《資訊管理與資通安全》

一、隨著寬頻網路與分散式運算技術的成熟與普及，企業與政府機關紛紛採用雲端運算（Cloud Computing）解決方案。（每小題15分，共30分）

(一)請敘述雲端運算的三種服務模式，並舉例說明。

(二)請敘上述三種雲端運算服務之核心技術。

試題評析	第一小題為雲端運算的基本題，服務模式的考題相似題型多如牛毛，若有充分練習，應屬容易拿分；第二小題雖類似題較少，但仍與100年地特四等、101年地特四等題目相似，考點都為雲端運算核心技術。惟需注意的是，此題是根據上述三種服務模式所需之技術，故在作答時仍需緊扣三種模式，才能拿到高分。
考點命中	《高點・高上資訊管理與資通安全講義》第一回，金乃傑編撰，頁20-34。

答：

(一) 雲端運算是以網格運算技術，配合無所不在、隨選動態的網路，共享廣大的運算資源（如網路、伺服器、儲存、應用程式、服務），可透過最少的管理工作及服務供應者互動，快速提供各項服務。其三種服務模式說明如下：

1. 軟體即服務（Software as a Service, SaaS）：供應商將軟體建置於網路上，讓使用者透過瀏覽器直接使用軟體，而不需要在電腦上進行任何的軟體安裝，可節省公司軟體採購的費用及安裝、維護的成本，並可跨平台跨裝置的存取服務及資料。例如Gmail網頁版提供線上收信、寄信的功能，使用者可以不需要安裝如Outlook的程式即可完成收發信；Salesforce.com提供線上的CRM系統，讓業務員可以在系統中快速紀錄顧客偏好，並存取產品資訊，而公司不必為此CRM系統建立中央伺服器。
2. 平台即服務（Platform as a Service, PaaS）：供應商提供開發軟體與運作環境，讓程式設計師在其平台上開發服務，可以節省工程師建置、更新、維護平台的成本，專注在程式開發上，提升開發效率。例如Google App Engine提供Python、PHP、Java的執行環境、Heroku提供Ruby及Node.js的執行環境，讓程式設計師可以在上面開發這些語言的網頁服務，快速建置網站。
3. 基礎建設即服務（Infrastructure as a Service, IaaS）：供應商提供計算設備，讓系統管理者在其平台上佈署自己的環境，節省建置機房、配置管理人員的成本。最有名的服務是Amazon提供的Amazon Web Service，其提供Windows及Linux伺服器的運行環境，讓系統管理員可以在上面安裝作業系統及其他所需軟體，並透過遠端連線登入使用，對管理員而言就像一台實體的伺服器，可以隨時隨地存取使用。

(二) 上述雲端運算服務的核心技術說明如下：

1. 公用運算（Utility Computing）：為雲端運算的計費模式，常為SaaS的商業模式，亦可使用在PaaS與IaaS。其依照使用量計費，例如根據雲端儲存空間使用量、CPU使用量或使用時間、網路流量…等，將運算資源視為水、電、瓦斯等公用設施，使用越多則付費越高。
2. MapReduce：為Google運用在雲端運算中的關鍵技術，主要使用在PaaS的程式設計，亦可提供IaaS模式使用，讓開發者開發大量資料的處理程式。其做法為先透過Map程式將資料切割成不相關的區塊，再交由不同的處理單元（電腦）處理，最後透過Reduce程式將結果彙整，才輸出開發者需要的結果。MapRecuce使用Divide-and-Conquer的方式，將大問題化簡為小問題，再一一擊破，適合進行大數據分析。
3. 虛擬化（Virtualization）：為IaaS的建置技術。將計算機系統的主要資源抽象化，直接將系統資源交付於特定軟體並透過其整合管理，作業系統則由虛擬出的抽象硬體層存取各項資源。如此可以解決硬體資源浪費，達到最大運算能力，並可減少系統維護、管理之成本。透過虛擬化可以方便的建置多系統的環境，再分租給不同的使用者。

二、行動商務（Mobile Commerce）與無所不在運算（Ubiquitous Computing）對企業與政府有許多

影響。一些組織為節省成本與員工使用的便利性，採用BYOD（Bring Your Own Device）政策，允許員工使用自己的設備辦公。針對此項政策，請說明：

每小題15分，30分）

(一)對該組織之資訊安全與資產有何影響？

(二)資訊部門應採取那些防禦措施？

試題評析	第一小題之核心為BYOD之議題，與104年關務三等的題目相近，但又更為深入。此題在撰寫時切忌蜻蜓點水，若羅列所想到的任何影響沒有加以說明很難拿到高分，宜條列寫出可能造成之危害，並搭配舉例，使答案較有架構；第二小題則為防禦措施，可以從基本的資訊安全三要素切入，分項說明可採取的手段。此題若對資訊安全有充分了解，又能有條理呈現答案，分數應會理想。
考點命中	《高點・高上資訊管理與資通安全講義》第一回，金乃傑編撰，頁75-76。

答：

(一) BYPD（Bring Your Own Device），是企業或政府讓員工用自己的設備連上內部網路（intranet），以存取內部系統進行決策，或連到企業行動商店（Enterprise App Store）下載員工專屬App執行公務。透過BYOD可以提升生產力、創意、使用系統的彈性、滿意度、降低電腦設備費用。其對組織資訊安全與資產的影響說明如下：

1. 機密資訊外洩：根據使用者的行為可以分為蓄意外傳或因為裝置遺失而洩漏。當使用者用自己的裝置處理組織的機密資料，很容易將內部資料透過網路或實體的方式傳送給與作業無關的第三人，造成商業秘密洩漏；另外亦可能因為行動裝置遺失而使內部重要資訊洩漏，如Apple員工常常將手機遺忘在酒吧使新型iPhone的設計圖曝光，破壞組織資訊資產的機密性。
2. 惡意程式入侵：若使用者的行動裝置遭受惡意程式的感染，當使用者連上內部網路時，則可能因此散佈到其他系統，例如當使用者開啟內部檔案伺服器的文件時，木馬自動附加到文件中，若其他使用者開啟文件，則可能亦受到感染，如此檔案伺服器成為組織中的毒窟，造成越來越多的電腦被入侵，甚至變為竊取公司重要資料的後門或可以發動攻擊的殭屍網路（Zombies）。另外也可能因為裝置感染蠕蟲，連上內部網路後不斷自我複製，而將內部網路癱瘓。如此都可能破壞組織資訊資產的機密性與可用性。
3. 未授權的安裝組織程式：內部員工常為了貪小便宜將公司內部的授權軟體（如Office、開發工具）攜帶到家中的其他電腦安裝或轉送給朋友，如此亦是對組織資訊資產的濫用；另一方面使用者亦可能在自己的裝置中安裝盜版軟體，若使用盜版軟體處理公務，亦可能使組織遭受裁罰，造成財產的損失。

(二) 資訊部門可以使用PDCA的方式建置防護體系，其可考慮採取的防護措施如下：

1. 建置資訊資產使用規則（Policy）：資訊部門必須明訂BYOD的使用限制，包括可以使用哪些型號的裝置，什麼樣的員工、為了什麼目的才可以使用，以及使用的期限、定期檢查的期限，攜帶裝置的申報程序、攜出裝置的檢查工作，另外也包括可以存取資料的範圍，存取內部資源的用途等，都須加以規範。此外還要考慮建立BYOD的教育訓練機制，以確保每位使用BYOD的員工都能妥善使用裝置。
2. 建置遠端裝置管理服務（Mobile Device Management, MDM）：透過中央控管程式對手持設備遠端進行設定、更新，原用在遠端更新裝置系統，但在BYOD時，常用在裝置遺失時，管理者透過遠端系統追蹤裝置的位置，讓裝置發出提示音或顯示特定資訊給拾獲的人，在有必要時亦可從遠端鎖定或刪除裝置中的敏感資訊，以免機密外洩。
3. 建置遠端應用程式管理服務（Mobile Application Management, MAM）：透過中央控管程式遠端安裝、更新予刪除應用程式，原用在應用程式自動更新。在BYOD時，企業透過內部的企業行動商店讓員工安裝企業專屬的App，則可在裝置遺失時將App刪除，亦可以管理使用者裝置中的App，避免使用者安裝不符合規定的程式。
4. 加入網域（Domain）：透過LDAP協議，將裝置加入網域中，可以透過domain policy遠端設定裝置能使用的功能，包括能安裝的程式、能存取的檔案、能連結的網頁…等等，以確保裝置都在規範下使用。而加入網域的電腦亦可設定成在內部網路時才可以登入，確保員工雖使用自己的裝置，但在

公司外部卻不能用公司內部帳號登入使用，防止將資料攜出。

BYOD就像一把兩面刃，可以讓員工更方便，但也帶來許多資安風險，因此必須要建立妥善的配套措施，才能讓BYOD發揮應有的價值。

三、企業與政府組織需要一些決策資訊系統，協助主管做政策決定。請說明：（每小題10分，20分）

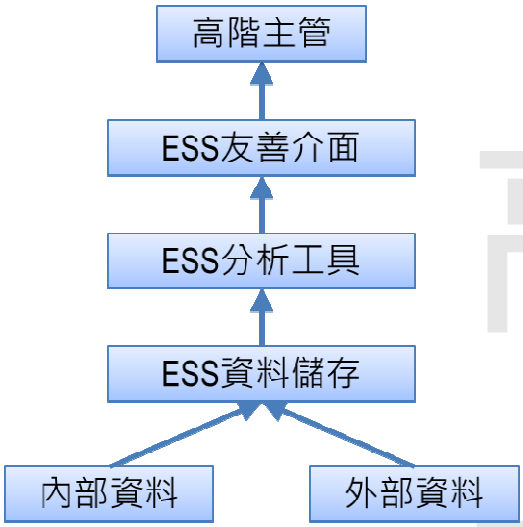
(一)高階主管支援管理系統。

(二)企業智慧（Business Intelligence）。

試題評析	本題打破傳統的MIS考題，將兩相近觀念EIS與BI放在同一題，並各配10分必須深入解釋才能拿到高分。在實務上新版的EIS稱為ESS，甚至亦有人稱為BI，因為兩者架構與使用的技術幾乎是相同的，資料皆從組織內外蒐集，皆可進行績效管理與策略規劃，差別僅在使用者不同。EIS強調為高階主管使用，但BI則使用者可能來自組織內外。在解題時EIS可考慮用架構圖說明系統的層次及使用者；BI則可用他的兩隻腳 – MI與CI進行說明。
考點命中	《高點・高上資訊管理與資通安全講義》第一回，金乃傑編撰，頁80-81。

答：

(一) 高階主管支援系統（Executive Information System, EIS）：為企業高階主管掌握營運狀況、制定決策的重要資訊系統。其利用資訊科技追蹤組織外在事件（如網路評價、競爭對手新產品、市場研究指標…等）與內部關鍵資料（如從ERP來的庫存資料、CRM取得的客戶滿意度調查…等），並將之整合儲存，配合電腦運算優勢，即時產出組織營運相關最重要的多維度資訊，例如以數位儀表板呈現各KPI達成狀況，並提供drill down向下挖掘，找到問題發生原因，讓高階主管一目了然掌握企業營運狀態。進而協助決策判斷，提升企業競爭力。其架構如下圖所示：



其中資料儲存常採用資料倉儲（Data Warehouse）技術，而常見的分析工具如OLAP或Data Mining。

(二) 商業智慧（Business Intelligence, BI）：為企業洞悉組織內外重要資料、資訊甚至是智慧的工具，透過資訊科技追蹤外在事件與內部關鍵資料，並將之整合儲存，配合電腦運算優勢，並結合企業入口網站（EIP）或企業知識入口（EKP），驗證使用者權限，根據權限提供內部員工、顧客、供應商或合作夥伴取得重要的報告、即時搜尋、執行模擬情境與預測等功能，以利決策。其組成元素如下：

1. 管理智慧（Management Intelligence, MI）：從企業內部的資訊系統，如TPS、MIS、DSS、ERP、CRM、SCM、KM取得資料，產出數位儀表板等績效指標，協助管理者掌握內部經營績效。
2. 競爭智慧（Competitive Intelligence, CI）：透過Internet、Extranet與外部資料庫，使用搜尋引擎、智慧代理人等工具，蒐集競爭環境的資訊，如市場、競爭對手、產業、產品與顧客，產出企業整體競

爭環境改變資訊、新競爭者與新產品資訊、對手動向資訊、顧客滿意度資訊。透過企業在產業環境所累積的經驗與知識，提供未來競爭策略的決策參考。

四、許多公共場所提供無線網路，方便使用者上網。請說明：（每小題10分，20分）
(一)以通訊協定角度看，IEEE 802.3所定義之LAN與IEEE 802.11所定義之WLAN有何差異？
(二)以資訊安全角度看，IEEE 802.3所定義之LAN與IEEE 802.11所定義之WLAN有何差異？

試題評析	本題必須要對網路標準有基本的認知，不然難以作答。其解題的關鍵即是802.3為有線的乙太網路；802.11為無線網路，若考生能了解此一根本的差別，要切入就不是難事。第一小題必須從網路技術的角度比較差異，而第二題可結合講義中資訊安全的攻擊方式作為答題主軸。若同學從正確方向切入，且充分了解網路攻擊之方式，此題要拿高分應非難事。
考點命中	《高點・高上資訊管理與資通安全講義》第四回，金乃傑編撰，頁48-75。

答：

(一) 從通訊協定的角度，IEEE 802.3與802.11主要差異是有線與無線，802.3又稱為乙太網路（Ethernet），為有線網路；802.11則為無線網路（一般常見為Wi-Fi）。下表比照兩協定之差異：

	802.3 LAN	802.11 WLAN
傳輸載具	雙絞線、光纖、同軸電纜	無線
最高速率	一般為100M~1Gbps，但802.3ba使用單模光纖已可達到100Gbps。	一般為54~500Mbps，但802.11ac使用8隻MIMO天線可到6.93Gbps。
傳輸距離	一般為100公尺，但802.3ba使用單模光纖已可達到40公里。	一般為半徑100公尺，但802.11p在戶外可達到1公里之半徑
共享通道方法	CSMA/CD（載波偵聽多路存取／碰撞檢測，Carrier Sense Multiple Access / Collision Detection）	CSMA/CA（載波偵聽多路存取／碰撞避免，Carrier Sense Multiple Access/Collision Avoidance）
建置難易度	成本高，因需要佈置實體線路	成本低，只要購置無線基地台即可佈建
訊號穩定度	配合switch連線等裝置後穩定度高	穩定度隨裝置數量增加而明顯降低
主要連接裝置	伺服器、個人電腦為主	筆記型電腦、智慧型手機

(二) 從資訊安全之角度，主要差異比較如下：

	802.3 LAN	802.11 WLAN
特有的安全威脅	1. 竊聽（Sniffer）：資料網路傳輸過程中被非法的第三者得知。由於區域網路（Ethernet）是共享式架構，攻擊者只要將自己的網路介面卡設定為混亂模式（promiscuous mode），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。 2. ARP欺騙（ARP Spoofing）：或稱ARP下毒。攻擊者假冒合法主機的MAC位址，使得被欺騙的主機將所有原本要送往合法主機的封包，都送至攻擊者主機上。	1. 去授權攻擊（De-authentication DoS Attack）：攻擊者不斷發出解除認證的封包給AP，由於解除連線的封包都不會經過認證，因此AP就會對正常使用者斷線。 2. 授權攻擊（Authentication DoS Attack）：攻擊者不斷發出認證的封包給AP，卻不進行後續的連線動作，請求的封包就會停在AP的request queue中，使正常的使用者無法連線。 3. 惡意無線基地台（Rogue Access Point）：又稱雙面惡魔（Evil Twins），由於只有AP對使用者確認身份，使用者卻無法對AP確認，因此攻擊者可以很容易偽造出假AP提供網際網路連線，進行竊聽。

		4. 驅車攻擊（War Driving）：攻擊者開車刺探沿途的AP，以收集AP的相關資訊，如SSID、加密種類等資訊。 5. 無線電波阻斷（Radio Frequency jamming）：利用眾多的雜訊來干擾正常的通訊，使正常的通訊在這個頻道裡無法進行溝通。
防禦優勢	攻擊皆從實體線路而來，因此遭受攻擊時只要透過防火牆阻斷攻擊端即可停止攻擊，較容易受到防火牆、入侵偵測系統或入侵防禦系統保護。	每台電腦單獨與無線基地台連線，若其中電腦遭受感染，不容易影響其他電腦；此外只要無線基地台使用WAP以上之加密協議，安全性可受到一定程度保障。
防禦限制	因乙太網路常以Hub方式連接，若區域網路內的電腦感染，容易直接影響到大批電腦，造成集體淪陷。	以現有架構無線基地台難進行統一設定，因此汰換安全的基地台或更改設定皆需要較高的成本。