申論題

一、依據 2024 年美國國家標準及技術研究所（National Institute of Standards and Technology，簡寫 NIST ）公布的新版資安框架（Cybersecurity Framework 2.0），請詳述符合管理實務要求的資安框架應涵蓋那些核心功能。

擬答：

根據 NIST 資安框架 2.0，資安框架的核心功能（Core Functions）旨在幫助企業全面管理與降低資安風險，新增「治理（Govern）」功能，總計六大核心功能。以下詳述各功能及其管理實務要求：

(一)識別（Identify）
1.功能：建立組織對資安風險的理解，識別關鍵資產、系統、資料及風險來源。
2.管理實務要求：
(1)盤點資產（如硬體、軟體、資料）並評估其重要性。
(2)識別業務環境、供應鏈風險及法規要求。
(3)進行風險評估，制定風險管理策略。
3.範例：建立資產清單，分析潛在威脅與漏洞，設定風險優先級。

(二)保護（Protect）
1.功能：實施適當的防護措施，確保關鍵服務的持續性並限制資安事件的影響。
2.管理實務要求：
(1)實施身份管理與存取控制（如多因素認證 MFA）。
(2)提供員工資安意識培訓，確保安全操作規範。
(3)部署資料保護措施（如加密、備份）以保護機密性與完整性
3.範例：使用防火牆與防毒軟體，保護內部網路與敏感資料。

(三)偵測（Detect）
1.功能：及時發現資安事件，確保快速識別潛在威脅。
2.管理實務要求：
(1)部署即時監控系統（如入侵偵測系統 IDS）。
(2)分析網路流量與日誌，識別異常行為。
(3)建立事件偵測流程，確保快速報告。
3.範例：使用 SIEM 系統（如 Splunk）監控異常登入或惡意活動。

(四)應變（Respond）
1.功能：在資安事件發生後採取適當行動，遏制並減輕影響。
2.管理實務要求：
(1)制定事件應變計畫，明確遏制、分析與通報流程。
(2)與內外部利益相關者（如法務、供應商）協調應對。
(3)記錄事件詳情與應對措施，供後續分析。
3.範例：隔離受感染系統，通報主管機關，執行事件後分析。

(五)恢復（Recover）
1.功能：恢復受影響的系統與服務，確保業務快速回歸正常運作。
2.管理實務要求：
(1)制定災難復原計畫（DRP），定期測試備份與還原流程。
(2)實施復原措施，修復受損系統與資料。
(3)總結事件教訓，改進資安策略。
3.範例：從離線備份還原資料，更新漏洞修補，優化復原流程。

(六)治理（Govern）
1.功能：建立並監督資安風險管理策略，確保與組織目標及法規要求一致。
2.管理實務要求：
(1)定義資安政策、角色與責任，確保高層領導參與。
(2)建立治理架構，監控資安策略執行與合規性。
(3)整合供應鏈風險管理（C-SCRM），評估第三方風險。
3.範例：董事會定期審查資安報告，確保符合 GDPR 或 NIST 800-53 要求。

二、因應量子電腦的發展潮流，量子密碼學及後量子密碼學等兩大新興的密碼科學類型已被提出。
(一)請說明何謂量子密碼學及後量子密碼學，試比較之。
(二)請詳述量子密碼基於那些特性來確保其安全性。

擬答：

(一)量子密碼學與後量子密碼學的定義與比較
1.量子密碼學（Quantum Cryptography）
(1)定義：量子密碼學利用量子力學原理（如量子態不可複製、測量干擾）設計加密系統，直接在量子硬體上實現安全通訊。
(2)特點：依賴量子物理特性（如光子偏振），以量子態傳輸密鑰或資料，理論上不可破解。
(3)應用範例：量子密鑰分發（QKD），如 BB84 協議。
2.後量子密碼學（Post-Quantum Cryptography）
(1)定義：後量子密碼學開發在經典電腦上運行的加密演算法，旨在抵抗量子電腦的破解能力（如 Shor 演算法破解 RSA）。
(2)特點：基於數學問題（如格密碼、基於編碼的密碼），不依賴量子硬體，可與現有基礎設施相容。
(3)應用範例：NIST 標準化的後量子演算法，如 CRYSTALS-Kyber。
3.比較
(1)技術基礎：量子密碼學依賴量子力學與專用硬體；後量子密碼學基於數學問題，運行於經典電腦。
(2)實作難度：量子密碼學需量子通訊設備（如光纖、量子衛星），成本高且部署複雜；後量子密碼學可直接升級現有系統，實作較簡單。
(3)安全性：量子密碼學理論上無條件安全（基於物理定律）；後量子密碼學依賴未被量子電腦破解的數學問題，安全性具條件性。
(4)應用範圍：量子密碼學適用於高安全需求場景（如軍事通訊）；後量子密碼學適用於廣泛應用（如 HTTPS、區塊鏈）。

(二)量子密碼學的安全特性
1.量子不可複製定理（No-Cloning Theorem）
(1)說明：量子態無法被精確複製，任何嘗試複製量子密鑰的行為都會改變原始量子態，導致無法複製密鑰。
(2)安全性貢獻：防止攻擊者複製竊取的量子密鑰，確保密鑰分發的獨特性。
2.測量干擾原理（Measurement Disturbance）
(1)說明：對量子態的測量會改變其狀態，攻擊者竊聽量子通訊（如 BB84 協議中的光子偏振）會引入可偵測的錯誤。
(2)安全性貢獻：允許通訊雙方檢測是否有中間人攻擊（如竊聽），確保密鑰分發的隱私性。
3.量子糾纏（Quantum Entanglement）
(1)說明：量子糾纏使兩個粒子狀態相互關聯，改變一方的狀態會即時影響另一方，可用於安全密鑰生成或驗證
(2)安全性貢獻：提供基於物理定律的密鑰一致性檢查，增強通訊安全性。
4.隨機性與不確定性
(1)說明：量子力學的內在隨機性（如光子偏振的隨機選擇）確保密鑰生成具有高度不可預測性。
(2)安全性貢獻：生成的密鑰難以被猜測或暴力破解，增強加密系統的抗攻擊能力。

三、加密機制可區分為對稱式或非對稱式加密機制，請說明這兩種機制的原理，優缺點，及功能上的差異。DES，RSA 與公開金鑰系統分別屬於那種機制？

擬答：

(一)
1.對稱式加密系統：其特性為運作時加密鍵與解密鍵相同，因此加密鍵與解密鍵需保持秘密（private key）。其優點為加解密速度快，但是鍵的傳送困難。因此適合用來保護個人資料、資料庫。
2.非對稱式加密系統的特性主要是加密鍵（public key）與解密鍵（secret key）不同，加密鍵公開，解密鍵需保持秘密。其缺點為加解密速度較慢，且鍵產生困難；其優點主要是較難破解，且易於管理（但需要 CA 之配合）、無密鑰之傳遞難題，適合於網路系統運作。

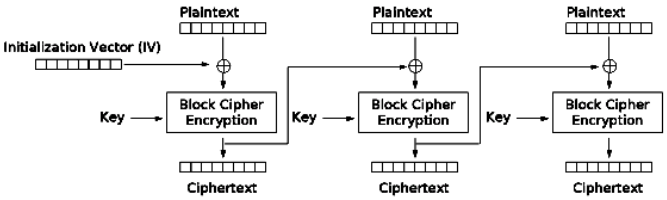
(二)DES 屬於對稱式加密系統；RSA 與公開金鑰系統 PKI 則屬於

非對稱式加密系統。

四、密碼塊連結(Cipher Block Chaining, CBC)為區塊加密(Block Cipher) 之常用模式。試說明密碼塊連結之運作方式。

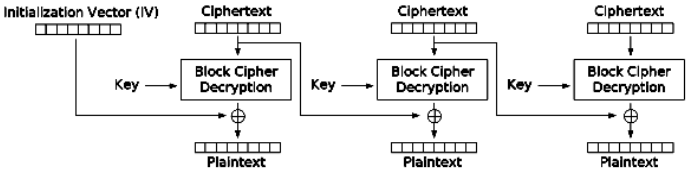
擬答：

(一)在 CBC 模式中，每個明文區塊先與前一個密文區塊進行互斥或（XOR）後，再進行加密。在這種方法中，每個密文區塊都依賴於它前面的所有明文區塊。同時，為了保證每條訊息的唯一性，在第一個區塊中需要使用初始向量（IV）。如下圖：



Cipher Block Chaining (CBC) mode encryption

(二)CBC 解密時，則反向進行，先解密後再與前一個密文區塊進行互斥或（XOR）運算，才能得到明文區塊。如下圖：



Cipher Block Chaining (CBC) mode decryption

五、(一)網際網路（Internet）上常見的視訊串流（Video Streaming）應用中，接收端在播放前必須將收到的視訊資料存入一緩衝器（Buffer），試說明原因。

(二)網路電話的通話雙方透過網際網路將壓縮的語音訊號傳送至對方，除了 UDP（User Datagram Protocol）之外，RTP（Real-time Transport Protocol）也是必要的協定。請說明這兩個協定在語音傳輸過程中的主要功能。

擬答：

(一)視訊串流為即時播放下載影像的服務，可傳送現場影音或預存於伺服器上的影片，當觀看者在收看這些影音檔時，影音資料在送達觀賞者的電腦後立即由特定播放軟體播放，但由於網路傳輸流量不一定能保持穩定，故接收端先將收到的視訊資料存入緩衝區中，當傳輸狀況不穩定時，仍可先行處理緩衝區資料，維持播放品質。

(二)目前網路電話（VoIP）中常用 SIP（Session Initiation Protocol），簡化 H.323 的複雜性，且在語音傳遞功能提供較高的延展性。不過若要達成前述功能，需要搭配 RTP 與 RTCP。RTP 協定詳細說明了在網際網路上傳遞音訊和影片的標準封包格式。RTCP 為 RTP 媒體流提供信道外（out-of-band）控制。且兩者均建立在 UDP 協定上，因此 VoIP 進行封包化時會將一定時長的數位化之後的語音訊號組合為一影格，隨後這些話音影格被封裝到一個 RTP 報文中，並被進一步封裝到 UDP 報文和 IP 報文中，並透過 RTCP 進行控制。

六、要確認網路資料傳輸是否正確，有一種方法是檢查檢驗和（checksum），如 TCP 中的虛擬標頭所使用的方式。請問在 IPv4 的網路中，虛擬標頭的作用為何？包含那些欄位，長度又為何？請描述 TCP 封包傳送時，發送端與接收端對虛擬標頭的檢驗和計算過程。

擬答：

(一)TCP 協定中進行錯誤檢查時，會以檢查和方式檢查標頭、資料與如下圖所示的概念性虛擬標頭，以偵測傳輸是否發生錯誤。概念性虛擬標頭並不真正傳送，而是由 IP 標頭與 TCP 標頭中取出下列欄位：

1.傳送端位址（Source Address）：取自 IP 標頭 32 位元的傳送端 IPv4 位址。

2.接收端位址（Destination Address）：取自 IP 標頭 32 位元的接收端 IPv4 位址。

3.Zero：8 位元全為 0（00000000）。

4.通訊協定（protocol）：長度為 8 位元，用來指示使用的通訊協定的代號，TCP 為 6（00000110），UDP 為 17（00010001）。

5.TCP 區段長度：長度為 16 位元，是 TCP Segment 的長度（表頭+資料），並且它不包含虛擬表頭的 12 個位元組。

(二)TCP 協定中進行錯誤檢查時，會以檢查和方式檢查標頭、資料與概念性虛擬標頭存入 TCP 標頭的檢查碼欄位，以偵測傳輸是否發生錯誤，過程如下：

1.發送端：欲發送 TCP 區段前，利用下列計算方式算出檢查碼值，並置於檢查碼欄位。

(1)先清除檢查碼欄位。

(2)將欲計算檢驗和的相鄰位元組，配對為 16-bit 整數，包含虛擬標頭、TCP 區段（表頭+資料），清空的檢查碼欄位，若資料長度為奇數，則暫時填補 1 個全部為 0 的位元組。

(3)計算這些 16-bit 整數的 1 的補數和。

(4)將此 1 的補數和經過 1 的補數運算後，放入檢查碼欄位中。

2.接收端：將收到的區段，透過上列發送端計算方式的(1)-(4)算出檢查碼值，並與收到 TCP 區段的檢查碼欄位值做比較，若兩者不相等，目的端會丟棄此區段，並視同區段遺失。

七、(一)虛擬線路（virtual circuit）網路與線路交換（circuit-switched）網路，有何相同和不同之處？至少各舉兩個。

(二)考慮下面虛擬線路網路的一個交換器（switch），其交換表格如下：

進來的（Incoming）		出去的（Outgoing）	
埠（Port）	虛擬線路辨識碼（VCI）	埠（Port）	虛擬線路辨識碼（VCI）
1	14	3	22
2	71	4	41
2	92	1	45
3	58	2	43
3	78	2	70
4	56	3	11

1.從第 3 埠進來的封包，其虛擬線路辨識碼（VCI：virtual circuit identifier）為 78，會從那個埠出去？其帶有的虛擬線路辨識碼會變成多少？

2.從第 2 埠進來的封包，其進來的虛擬線路辨識碼為 92，會從那個埠出去？其帶有的虛擬線路辨識碼會變成多少？

擬答：

(一)

	線路交換	虛擬線路
實質傳輸路徑	有（保留頻寬）	無
資料傳送法	連續傳送	分封為單位
適交談作業？	是	是
路徑使用	整個交談	整個交談
先建立線路	是	是
節點暫存資料	無	有，分封為單位
延遲現象	無	有，分封為單位
資料漏失	使用者處理	網路負責，分封為單位
使用頻寬	固定	機動
額外位元	無	有，分封為單位
網路超載	不能建立路徑	不能建立路徑
計費方式	距離、時間	分封、時間

(二)

1.會從埠 2 出去，其帶有的虛擬線路辨識碼會變成 70。

2.會從埠 1 出去，其帶有的虛擬線路辨識碼會變成 45。