《資訊管理與資通安全》

一、公務和非公務機關平時應實施資通安全之管控與稽核工作，以減少電腦網路功能弱點（Vulnerability）的發生。這些功能弱點包括如下：

(一)身分驗證（Identification and Authentication）

(二)存取控制（Access Control）

(三)責任歸屬（Accountability）

(四)物件再用（Object Reuse）

(五)準確度（Accuracy）

(六)服務可靠性（Reliability of Service）

試從資通安全觀點，說明上述六項的功能弱點特性。（25 分）

試題評析	此題是可信賴運算的考題，算是資訊安全中較早期的議題，而可信賴運算最後發展便是微軟的Vista作業系統。不過在應考上，考生即使不知道可信賴運算的發展歷史，應不影響作答，雖然題目中的議題分布在資訊安全的各個主軸中，但若能充分掌握各個特性的意義，將資訊安全概念融會貫通，再配合各種破壞的手段切入，獲得高分亦非難事。
考點命中	《高上資訊管理與資通安全第六回》，金乃傑編撰，頁2, 86, 89, 91。

答：

依照題意以資訊安全觀點說明以下功能弱點的特性：

(一)身分認證（Identification and authentication）：透過一定的手段，瞭解使用者聲稱的身分爲何，並確認當前所聲稱爲某種身份的使用者確實是該身分。身分認證是根據所知之事、所持之物與所具之形進行判別，其最常見的弱點便是脆弱的密碼，例如太過簡單、長度不足、或包含人名、生日等基本資料。此外長年不改密碼或將密碼交給他人也都會造成身分認證機制被破壞。另一方面功能也可能因爲驗證傳送時被監聽，或是使用社交工程等技術欺騙使用者交出認證而遭到破壞。

(二)存取控制（Access control）：藉由使用權限、使用者權限與物件稽核等方式，授權使用者、群組及電腦存取使用某種資源的管制程序。存取控制包含了認證、授權以及稽核。由於組織的系統、原則必須隨環境不斷更新或增加，所以若沒有將新的設定文件化，就會使得權限設定時有所遺漏，而讓某些使用者擁有過大的權限而無法自知及管理。

(三)責任歸屬（Accountability）：指組織架構中，各單位應負的責任，以及能監督與釐清責任歸屬的制度，在安全性遭受影響時，必須要能追蹤到負責人。資訊系統責任歸屬的漏洞來自於缺乏有效的紀錄資訊，例如對使用者變更檔案權限的操作沒有紀錄，如此檔案遭受未授權存取時便無法釐清權責。另一種常出現的問題是使用者使用他人身分操作系統，這在歷史悠久的機關中相當常見，因爲以往可能電腦系統資源不足要共同使用，如此也會造成操作稽核的困擾。

(四)物件再用（Object reuse）：從安全性的角度而言，在用意味著系統資源的重複利用，如此可以確保安全性設定的精簡化及減少錯誤。例如使用者驗證的功能會指派使用者權限，透過再用可以只修改此功能便能確保整個系統的權限更新並維持一致性；另外也可以確保在不使用某種資源時能徹底清除乾淨。就弱點而言再用可能使系統效能降低，且若無一套有效的管理機制，會使系統充斥著許多未被使用的功能元件而不自知，增加系統漏洞及負荷。

(五)準確度（Accuracy）：包括資料的完整性（Integrity）與精確性，指資料在操作的流程中保持一致沒有遺失的特性，其中包括蒐集、儲存、處理與傳遞。例如避免蒐集及處理時的誤差，傳送及儲存時遭受竄改或資料遺漏等等。其弱點包括有傳遞時的竄改，或線路遭受破壞而使訊號出現異常；在處理時則可能受到入侵或緩衝區溢位的攻擊使得資料內容出現異常；最後儲存時如果沒有妥善的安全防護及權限控管，也會使資料的準確性遭到破壞。

(六)服務可靠性（Reliability of service）：在資訊安全中即可取用性（Availability），系統必須提供合法經授權的使用者可隨時取得所需的資訊。尤其對於具有時效性的操作必須要能快速反應，也要確保系統能在合理的時間內處理被下達的指令。服務可靠性的弱點來自於硬體及軟體的穩定性，硬體包括網路環境、硬碟讀

寫效能、記憶體容量與處理器效率等。例如攻擊者可以透過阻斷服務攻擊（Deny of Service, DoS）消耗伺服器的記憶體，致使伺服器停止回應合法的請求；另一方面也可能遭受蠕蟲耗盡網路資源的破壞。而軟體上可能因爲軟體漏洞使系統中毒或當機而停止服務。

以上特性均來自可信賴計算系統評估準則（Trusted Computer System Evaluation Criteria, TCSEC）的功能層級分類，實際上是層層遞進的概念，可以協助管理者釐清問題，並建構可信賴的電腦設備。

二、請試述下列名詞之意涵：（每小題 5 分，共 25 分）

(一) 揮發性資料（Volatile Data for Digital Acquisition）

(二) App 程式

(三) 智慧型代理人（Intelligent Agent）

(四) 零時差或零日攻擊（Zero-day Attack）

(五) 數位鑑識（Digital Forensics）

試題評析	此題爲名詞解釋題，但資訊安全的比重相當高，也包含兩題「數位鑑識」的概念，與以往名詞解釋題方向差異甚大，也可以推測未來資訊安全的比重可能繼續增加，必須要更著重相關章節或技術。若考生缺乏實務經驗且沒有系統的蒐集資訊安全知識，可能不易回答；不過對於使用今年新版教材的考生，應能得心應手。
考點命中	《高點資訊管理與資通安全第二回》，金乃傑撰，頁56、頁99及上課補充。 《高點資訊管理與資通安全第三回》，金乃傑撰，頁18-19及上課補充。 《高點資訊管理與資通安全第六回》，金乃傑撰，頁99、頁56-57及上課補充。

答：

(一)揮發性資料（Volatile Data for Digital Acquisition）：又稱消逝性資料，是在數位鑑識中相對於非揮發性資料的資料類型。揮發性資料會隨著電路中斷或系統狀態改變而消失，例如記憶體中的資料、使用者登入狀態、網路封包…等等。揮發性資料在數位鑑識時必須要在現場優先取證，以確保這些資料不會被丟失而影響鑑識的結果。

(二)App程式：App是application的簡稱，一般來說特別指安裝於行動裝置（Mobile Device）如智慧型手機、平板電腦上的小型應用程式，這些應用程式通常必須要透過網路市集下載，有名的網路市集如蘋果公司的App Store、Google公司的Google Play以及微軟的Windows Phone Store。使用者可以藉由這些程式擴充智慧型手機的功能，例如民眾可以自行下載政府設計的國道資訊App，透過智慧型手機掌握國道的車流量、即時路況等交通狀況，使路線規劃更爲便利。

(三)智慧型代理人（Intelligent Agent, IA）：幫助使用者完成某些任務的軟體程式，其本身具有某種能力的智慧、學習、判斷與獨立自主的能力，期能在不干擾使用者的情況下，利用本身所具備的邏輯能力來幫主人自動執行某項任務。例如某些電子郵件伺服器或電子信箱軟體就會使用智慧型代理人將郵件進行分類，自動判斷郵件是否是垃圾郵件，還是合法的信件。對於垃圾郵件，智慧型代理人可以在背景自動將之歸類到垃圾郵件資料夾，以不干擾主人的正常操作，並能提升使用者收信工作的效率。

(四)零日攻擊（Zero-day Attack）：是當系統或應用程式被發現具有風險性之弱點後，在修正程式發佈之前，或使用者更新前所進行的惡意攻擊行爲。其實大部分大規模的惡意程式都是利用零時差攻擊對電腦系統造成傷害，有名的攻擊如疾風（Blast）病毒，在漏洞被發現不到25天就被利用，中毒的電腦開機後便會出現警告將於60秒自動關機，造成許多使用者的困擾。避免零日攻擊管理者要確保作業系統及防毒程式在最新的狀態，也應多閱讀資訊安全相關資訊，以避免漏洞在發現後還被惡意使用者利用。

(五)數位鑑識（Digital Forensics）：針對具有使用紀錄的電子設備如電腦、伺服器、隨身資訊產品、網路設備或儲存媒體等，應用嚴謹的程序及科技的方法進行蒐證、檢驗、認證、保存與分析，做爲日後法庭能據以判別的法律依據。例如查獲線上賭博網站時，就必須要使用數位鑑識的技術從犯罪伺服器中找出賭博交易的紀錄，做爲起訴賭博網站經營嫌犯的法庭證據。

三、資訊科技可用來支援組織（如民間和政府等）之各種資訊化活動，包括作業性、管理性和策略性等活動。請回答下列問題：

(一) 何謂作業性、管理性和策略性等活動。（6 分）
(二) 指出並說明作業性活動之五種任務項目及其相對應軟體名稱與其功能的作業支援。（10 分）
(三) 近來國內發生一連串食品安全事件，引起各級政府對食品安全的重視。試從管理性活動觀點，提出政府如何善用資訊科技於國內食品安全管控與稽核的看法。（9 分）

試題評析	此題罕見記憶性的「交易處理系統」題目占相當的比重，是在以往三等考試中較少見的。唯第三子題出現食品安全的管理議題，同學若能掌握品質來自於「流程」的基本概念，並配合如COBIT、六個標準差等品質管理相關知識及所使用的資訊技術，並配合新聞時事及供應鏈管理等相關知識，獲得高分應不難。
考點命中	《高點資訊管理與資通安全第一回》，金乃傑撰，頁18-20, 53-54, 73。 《高點資訊管理與資通安全第五回》，金乃傑撰，頁64。

答：

(一)根據Anthony（1965）的分類，組織活動可以分爲作業性、管理性和策略性三類，說明如下：

1.作業性（Operational）活動：作業人員在既定的政策與預算下，執行組織所交付的交易行爲，如採購、存貨、現金管理、員工薪資、生產與訂單追蹤…等活動。本層級目的是提昇作業效率，有效的完成預定的目標。

2.管理性（Managerial）活動：中階主管或內部專家透過報表或圖像化工具掌握功能部門營運狀況，或在突發狀況時尋找問題的解決方案，以對各功能部門的任務進行有效的規劃、決策、協調與控制。

3.策略性（Strategic）活動：高階主管或組織擁有者透過策略分析工具或大量的內外部情報，以預測未來長期市場活動，並據以建立組織目標、政策、一般管理原則，目的是提高公司的競爭優勢。

(二)作業性活動的五種任務項目爲：生產製造、倉儲庫存、行銷銷售、人力資源、財務會計，下表說明相對應的軟體名稱與作業支援：

任務項目	軟體名稱	作業支援
生產製造	生產排程系統	生產排程、生產活動
倉儲庫存	倉儲管理系統	進貨出貨、物料管理
	採購系統	物料採購
行銷銷售	訂單處理系統	訂單處理、訂單追蹤
	市場研究系統	市場研究、價格釐訂
	POS系統	銷售管理
人力資源	薪資系統	人事資料、總務資料、會計資料管理
	福利系統	福利、補助
	員工技能紀錄	個人紀錄、教育訓練
財務會計	總帳系統	總帳管理
	應收/應付帳系統	明細帳管理
	現金管理系統	現金管理
	預算管理系統	成本會計管理、預算編列

(三)品質管理大師戴明（Deming）曾說過：「產品品質是生產出來的，不是檢驗出來的」，我想用在食品安全的控管上再適當不過。所謂生產出來，就是對「流程」加以控管，在所有活動環節上進行稽核。站在政府的角度，應加強輔導食品製造商通過ISO9001等品質管理認證，而在資訊科技方面，可以利用以下工具進行安全控管的協助：

1.流程分析工具：如STATISTICA、IBM Websphere Business Modeler等軟體避免流程的缺失，並改善產品的製造流程。

2.生命週期的專案協調工具：如Sigma Flow Integrated、Grouputer Sigmasense以對整個產品製造的生命週期加以控管，確保每個步驟都妥當符合要求。

3.物流追蹤工具：如RFID、QR code、GPS、行動裝置等技術追蹤食品原料的來源與運送流程，並在加工過程對食品註記，提供消費者追蹤源頭，也能對每個製造流程把關。

此外政府也可以與現有許多民間食品安全網站、App合作，透過群眾智慧提供食品安全資訊。例如透過網站公布食品安全的檢驗結果，並配合民間團體的力量，整理使用相關原料的食品成品，再搭配食品安全的App，讓民眾可以在購買前掃描食品的條碼便可得知食品檢驗結果，如此也能有效率地找到尚未稽查但民生常用的消費食品，以提升稽查的效益。

四、有關數位簽章（Digital Signature），請回答下列問題：（每小題 5 分，共 25 分）

(一)何謂雜湊值（Hash Value）？

(二)雜湊函數（Hash Function）的主要用途。

(三)若有文字型態之內容、編輯格式和字體大小等完全相同的兩個檔案，經由 MD5（Message-Digest Algorithm 5）所產生的雜湊值卻不相同，請說明其可能原因。

(四)在蜜罐誘捕系統（Honeypot）之惡意程式網路活動分析上，說明採用 MD5（或 SHA-256）之目的。

(五)我國《個人資料保護法》（修正日期：民國 99 年 5 月 26 日）第 22 條第 2 項規定：「中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。」請說明如何進行證據之取證（Acquisition）及使用 MD5（或 SHA-256）目的為何？

試題評析	此題爲考驗同學對於雜湊的理解及功能的應用，亦屬於新增題型，必須有豐富的實務經驗才能寫出完整的答案。但這些概念大多在新版講義中有提及，若能對教材概念充分掌握，用自己的話將功能加以說明補充，應能得到不錯的分數。
考點命中	《高點資訊管理與資通安全第六回》，金乃傑撰，頁27, 75, 99-100及上課補充。

答：

(一)雜湊值（Hash Value）：又稱訊息摘要（message digest），是雜湊函數的輸出，爲一固定長度的亂數值。

(二)雜湊函數（Hash Function）：一個可將不定長度的訊息轉換成固定長度雜湊值的函數，典型的雜湊演算法有產生128位元雜湊值的MD5（message digest 5）與產生160位元的SHA-1（Secure Hash Algorithm）。設計妥當的雜湊函數在輸入不同訊息時，幾乎不可能產生相同的雜湊值，且也很難從雜湊值推論函數的輸入。基於這些特性，雜湊函數有兩種常見用途：

1.驗證訊息的完整性（Integrity）：因爲不同的輸入訊息雜湊值都不相同，那怕只差了一個bit。因此可在傳送前先做一次雜湊，將雜湊與訊息一併傳送，接收端再對收到的訊息做一次雜湊，與先前的雜湊值比較，若不同則代表訊息在傳輸過程中有遺失或遭到竄改。

2.儲存密碼或機密資料：因爲雜湊很難從結果推斷原始的輸入訊息，可以做爲系統中保護使用者密碼的一種安全機制。例如爲了避免資料庫管理員檢視使用者密碼的明文，就可以將使用者輸入的密碼轉成雜湊值儲存，將來使用者輸入時只要再將密碼轉成雜湊值與資料庫中的值比對，即可達到驗證身分。

(三)MD5是對整個檔案的位元進行雜湊，因此除了檔案內容的比對外，還包括對檔案的描述資料（metadata）。所謂描述資料如Word檔案中的建立時間、修改次數、作者、公司、標題、描述…等欄位，如果描述資料不同，則整個檔案的雜湊值也會不同。因此假使攻擊者在檔案中加上惡意程式，即使檔案內容看起來完全相同，但雜湊值一定不相同，透過雜湊比對便能保護使用者使用檔案的安全（檔案完整性）。

(四)蜜糖罐誘捕系統（Honeypot）是一個精心規劃成有缺陷的系統，以大量的陷阱吸引攻擊者，引誘攻擊者發動攻擊，藉此欺敵來保護重要的系統或是對攻擊者的行爲進行分析。如Nepenthes是一種蜜糖罐系統，可模擬一般伺服器提供的服務與常見的漏洞，藉以騙取攻擊並下載惡意程式。在下載惡意程式後，Nepenthes會將惡意程式的內容進行雜湊並加以儲存。未來管理者只要發現其他連線的程式的雜湊值與惡意程式儲存庫中的雜湊值相同，即可快速分辨爲惡意程式，加強系統防禦能力。

(五)以下分別說明數位證據的取證與使用雜湊的目的：

1.數位證據的取證：根據數位證據特性不同，取證也可分消逝性資料與非消逝性資料取證兩類。消逝性資料必須要在事件現場進行，透過LiveDectector等工具傾印記憶體與作業系統狀態，並使用NetWitness等工具側錄網路封包。對於非消逝性資料如硬碟、光碟、隨身碟等必須要在事件現場進行包裝存封，並送到鑑識實驗室進行進一步的分析、比對、搜尋等工作。

2.使用雜湊的目的：爲了避免數位證據的原始證物在鑑識中被破壞，在鑑識前會先製作原始證物的映像檔（Image），此映像檔的數位內容將必需與原始證物的數位內容完全相同。製作映像檔時使用Bit-Stream的方式，將原始證物磁碟的所有位元完整複製。爲了確保複製結果相同，鑑識人員會使用雜湊函數（如MD5或SHA-1）做資料完整性的檢查，比對映像檔與原始證物檔案的雜湊值。