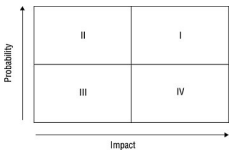
D1-002 結果 2022 年 11 月 22 日

問題一

tb787631.CISSPPT3E.c01.081

Domer Industries 風險評估團隊最近進行了定性風險評估，並開發了一個類似於此處顯示的矩陣。哪個像限包含需要最直接關注的風險？



A.我

B.二

C.III

D.IV

你回答正確！

風險評估小組應該最直接地關注出現在像限 I 中的那些風險。這些風險

發生的可能性很高，如果發生的話對組織的影響也很大。

問題 2

tb787631.CISSPPT3E.c01.035

羅伯特負責保護用於處理信用卡信息的系統。什麼樣的安全控制框架應該指導他的行動？

A. HIPAA

B. PCI DSS

C、SOX

D. GLBA

你回答正確！

支付卡行業數據安全標準 (PCI DSS) 管理信用卡信息的存儲、處理和傳輸。薩班斯奧克斯利法案 (SOX) 規範上市公司的財務報告活動。健康保險流通與責任法案 (HIPAA) 規範了受保護健康信息 (PHI) 的處理。

Gramm Leach Bliley 法案 (GLBA) 規範了個人財務信息的處理。

問題三

tb787631.CISSPPT3E.c01.039

Tom 啟用了由他的雲基礎架構作為服務提供商提供的應用程序防火牆，旨在阻止多種類型的應用程序攻擊。從風險管理的角度來看，Tom 試圖通過實施此對策來降低什麼指標？

A. 影響

B、RPO

C. 甲基丙烯酸甲酯

D、可能性

你回答正確！

安裝可阻止攻擊的設備是通過降低應用程序攻擊成功的可能性來降低風險的嘗試。添加防火牆不會解決風險、恢復點目標 (RPO) 或最大可容忍中斷 (MTO) 的影響。

問題四

tb787631.CISSPPT3E.c01.020

凱利認為，一名員工未經授權將計算資源用於副業。在與管理層協商後，她決定發起行政調查。她在這次調查中必須滿足的舉證責任是什麼？

A. 優勢證據
B. 排除合理懷疑
C. 毫無疑問
D、沒有標準

您回答錯誤。

與刑事或民事案件不同，行政調查是內部事務，沒有凱利必須適用的固定證據標準。然而，對於她的組織來說，在他們自己的內部程序中加入標準的舉證責任以確保調查的徹底性和公平性仍然是明智的。

問題 5

tb787631.CISSPPT3E.c01.043

Gary 正在分析一個安全事件，在他的調查過程中，遇到了一個用戶，該用戶否認執行了 Gary 認為他確實執行過的操作。STRIDE 模型下發生了什麼類型的威脅？

A. 否認

B、信息披露

C. 篡改

D. 特權提升

你回答正確！

否認威脅允許攻擊者在另一方無法證明不同的情況下否認執行過某項操作或活動。沒有證據表明攻擊者參與了信息洩露、篡改或特權提升。

問題 6

tb787631.CISSPPT3E.c01.029

以下哪一個組織如果從事電子交易，不會自動遵守 HIPAA 的隱私和安全要求？

A. 醫療保健提供者

B. 健康健身應用開發商

C. 健康信息交換所

D. 健康保險計劃

您回答錯誤。

健康和健身應用程序開發人員不一定會收集或處理醫療保健數據，並且

HIPAA 的條款不適用於此類業務。HIPAA 監管三種類型的實體——醫療

保健提供者、健康信息交換所和健康保險計劃——以及任何這些涵蓋實體

的業務夥伴。

問題 7

tb787631.CISSPPT3E.c01.048

請參考以下場景：

- Juniper Content 是一家網絡內容開發公司，擁有 40 名員工，分佈在兩個辦公室：一個在紐約，一個較小的辦公室在舊金山灣區。每個辦公室都有一個由外圍防火牆保護的局域網。局域網 (LAN) 包含連接到有線和無線網絡的現代交換機設備。
- 每個辦公室都有自己的文件服務器，信息技術 (IT) 團隊每小時運行一次軟件，在兩個服務器之間同步文件，在辦公室之間分發內容。這些服務器主要用於存儲與公司開發的網絡內容相關的圖像和其他文件。該團隊還在大部分工作中使用基於 SaaS 的電子郵件和文檔協作解決方案。
- 您是 Juniper Content 新任命的 IT 經理，您正在努力增強現有的安全控制以提高組織的安全性。

您還擔心存儲在每個辦公室服務器上的數據的可用性。您希望添加即使服務器中的硬盤驅動器發生故障也能繼續訪問位於服務器上的文件的技術。什麼控件允許您在不添加額外服務器的情況下增加穩健性？

A. 服務器集群

B、負載均衡

C、RAID

D、定時備份

你回答正確！

RAID 使用額外的硬盤驅動器來保護服務器免受單個設備故障的影響。負載平衡和服務器集群確實增加了健壯性，但需要添加服務器。計劃備份可防止數據丟失，但在硬盤驅動器發生故障時不提供對數據的即時訪問。

問題 8

tb787631.CISSPPT3E.c01.032

吉娜正在努力保護她的公司將用於他們即將推出的新產品的徽標。她對這個標識的知識產權保護流程有疑問。哪個美國政府機構最能回答她的問題？

A. 美國專利商標局

B. 國會圖書館

C、美國國家安全局

D. 美國國家標準與技術研究院

您回答錯誤。

首先，您必須認識到商標是標識的正確知識產權保護機制。因此，吉娜應該聯繫負責商標註冊的美國專利商標局（USPTO）。國會圖書館負責管理版權計劃。美國國家安全局 (NSA) 和美國國家標準技術研究院 (NIST) 在知識產權保護方面沒有任何作用。

問題 9

tb787631.CISSPPT3E.c01.026

卡爾是一名調查計算機犯罪案件的聯邦特工。他確定了一名從事非法行為的襲擊者，並希望對該人提起訴訟，這將導致他入獄。卡爾必須滿足什麼證明標準？

A. 毫無疑問
B. 優勢證據
C. 排除合理懷疑
D. 大部分證據

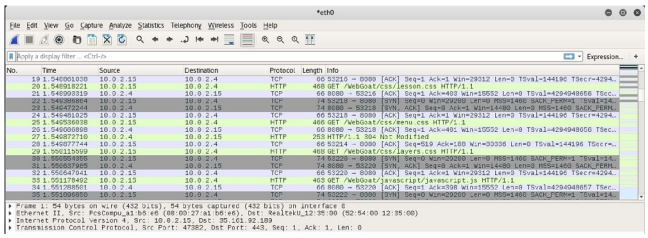
您回答錯誤。

回答這個問題有兩個步驟。首先，你必須意識到，要導致入獄的案件，必須是刑事調查的結果。其次，要知道刑事偵查的舉證標準一般都是排除合理懷疑的標準。

問題 10

tb787631.CISSPPT3E.c01.086

您發現網絡上的用戶一直在使用 Wireshark 工具，如此處所示。進一步調查顯示他將其用於非法目的。信息安全的哪個支柱最有可能遭到侵犯？



A. 誠信

B. 拒絕

C. 可用性

D. 保密

你回答正確！

Wireshark 是一種協議分析器，可用於竊聽網絡連接。竊聽是對機密性的攻擊。

問題 11

tb787631.CISSPPT3E.c01.021

Keenan Systems 最近開發了一種新的微處理器製造工藝。該公司希望將該技術授權給其他公司使用，但希望防止未經授權使用該技術。哪種類型的知識產權保護最適合這種情況？

一、專利

B、商業秘密

三、版權

D、商標

您回答錯誤。

專利和商業秘密都可以保護與製造過程相關的知識產權。只有當細節可以

在組織內部得到嚴格控制時，商業秘密才是合適的，因此在這種情況下專

利是合適的解決方案。版權用於保護創意作品，而商標用於保護名稱、徽

標和符號。

問題 12

tb787631.CISSPPT3E.c01.038

Florian 收到美國聯邦政府機構發來的傳單，宣布一項新的行政法將影響他的業務運營。他應該去哪裡尋找法律文本？

A. 美國法典

B. 最高法院的裁決

C. 聯邦法規

D. 法律綱要

你回答正確！

聯邦法規 (CFR) 包含聯邦機構頒布的所有行政法的文本。美國法典包含

刑法和民法。最高法院的裁決包含對法律的解釋，而不是法律本身。法律

綱要不存在。

問題 13

tb787631.CISSPPT3E.c01.046

瓊正在尋求保護她根據知識產權法開發的一款計算機軟件。以下哪一項保護途徑不適用於軟件？

一、商標

B.版權

C、專利

D、商業秘密

你回答正確！

商標保護代表產品或服務的文字和圖像，但不保護計算機軟件。

問題 14

tb787631.CISSPPT3E.c01.061

Elise 正在幫助她的組織準備評估和採用新的基於雲的人力資源管理 (HRM) 系統供應商。她對可能的供應商提出的最合適的最低安全標準是什麼？

A. 遵守所有法律法規

B. 以與組織相同的方式處理信息

C. 消除所有已識別的安全風險

D. 遵守供應商自己的政策

你回答正確！

在評估供應商時用作基準的最合適的標準是確定供應商的安全控制是否符合組織自己的標準。遵守法律法規應包含在該要求中，並且是與供應商合作的必要條件，但不是充分條件。供應商遵守他們自己的政策也屬於必要但不充分的控制類別，因為供應商的政策可能弱於組織自己的要求。消除所有已識別的安全風險是潛在供應商不可能滿足的要求。

問題 15

tb787631.CISSPPT3E.c01.054

Chris 的組織最近遭受了一次攻擊，致使付費客戶在數小時內無法訪問他們的網站。哪個信息安全目標受到的影響最直接？

A. 保密

B. 誠信

C. 可用性

D. 拒絕

你回答正確！

拒絕服務 (DoS) 攻擊和分佈式拒絕服務 (DDoS) 攻擊試圖通過向受害者

註入流量或以其他方式中斷服務來破壞信息系統和網絡的可用性。

問題 16

tb787631.CISSPPT3E.c01.078

什麼信息安全原則規定組織應盡可能實施重疊的安全控制？

A. 最小權限

B. 職責分離

C、縱深防禦

D. 默默無聞的安全

您回答錯誤。

縱深防禦指出，組織應該有重疊的安全控制，旨在盡可能滿足相同的安全

目標。這種方法在單個控制失敗的情況下提供安全性。最小權限確保個人

僅具有執行其分配的工作職能所需的最少權限集，並且不需要重疊控制。

職責分離要求一個人無權執行兩項單獨的操作，這些操作結合起來執行敏

感功能。通過模糊實現安全性試圖隱藏安全控制的細節以增加安全性。職

責分離和通過模糊實現的安全都不涉及重疊控制。

問題 17

tb787631.CISSPPT3E.c01.071

Ben 正在尋找一個在世界範圍內被廣泛接受並特別關注信息安全控制的控制目標框架。以下哪一個框架最能滿足他的需求？

A. ITIL

B. ISO 27002

三坐標測量機

D.PMBOK 指南

你回答正確！

ISO 27002 是一項專注於信息安全的國際標準，名為“信息技術——安全

技術——信息安全管理實踐守則”。信息技術基礎設施庫 (ITIL) 確實包含

安全管理實踐，但它不是文檔的唯一重點，ITIL 安全部分源自 ISO

27002。能力成熟度模型 (CMM) 側重於軟件開發，並且項目管理知識體

系 (PMBOK) 指南側重於項目管理。

問題 18

tb787631.CISSPPT3E.c01.050

Beth 是一名人力資源專家，準備協助解僱一名員工。以下哪項通常不是終止流程的一部分？

A. 離職面談
B. 追回財產
C. 賬戶終止
D. 簽署 NCA

您回答錯誤。

簽署競業禁止或保密協議通常是在招聘時完成的。離職面談、收回組織財產和終止賬戶都是終止流程的常見要素。在離職面談期間，團隊可能會選擇審查仍然有效的僱傭協議和政策，例如競業禁止或保密協議。

問題 19

tb787631.CISSPPT3E.c01.014

您正在完成業務連續性規劃工作，並決定要接受其中一項風險。接下來你應該做什麼？

A. 實施新的安全控制以降低風險級別。
B. 設計災難恢復計劃。
C. 重複業務影響評估。
D. 記錄你的決策過程。

你回答正確！

每當您選擇接受風險時，您都應該保留風險接受過程的詳細文檔，以便將來讓審計人員滿意。這應該在實施安全控制、設計災難恢復計劃或重複業務影響分析 (BIA) 之前發生。

問題 20

tb787631.CISSPPT3E.c01.010

Yolanda 是一家金融機構的首席隱私官，正在研究與客戶支票賬戶相關的隱私要求。以下哪一項法律最有可能適用於這種情況？

A. GLBA
B. SOX
C. HIPAA
D. FERPA

您回答錯誤。

Gramm-Leach-Bliley 法案 (GLBA) 包含規範客戶財務信息隱私的條款。它特別適用於金融機構。薩班斯奧克斯利法案 (SOX) 規範上市公司的財務報告活動。健康保險流通與責任法案 (HIPAA) 規範了受保護健康信息

(PHI) 的處理。家庭教育權利和隱私法案 (FERPA) 規定了學生教育記錄的處理。

問題 21

tb787631.CISSPPT3E.c01.031

Renee 正在為她的組織設計長期安全計劃，規劃範圍為三到五年。她的主要目標是使安全職能與更廣泛的業務計劃和目標保持一致。她正在製定什麼類型的計劃？

A. 可操作的
B.戰術
C. 總結
D. 戰略

你回答正確！

在大多數情況下，戰略計劃的長期規劃範圍長達五年。它們旨在從戰略上使安全功能與業務目標保持一致。作戰和戰術計劃的期限較短，為一年或更短。

問題 22

tb787631.CISSPPT3E.c01.057

James 正在為其組織進行風險評估，並試圖為其數據中心的服務器分配資產價值。該組織的主要關注點是確保它有足夠的資金可用於在數據中心損壞或毀壞時重建數據中心。在這種情況下，下列哪一種資產估值方法最合適？

A、採購成本

B. 折舊成本

C. 重置成本

D、機會成本

你回答正確！

如果組織最關心的是重建數據中心的成本，James 應該使用重置成本法

來確定等效服務器的當前市場價格。

問題 23

tb787631.CISSPPT3E.c01.049

請參考以下場景：

- Juniper Content 是一家網絡內容開發公司，擁有 40 名員工，分佈在兩個辦公室：一個在紐約，一個較小的辦公室在舊金山灣區。每個辦公室都有一個由外圍防火牆保護的局域網。局域網 (LAN) 包含連接到有線和無線網絡的現代交換機設備。
- 每個辦公室都有自己的文件服務器，信息技術 (IT) 團隊每小時運行一次軟件，在兩個服務器之間同步文件，在辦公室之間分發內容。這些服務器主要用於存儲與公司開發的網絡內容相關

的圖像和其他文件。該團隊還在大部分工作中使用基於 SaaS 的電子郵件和文檔協作解決方案。

- 您是 Juniper Content 新任命的 IT 經理，您正在努力增強現有的安全控制以提高組織的安全性。

最後，服務器上保存著對業務極其重要的歷史記錄，絕對不能修改。您想要添加一個完整性控制，允許您定期驗證文件未被修改。您可以添加什麼控件？

A.散列

B.ACL

C. 只讀屬性

D. 防火牆

您回答錯誤。

散列允許您通過計算驗證文件在散列計算之間是否未被修改。ACL 和只讀屬性是有用的控件，可以幫助您防止未經授權的修改，但它們無法驗證文件是否未被修改。防火牆是網絡安全控制，不驗證文件完整性。

問題 24

tb787631.CISSPPT3E.c01.036

以下哪一位通常負責履行高級管理層委派的運營數據保護職責，例如驗證數據完整性、測試備份和管理安全策略？

A. 數據保管人

B. 數據所有者

C、用戶

D. 審計員

你回答正確！

數據保管人角色被分配給負責實施政策和高級管理層定義的安全控制的個

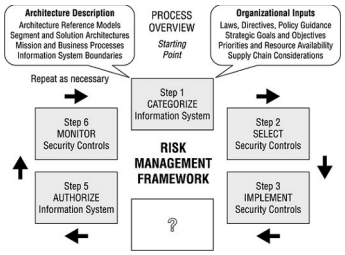
人。數據所有者確實對這些任務負有最終責任，但數據所有者通常是將運

營責任委派給數據保管人的高級領導。

問題 25

tb787631.CISSPPT3E.c01.062

下圖顯示了缺少步驟 4 的 NIST 風險管理框架。缺少的步驟是什麼？



A. 評估安全控制。

B. 確定控制差距。

C. 補救控制漏洞。

D. 評估用戶活動。

你回答正確！

NIST 風險管理框架的第四步是評估安全控制。這是該過程的重要組成部分。該組織已經對系統進行了分類，選擇了適當的控制措施，並實施了這些控制措施。在授權使用系統之前，他們必須評估這些控制措施的有效性，以確保它們滿足安全要求。

問題 26

tb787631.CISSPPT3E.c01.034

FISMA 的規定最有可能涵蓋以下哪一類組織？

A. 銀行
B. 國防承包商
C. 學區
D. 醫院

您回答錯誤。

美國聯邦信息安全管理法 (FISMA) 適用於聯邦政府機構和承包商。在列出的實體中，國防承包商最有可能擁有受 FISMA 約束的政府合同。

問題 27

tb787631.CISSPPT3E.c01.096

作為一家在線銀行的開發人員，Lisa 需要提交她的代碼進行測試和審查。通過此流程並獲得批准後，另一名員工將代碼移至生產環境。這個過程描述了什麼安全管理？

A. 回歸測試

B、代碼審查

C. 變革管理

D、模糊測試

你回答正確！

變更管理是一個關鍵的控製過程，涉及系統地管理變更。沒有它，Lisa 可能會在沒有監督、文檔或測試的情況下簡單地將她的代碼部署到生產環境中。回歸測試側重於測試以確保新代碼不會帶回舊缺陷，而模糊測試則為代碼提供意外輸入。代碼審查審查源代碼本身，可能涉及變更管理過程，但不是此處描述的內容。

問題 28

tb787631.CISSPPT3E.c01.063

HAL Systems 最近決定停止提供公共 NTP 服務，因為擔心其 NTP 服務器會被用於放大 DDoS 攻擊。HAL 對其 NTP 服務採取了何種風險管理策略？

A. 風險緩解

B. 風險接受

C. 風險轉移

D. 規避風險

你回答正確！

由於存在風險，HAL Systems 決定停止提供該服務。這是風險規避策略的一個例子。該公司以消除 NTP 濫用風險的方式改變了其運營方式。風險接受包括有意識地決定接受風險而不採取進一步行動。風險緩解採取措施降低風險的可能性和/或影響。風險轉移將風險成本轉移到另一個組織，例如保險公司。

問題 29

tb787631.CISSPPT3E.c01.047

請參考以下場景：

- Juniper Content 是一家網絡內容開發公司，擁有 40 名員工，分佈在兩個辦公室：一個在紐約，一個較小的辦公室在舊金山灣區。每個辦公室都有一個由外圍防火牆保護的局域網。局域網 (LAN) 包含連接到有線和無線網絡的現代交換機設備。

- 每個辦公室都有自己的文件服務器，信息技術 (IT) 團隊每小時運行一次軟件，在兩個服務器之間同步文件，在辦公室之間分發內容。這些服務器主要用於存儲與公司開發的網絡內容相關的圖像和其他文件。該團隊還在大部分工作中使用基於 SaaS 的電子郵件和文檔協作解決方案。

- 您是 Juniper Content 新任命的 IT 經理，您正在努力增強現有的安全控制以提高組織的安全性。

兩個辦公室的用戶希望通過 Internet 訪問彼此的文件服務器。什麼控制可以為這些通信提供機密性？

A. 數字簽名

B. 虛擬專用網

C. 虛擬局域網

D. 數字內容管理

您回答錯誤。

虛擬專用網絡 (VPN) 使用加密在其他不安全的網絡（例如互聯網）上提供安全的通信通道。如果您在兩個辦公室之間建立 VPN 連接，一個辦公室的用戶可以通過 Internet 安全地訪問位於另一個辦公室服務器上的內容。數字簽名用於提供不可否認性，而不是機密性。虛擬 LAN (VLAN)

在本地網絡上提供網絡分段，但不跨越 Internet。數字內容管理解決方案

旨在管理 Web 內容，而不是訪問位於文件服務器上的共享文件。

問題 30

tb787631.CISSPPT3E.c01.097

在完成安全意識計劃的第一年之後，Charles 查看了完成培訓的員工人數與分配培訓的員工人數的數據，以確定他是否達到了 95% 的完成率目標。這種措施叫什麼？

A. 關鍵績效指標

B. 一個指標

C. 意識控制

D.投資回報率

你回答正確！

Charles 正在跟踪一個關鍵績效指標 (KPI)。KPI 用於衡量績效（和成功）。如果沒有成功的定義，這將只是一個指標，但 Charles 正在朝著一個已知的目標努力，並且可以根據它進行衡量。本題沒有回報投資計算，措施不是對照。

問題 31

tb787631.CISSPPT3E.c01.003

Francine 是美國一家在線服務提供商的安全專家。她最近收到版權所有者的索賠，稱用戶在她的服務上存儲的信息侵犯了第三方的版權。什麼法律管轄弗朗辛必須採取的行動？

A. 版權法

B. 蘭哈姆法案

C. 數字千年版權法案

D. Gramm Leach Bliley 法案

您回答錯誤。

數字千年版權法案 (DMCA) 規定了在線服務提供商在處理來自第三方的版權投訴時的要求。《版權法》創建了發布和執行版權的機制，但不涵蓋在線服務提供商的行為。《蘭哈姆法》規範了商標的發行，以保護知識產權。Gramm-Leach-Bliley 法案規範了個人財務信息的處理。

第 32 題

tb787631.CISSPPT3E.c01.008

Henry 最近協助他的一位同事準備 CISSP 考試。在此過程中，Henry 洩露了有關考試內容的機密信息，這違反了道德規範的 Canon IV：“促進和保護職業。” 誰可以就此違規行為對 Henry 提出道德指控？

A. 任何人都可以提出指控。

B. 任何經過認證或許可的專業人士都可以提出指控。

C. 只有 Henry 的雇主可以提出指控。

D. 只有受影響的員工可以提出指控。

您回答錯誤。

這是一個關於誰有資格提出道德投訴的問題。具有地位的個人群體因違反的經典而異。在這種情況下，我們正在檢查 Canon IV，它允許任何訂閱道德規範的認證或許可專業人員提出指控。任何人都可以提出違反教規 I 或 II 的指控。對違反佳能 III 的指控只能由與被告有雇主/承包商關係的委託人提出。

問題 33

tb787631.CISSPPT3E.c01.028

Mary 正在幫助一位計算機用戶，他看到以下消息出現在他的計算機屏幕上。發生了什麼類型的攻擊？

A. 可用性

B. 保密

C. 披露

D、分佈式

你回答正確！

顯示的消息是勒索軟件的示例，它會對用戶計算機的內容進行加密以防止

合法使用。這是可用性攻擊的示例。沒有跡象表明數據已透露給他人，因

此不存在保密/披露風險。也沒有跡象表明其他系統參與了分佈式攻擊。

第 34 題

tb787631.CISSPPT3E.c01.023

在進行業務影響分析時，團隊應首先創建資產列表。接下來會發生什麼？

A. 識別每項資產中的漏洞。

B. 確定資產面臨的風險。

C. 為每項資產製定價值。

D. 確定每項資產面臨的威脅。

你回答正確！

制定資產清單後，業務影響分析團隊應為每項資產分配價值。此處列出的

其他活動僅在資產賦值後發生。

問題 35

tb787631.CISSPPT3E.c01.083

Rolando 是一家大型企業的風險經理。該公司最近評估了加利福尼亞泥石流對其在該地區運營的風險，並確定應對成本超過了它可以實施的任何控制措施的好處。該公司此時選擇不採取任何行動。羅蘭多的組織奉行什麼風險管理策略？

A. 規避風險
B. 風險緩解
C. 風險轉移
D. 風險接受

你回答正確！

在風險接受策略中，組織決定不採取任何行動是管理風險的最有利途徑。

問題 36

tb787631.CISSPPT3E.c01.041

高級管理人員通常在業務連續性計劃團隊中扮演什麼重要角色？

A. 仲裁關於關鍵性的爭議

B. 評估法律環境

C. 培訓人員

D. 設計故障控制

你回答正確！

高級管理人員扮演著多個業務連續性規劃角色。這些包括設置優先級、獲取資源和仲裁團隊成員之間的爭端。

問題 37

tb787631.CISSPPT3E.c01.080

Ben 負責存儲在數據庫中的支付卡信息的安全。政策指示他從數據庫中刪除信息，但由於操作原因他不能這樣做。他獲得了政策例外，並正在尋求適當的補償控制來降低風險。他最好的選擇是什麼？

A、購買保險

B. 加密數據庫內容

C. 刪除數據

D. 反對例外

您回答錯誤。

Ben 應該加密數據以提供額外的保護層作為補償控制。組織已經做了政

策例外，他不應該做出反對例外或擅自刪除數據的反應。購買保險可能會

轉移部分風險，但不是緩解控制措施。

問題 38

tb787631.CISSPPT3E.c01.099

以下哪項通常被視為供應鏈風險？（選擇所有符合條件的。）

A. 對手在運送給最終客戶之前篡改硬件

B. 攻擊者入侵組織在 IaaS 環境中運行的 Web 服務器

C. 對手使用社會工程來危害 SaaS 供應商的員工以獲取對客戶帳戶的訪問權限

D. 對手使用殭屍網絡進行拒絕服務攻擊

您回答錯誤。

當對手干擾從供應商向客戶交付商品或服務時，就會出現供應鏈風險。這

可能涉及在客戶收到硬件之前篡改硬件，或使用社會工程來危害供應商員

工。侵入在 IaaS 環境中運行的 Web 服務器不是供應鏈風險，因為 Web

服務器已經在客戶的控制之下。使用殭屍網絡進行拒絕服務攻擊不涉及任

何供應鏈元素。

第 39 題

tb787631.CISSPPT3E.c01.073

每年，Gary 都會收到他開戶的金融機構寄來的隱私通知。什麼法律要求機構向加里發送這些通知？

A. FERPA
B、GLBA
C. HIPAA
D. 高科技

你回答正確！

Gramm-Leach-Bliley 法案 (GLBA) 對金融機構制定了嚴格的隱私法規，

包括向客戶提供有關隱私慣例的書面通知。

問題 40

tb787631.CISSPPT3E.c01.055

Yolanda 正在編寫一份文檔，該文檔將提供有關組織中每個系統必須滿足的最低安全級別的配置信息。她正在準備什麼類型的文件？

一項政策

B. 基線

C. 指南

D. 程序

你回答正確！

基線提供了整個組織中的每個系統都必須滿足的最低安全級別。此類信息

不會出現在政策、指南或程序中。

問題 41

tb787631.CISSPPT3E.c01.015

您正在完成對用於保護組織中媒體存儲設施的控件的審查，並希望對當前存在的每個控件進行正確分類。以下哪個控制類別準確描述了設施周圍的圍欄？（選擇所有符合條件的。）

A. 物理的

B.偵探

C. 威懾力

D. 預防

您回答錯誤。

柵欄沒有檢測入侵的能力。但是，它確實具有防止和阻止入侵的能力。柵

欄是物理控制的一個例子。

問題 42

tb787631.CISSPPT3E.c01.094

John 正在分析針對他公司的一次攻擊，攻擊者在 HTML 代碼中發現了嵌入的註釋，這些註釋提供了利用軟件漏洞所需的線索。使用 STRIDE 模型，他發現了哪種類型的攻擊？

A. 欺騙
B. 否認
C、信息披露
D. 特權提升

您回答錯誤。

信息洩露攻擊依賴於洩露私人、機密或受控信息。嵌入 HTML 代碼中的

編程註釋是此類攻擊的一個示例。

問題 43

tb787631.CISSPPT3E.c01.019

Brenda 的組織最近完成了對一家競爭對手公司的收購。以下哪一項任務最不可能成為收購期間處理的組織流程的一部分？

A. 安全功能的整合

B. 安全工具的集成

C. 知識產權保護

D. 安全政策文件

你回答正確！

在資產剝離過程中，知識產權保護是一個更大的問題，在資產剝離過程中，一家子公司被剝離到一個單獨的組織中，而不是在一家公司購買另一家公司的收購過程中。採購問題包括整合安全功能和策略以及集成安全工具。

問題 44

tb787631.CISSPPT3E.c01.033

Acme Widgets Company 正在為其會計部門實施新的控制措施。管理層擔心流氓會計師可能會創建一個新的虛假供應商，然後向該供應商開出支票作為對從未提供的服務的付款。什麼安全控制最能幫助防止這種情況發生？

A. 強制休假

B. 職責分離

C、縱深防禦

D. 工作輪換

你回答正確！

當遵循職責分離原則時，組織將關鍵任務分成離散的部分，並確保沒有人

有能力執行這兩項操作。這可以防止單個流氓個人以未經授權的方式執行

該任務。強制休假和工作輪換旨在發現欺詐，而不是防止欺詐。縱深防禦

不是這裡的相關原則，因為答案是尋求初步控制。我們可能會選擇在以後

添加額外的控制，但這裡的主要目標是實施職責分離。

問題 45

tb787631.CISSPPT3E.c01.084

海倫是一家美國網站的所有者，該網站為初中和高中學生準備考試提供信息。她正在撰寫網站的隱私政策，並希望確保其符合兒童在線隱私保護法 (COPPA) 的規定。根據 COPPA，父母必須提前同意從他們的孩子那裡收集個人信息的截止年齡是多少歲？

A.13
B. 15
C. 17
D. 18

你回答正確！

COPPA 要求網站收集 13 歲以下兒童的個人信息必須事先獲得父母的同意。

問題 46

tb787631.CISSPPT3E.c01.093

請參考以下場景：

- Henry 是美國中西部度假社區 Atwood Landing 的風險經理。該度假村的主要數據中心位於印第安納州北部一個容易發生龍捲風的地區。Henry 最近進行了重置成本分析，並確定重建和重新配置數據中心將花費 1000 萬美元。
- 亨利諮詢了龍捲風專家、數據中心專家和結構工程師。他們共同確定，一次典型的龍捲風會對設施造成大約 500 萬美元的損失。氣象學家確定阿特伍德的設施所在的區域可能會每 200 年發生一次龍捲風。

根據此情景中的信息，Atwood Landing 數據中心龍捲風的年損失預期是多少？

A. 25,000 美元
B. 50,000 美元
C. 250,000 美元
D. 500,000 美元

您回答錯誤。

年化損失預期是通過將單次損失預期 (SLE) 乘以年化發生率 (ARO) 計算得出的。在這種情況下，SLE 為 5,000,000 美元，ARO 為 0.005。將這些數字相乘得到 25,000 美元的 ALE。

問題 47

tb787631.CISSPPT3E.c01.076

以下哪一個利益相關者通常不包括在業務連續性計劃團隊中？

A. 核心業務職能負責人
B. 信息技術人員
C、首席執行官
D. 支持部門

您回答錯誤。

雖然 BCP 團隊中應該有高級管理層的代表，但 CEO 親自擔任這一角色是極不尋常的。

問題 48

tb787631.CISSPPT3E.c01.005

在對其組織進行定性風險評估後，Sally 建議購買網絡安全漏洞保險。她推薦哪種類型的風險應對行為？

A.接受

B、轉移

C.減少

D、拒絕

你回答正確！

購買保險是一種轉移風險的手段。如果 Sally 曾努力降低事件發生的可能性，她就會使用減少或風險緩解策略，而簡單地繼續按照組織的方式運作將是接受策略的一個例子。拒絕或否認風險不是有效的策略，即使它發生了！

問題 49

tb787631.CISSPPT3E.c01.009

Wanda 正與其組織的歐盟業務合作夥伴之一合作，以促進客戶信息的交換。萬達的機構設在美國。萬達確保 GDPR 合規性的最佳方法是什麼？

A. 具有約束力的公司規則

B. 隱私盾

C. 標準合同條款

D. 安全港

您回答錯誤。

歐盟提供了可用於促進數據傳輸的標準合同條款。在兩家不同的公司共享數據的情況下，這將是最佳選擇。如果數據在公司內部共享，則具有約束力的公司規則也是一種選擇。歐盟/美國隱私盾是一個安全港協議，以前允許傳輸但不再有效。

第 50 題

tb787631.CISSPPT3E.c01.053

Jeff 希望採用行業標準方法來評估他的組織用於管理風險的流程。哪種成熟度模型最適合他使用？

A. 三坐標測量機
B. 軟件三坐標測量機
C、RMM
D.COBIT

您回答錯誤。

風險成熟度模型 (RMM) 專為評估企業風險管理計劃而設計。Jeff 可以想像使用更通用的能力成熟度模型 (CMM)，但這不太合適。軟件能力成熟

度模型 (SW-CMM) 旨在評估開發項目，而不是風險管理工作。信息技術

控制目標 (COBIT) 是一組安全控制目標，而不是成熟度模型。

問題 51

tb787631.CISSPPT3E.c01.016

Tony 正在製定一項業務連續性計劃，但由於難以將有關有形資產和無形資產的信息結合起來，因此難以確定資源的優先級。對他來說，最有效的風險評估方法是什麼？

A. 定量風險評估
B. 定性風險評估
C. 既不定量也不定性的風險評估
D. 定量和定性風險評估相結合

你回答正確！

通過結合定量和定性風險評估的要素，Tony 會看到最好的結果。定量風險評估擅長分析金融風險，而定性風險評估是分析無形風險的好工具。結合這兩種技術可以提供全面的風險圖景。

問題 52

tb787631.CISSPPT3E.c01.058

羅傑的組織遭受了客戶信用卡記錄的破壞。根據 PCI DSS 的條款，哪個組織可以選擇對此事進行調查？

A. 聯邦調查局

B. 地方執法

C、銀行

D. PCI 共享服務中心

你回答正確！

PCI DSS 是由支付卡行業安全標準委員會 (PCI SSC) 頒布的標準，但通過商家與其銀行之間的合同關係強制執行。因此，銀行將是根據 PCI DSS 發起調查的合適實體。如果情況允許，地方和聯邦執法機構（例如 FBI）可以決定進行刑事調查，但他們無權執行 PCI DSS 要求。

問題 53

tb787631.CISSPPT3E.c01.013

Bobbi 正在調查一起安全事件，發現攻擊者從普通用戶帳戶開始，但設法利用系統漏洞為該帳戶提供管理權限。在 STRIDE 威脅模型下發生了什麼類型的攻擊？

A. 欺騙

B. 否認

C. 篡改

D. 特權提升

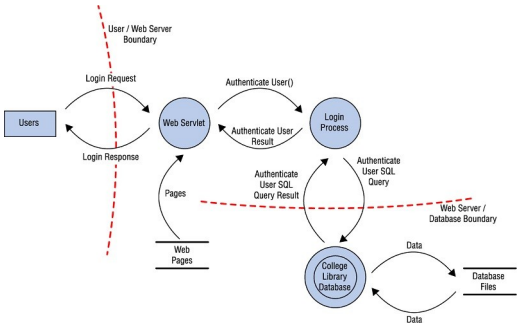
您回答錯誤。

在特權提升攻擊中，攻擊者將有限的用戶帳戶轉換為具有更高特權、權力和/或對系統的訪問權限的帳戶。欺騙攻擊偽造身份，而否認攻擊則試圖否認對行為的責任。篡改攻擊試圖破壞信息或資源的完整性。

問題 54

tb787631.CISSPPT3E.c01.087

艾倫正在執行威脅建模，並決定將系統分解為此處顯示的核心元素會很有用。他用什麼工具？



A. 脆弱性評估

B. 模糊測試

C.還原分析

D. 數據建模

您回答錯誤。

在還原分析中，安全專業人員將系統分解為五個核心元素：信任邊界、數據流路徑、輸入點、特權操作和安全控制細節。

問題 55

tb787631.CISSPPT3E.c01.079

Ryan 是一名在非營利組織工作的 CISSP 認證網絡安全專家。以下哪些道德義務適用於他的工作？（選擇所有符合條件的。）

A. (ISC)^2 道德規範

B. 組織道德守則

C. 聯邦道德守則

D.RFC 1087

你回答正確！

所有 (ISC)^2 認證的專業人員都必須遵守 (ISC)^2 道德規範。組織的所有員工都必須遵守組織的道德規範。聯邦道德準則（或更正式地說，政府服務道德準則）不適用於非營利組織，因為它僅適用於聯邦僱員。RFC 1087 確實為互聯網提供了道德規範，但它對任何個人都沒有約束力。

問題 56

tb787631.CISSPPT3E.c01.095

Chris 擔心他的組織最近購買的筆記本電腦在交付前被第三方修改以包含鍵盤記錄程序。他應該在哪裡集中精力來防止這種情況發生？

A. 他的供應鏈

B. 他的供應商合同

C. 他購買後的構建過程

D.原始設備製造商（OEM）

您回答錯誤。

供應鏈管理可以幫助確保組織獲得的硬件、軟件和服務的安全性。Chris 應該關注他的膝上型電腦從原始設備製造商到交付的每個步驟。

問題 57

tb787631.CISSPPT3E.c01.017

文森特認為，一名前僱員從他的公司獲取了商業秘密信息，並將其帶給了競爭對手。他想採取法律行動。他可以根據什麼法律起訴？

A. 著作權法

B. 蘭哈姆法案

C. 格拉斯-斯蒂格爾法案

D. 經濟間諜法

你回答正確！

《經濟間諜法》對任何被認定犯有竊取美國公司商業機密罪的人處以罰款和監禁。它真正保護了商業秘密所有者的知識產權。版權法不適用於這種情況，因為沒有跡象表明該信息受版權保護。《蘭哈姆法》適用於商標保護案件。格拉斯-斯蒂格爾法案是一項銀行業改革法案，與這種情況無關。

問題 58

tb787631.CISSPPT3E.c01.007

Renee 正在與她的董事會討論他們審查網絡安全控制的責任。什麼規則要求高級管理人員對信息安全事務承擔個人責任？

A. 盡職調查規則
B. 個人責任規則
C. 審慎人治
D. 正當程序規則

你回答正確！

審慎的人規則要求高級管理人員承擔個人責任，以確保普通審慎的人在相同情況下會行使應有的注意。該規則最初適用於金融事務，但聯邦量刑指南於 1991 年將其適用於美國的信息安全事務。

問題 59

tb787631.CISSPPT3E.c01.056

誰應該在組織中接受初始業務連續性計劃培訓？

A、高級管理人員

B. 具有特定業務連續性角色的人員

C. 組織中的每個人

D. 急救人員

你回答正確！

組織中的每個人都應該接受有關業務連續性計劃的性質和範圍的基本培訓。

那些具有特定角色的人，如急救人員和高級管理人員，也應該接受詳細的、針對特定角色的培訓。

問題 60

tb787631.CISSPPT3E.c01.042

您是一家大型醫院系統的 CISO，正準備與軟件即服務 (SaaS) 電子郵件供應商簽訂合同，並希望執行控制評估以確保其業務連續性計劃措施合理。您可能要求進行哪種類型的審計來實現此目標？

A.SOC 1

B. FISHMA

C. PCI DSS

D.SOC 2

你回答正確！

服務組織控制審計計劃包括 SOC 2 中的業務連續性控制，但不包括

SOC 1 審計。儘管 FISMA 和 PCI DSS 可以審核業務連續性，但它們不

適用於醫院使用的電子郵件服務。

問題 61

tb787631.CISSPPT3E.c01.066

Chas 最近完成了其組織的業務連續性計劃的製定。誰是批准組織業務連續性計劃的理想人選？

A. 首席信息官

B、首席執行官

C. 首席信息安全官

D、首席運營官

你回答正確！

儘管 CEO 通常不會在 BCP 團隊任職，但最好為您的計劃獲得高層管理

人員的批准，以增加成功採用的可能性。

第 62 題

tb787631.CISSPPT3E.c01.051

Frances 正在審查其組織的業務連續性計劃文檔的完整性。以下哪一項通常不包含在業務連續性計劃文檔中？

A. 賬目報表
B. 重要性聲明
C. 優先事項說明
D. 組織責任聲明

你回答正確！

業務連續性計劃文件通常包括連續性計劃目標、重要性聲明、優先級聲明、組織責任聲明、緊迫性和時間安排聲明、風險評估和風險接受與緩解文件、重要記錄程序、應急響應指南，以及用於維護和測試計劃的文檔。

問題 63

tb787631.CISSPPT3E.c01.069

Becka 最近與備用數據處理設施簽訂了一份合同，該設施將在發生災難時為她的公司提供空間。該設施包括 HVAC、電源和通信電路，但不包括硬件。Becka 使用什麼類型的設施？

A、冷場
B、暖場
C、熱點站點
D、手機網站

你回答正確！

冷站點包括數據中心運營所需的基本能力：空間、電力、HVAC 和通信 ，

但不包括恢復運營所需的任何硬件。熱站點、熱站點和移動站點都將包含

硬件。

第 64 題

tb787631.CISSPPT3E.c01.030

John 的網絡開始出現緩慢的症狀。經過調查，他意識到網絡正受到 TCP SYN 數據包的轟炸，並認為他的組織是拒絕服務攻擊的受害者。違反了什麼信息安全原則？

A. 可用性
B. 誠信
C. 保密
D. 拒絕

你回答正確！

smurf 攻擊是拒絕服務攻擊的一個例子，它危及目標網絡的可用性 。

Smurf 攻擊不針對完整性或機密性。雖然這是拒絕服務攻擊，但拒絕並

不是正確的答案，因為系統會詢問您違反了哪條原則，而不是發生了哪種

類型的攻擊。拒絕服務攻擊以資源可用性為目標。

問題 65

tb787631.CISSPPT3E.c01.089

在嘗試評估故障對客戶信心的影響時，哪種類型的業務影響評估工具最合適？

A. 定量

B. 定性

C. 年化損失預期

D. 減少

你回答正確！

定性工具通常用於業務影響評估，以捕捉對客戶信心、員工士氣和聲譽等

無形因素的影響。

第 66 題

tb787631.CISSPPT3E.c01.098

以下哪項通常不包括在僱用前篩選過程中？

A. 藥物測試

B. 背景調查

C. 社交媒體評論

D. 健身評估

您回答錯誤。

適合度評估不是招聘過程的典型部分。藥物測試、背景調查和社交媒體調

查都是當前招聘實踐的常見部分。

問題 67

tb787631.CISSPPT3E.c01.012

克里斯正在為來自他的組織的旅行者提供建議，這些旅行者將訪問海外許多不同的國家。他擔心遵守出口管制法律。以下哪種技術最有可能觸發這些法規？

A、存儲芯片

B. 辦公生產力應用

C、硬盤

D、加密軟件

你回答正確！

向某些國家/地區出口加密軟件受美國出口管制法的管制。這些法規不太

可能涵蓋內存芯片、辦公生產力應用程序和硬盤驅動器。

第 68 題

tb787631.CISSPPT3E.c01.025

勞拉被要求執行 SCA。她最有可能在什麼類型的組織中？

A. 高等教育

B. 銀行業

C. 政府

D. 醫療保健

你回答正確！

安全控制評估 (SCA) 通常是指美國政府評估安全控制的正式流程，通常與安全測試和評估 (ST&E) 流程搭配使用。這意味著 Laura 可能是政府組織或承包商的一部分。

第 69 題

tb787631.CISSPPT3E.c01.040

以下哪一個人是信息安全計劃最有效的組織負責人？

A. CISSP 認證分析師

B、首席信息官（CIO）

C. 網絡安全經理

D. 總裁兼首席執行官

你回答正確！

信息安全程序的所有者可能不同於負責實施控制的個人。此人應盡可能資

深，能夠專注於安全計劃的管理。總裁兼首席執行官將不是一個合適的選

擇，因為這個級別的高管不太可能有必要的時間專注於安全。在剩下的選

擇中，CIO 是最高級的職位，他將成為行政級別最有力的支持者。

第 70 題

tb787631.CISSPPT3E.c01.064

Susan 正在與她公司的管理團隊合作對數據進行分類，以嘗試應用額外的安全控制來限制數據洩露的可能性。Susan 試圖執行什麼信息安全原則？

A. 可用性
B. 拒絕
C. 保密
D. 誠信

您回答錯誤。

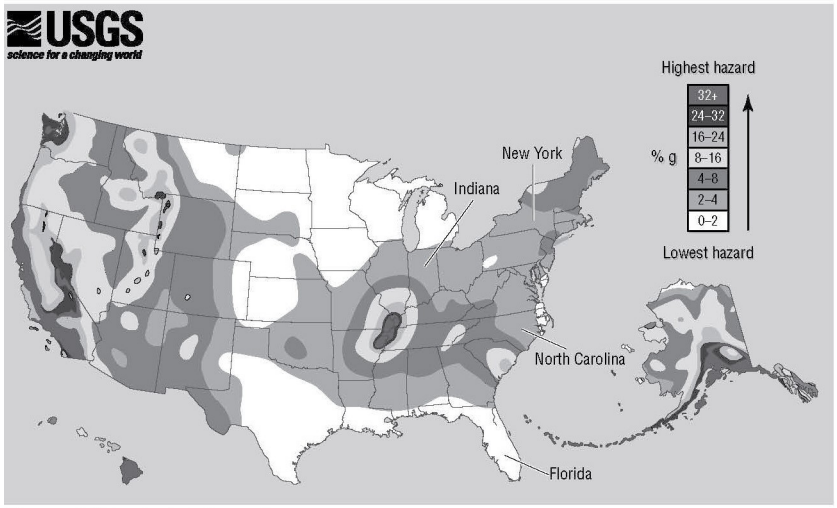
保密控制可防止將敏感信息洩露給未經授權的個人。限制數據洩露的可能

性是為了防止未經授權的披露。

第 71 題

tb787631.CISSPPT3E.c01.088

Craig 正在為新數據中心選址，必須選擇美國境內的某個位置。他從美國地質調查局獲得了這裡顯示的地震風險圖。如果他主要擔心地震風險，那麼以下哪一個是最安全的設施建設地點？



(Source: US Geological Survey)

A、紐約

B. 北卡羅來納州

C. 印第安納州

D. 佛羅里達州

你回答正確！

在列出的各州中，佛羅里達州是唯一一個未用陰影表示大地震嚴重風險的州。

第 72 題

tb787631.CISSPPT3E.c01.082

Tom 計劃今天下午以欺詐為由解僱一名員工，並預計這次會議會有些敵意。他正在協調與人力資源部的會議，並希望保護公司免受損害。以下哪一個步驟對於及時協調終止會議最重要？

A. 將終止通知其他員工

B. 檢索員工的照片 ID

C. 計算最終薪水

D. 撤銷電子訪問權限

您回答錯誤。

必須仔細協調對公司資源的電子訪問。在被終止後保留訪問權限的員工可以使用該訪問權限採取報復行動。另一方面，如果過早終止訪問，員工可能會發現他或她即將被終止。

第 73 題

tb787631.CISSPPT3E.c01.090

Ryan 是一家保險公司的安全風險分析師。他目前正在研究一種情況，在這種情況下，由於公司 Web 應用程序中缺少補丁，惡意黑客可能會使用 SQL 注入攻擊來破壞 Web 服務器。在這種情況下，威脅是什麼？

A. 未打補丁的 Web 應用程序

B. 網頁污損

C、惡意黑客

D、操作系統

你回答正確！

風險是威脅和脆弱性的結合。威脅是尋求破壞安全的外部力量，例如本例中的惡意黑客。漏洞是可能使威脅得逞的內部弱點。在這種情況下，缺少的補丁就是漏洞。在這種情況下，如果惡意黑客（威脅）試圖對未打補丁的服務器（漏洞）進行 SQL 注入攻擊，結果就是網站被篡改。

第 74 題

tb787631.CISSPPT3E.c01.067

以下哪一項行動通常不是業務連續性計劃的項目範圍和計劃階段的一部分？

A. 組織結構分析
B. 審查法律和監管環境
C. 創建 BCP 團隊
D. 計劃文件

您回答錯誤。

項目範圍和規劃階段包括四項行動：組織的結構化分析、BCP 團隊的創建、可用資源的評估以及法律和監管環境的分析。

第 75 題

tb787631.CISSPPT3E.c01.068

Gary 正在實施一種新的網站架構，該架構在負載平衡器後面使用多個小型 Web 服務器。Gary 尋求執行什麼信息安全原則？

A. 拒絕
B. 保密
C. 誠信
D. 可用性

你回答正確！

保持服務器正常運行是可用性控制的一個示例，因為它增加了服務器保持可用以響應用戶請求的可能性。

第 76 題

tb787631.CISSPPT3E.c01.022

以下哪一項行動可以作為業務連續性計劃的一部分？

A. 從備份磁帶恢復
B. 實施 RAID
C. 搬遷到寒冷的地方
D. 重新開始業務運營

你回答正確！

RAID 技術為硬盤驅動器故障提供容錯能力，是業務連續性行動的一個例子。從備份磁帶恢復、遷移到冷站點、重新開始業務運營都是災難恢復動作。

第 77 題

tb787631.CISSPPT3E.c01.002

Gavin 正在就他最近的風險評估結果向管理層提交一份報告。在他的報告中，他想確定在採用安全控制措施後組織面臨的剩餘風險級別。哪個術語最能描述當前的風險水平？

A. 固有風險
B. 剩餘風險
C、控制風險
D. 減輕風險

你回答正確！

剩餘風險是在應用控制以減輕風險後仍然存在的風險水平。固有風險是控制之前存在的原始風險。控制風險是由於對環境增加控製而引入的新風險。減輕的風險是已通過現有控制措施解決的風險。

第 78 題

tb787631.CISSPPT3E.c01.024

Mike 最近實施了一個入侵防禦系統，旨在阻止常見的網絡攻擊影響他的組織。Mike 奉行哪種風險管理策略？

A. 風險接受

B、風險規避

C. 風險緩解

D. 風險轉移

你回答正確！

風險緩解策略試圖降低風險發生的可能性和/或影響。入侵防禦系統試圖降低成功攻擊的可能性，因此是風險緩解的例子。風險接受包括有意識地決定接受風險而不採取進一步行動。規避風險會改變業務活動，使風險變得無關緊要。風險轉移將風險成本轉移到另一個組織，例如保險公司。

第 79 題

tb787631.CISSPPT3E.c01.045

以下哪一項問題通常不會在服務級別協議 (SLA) 中解決？

A. 客戶信息的保密

B、故障轉移時間

C. 正常運行時間

D. 最大連續停機時間

你回答正確！

SLA 通常不解決數據機密性問題。這些條款通常包含在保密協議 (NDA)

中。

問題 80

tb787631.CISSPPT3E.c01.075

(ISC) 2 道德規範適用於所有 CISSP 持有者。以下哪項不是該法典的四大強制性準則之一？

A. 保護社會、共同利益、必要的公眾信任和信心以及基礎設施。

B. 披露違反隱私、信任和道德的行為。

C. 為原則提供勤奮和稱職的服務。

D. 促進和保護職業。

你回答正確！

(ISC) 2 道德準則還包括“以誠實、誠實、公正、負責任和合法的方式行事

”，但沒有特別要求證書持有人披露所有違反隱私、信任或道德的行為。

問題 81

tb787631.CISSPPT3E.c01.052

Doolittle Industries 的一名會計員工最近因參與貪污計劃而被捕。該員工將錢轉入個人賬戶，然後每天在其他賬戶之間轉移資金，以掩飾欺詐行為長達數月之久。以下哪一項控制可能最有助於及早發現此欺詐行為？

A. 職責分離

B. 最小權限

C、縱深防禦

D. 強制休假

你回答正確！

強制休假計劃要求員工每年連續休假一段時間，並在這段時間內取消他們的系統特權。這些規定的休假期的目的是破壞任何企圖進行必要的掩蓋行動以隱藏欺詐並導致暴露威脅的企圖。職責分離、最小特權和深度防禦控制都可能有助於首先防止欺詐，但不太可能加快對已經發生的欺詐的檢測。

問題 82

tb787631.CISSPPT3E.c01.001

Alyssa 負責其組織的安全意識計劃。她擔心技術的變化可能會使內容過時。她可以採取什麼控制措施來防範這種風險？

A. 遊戲化

B. 基於計算機的培訓

C. 內容審查

D、現場訓練

你回答正確！

Alyssa 應該使用定期的內容審查來持續驗證她的計劃中的內容是否滿足

組織的需求，並且根據不斷變化的風險形勢是最新的。她可以結合使用基

於計算機的培訓、現場培訓和遊戲化來做到這一點，但這些技術不一定能

驗證內容是否已更新。

問題 83

tb787631.CISSPPT3E.c01.070

Greg 的公司最近發生了一起涉及許多客戶個人數據的重大數據洩露事件。他們應該審查哪些違反法律以確保他們採取適當的行動？

A. 違反總部所在州的法律。

B. 違反他們開展業務所在州的法律。

C. 只有聯邦違反法律。

D. 違反法律只涉及政府機構，不涉及私營企業。

你回答正確！

一般而言，公司應了解其開展業務的任何地點的違規法律。美國各州有各種各樣的違規法律和要求，這意味著在這種情況下，Greg 的公司可能需要審查許多不同的違規法律，以確定他們在該州或與該州居民開展業務時可能需要遵守哪些法律。

問題 84

tb787631.CISSPPT3E.c01.059

Rick 最近在其組織的每個業務部門中聘請了關鍵員工，請求他們協助實施他的安全意識計劃。他們將負責與同行分享安全信息並回答有關網絡安全問題的問題。哪個術語最能描述這種關係？

A. 安全冠軍
B、安全專家
C. 遊戲化
D. 同行評審

你回答正確！

這是一個安全冠軍計劃的示例，該計劃使用在業務部門中擔任其他角色的個人來共享安全消息傳遞。擔任這些角色的個人不一定是安全專家，也沒有同行評審的角色。

問題 85

tb787631.CISSPPT3E.c01.065

組織的應急響應指南中應包括以下哪一個組成部分？

A. 應通知緊急事件的人員名單
B. 長期業務連續性協議
C. 組織冷站啟動程序
D. 訂購設備的聯繫信息

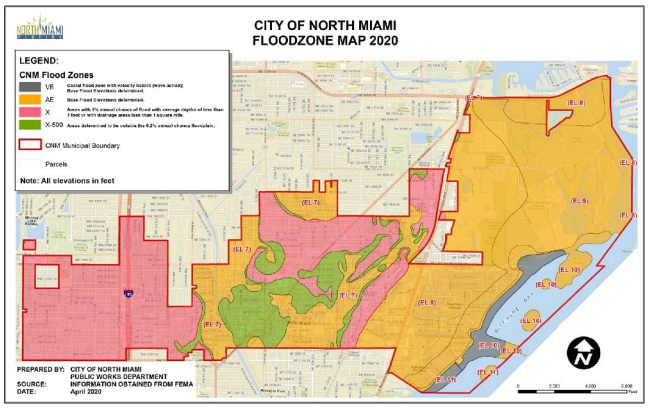
你回答正確！

應急響應指南應包括組織在響應緊急情況時應立即採取的步驟。其中包括即時響應程序、應通知緊急情況的人員名單以及第一響應者的二級響應程序。它們不包括長期操作，例如激活業務連續性協議、訂購設備或激活 DR 站點。

問題 86

tb787631.CISSPPT3E.c01.085

Tom 正在考慮在佛羅里達州邁阿密市中心地區開設一家公司。他查閱了此處顯示的該地區的 FEMA 洪氾區地圖，並確定他正在考慮的區域位於 100 年一遇的洪氾區內。該地區洪水的 ARO 是多少？



答：100

B.1

C.0.1

D、0.01

你回答正確！

年化發生率 (ARO) 是您預計每年風險發生的頻率。在 100 年一遇的洪氾區，風險分析師預計洪水每 100 年發生一次，即每年 0.01 次。

問題 87

tb787631.CISSPPT3E.c01.027

國際信息系統安全認證聯盟使用此處顯示的徽標在網上和各種論壇中代表自己。它可以使用什麼類型的知識產權保護來保護其在該標識中的權利？

(ISC)²

一、版權

B、專利

C、商業秘密

D、商標

你回答正確！

商標保護擴展到用於代表市場中的組織、產品或服務的文字和符號。版權用於保護創意作品。專利和商業秘密用於保護髮明和類似的知識產權。

問題 88

tb787631.CISSPPT3E.c01.044

貝絲是公立學區的安全管理員。她正在實施一個新的學生信息系統，並正在測試代碼以確保學生無法更改自己的成績。Beth 執行的信息安全原則是什麼？

A. 誠信

B. 可用性

C. 保密

D. 拒絕

你回答正確！

完整性控制，例如 Beth 在本例中實施的控制，旨在防止未經授權修改信息。沒有證據表明針對可用性或機密性的攻擊。拒絕是攻擊者的目標，而不是安全專業人員的目標，並且與以完整性為目標的這種情況無關。

問題 89

tb787631.CISSPPT3E.c01.092

請參考以下場景：

- Henry 是美國中西部度假社區 Atwood Landing 的風險經理。該度假村的主要數據中心位於印第安納州北部一個容易發生龍捲風的地區。Henry 最近進行了重置成本分析，並確定重建和重新配置數據中心將花費 1000 萬美元。
- 亨利諮詢了龍捲風專家、數據中心專家和結構工程師。他們共同確定，一次典型的龍捲風會對設施造成大約 500 萬美元的損失。氣象學家確定阿特伍德的設施所在的區域可能會每 200 年發生一次龍捲風。

根據此情景中的信息，Atwood Landing 數據中心龍捲風的年發生率是多少？

答：0.0025

B、0.005

C.0.01

D、0.015

您回答錯誤。

年化發生率是風險分析師預計風險在任何給定年份發生的次數。在這種情

況下，分析師預計龍捲風每 200 年發生一次，即每年 0.005 次。

問題 90

tb787631.CISSPPT3E.c01.077

Ben 正在為一家銀行設計消息傳遞系統，他希望包含一項功能，允許消息的接收者向第三方證明該消息確實來自聲稱的發件人。Ben 想要達到什麼目標？

A. 認證

B、授權

C. 誠信

D. 不可否認性

你回答正確！

不可否認性允許收件人向第三方證明消息來自聲稱的來源。身份驗證將向

Ben 證明發件人是真實的，但 Ben 無法向第三方證明這一點。

問題 91

tb787631.CISSPPT3E.c01.091

請參考以下場景：

- Henry 是美國中西部度假社區 Atwood Landing 的風險經理。該度假村的主要數據中心位於印第安納州北部一個容易發生龍捲風的地區。Henry 最近進行了重置成本分析，並確定重建和重新配置數據中心將花費 1000 萬美元。
- 亨利諮詢了龍捲風專家、數據中心專家和結構工程師。他們共同確定，一次典型的龍捲風會對設施造成大約 500 萬美元的損失。氣象學家確定阿特伍德的設施所在的區域可能會每 200 年發生一次龍捲風。

根據此情景中的信息，龍捲風對 Atwood Landing 數據中心的影響的暴露因子是多少？

A. 10%

B、25%

C. 50%

D、75%

您回答錯誤。

暴露係數是風險管理者預計在風險發生時將受損的設施的百分比。它的計算方法是將損失金額除以資產價值。在這種情況下，這是 500 萬美元的損失除以 1000 萬美元的設施價值，即 50%。

問題 92

tb787631.CISSPPT3E.c01.037

艾倫在一家電子商務公司工作，該公司最近有一些內容被另一個網站竊取並未經許可重新發布。哪種類型的知識產權保護最能保護艾倫公司的權利？

A、商業秘密

B.版權

C、商標

D.專利

你回答正確！

書面作品，例如網站內容，通常受版權法保護。商業秘密狀態在這裡不合適，因為內容是在線的並且可以在公司外部獲得。專利保護髮明，商標保護用於代表品牌的文字和符號，在這種情況下兩者都不相關。

問題 93

tb787631.CISSPPT3E.c01.074

以下哪一項協議通常要求供應商不得披露在業務範圍內獲悉的機密信息？

A. NCA

B、服務水平協議

C. 保密協議

D. 反收購行動

你回答正確！

保密協議 (NDA) 通常要求在業務關係中相互保密或單向保密。服務水平協議規定了服務正常運行時間和其他績效衡量標準。競業禁止協議 (NCA) 限制了員工未來的就業可能性。恢復時間目標 (RTO) 用於業務連續性規劃。

問題 94

tb787631.CISSPPT3E.c01.011

Tim 的組織最近收到一份合同，作為政府承包商開展贊助研究。什麼法律現在可能適用於本合同中涉及的信息系統？

A、FISMA
B. PCI DSS
C. HIPAA
D. 吉斯拉

你回答正確！

聯邦信息安全管理法 (FISMA) 特別適用於政府承包商。政府信息安全改革法案 (GISRA) 是 FISMA 的前身，於 2002 年 11 月到期。HIPAA 和 PCI DSS 分別適用於醫療保健和信用卡信息。

問題 95

tb787631.CISSPPT3E.c01.072

馬特在一家電信公司工作，一名聯邦特工找到他，尋求協助根據搜查令竊聽馬特的一位客戶。以下哪一項法律要求通信服務提供商配合執法請求？

A.ECPA

B. 路徑

C. 隱私法

D. 高科技法案

您回答錯誤。

《執法通信協助法》(CALEA) 要求所有通信運營商為擁有適當法院命令的執法人員提供竊聽服務。

問題 96

tb787631.CISSPPT3E.c01.006

以下哪一項信息元素不被視為會觸發大多數美國 (US) 州數據洩露法律的個人身份信息？

A. 學生證號碼

B. 社會安全號碼

C、駕照號碼

D. 信用卡號碼

您回答錯誤。

大多數州的數據洩露通知法均以加利福尼亞州的數據洩露通知法為藍本，

其中涵蓋社會保險號、駕照號、州身份證號、信用卡/借記卡號和銀行帳

號（連同 PIN 或密碼）。加利福尼亞州的違規通知法還保護其他州法律

中不常見的一些項目，包括醫療記錄和健康保險信息。這些法律獨立於隱

私法，例如更廣泛地規範個人信息處理的加州消費者隱私法 (CCPA)。

問題 97

tb787631.CISSPPT3E.c01.060

弗蘭克在公司首席執行官的筆記本電腦上發現了隱藏的鍵盤記錄器。鍵盤記錄器最有可能破壞什麼信息安全原則？

A. 保密
B. 誠信
C. 可用性
D. 拒絕

你回答正確！

鍵盤記錄器監視個人的擊鍵並將其報告給攻擊者。它們旨在竊取敏感信息，

破壞機密性目標。

問題 98

tb787631.CISSPPT3E.c01.018

以下哪一項原則對個人施加了寬泛且等同於人們在這種情況下對一個合理的人的期望的注意標準？

A. 盡職調查

B. 職責分離

C. 應有的注意

D. 最小特權

您回答錯誤。

應有的注意原則規定，個人應對情況做出反應時應使用與任何合理的人所期望的相同程度的注意。這是一個非常廣泛的標準。盡職調查原則是應有註意的一個更具體的組成部分，它規定被分配責任的個人應該盡到應有的注意，準確及時地完成它。

問題 99

tb787631.CISSPPT3E.c01.004

FlyAway Travel 在歐盟 (EU) 和美國均設有辦事處，並定期在這些辦事處之間傳輸個人信息。他們最近收到了一位歐盟客戶的請求，要求終止他們的帳戶。

根據一般數據保護條例 (GDPR)，處理個人信息的哪項要求規定個人可以要求不再傳播或處理他們的數據？

A. 訪問權

B. 隱私設計

C. 被遺忘權

D.數據可攜權

你回答正確！

被遺忘權，也稱為刪除權，保證數據主體能夠將其信息從處理或使用中刪除。它可能與數據處理的同意有關；如果主體撤銷對處理的同意，數據控制者可能需要採取其他步驟，包括刪除。