CH 8 資訊安全

1. 為什麼 IS 容易受到破壞(destruction)、錯誤(Error)和濫用(Abuse)

列出並描述針對 IS 的常見威脅 – 技術、通訊、伺服器、公司系統、管理決策不當
定義惡意軟體，並區分病毒、蠕蟲和特洛伊木馬 – SQL Injection、
定義計算機犯罪，舉出 2 個以計算機為目標與使用計算機犯罪的例子
定義 DoS 和 DDoS 攻擊，並說明它們與殭屍網路的關係
定義身份盜用和網絡釣魚，並解釋為什麼為大問題
描述員工產生的安全性和系統可靠性問題 – 內部威脅：安全程序不足、缺乏知識、社會工程、軟體缺陷、輸入錯誤資料
解釋軟體缺陷如何影響系統可靠性和安全性

2. 安全(security)和控制(control)的價值

解釋安全和控制如何為企業創造價值 – 安全：防止 IS 非法行為之策略、程序、技術 控制：確保組織資產安全、準確、可靠、照標準運行
定義和描述計算機取證(forensics)中涉及的技術

3. 組織的安全和控制框架的組成元件？

定義一般控制(general controls)並描述每種類型的一般控制 – 軟、硬、運算控制、資安、系統導入、行政控制
定義應用控制(application controls)並描述各類型的應用控制 – 輸入、處理、輸出
描述風險評估(risk assessment)的功能並說明如何評估 – 未適當控制時，其況狀下的險等級→辨識資產、辨識威脅
定義描述安全策略(security policy)、使用規章(acceptable use policy)和身份管理 – 對資訊風險進行排名、確定可接受之目標
區分災難恢復計劃和營運持續規劃(Business Continuity Planning)
解釋 IS 稽核如何促進安全性和控制性

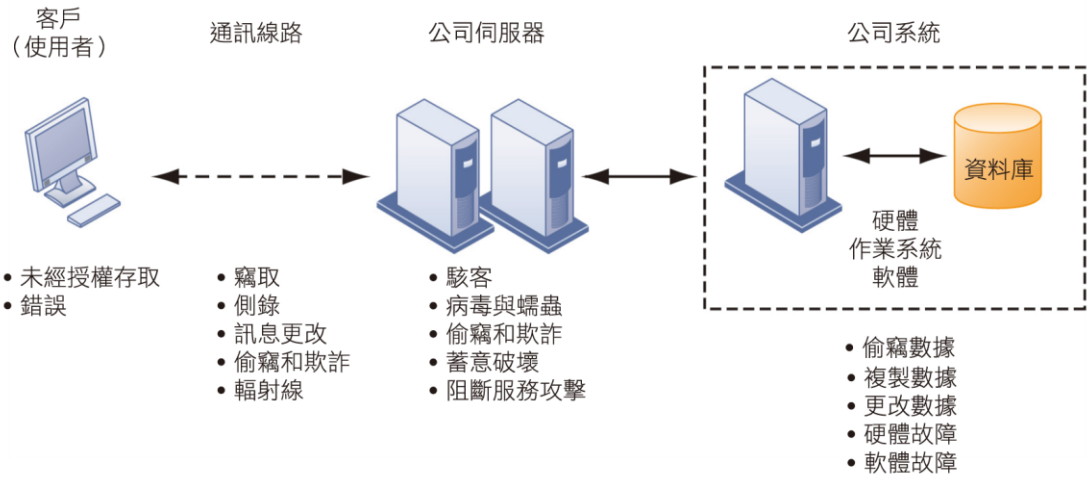
4. 維護資訊資源最重要的工具和技術?

列出並描述三種身份驗證方法 – 身分認證、許可證、生物辨識認證
描述防火牆、入侵偵測系統和防病毒軟體在提高安全性方面的作用
解釋加密如何保護資訊
描述公開金鑰基礎建設中加密和數位憑證的作用
描述公司用來確保系統可用性的技術 – 容錯系統、DPI、MSSPs、高可用性計算
確定並描述雲端計算帶來的安全問題 – SLA
描述提高軟體品質和可靠性的措施 – 軟體評量與測試

列出並描述針對 IS 的常見威脅

(1) **技術**：未經授權的存取、引入錯誤
(2) **通訊**：竊聽、嗅探(sniffing)、資訊更改、偷竊和詐欺(spoofing)、輻射線(Radio)
(3) **公司伺服器**：駭客、病毒和蠕蟲、偷竊和詐欺、故意破壞(Vandalism)、DDoS
(4) **公司系統**：資訊竊取、複製資訊、變更資訊、硬體軟體電源故障、自然災害
(5) **管理決策不當**：保護措施設計不當

圖 8-1 當代安全挑戰和破壞



網頁上的應用架構通常包括一位上網的客戶、一台伺服器和連接到資料庫的公司資訊系統。這些組成元件代表著安全的挑戰與易受攻擊的弱點。水災、火災、停電和其他電氣問題會在網路上的任一點引起當機。

[補充]
偽裝（spoofing）：有時是將原來的網址連接至其他的網站，假裝成是要連接的目的地
網路竊聽器（sniffer）：是一種偷聽的程式，它監控網路上資訊的流動

定義惡意軟體，並區分病毒，蠕蟲和特洛伊木馬

惡意軟體：是對計算機用戶有害的任何程式或檔案

病毒：是一種流氓軟體程式，通常在使用者不知情或未經使用者許可的情況下，附加在其他軟體程式或資料檔案上來執行。多數的電腦病毒會傳遞一份暗藏程式(payload)這份程式有時較不具威脅性，如執行指令去顯示一些文字訊息或影像，也可能極具有破壞性，像是銷毀程式或資料、阻礙電腦記憶體運作、重新格式化硬碟或是讓程式不正常執行

蠕蟲：與電腦病毒相似，是一種能夠自我複製的電腦程式。與電腦病毒不同的是，電腦蠕蟲不需要附在別的程式內，可能不用使用者介入操作也能自我複製

或執行。

特洛伊木馬 ： 其中惡意或有害程式碼包含在無害的程式或資料中，不像電腦病毒一樣會感染其他檔案，特洛伊木馬程式通常都會以一些特殊管道進入使用者的電腦系統中，然後伺機執行其惡意行為（如格式化磁碟、刪除檔案、竊取密碼等）

[補充]
SQL Injection(SQL 注入、SQL 隱碼)：藉由在輸入字串中夾帶惡意指令，試圖改變 SQL 語法上的邏輯，得以非法破壞、入侵資料庫伺服器，例如竊取使用者機密資料，帳戶資料，密碼等，倘若駭客取得系統權限，甚至可能癱瘓全系統

防範 SQL injection 方法 ：
(1) 使用正規化的方式驗證過濾輸入值 → 將含有 SQL 指令過濾掉、或是將單引號變換成雙引號`
(2) 控制資料庫存取程度
(3) 避免透漏錯誤資訊
(4) 在不需要使用到更新、插入資料時，資料庫以 view 方式處理供使用者查詢資料
(5) 部屬 Web 應用程式防火牆，過濾掉 OSI 應用層的威脅

Ransomware(勒索軟體)：試圖通過控制用戶的計算機或顯示令人討厭的彈出消息來勒索用戶金錢 → WannaCry(中油)

Spyware(間諜軟體)：任何在電腦上安裝元件，企圖記錄網際網路瀏覽活動 (主要作為行銷之用) 的軟體

Hacker：未經授權存取電腦系統的個人→會告知管理者安全漏洞的所在，並教導如何解決，有時會直接給予修正檔(建設/有道德，白帽)

Cracker：具有犯罪意圖，試圖破解或破壞某個程式、系統及網路安全的人(破壞/沒道德，黑帽)

Cybervandalism(電腦暴力行為)：蓄意破壞、 毀損甚至是摧毀網站或公司資訊系統等

定義計算機犯罪舉出 2 個以計算機為目標與使用計算機犯罪的例子

計算機犯罪(Crime)：通過使用計算機或針對計算機系統實施的非法行為

以計算機為犯罪目標 ：
(1) 有意或無意地存取受保護的計算機並造成損壞
(2) 未經授權存取計算機系統

以計算機作為犯罪手段 ：
(1) 使用電子郵件威脅或騷擾他人
(2) 非法存取電子通訊內容，包括電子郵件和語音郵件

表 8-2　電腦犯罪範例

以電腦作為犯罪目標
突破受保護的電腦化資料的機密性
侵入使用未經授權的電腦系統
蓄意入侵受保護的電腦，進行詐欺
蓄意入侵受保護的電腦，並有意或無意造成損壞
蓄意傳送一個程式、程式代碼或指令，引起電腦內部損害
威脅造成電腦內部損害
以電腦作為犯罪工具
偷竊商業機密
非法複製有版權之軟體或是有著作權之智慧財產，如文章、書、音樂與錄影帶
詐欺計畫
以電子郵件威脅或騷擾他人
意圖攔截他人的電子通訊內容
非法存取他人的電子通訊內容，包括電子郵件和語音郵件
用電腦傳送或處理兒童色情圖片

定義 DoS 和 DDoS 攻擊，並說明它們與殭屍網路的關係

denial-of-service (DoS)：送出大量錯誤請求的方式來耗盡提供服務伺服器的資源或是頻寬，以達到讓其他的使用者無法使用到服務 →ICMP / IGMP 洪水攻擊、UDP 洪水攻擊、ACK 反射攻擊、DNS 放大攻擊、SYN 洪水攻擊

distributed denial-of-service attack (DDoS)：又稱洪水攻擊，當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時稱之

殭屍網路 ：駭客利用自己編寫的分散式阻斷服務攻擊程式將數萬個淪陷的機器，組織成一個個命令與控制節點，用來傳送偽造包或者是垃圾封包，使預定

攻擊目標癱瘓並「阻斷服務」

定義身份盜用(Identity theft)和網路釣魚，並解釋為什麼現為大問題

身份盜用 ： 冒名頂替者獲得的關鍵個人資訊以冒充他人的一種犯罪，可用於以受害者的名義獲得信用，商品或服務，或為小偷提供虛假的憑證

網路釣魚 ： 涉及建立假網站或發送類似於合法企業的電子郵件的消息，要求用戶提供機密的個人數據
→ 因為網際網路使身份盜用者更容易使用被盜的資訊與獲取個人資訊

[補充]
evil twins： 是一種假裝可提供值得信任的無線網路連線至網際網路，詐騙者試圖讓不知情的使用者在登入這個網路的同時，竊取他們密碼或是信用卡號碼

spear phishing： 只針對特定目標進行攻擊的網路釣魚攻擊。當進行攻擊的駭客鎖定目標後，會以電子郵件的方式，假冒該公司或組織的名義寄發難以辨真偽之檔案，誘使員工進一步登錄其帳號密碼，使攻擊者可以以此藉機安裝特洛伊木馬或其他間諜軟體，竊取機密；或於員工時常瀏覽之網頁中置入病毒自動下載器，並持續更新受感染系統內之變種病毒，使使用者窮於應付

Click Fraud： 是個人或電腦程式故意地點選線上廣告，讓競爭對手的 PPC(Pay-per-Click, 按點擊付費)的廣告支出增加的操作行為，但是並不想瞭解這個廣告或是購買產品

Cyberterrorism and Cyberwarfare(電腦恐怖份子與電腦戰爭)

描述員工產生的安全性和系統可靠性問題

安全威脅通常源自組織內部
(1) 馬虎的安全程序
(2) 用戶缺乏知識
(3) 社會工程
(4) 輸入錯誤數據或不按照正確的說明處理數據和使用計算機設備而引入錯誤
(5) 設計和開發新軟體或維護現有程序時可能會產生軟體錯誤

解釋軟體缺陷如何影響系統可靠性和安全性

商業軟體包含一些漏洞，這些漏洞會造成安全漏洞，對系統造成威脅，導致無

數的生產力減少 ：
(1) Bugs：程式碼缺陷
(2) 無法達成零缺陷 ：由於大型程序無法進行全面測試，因此無法實現零缺陷
(3) 錯誤的設計引起的錯誤或缺陷
→patch 更新
[補充] zero-day vulnerabilities：軟體創造者為未知的漏洞，黑客會在供應商意識到問題並趕緊修復之前利用此安全漏洞

解釋安全和控制如何為企業創造價值

Security(安全)：用於防止對 IS 進行未經授權的存取、篡改、偷取或實體損壞的策略、程序和技術措施

Control(控制)：包含所有的方法、政策與組織程序，用來確保組織的資產安全、記錄的準確與可靠，以及依照管理標準的運作

安全和控制的企業價值：
(1) 依靠計算機系統實現核心企業功能的公司可能會損失銷售和生產力
(2) 資訊資產如果洩露給外部人會使公司承擔法律責任，則其價值會損失更多

定義和描述計算機取證(forensics)中涉及的技術

計算機取證 ：從計算機儲存媒體上檢索出的資訊進行科學的收集、檢查、認證、保存和分析，以作為日後法庭能據以判決的法律證據

涉及技術 ：
(1) 從計算機恢復數據，同時保留證據的完整性
(2) 安全地存儲和處理恢復的電子數據
(3) 在大量電子數據中尋找重要資訊

[補充]

定義一般控制(general controls)並描述每種類型的一般控制

一般控制 ：指的是整個組織資訊科技基礎架構的設計、安全和電腦程式的使用與資料檔案的安全 →與資訊系統控制環境有關，在於確保組織具有穩定及管理優良的控制環境

(1) software：監控軟體使用、防止未經授權者

(2) hardware：確保硬體安全、沒故障
(3) computer operation：程式一致性、正確處理資料，包含備份及不正常關機的處理程序
(4) data security：商業資料在使用中不會被未經授權者濫用
(5) implementation：稽核系統開發過程
(6) administrative：將各項標準、規章正式化

表 8-3　一般控制

一般控制類型	描　述
軟體控制	監控系統軟體的使用和防止未經授權者進入軟體程式、系統軟體和電腦程式。
硬體控制	保證電腦硬體是安全的，並且檢查設備是否故障。組織的運作嚴重依賴它們的電腦，對電腦應有備援或能持續運作以保持正常服務。
電腦運算控制	監督電腦部門的工作以保證程式的一致性，並正確地用於儲存媒體和處理資料。它們包括對設定電腦處理的控制工作與備份和不正常關機的恢復處理程序。
資料安全控制	保證儲存在磁片或者磁帶上有價值的商業資料文件，在使用或儲存的過程中，不會受到未經授權的存取、改變或損壞。
系統導入控制	在不同時點稽核系統開發流程，以確保流程被正確地控制和管理。
行政控制	將各項標準、規章、程序與控制方式正式化，以保證組織的一般控制和應用控制被正確地執行與實施。

定義應用控制(application controls)並描述各類型的應用控制

應用控制的目的針對每一個電腦應用系統特定的控制；ex. 在交易處理過程中，預防、偵測及改正相關的錯誤與舞弊

(1) 輸入控制：資料輸入的正確性與完整性
(2) 處理控制：確保更新期間數據完整且正確
(3) 輸出控制：確保處理結果的正確與完整性

描述風險評估(risk assessment)的功能並說明如何評估

風險評估 ：如未適當控制地特定活動或流程時，用於評估此狀況下公司的風險等級；涉及確定需要保護的內容，需要從哪裡保護以及如何保護它

風險分析中應考慮的兩個要素是：
(1) 識別資產
(2) 識別威脅
→先確定需要保護的事物，再從威脅如何影響這些事物的構面來分析各個威脅

定義描述安全策略(security policy)、使用規章(acceptable use policy)

和身份管理

安全策略(security policy)：包括對資訊風險進行排名敘述，確定可接受的安全目標以及達成這些目標的機制 →驅使一些策略，這些策略確定公司資訊資源的使用以及公司的哪些成員可以訪問其資訊資產

使用規章(acceptable use policy, AUP)：規範了公司資訊資源和計算設備的使用 →該政策應闡明有關隱私，用戶責任以及公司設備和網絡的個人使用的公司政策，好的 AUP 為每個用戶定義了不可接受和可接受的操作，並確定了不合規的後果

身份管理(identity management)：由企業流程和軟體工具組成，用於識別有效的系統用戶並控制他們對系統資源的存取，包括用於標識和授權不同類別的系統用戶，指定每個用戶被允許訪問哪些系統或系統部分以及用於認證用戶並保護其身份的過程和技術的策略

區分災難恢復計劃和營運持續規劃(Business Continuity Planning)

disaster recovery planning：在發生災難時如何恢復中斷的計算和通訊服務的計畫，例如需要備份哪些檔案和系統，其相應的備份頻率和方法

business continuity plan：涉及有關公司在災難或長期中斷後如何恢復和還原關鍵業務運營和系統的詳細資訊，主要重點在如何在災後重新恢復公司的正常營運

差異：災難恢復計劃指的是還原資料和備份，而營運持續規劃指的是使系統恢復狀態以及與運營相關的業務

解釋 IS 稽核如何促進安全性和控制性

全面地檢查公司的整體安全環境以及單個資訊系統的控制有效性，還可能會檢查資料品質；列出控制弱點及其發生的可能性；如果需要，審核結果可以用作加強控制的指南

列出並描述三種身份驗證方法

Authentication：確認對方是否為誰的能力
(1) 你知道甚麼：僅授權用戶知道的密碼
(2) 你有什麼：smart card → 一種包含帶有訪問權限和其他數據格式的晶片設備

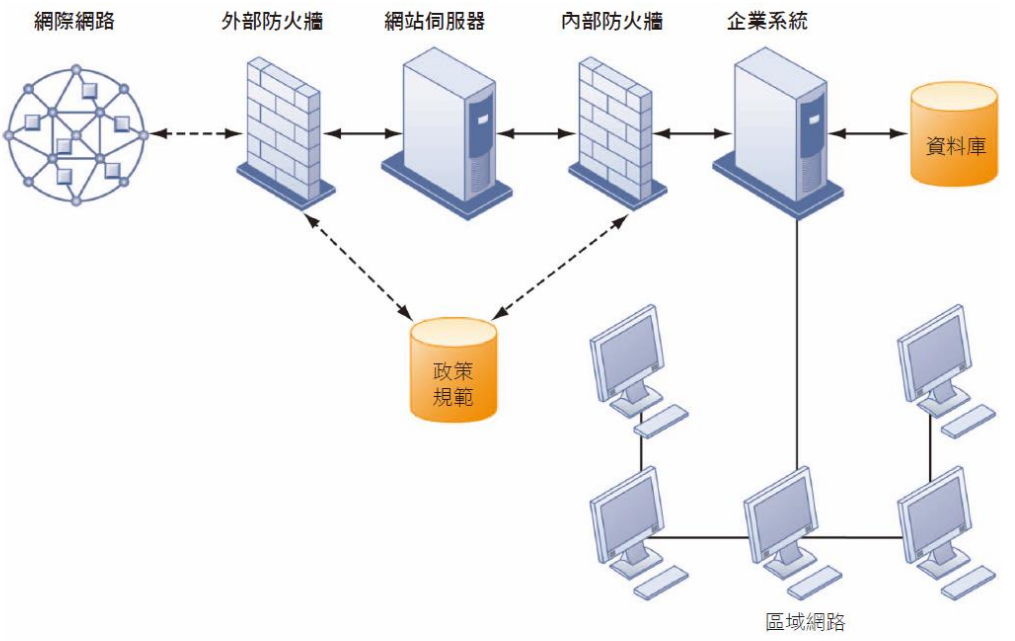
(3) 你是什麼 ： 生物識別技術

[補充] identification：宣稱是誰

描述防火牆、入侵偵測系統和防病毒軟體在提高安全性方面的作用

防火牆 ： 控制出入網路流量的硬體和軟體之組合，可防止未經授權的用戶訪問內部網路，通過監視封包的錯誤來源或目的地，或藉由代理服務器提供對內部檔案和系統的訪問權限，或者通過限制獲取的資訊類型來保護內部系統 → **Static packet filtering**、**Stateful inspection**、NAT、Application proxy filtering

圖 8-5 公司的防火牆



防火牆被安置在公司的私有網路和公用網際網路或其他不可信任的網路間，以防止未經授權的通訊。

入侵檢測系統(Intrusion Detection Systems)：監視網絡中最脆弱的點或“熱點”，以檢測和阻止未經授權的入侵者；還經常監控事件發生時，正在尋找正在進行的安全攻擊，如果收到未經授權的流量，可以對它們編寫程式以關閉網路中特別敏感的部分

防病毒軟體(Antivirus and Antispyware Software)：旨在檢查計算機系統和 driver 中是否存在計算機病毒和蠕蟲，通常會清除惡意軟體，而反間諜軟件則與侵入性和有害的間諜軟體程序對抗

[補充]
Unified Threat Management Systems (UTM)：整合不同安全防護工具至單一包裝
無線網路 ： WEP(Wired Equivalent Privacy)、WPA2

解釋加密如何保護資訊

加密是一種廣泛使用的技術，將明文或資料轉換為密文的過程，用於保護 Internet 和 wi-fi 網絡上的電子數據傳輸，使消息或資訊讓未授權的人無法得知內容，從而提供了保護；加密對於確保組織與客戶之間以及組織與供應商之間的電子商務成功至關重要

FIGURE 8.6 PUBLIC KEY ENCRYPTION

A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

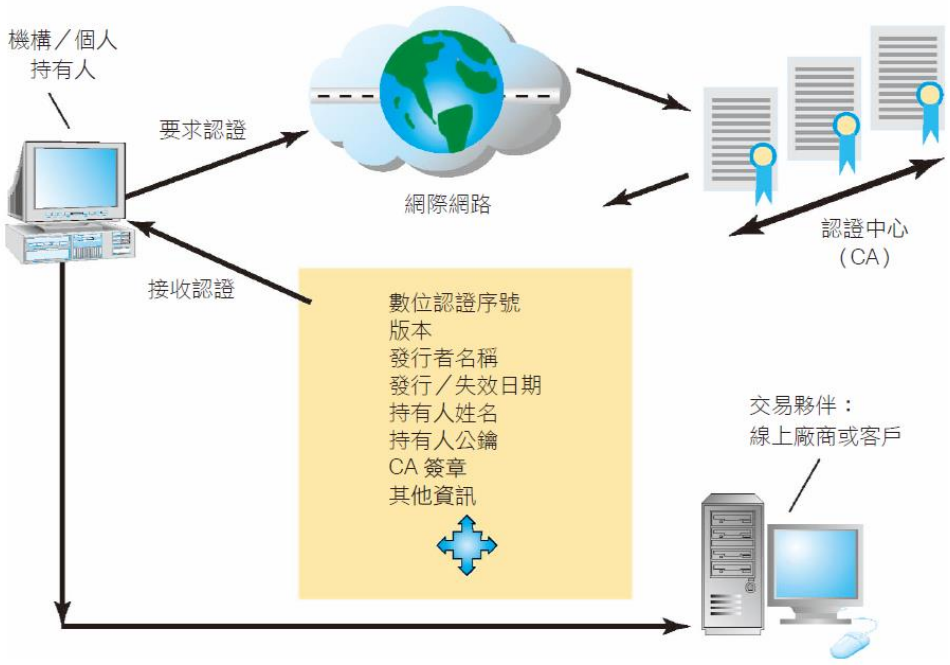
[補充] SSL、TLS(傳輸層)→HTTPS 藉由此加密

描述加密和數位憑證在公開金鑰基礎建設中的作用

結合公共密鑰加密的數字憑證可通過驗證用戶的身份來進一步保護電子交易

數位憑證(digital certificates)：用於建立用戶和電子資產身份以保護在線交易的資料檔案，使用來第三方受信任的 CA 所認證的數位化憑證，此憑證以數據化的方式儲存，內含傳輸者的有關資訊與公鑰，用於識別發送者身份並為接收者提供對回復內容的方法

公開金鑰基礎建設(Public Key Infrastructure , KPI)：是一組由硬體、軟體、參與者、管理政策與流程組成的基礎架構，其目的在於創造、管理、分配、使用、儲存以及復原數位憑證



數位認證可以用來確認個人及電子資產。它們透過提供安全、隱密與線上的傳輸環境來保護線上的交易。

[補充]對稱式加密(AES、DES、RC5)、非對稱式加密(RSA、ElGamal、ECC、DSA、ECDSA)、雜湊(MD5、SHA)

描述公司用來確保系統可用性的技術

Fault-tolerant computer systems(容錯電腦系統)：包含額外的硬體、軟體和電源組件，可以備份系統並使之保持運行狀態以防止系統故障，還可使用電路中內有特殊軟體的例行性程序或自我檢測邏輯來檢測硬體故障並自動切換到備用設備 → 確保了持續的可用性並完全消除了恢復時間

Deep Packet Inspection(DPI)：幫助檢查資料檔案並排序找出重要性低的線上資料，並將關鍵的商業檔案標示為較高的優先順序

Managed security service providers (MSSPs)：將許多資訊安全功能委外給專業的資訊安全管理服務供應商，監視網路活動並執行漏洞測試和入侵檢測

High-availability computing：最大程度地提高應用程序和系統的可用性和幫助企業從意外(crash)中快速恢復

確定並描述雲端計算帶來的安全問題

明確責任歸屬、須確保能提供滿足公司需求的保護等級，儲存的規則與如何處

理數據，數據是否與其他公司的數據隔離，災難發生後的恢復機制，外部審查與安全認證 → service level agreement (SLA) (服務級別協議)

Cloud Security Alliance (CSA)：創建了針對雲端安全的行業標準，並指定了保護雲端計算安全的最佳做法

[補充] Securing Mobile Tool : Authorization、Inventory records、Control updates、Lock down/erase lost devices、Encryption

描述提高軟體品質和可靠性的措施

(1) 軟體評量(Software metrics)：以量化測量形式對系統進行客觀評估 → 持續使用評量指標可讓資訊系統部門與終端使用者一同量測系統績效，並確認所發生的問題
(2) 軟體測試(Software test) : Walkthroughs(由一小組合格人員審查規格或設計文件)、Coding walkthroughs(開發人員開始編寫軟體後，可將其用於檢查程式碼)、Debugging