《資訊管理與資通安全》

一、電子商務（EC）的分類架構有許多種，例如：以經營模式來分類、以虛實的經營方式來分類、以交易雙方對象來分類。以交易雙方對象分類，主要分成四類：B2B、B2C、C2B與C2C，請描述每一類別的意義，並分別舉一實例對照之。（20分）

試題評析	本題爲經典的電子商務分類考題，與98年地特4等題目幾乎如出一轍，是較好準備、較好拿分的題目。惟考生在撰寫時，必須依照題意將答案分爲「意義」與「實例」，若能搭配表格整理會是較完整、較有條理的答案。 值得注意的是，實例部分不求廣度，相對於列出一大堆網站的名稱，針對單一網站敘寫其功能與模式會是更佳的答案。若同學準備時掌握好考古題，此題得到滿分易如反掌！
考點命中	1.《高點資訊管理與資通安全講義》第三回，金乃傑編撰，頁2-5。 2.《高點資訊管理與資通安全總複習講義》，金乃傑編撰，資管議題2，頁4。

答：

電子商務是以網路科技爲基礎，支援企業與客戶買賣之間的交易執行、資訊分享及關係維持的一些流程系統與經營模式。以交易對象分類的內容與例子以下表說明之：

分類	意義	實例
B2B	Business-to-Business，企業對企業電子商務。爲企業與其他企業或合作夥伴間透過Extranet或其他網路連線從事的交易或協助的商務活動，其最主要目的是降低交易成本與加速供應鏈反應能力，以因應市場變化。	Apple與鴻海間的供應鏈使用B2B的方式進行，Apple跟鴻海下訂單，並提供iPhone、iPad設計圖交給鴻海進行組裝代工；而鴻海生產的iPhone、iPad賣回給Apple與之銷售。
B2C	Business-to-Customer，企業對顧客電子商務。企業透過網際網路平台與顧客直接交易的電子商務模式，其主要目的是降低零售商、批發商的中介成本與市場可及性，因爲透過電子商務，可以不受時間空間限制，接觸全世界的潛在消費者。	小米手機透過網站進行銷售，消費者只要連到網站上就可以直接購買手機，而不需要透過一般的電信門市等中間商。
C2B	Customer-to-Business，顧客對企業電子商務。顧客於電子商務平台凝聚需求，形成較大的議價能力與目標企業交涉，使企業提供更便宜或高檔的產品服務的模式。其主要目標爲降低顧客購買成本。	Groupon團購網站，提供團購優惠券，讓消費者在上面購買各種商務活動的優惠券，以優惠價買到物超所值的產品或服務。
C2C	Customer-to-Customer，顧客對顧客電子商務。電子商務的買賣雙方爲一般消費者，透過電子商務平台進行商品或服務交易。其主要目標是「貨暢其流」，讓任何人都能透過平台出售自己的產品，賺取利潤；並透過大量賣家提升平台中商品豐富的程度，形成長尾效應。	Yahoo!拍賣，會員經過認證後即可成爲賣家，在拍賣網頁上上架自己的產品。消費者可以透過搜尋或分類瀏覽找到賣家的產品，與賣家聯絡進行消費。

二、請解釋何謂IT治理（Corporate governance of information teehnology）？它與IT管理（IT management）的差別在那裡？（20分）

試題評析	IT治理與IT管理實爲99年政大的研究所考題，但在100年普考時也出現過IT治理的定義。此題由於配20分，可將第一小題名詞解釋配5分敘寫，後面的敘述乃此題精華，則以15分的版面撰寫，搭配表格強調其差異性，並加上簡短結論。 由於此題的比較表在正課講義中完全命中，所以認真準備的同學應可拿到高分。

考點命中	1.《高點資訊管理與資通安全講義》第五回，金乃傑編撰，頁42。 2.《高點資訊管理與資通安全總複習講義》，金乃傑編撰，資管議題15，頁52。

答：

(一)IT治理是公司治理在資訊時代的重要發展，主要目的是幫助企業的投資者來指導、監督、稽核與評估企業有無合法、有效的使用IT資源來提升企業的價值，降低企業風險的一個管理方法論與流程規範。旨在保持資訊科技與業務目標一致，推展業務發展，促使收益最大化，合理利用資訊科技資源，適當管理與資訊科技相關的風險，增加價值，以實現企業目標。

(二)而IT管理指的是根據組織已訂定的IT策略，去確認、監控、調整、執行IT，進而達到最大效益的一種手段。將IT治理與IT管理的差別以下表比較：

	IT治理	IT管理
內容	企業最高管理層（如董事會、投資人）監督營運管理層在IT策略上的流程、結構和連結，以確保IT策略符合組織策略，提升IT營運的正確性與效率。	根據組織的IT策略，管理企業資訊及資訊系統的營運，調整、確認IT目標以及實現策略目標所採取的行動。
目標	讓企業從IT中獲得最大的價值，評估管理者有無組織最大利益有效利用IT資源。	從管理者角度來思考IT投資與運行，發揮IT應有之功能價值。
執行者	董事會、投資者	管理階層
依據	組織策略	IT策略
操作	產出IT策略，IT運作的基本框架。	在IT運作的框架下駕馭企業奔向目標。
比喻	房子的設計圖。 如果空有設計圖而缺乏工程，只是紙上談兵，無法對企業發揮實質效益。	蓋房子的工程。 如果缺乏完善的設計圖，往往事倍功半，要蓋出符合需求的房子根本不可能。

實際上，IT治理與IT管理就像企業使用IT營運的一體兩面。但IT治理扮演大目標的角色，如果目標錯了，再努力常常都是枉然。根據統計，IT治理出色的企業可以獲得比競爭對手高出40%的IT投資回報；在相同的業務策略下，IT治理處於平均水準的企業比IT治理效率低下的企業多獲得20%的利潤。

三、在企業或組織導入資訊安全管理系統（Information Security Management Systems, ISMS）的過程中，PDCA的管理模型常常用來持續改進ISMS的整體運作。請問PDCA英文全名為何？在ISMS中，PDCA的工作項目具體為何？（25分）

試題評析	ISMS透過PDCA來執行一直是重要的觀念，相似題出現在98年高考二級與98年普考，雖然以往此概念配分不高，如98年普考只配4分，但已算是經典考題。此題必須對PDCA所代表的意義有所了解，再搭配ISMS的14個安全控制項目敘寫，才能寫出較完整的答案。 若爲班內的學生，以口訣記憶14個安全項目，搭配對ISMS的了解，要拿到超過20分絕非難事。
考點命中	1.《高點資訊管理與資通安全講義》第六回，金乃傑編撰，頁102-105。 2.《高點資訊管理與資通安全總複習講義》，金乃傑編撰，資安議題9，頁84。

答：

(一)PDCA是由品質管理大師戴明（Deming）所提出，指品質管理工作的規劃（Plan）、執行（Do）、查核（Check）與行動（Action）等所形成的循環流程，故又稱戴明循環（Deming Cycle），現已被應用在許多品質管理的領域。

(二)資訊安全管理系統（Information Security Management System, ISMS）是國際標準，可以幫助組織鑑別、管理和減少資訊所面臨的各種風險。包括建置組織管理系統所需要的PDCA管理架構及廣泛的安全控制措施指引。PDCA被應用於執行資訊安全管理系統（ISMS），以下說明其主要工作項目：

1.計畫（Plan）：目標爲建立資訊安全管理系統，分爲三個工作：組織業務分析、建立資訊安全政策與成立資訊安全組織，說明如下：

(1)組織業務分析與安全政策制定：透過參考現行制度法規訂定與評估ISMS原則，並根據組織實際情況，考量以下範疇：安全政策、安全組織、資產管理、密碼學、作業安全、供應商關係、人力資源安全、實體與環境安全、存取控制、通訊安全、系統開發與維護安全、持續營運管理、資訊安全事件管理、遵行等，制定安全政策。

(2)成立資訊安全組織：成立資訊安全委員會，並由資訊安全委員會指派資訊安全官、資訊安全小組、資訊安全稽核小組，有需要時再根據任務成立緊急處理組。

2.執行（Do）：目標爲實施與操作資訊安全管理系統，工作有：資訊資產分類與管制、風險管理與產出適用性聲明、建立資訊安全文件體系，說明如下：

(1)資訊資產分類與管制：建立資訊資產清單，依照資訊資產性質分類，並依照機密性、完整性、可用性鑑別資訊資產之價值。

(2)風險管理與產出適用性聲明：依照資訊資產價值、發生威脅可能性、脆弱性進行風險估算，並對風險高者提出「風險改善計畫表」與「適用性聲明書」，說明風險控管措施之執行辦法。

(3)建立資安文件體系：以四階層紀錄（政策、程序書、作業說明書、表單與紀錄），並對文件安全進行控管。

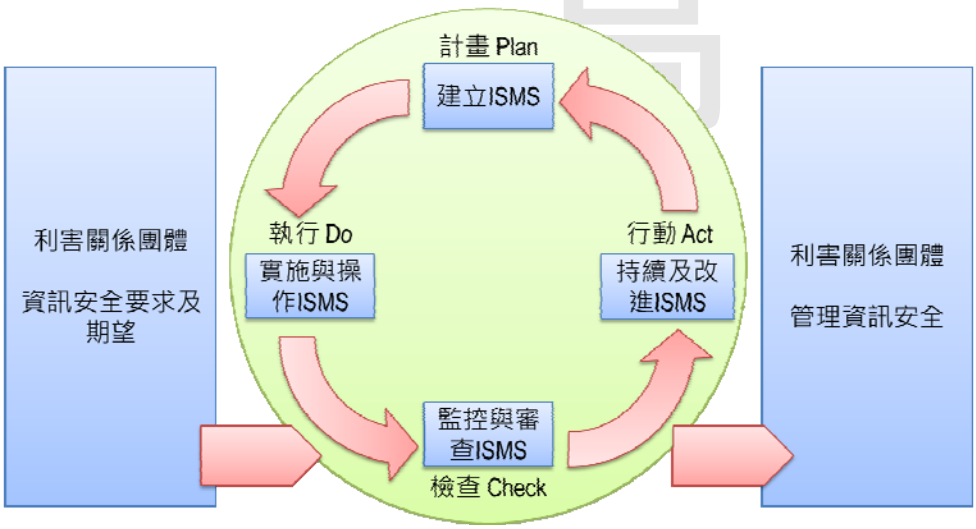
3.檢查（Check）：目標爲監控與審查資訊安全管理系統，分爲兩項工作：建立持續營運計畫、資訊安全內部稽核作業。

(1)建立持續營運計畫：對業務流程的重要性、風險等級、恢復時間等進行綜合分析，製作「業務流程衝擊分析表」，並將高風險業務流程加入持續營運計畫，將業務災害或故障降低到可接受的範圍。

(2)資訊安全內部稽核作業：審查組織之資訊安全控制、風險評鑑與持續營運計畫，建立「資訊安全管理制度內部稽核表」，並依照稽核表執行稽核，逐項填寫稽核結果。

4.行動（Act）：目標爲維護與改善資訊安全管理計畫，主要工作爲審查委員會的管理。如針對資訊安全稽核結果進行建議改善事項、矯正及預防措施檢討、報告資訊安全目標執行狀況、擬定資訊安全制度執行之各項改進措施，說明風險再評鑑與風險處理計畫執行結果……。

將PDCA與資訊安全管理系統執行關係以圖表示如下：



四、在一通訊網路中，針對資訊流的安全攻擊（Security Attacks）依據X.509及RFC4949分類為被動式攻擊（Passive Attacks）與主動式攻擊（Active Attacks），請解釋被動式攻擊與主動式攻擊，並請分別舉例兩種被動式攻擊與兩種主動式攻擊的方法。（20分）

試題評析	雖然將網路攻擊分爲主動、被動是初次出現在國家考試中，但若對網路攻擊方法有充分的掌握，只要能區別被動是不造成影響的竊取；主動是對資料的破壞，仍是可以順利寫出正確答案。 值得注意的是，由於本題題目有明確規定，要舉出各兩個例子，一定要依照題意回答。若考生不確定舉例是否正確，亦可多舉出幾項，以減少被扣分的機會。此外，由於是初次出現的題目，可

	預期的是此題將會出現在其他類似考試中（如地方特考、關務特考或警察鐵路等考試），希望同學多加留意準備。
考點命中	1.《高點資訊管理與資通安全講義》第六回，金乃傑編撰，頁43-69。 2.《高點資訊管理與資通安全總複習講義》，金乃傑編撰，資安議題5，頁68-72。

答：

根據網路攻擊的型態，可分爲被動式與主動式攻擊，以下解釋並列舉各兩種攻擊方法：

(一)被動式攻擊（Passive Attacks）：竊取網路上傳送的訊息的內容或偵測訊息長度、頻率、來源/目的等資訊，但以不影響系統運作爲原則。這些訊息可能是敏感的資料，如帳號密碼、個人資訊、信用卡號碼、銀行帳號……，一旦洩漏極可能造成使用者的損失。被動式攻擊不易偵測，但只要透過加密等技術就容易達到預防的作用。典型的被動式攻擊如竊聽，以下說明：

1.區域網路竊聽（Sniffer）：在區域網路（Ethernet）中攔截傳輸的封包，而得知他人傳輸的資訊。主要原理是由於區域網路是共享式架構，攻擊者只要將網路介面卡設定爲混亂模式，當有封包流經時網路卡便會將封包紀錄下來並分析該封包內容，若訊息未經加密，只需要透過分析工具即可完整解讀傳送內容。

2.無線網路竊聽（Eavesdropping）：在WEP等安全性較低的無線網路中，可以在很短的時間內破解無限存取點的加密金鑰，而只要在無線網路範圍內，就可以監聽所有連到此存取點電腦傳送的資料，主要可以竊取登入網站的帳號密碼或信用卡號碼。

(二)主動式（Active Attacks）：對網路上傳送的資訊進行破壞、竄改、阻斷、延遲，造成訊息接收者無法收到資訊或收到錯誤的資訊，而影響系統正常執行。主動式攻擊可分爲四類：僞裝攻擊（Masquerade）、修改訊息內容（Modification of Message Content）、重送攻擊（Replay）與阻斷服務（Denial of Service，DoS）等。此類攻擊雖然不易預防阻擋，但相對而言容易偵測。典型的主動攻擊如：DNS Spoofing及SYN Flooding，以下說明：

1.DNS Spoofing：透過刻意製造的DNS封包，把網域名稱查詢結果指向惡意網站的IP位址，屬於僞裝或修改訊息內容的主動式攻擊。實作方法有改變被攻擊者電腦的DNS設定，使被攻擊者在DNS查詢時是連向攻擊者主機，此法稱爲DNS ID spoofing；另一種方式是透過僞裝的回應修改上層DNS伺服器的快取資料，讓上層DNS伺服器直接將網址對照成錯誤的IP，此法影響範圍較大，稱爲DNS cache spoofing。

2.SYN Flooding：屬於資源占用型的DoS攻擊，使用TCP同步訊號洪水攻擊，通常用以癱瘓網頁伺服器。主要原理是利用TCP三向交握（Three-way Handshake）協議缺陷，發送大量僞造的TCP連接請求，使被攻擊方的CPU或記憶體超過負荷而至當機。SYN Flooding可以透過建立SYN Cookie，在檢查完合法的回應後，再分配專門的資料區進行TCP連接。

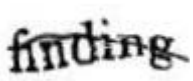
五、通常在入口網站的建置上，經常使用CAPTCHA技術。請寫出CAPTCHA的目的為何？它有何應用？reCAPTCHA是由卡內基美濃大學所發展的系統，它的作法為何？（15分）

試題評析	本題爲相當活用的題目，且爲行之有年的技術，出現在許多網站中。若同學在上網時有留意此機制，前面兩小題應不難寫出答案。惟第三小題是較少用的名詞，除非對此技術發展有更深層的了解，要回答出來實在不容易。 鑒於此題趨勢，考生應對日常生活中會接觸到的資訊安全機制有更高的敏感性，如簡訊的一次性密碼也可能成爲未來的考題。對於班內學生，若在課堂中有記錄老師補充，此題應可獲得一半以上的分數。
考點命中	《高點資訊管理與資通安全講義》第六回，金乃傑編撰，頁91-92，暴力破解法上課補充。

答：

(一)CAPTCHA是全自動區分電腦和人類的圖靈測試（Completely Automated Public Turing test to tell Computers and Humans Apart）的縮寫，在2002年由卡內基美濃大學所提出，用以區分使用者是機器人還是自然人的程式。在CAPTCHA測試中，伺服器會自動產生一個問題由使用者來解答，這個問題的答案可以由伺服器評判，但是必須是人類才能解答。由於機器人無法解答CAPTCHA的問題，所以回答出問題的使用者就可以被認爲是人類。常見的CAPTCHA有辨識加上線條且扭曲的文字（如下圖）、出現計算公式讓使用者填

寫答案、辨識圖片中的人物是誰、閱讀廣告中的文字回答問題等。



(二)CAPTCHA的主要應用如網站註冊會員的頁面，爲了避免受到機器人自動註冊會員形成的殭屍會員大軍或浪費網站資源，會再填寫基本資料的地方加上CAPTCHA，讓使用者辨認圖片中的文字，若正確解讀才可以註冊。

另外CAPTCHA也常應用在留言板、討論區上，避免廣告機器人自動洗版，造成留言板充斥垃圾訊息；也會出現在重要資源查詢的頁面，以避免資源被機器人濫用，而影響到自然人使用的權益；在Google登入系統中，當密碼打錯三次後，也會出現CAPTCHA，以確保不是機器人在用暴力破解法嘗試密碼組合。

(三)reCAPTCHA是利用CAPTCHA技術來幫助典籍數位化的計畫。reCAPTCHA將書本掃描中無法準確被電腦自動辨識的文字（光學文字辨識技術，Optical Character Recognition, OCR）顯示在CAPTCHA問題中，讓人類在回答CAPTCHA問題時順便告訴電腦這組字的正確答案。在reCAPTCHA中，爲了保有「防機器人」的功能，會一次顯示兩組文字，一組是電腦無法辨識的字，另一組是已經知道正確答案的字，如果使用者正確回答出後者，就假設前者答案也是正確的。在通過驗證的同時，系統會順便將人工辨識的字回傳到reCAPTCHA計畫主機，回報數位典藏系統的辨識結果，一舉兩得。