụ chia việc cho nhiều người để ngăn gian lận. Phòng thủ nhiều lớp không phải nguyên tắc truy cập. Manh mối: "không có lý do công việc".

42. B COBIT (Control Objectives for Information and Related Technologies) được thiết kế để gắn quản trị CNTT với mục tiêu kinh doanh. ISO 27002 là bộ quy tắc thực hành về biện pháp bảo mật, thiên về kỹ thuật và vận hành. NIST SP 800-53 nêu rất chi tiết các biện pháp cho hệ thống liên bang, không nhằm gắn với mục tiêu kinh doanh. CIS Controls là các hành động ưu tiên, mang tính chiến thuật. Hãy nghĩ đến quản trị trước, biện pháp kiểm soát sau.

43. D Due care là làm điều đúng vào đúng lúc, như một người hợp lý sẽ làm. Báo cáo sự cố cho hội đồng quản trị (và cho cơ quan quản lý, nếu bắt buộc) là một ví dụ. Due diligence là tìm hiểu rủi ro và liên tục xác minh các biện pháp bảo vệ còn hiệu quả. Prudent man rule nói lãnh đạo có nghĩa vụ ủy thác (fiduciary duty) bảo vệ tài sản một cách cẩn trọng, nhưng đề hỏi hành động báo cáo thể hiện điều gì. Phân tách nhiệm vụ không liên quan.

44. D BCP là khung chiến lược toàn diện giúp các chức năng quan trọng tiếp tục trong và sau gián đoạn, gồm con người, quy trình, cơ sở vật chất, chuỗi cung ứng, truyền thông và công nghệ. DRP hẹp hơn, mang tính chiến thuật, nêu cách khôi phục hệ thống CNTT, dữ liệu và hạ tầng sau thảm họa. DRP là một phần của BCP, không phải ngược lại. Hai kế hoạch bổ sung cho nhau nhưng không thay thế nhau.

45. D Kiểm thử và diễn tập thường xuyên xác nhận quy trình khôi phục hoạt động được, kể cả bản sao lưu còn nguyên vẹn. Băng từ không đọc được khi diễn tập nghĩa là trước đó kiểm thử chưa đủ hoặc chưa từng làm. Phân tích tác động kinh doanh xác định hệ thống quan trọng và RTO. Đánh giá rủi ro xác định mối đe dọa và lỗ hổng. Xây dựng kế hoạch chỉ tạo ra quy trình bằng văn bản. Có kế hoạch là chưa đủ, phải kiểm thử.

46. A ALE = SLE × ARO. SLE (Single Loss Expectancy, tổn thất dự kiến mỗi lần) = $50,000. ARO (Annualized Rate of Occurrence, tần suất xảy ra hằng năm) = 0.20 (20%). Vậy ALE = $50,000 × 0.20 = $10,000. $50,000 chỉ là SLE, chưa tính tần suất. $250,000 là do nhân nhầm với 5. $40,000 không có cơ sở từ các số đã cho. Nếu biện pháp bảo vệ tốn hơn phần ALE nó ngăn được, có thể không đáng đầu tư.

47. B Tiêu chuẩn (standard) quy định cấu hình, thiết lập hoặc yêu cầu cụ thể và bắt buộc (ví dụ: mọi mật khẩu phải từ 12 ký tự trở lên). Chính sách (policy) nêu ý định của ban lãnh đạo ở mức cao, ít cụ thể hơn. Quy trình (procedure) mô tả từng bước thực hiện chính sách và tiêu chuẩn, và cũng có thể bắt buộc. Hướng dẫn (guideline) chỉ là khuyến nghị. Tiêu chuẩn là đáp án tốt nhất vì nêu yêu cầu bắt buộc, còn quy trình nêu các bước làm.

48. B Privacy by Design là đưa quyền riêng tư vào kiến trúc hệ thống ngay từ đầu, gồm tối thiểu hóa dữ liệu (chỉ thu thập dữ liệu cần thiết) và mặc định ở mức bảo vệ cao nhất. Đánh giá tác động quyền riêng tư sau khi phát triển là bị động. Mã hóa và kiểm soát truy cập trước khi triển khai giải quyết bảo mật nhưng chưa thể hiện đủ cách làm này. Đào tạo lập trình viên có ích nhưng không bảo đảm quyền riêng tư được đưa vào kiến trúc từ đầu.

49. B Chuyển giao rủi ro (risk transference) đẩy tác động tài chính sang bên khác, thường qua bảo hiểm mạng hoặc hợp đồng (như SLA của nhà cung cấp đám mây có điều khoản phạt). Né tránh là bỏ hoạt động gây rủi ro. Giảm thiểu là dùng biện pháp kiểm soát để giảm khả năng hoặc tác động. Chấp nhận là ghi nhận mà không hành động. Chuyển giao không làm rủi ro biến mất, chỉ chuyển gánh nặng tài chính.

50. C Đưa cơ quan thực thi pháp luật vào là quyết định kinh doanh và pháp lý, cần lãnh đạo cấp cao hoặc cố vấn pháp lý phê duyệt vì có thể phát sinh nghĩa vụ theo quy định, rủi ro kiện tụng và hệ quả công bố thông tin. Nhóm ứng phó sự cố chỉ cung cấp chi tiết kỹ thuật. CISO tư vấn về bảo mật, nhưng quyết định này cần thẩm quyền của cấp lãnh đạo. Cán bộ liên lạc chỉ hỗ trợ liên hệ. Đội kỹ thuật báo cáo lên, lãnh đạo quyết định.

Từ tiếng Anh cần biết

due care	sự cẩn trọng hợp lý	Làm điều mà người cẩn trọng sẽ làm để bảo vệ tổ chức.

due diligence	sự thẩm định	Tìm hiểu rủi ro và liên tục kiểm tra biện pháp còn hiệu quả.
risk owner	người chịu trách nhiệm rủi ro	Người có quyền quyết định cách xử lý một rủi ro.
risk acceptance	chấp nhận rủi ro	Biết rõ rủi ro còn lại và chính thức giữ nó.
risk transference	chuyển giao rủi ro	Đẩy thiệt hại tài chính sang bảo hiểm hoặc bên khác.
risk avoidance	né tránh rủi ro	Ngừng hoạt động gây ra rủi ro.
risk mitigation	giảm thiểu rủi ro	Dùng biện pháp kiểm soát để giảm khả năng hoặc tác động.
residual risk	rủi ro còn lại	Phần rủi ro vẫn còn sau khi đã áp dụng biện pháp.
annualized loss expectancy (ALE)	tổn thất dự kiến hằng năm	Thiệt hại dự kiến mỗi năm, bằng SLE nhân ARO.
single loss expectancy (SLE)	tổn thất dự kiến mỗi lần	Số tiền dự kiến mất trong một lần xảy ra.
annualized rate of occurrence (ARO)	tần suất xảy ra hằng năm	Số lần dự kiến xảy ra trong một năm.
business continuity plan (BCP)	kế hoạch duy trì hoạt động kinh doanh	Kế hoạch giữ các hoạt động quan trọng khi có gián đoạn.
disaster recovery plan (DRP)	kế hoạch khôi phục sau thảm họa	Các bước khôi phục hệ thống IT và dữ liệu sau thảm họa.
business impact analysis (BIA)	phân tích tác động kinh doanh	Xác định hệ thống quan trọng và thời gian cần khôi phục.
recovery time objective (RTO)	mục tiêu thời gian khôi phục	Mục tiêu về thời gian đưa hệ thống trở lại sau gián đoạn.
recovery point objective (RPO)	mục tiêu điểm khôi phục	Lượng dữ liệu tối đa được phép mất, tính theo thời gian.
maximum tolerable downtime (MTD)	thời gian gián đoạn tối đa chấp nhận được	Quá mức này, thiệt hại với tổ chức là không chấp nhận được.
least privilege	đặc quyền tối thiểu	Chỉ cấp mức quyền vừa đủ để làm việc.
need-to-know	cần mới được biết	Chỉ được xem dữ liệu khi công việc thật sự cần.
separation of duties	phân tách nhiệm vụ	Chia một việc cho nhiều người để ngăn gian lận.
standard	tiêu chuẩn	Tài liệu nêu yêu cầu cụ thể và bắt buộc.
guideline	hướng dẫn	Tài liệu nêu khuyến nghị, không bắt buộc.
data owner	chủ sở hữu dữ liệu	Người quản lý quyết định mức phân loại và quyền truy cập.
data custodian	người bảo quản dữ liệu	Người triển khai biện pháp mà chủ sở hữu yêu cầu.
legal hold	lệnh giữ dữ liệu	Yêu cầu pháp lý không được hủy dữ liệu liên quan.

tailoring	điều chỉnh biện pháp	Chỉnh bộ biện pháp cơ sở cho hợp với tổ chức.
sanitization	xóa sạch dữ liệu	Làm cho dữ liệu trên thiết bị không thể khôi phục được.
confidentiality	tính bí mật	Thông tin không bị lộ cho người không được phép.
integrity	tính toàn vẹn	Dữ liệu không bị sửa đổi trái phép.
non-repudiation	chống chối bỏ	Người gửi không thể phủ nhận việc mình đã làm.
defense in depth	phòng thủ nhiều lớp	Nhiều lớp kiểm soát độc lập cùng bảo vệ tài sản.
compensating control	biện pháp bù đắp	Biện pháp thay thế khi không dùng được biện pháp chính.
mantrap	khoang cửa kép	Hai cửa liên tiếp, mỗi lúc chỉ mở được một cửa.
key escrow	ký gửi khóa	Gửi bản sao khóa mã hóa cho bên thứ ba giữ.
false positive	báo động giả	Hệ thống coi hoạt động hợp lệ là tấn công.
dwell time	thời gian ẩn náu	Thời gian kẻ tấn công ở trong hệ thống trước khi bị phát hiện.
order of volatility	thứ tự dễ mất	Thứ tự thu bằng chứng, dữ liệu dễ mất nhất thu trước.
Change Advisory Board (CAB)	hội đồng tư vấn thay đổi	Nhóm xét và phê duyệt thay đổi trước khi triển khai.

Examundo là trang độc lập, không liên kết với các đơn vị tổ chức những kỳ thi này và không được các đơn vị này phê duyệt. Câu hỏi được soạn riêng, không lấy từ đề thi thật. examundo.tech/vi/cissp/