《資訊管理與資通安全》

試題評析

第一題：主要測驗考生對於IT治理與組織結構的了解，主要重點在於配合治理概念的組織結構設計，屬於過往較少討論的議題。如果擁有良好的組織結構概念，由圖中可以或窺一、二；若能再深入了解、指出IT治理的精神，才能獲取較佳的成績。

第二題：應屬於今年考題中最直接、單純的題目，考生如果熟悉SET的基本觀念與形成技術，得分不算太難。

第三題：第一、二小題在入侵偵測系統中也算是基本題型，熟悉上課解析IDS、NIDS與HIDS應可得分，第二小題雖稱爲異常統計偵測及規則偵測，實際則是課堂所提異常偵測與特徵偵測。至於第三小題仍爲實作題，這些年來資訊管理依然秉持實務應用觀點的命題，因此有進行架構設計練習的考生應能獲得高分。

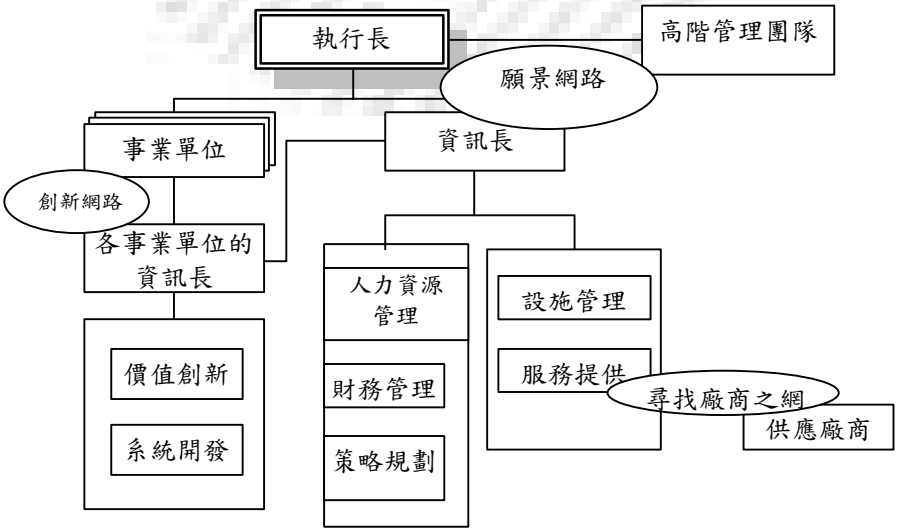
第四題：第一到第五小題在測驗考生對於資訊科技基礎建設的基本了解能力，除第二小題必須有更多的歷史觀點延伸思考，其餘均屬中規中矩的題目，得分不難。第六小題的運作模型主導融合論則是近年來討論的議題，考生如果只知道策略主導的調準論，而不了解運作模型主導的融合論，此題得分較爲不易。

一、IT的治理(Information Technology Governance)日受矚目，而IT若要提供商業價值，必須落實在IT每日運作的七個項目中，包括：「策略規劃」、「財務管理」、「價值創新」、「系統開發」、「服務提供」、「設施管理」、「人力資源管理」；並管理好「願景關係」、「創新關係」及「廠商關係」。IT部門在執行上述七項工作時，有些工作必須透過上述三項關係相關人員來合作完成。

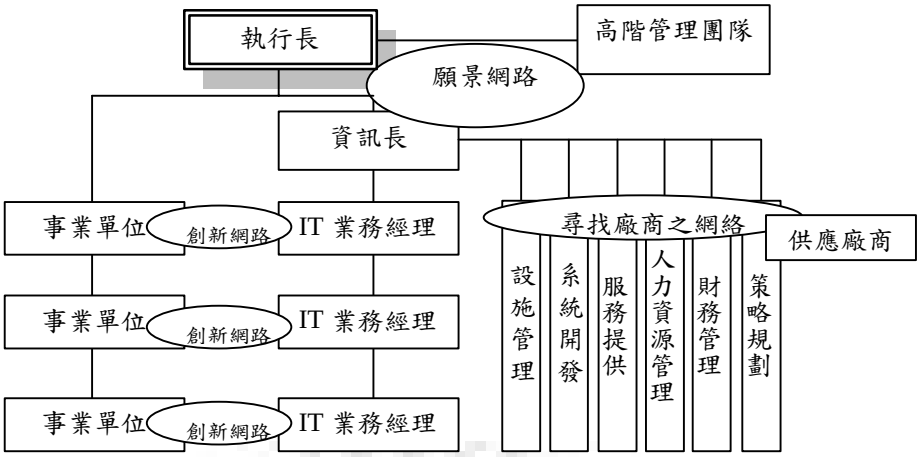
IT部門的組織設計，就是來設定執行上述七項工作時，IT人員與相關人員的職權如何劃分。學理上，IT部門組織設計原則有二：(一)鼓勵IT部門與企業其他部門共同進化(co-evolution)及(二)提供孕育IT創新應用之環境。

以下有兩種IT部門的組織圖(1)合夥式組織結構(Partner Model)、(2)平台式組織結構(Platform Model)：

(1)合夥式組織結構



(2)平台式組織結構



試討論上述兩種組織結構：

(一)在執行上述七項工作時有何不同？(5分)

(二)在管理上述三項關係時有何不同？(5分)

(三)各如何達成學理上所要求的兩項IT組織設計原則？(5分)

(四)各適合於怎樣的企業組織？(5分)

答：

(一)由組織結構可看出針對不同的組織運作，執行IT治理的七項主要工作差異爲：

1.合夥式組織：

事業部擁有自行掌握應用系統的權力，因資訊系統的創造與資金均屬事業部，故應用系統成本由其負責。而其他資訊科技設施之費用則採計費制度，由各事業部分攤。至於間接IT費用(如圖中的人力資源、財務管理與策略規劃)則由總公司處理。

2.平台式組織：

在資訊長之下設置個個IT業務經理，來和各事業單位溝通，這種模式下並不進行合夥關係，而只是形成事業單位價值創新的協助者。此模式的IT部門，依資訊長價值創造的程序分工來進行策略規劃、財務管理、人力資源管理、系統開發及設施管理的分工。

(二)在三項關係的管理上：

1.合夥式組織：

此模式由組織結構圖，可見總公司資訊長的角色較事業單位資訊長爲高，屬於企業高階領導人員，故IT能與企業願景網路連結產生IT的扭轉力。而在尋找廠商(供應商)網路上亦由資訊長指揮利用IT與客戶進行直接面對面活動。至於價值創新則由事業部門主管和事業部門資訊長攜手創造。

2.平台式組織：

由組織結構看出，此種組織模式較重視創新與尋求資源廠商(供應商)的網路，較不重視企業願景網路。

(三)

1.合夥式組織：

此模式中要達成共同進化與孕育價值創新的應用環境，資訊長形成時，IT應該已與企業策略進行調準，而爲了讓IT再創造附加價值、顧客關係、服務價值與品牌價值，成功關鍵在於公司的資訊長必須與事業單位主管合作，建立創新的IT應用。

2.平台式組織：

在此模式下組織的設計原則應由IT業務經理與負責事業單位的主管來進行IT能力的共同進化，並進行價值創新應用。

(四)

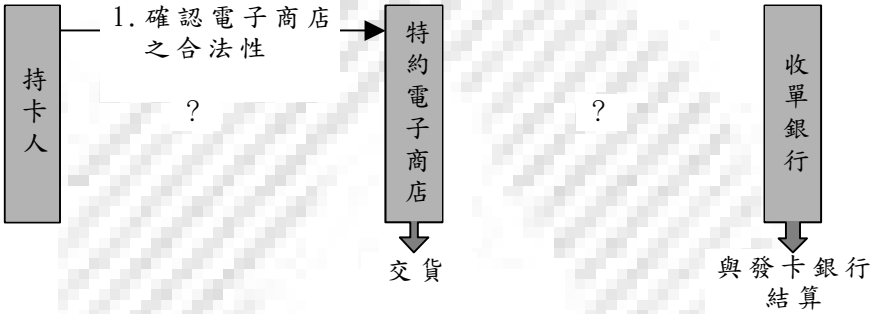
1.合夥式組織：

適合擁有多個事業部門的公司，期望利用IT創新產生跨事業部門的綜效。必須具備良好IT能力，而且IT部門與事業部門有良好的合作互動關係。

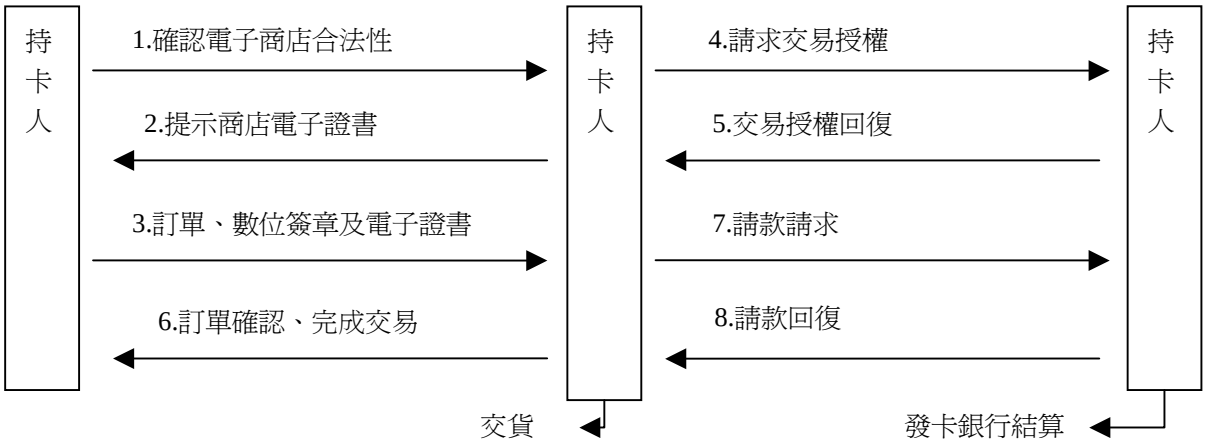
2.平台式組織：
適合全球型多事業部門公司，各事業部門尤其需特殊的IT需求，特別是高科技公司，通常其執行長或高階主管均有IT背景。

【參考書目】
1.《資訊管理：理論與實務》(六版)謝清佳、吳琮璠，智勝出版，第572頁-576頁。
2.劉英武老師上課補充講義「IT治理觀念」。

二、電子商務之交易安全，是推動電子商務的基本前提，目前用來保障線上交易安全的主要技術之一即安全電子交易SET(Secure Electronic Transaction)。SET能夠滿足付費與訂購資訊的保密性、確保所有傳輸資料的完整性、確保每一個信用卡帳戶持卡人都是合法的、確保商家與金融機構的關係、保護電子商務交易上的合法當事人及促成軟體與網路提供者之間的合作等需求。
(一)請列出SET的特色，以滿足以上的需求。(10分)
(二)請描繪完下圖，以說明SET的付款交易程序。(10分)



答：
(一)SET(Secure Electronic Transaction)採用現有的加密技術保護其線上交易，包括公開金鑰、祕密金鑰、訊息認證碼(MAC)等加密技術，也採用CA所頒發的憑證來證明交易雙方的身份，並利用數位簽章讓交易者對其進行過的交易不可否認，持卡用戶透過SET，可利用他人的個人電腦及軟體在公眾數據網路上與廠商的電腦伺服設備進行安全的交易，每筆受加密保護的交易資料將被傳送至信用卡銀行的電腦進行解密、轉帳的工作。其特性有：
1.使用訊息加密完成資訊機密性。
2.使用數位簽章確保資料完整性。
3.使用持卡人之電子證書和數位簽章雙重驗證持卡者。
4.使用商家電子證書和數位簽章雙重驗證商家。
5.使用明確的協定和訊息格式，提供不同軟體間的相融運作能力。
(二)



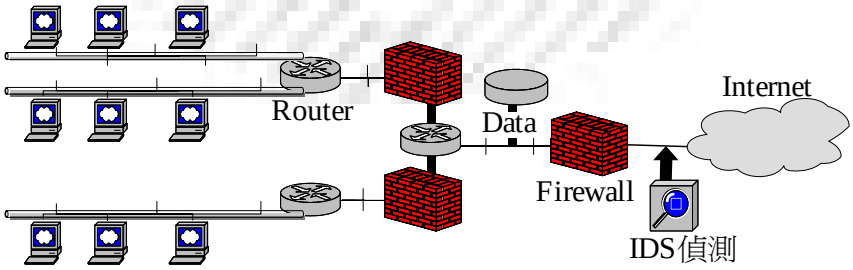
【參考書目】
劉英武老師，資訊管理講義第一回第199頁：資訊管理與資通安全單元十及上課補充SET作業流程。

三、全球熱門網站遭到入侵、攻擊的個案屢屢出現，造成了網站停擺、會員資料被盜等重大影響，因此，企業愈來愈重視網路安全的議題與入侵偵測系統(Intrusion Detection System，IDS)的建置。美國國家標準暨技術機構(National Institute of Standards and Technology，NIST)即建議企業需審慎選擇合適的偵測策略及解決方案。

(一)試簡述入侵偵測的目的。(3分)

(二)入侵偵測的方法，可分為(1)異常統計偵測法(statistical anomaly detection)，做法包括偵測門檻法與個人檔案基礎方法及(2)規則偵測法(rule-based detection)，做法包括偵測異常現象與分析辨識法，請分別說明這兩個方法的基本原理與做法。(18分)

(三)網路型IDS主要藉偵測器來蒐集資料，因此偵測器正確的配置極其重要，根據NIST，偵測器可擺於四個點，包括防火牆外側、主要網路骨幹、重要子網路及DMZ(Demilitarized Zone)，以監測不同的攻擊。網路圖與防火牆外側之配置點和功能分別如下圖、表。試以本圖為本，標示其餘三個偵測器配置點(各一個點即可)，並完成表格。(9分)



IDS偵測器配置點	功能
防火牆外側	可監測所有來自網際網路的攻擊，有利網管人員分析與掌握

答：

(一)入侵偵測目的如下：

1.監控網路(NIDS)和系統(HIDS)。

2.發現入侵企圖或異常現象。

3.主動警告，通知系統管理者現在的網路狀況。
4.將網路封包紀錄下來，以爲未來辨識或作爲證據之用。

(二)

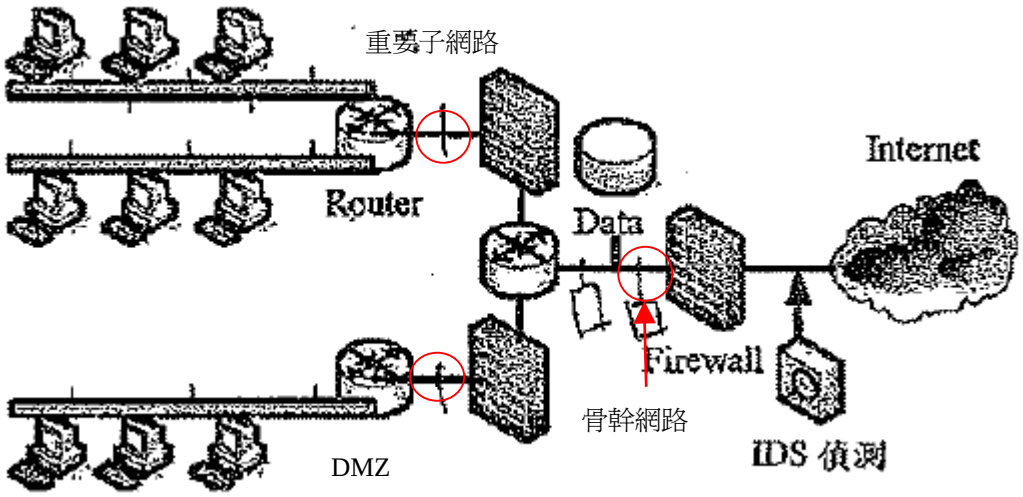
1.異常統計偵測法(Statistical anomaly detection)：這種方法是在一段時間之內，收集合法使用者的行爲，並且統計這些行爲資料進而產生檢驗規則，然後以這些規則檢視使用者是否出現不合法的行爲。這種偵測方法要定義檢測各種事件的發生頻率，也就是門檻值(Threshold)。另一種異常統計偵測的作法，是記錄每位使用者的行爲，然後以此來偵測使用者是否出現異常行爲。

2.規則偵測法(Rule-based detection)：也就是利用特徵來比對認親行爲的方式。這種方法定義了一組規則，然後比對規則與使用者的行爲，藉以決定使用者是否符合入侵者條件。這種方法會讓使用者以往的行爲與目前行爲有所差異。此外，也可以利用專家系統來辨識可疑的行爲。

簡單來說，異常統計偵測法所定義的是正常、標準或是意料中的行爲，規則偵測法則是定義適當的行爲。異常統計偵測法可以有效的防備僞裝者，因爲僞裝者通常無法模仿所冒用的使用者行爲。但是這種方法卻可能無法對付濫權者，而需要以規則偵測法才能加以辨識。實際上，爲了降低誤判，應該合併採用兩種方法，才能有效防範各種可能的入侵。

(三)

IDS偵測器配置點	功能
防火牆外側	可監測所有來自網際網路的攻擊，有利用網管人員分析與掌握。
防火牆內側	讓IDS把注意力集中在高水準的攻擊上。而且這樣可以把IDS保護在防火牆內，免於遭受攻擊。
連結DMZ的節點	DMZ (Demilitarized Zone) 爲一個放於企業私人和互聯網之間作爲緩衝地帶的電腦主機或小型網絡。它防止了外來入侵者直接存取放有企業內部資料的伺服器。互聯網上使用者只可以存取 DMZ 中的電腦。一般 DMZ 都會有企業網站，供外界提查詢及使用。
子網路節點	對子網路上所有訊息進行監聽，並發送警告與記錄所有通訊服務。



【參考書目】劉英武老師，資訊管理與資通安全第四回 第46頁-51頁。

四、自西元2000年以來，網路技術與整體網路環境越趨成熟，全世界各大企業的高階主管都十分確認，全球化創造了一個強大的需求——「組織內外要能共享資訊」，因此，功能強大而又具有彈性的資訊科技基礎建設(Information Technology Infrastructure，ITI)，遂成為做生意的先決條件。這些高階主管們都同樣關切著一個共同的議題——ITI的建置，ITI成為資訊管理主要的關鍵議題。

客製化加上全球化競爭，要求企業同時擁有兩種看似無法並存的能力：

●集中式的大規模經濟利益所帶來的成本效率和緊密整合的能力

●非集中式的快速回應個別客戶需求的能力

要同時擁有這兩種能力，企業才具競爭力，才能生存。

(一)試討論ITI能為企業提供怎樣的IT能力？(4分)

(二)ITI為什麼能讓企業同時擁有上述二種看似無法並存的能力？(4分)

(三)ITI包含那些資訊科技？(4分)

(四)ITI的核心理念就是標準化與整合，試問ITI涉及那些管理上的問題？(4分)

(五)ITI的建置，要考量那些關鍵性的議題？(4分)

(六)ITI建置的理論，有「策略主導的調準論」和「運作模型主導的融合論」，試問兩說的著重點何在？建置ITI該取那一個說法？兩說互斥嗎？兩說可以並用嗎？如何並用？(10分)

答：

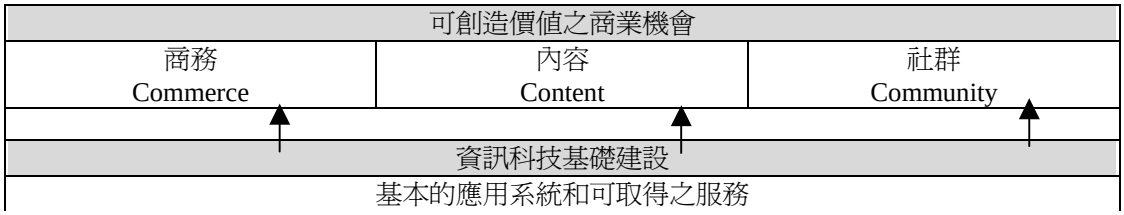
ITI自1980年代開始即是企業提升內部競爭效率的有力工具，時至今日因爲網際網路科技的IT能力讓ITI與企業和企業聯盟之間的整合運作模式更顯重要。

(一)根據ITI所包含的資訊科技，其能爲企業提供以下的能力：

1.透過網路科技的通訊能力。
2.透過網路科技建立通路管理能力。
3.結合網路科技的安全與風險管理能力。
4.利用資料庫技術的資料管理能力。
5.藉由整合資訊科技運作的IT設備管理能力。
6.協助IT運作的IT管理能力。
7.利用基礎建設創造應用系統的應用能力。
8.協助訂定企業IT架構與標準的能力。
9.IT研究與發展的能力。
10.IT教育訓練的能力。

(二)早期的資訊科技利用強大的運算能力快速產生協助經營決策的資訊，充分地創造出整合企業資料的運作模式而降低運作成本產生經營效率，此乃資料庫、軟體、硬體、區域網路與相關人員的IT能力產生的價值。而今日結合了網際網路的能力，讓企業間可以透過網際網路結合彼此的流程，分享彼此所需的營運資料，透過策略聯盟的關係，讓彼此的連結性和可達性擴張，更讓流程的運作突破時空限制而加速，從而同時掌握了與客戶、供應商之間快速回應的能力。

(三)資訊科技基礎建設包含如下：



<table>
<tr><td colspan="3">企業資源規劃(ERP)
供應鏈管理(SCM)
客戶關係管理(CRM)
決策支援系統(DSS)
專家系統(ES)
高階主管資訊系統(EIS)</td><td colspan="2">網際網路服務供應商(Interent Service Providers)
應用系統服務廠商(Application Service Providers)
委外承包商</td></tr>
<tr><td rowspan="4">技術平台</td><td colspan="4">軟體共同開發環境</td></tr>
<tr><td colspan="4">套裝軟體(如文字處理、計算表軟體、電子郵件軟體等)
程式語言(如 C++，Visual Basic，COBOL 等)
群組軟體
企業資訊貯存系統(Repository)
模式化工具
系統開發工具</td></tr>
<tr><td colspan="2">計算設施</td><td colspan="2">通訊設備</td></tr>
<tr><td colspan="2">電腦硬體
作業系統
資料庫管理系統
文件管理系統</td><td colspan="2">網路相關硬體
網路管理系統
電子郵件和檔案傳輸系統
智慧型代理軟體</td></tr>
</table>

(四)ITI透過資料標準化、作業標準化以及利用共同系統來支援跨事業單位的整合。然後利用資訊科技服務來形成大規模的經濟利益、降低運作成本。只是若完全仰賴標準和共同的系統，也常會使得企業的經營彈性降低、引發不必要的反彈，導致系統導入成本無法控制。因此ITI標準的制定便形成一項重要的管理議題。也就是我們必須要清楚認知ITI的服務是必要的工具抑或是能創造策略競爭優勢，唯有能確認企業ITI的服務方向，才能決定ITI是要利用新科技產生優勢還是重視可靠性？應該考量技術功能或者重視處理成本？應該自製或者委外？

(五)企業組織到底要不要去推行這樣的資訊科技架構，是很難以決定的事，作這個決定不應視爲單純的技術問題，這需要考量諸多建議提及綜合的組織因素來決定，其中關鍵議題包括：如何建置完善的ITI組合。

1.ITI層級的決定，決定ITI的服務項目應放置在公共基礎建設、全公司基礎建設或事業單位基礎建設中。

2.決定ITI資料標準化、流程標準化的原則。

3.決定ITI的作業架構應採集中式、分散式或混合式。

4.考量ITI的投資是一次性的全面投資或漸進的投資。

5.衡量ITI的自製或委外。

6.考量形成ITI的關係管理，包含高階主管與IT主管，IT供應商與IT人員，IT人員間，各事業單位主管與IT主管間的關係建立與維持。

7.必須衡量的組織因素則有：

(1)原有的陳舊系統；(2)組織文化與歷史；(3)資訊科技和企業領導地位；(4)IT專業人員的能力；(5)使用者的資訊素養；(6)企業環境的需求等項。

因此，組織中持續檢討「資訊科技架構」和「企業策略與組織」間的關係，十分重要。

組織面	是否適合目前的經營策略、組織結構、授權方式。 傳統的競爭對手將會如何改變市場結構。 競爭對手的價格優勢，以公司目前資訊科技架構能否承受。 公司的組織文化是否適合。 有哪些網路經營的模式適合於公司。 公司的網路策略。 如何讓銷售通路更有效。 如何對客戶提供更好的服務。
營運管理面	資訊政策是否執行的很徹底。

	如何運用資訊科技，來讓內部的作業流程更有效率。 如何運用資訊科技，來讓內部的管理流程更有效率。 如何應用網際網路，讓供應鏈更有效率。 有哪些實體轉移到虛擬基礎建設的作法？
人力面	經營網路商業的能力？ 工作小組和個人是否具有足夠的「資訊素養」？「科技素養」？ 員工是否積極並有效參與界定和管理人的資訊需求？ 教育訓練計畫。
資料管理面	交易層級的可用資料。 外在產業動態和內部的財務和市場績效之資料。 決策者能夠即時而有彈性的取得共用而一致的資料。 是否訂有資訊政策以管制組織間之資訊提取。 是否訂有跨組織間資訊溝通的政策。
技術面	用什麼技術管理資訊。 資訊溝通工具。 軟體開發工具。 應用系統。 資訊科技的行政策理結構爲何？ 資訊科技分配的情況如何？ 是否設有資訊科技推動委員會？ 資訊科技的角色爲何？ 有沒有利用資訊科技創造價值，掌握商機的機會？

(六)運作模式是描述企業未來如何運作的說明，亦即企業要如何產製產品服務，並將其交付客戶而必須進行流程整合與流程標準制定的水準。因此企業的運作模式是指將企業的產品與產品間產生交互的相關流程決定後，將IT與運作模式結合，以求IT運作的直接可行。在企業運作融合模式下的觀念乃是放棄「策略」選擇「運作」，不考慮「調準」改進行「融合」。而所謂的策略調準模式則是指資訊系統必須和企業策略相互調準，簡單來說，就是資訊系統的規劃與設計要能配合上企業的策略，只是這樣的觀念隨著經營環境的快速變遷，讓企業策略也隨之變化快速，導致將IT與企業策略配合變成相對的困難。雖然單純就運作模式或策略調準模式來看，二者似乎並不相容，不過實質上就企業而言，在建立ITI時因爲可以確立企業產品與產品間的服務相關流程，因此利用運作模式決定ITI是較爲可行的。一旦企業擁有相當的ITI後利用ITI來建立經營所需的應用系統，將應用系統的需求與策略調準相互配合，則可以幫企業帶來策略調準的彈性能力，強化企業的競爭優勢。也就是說在資訊科技基礎建設建立時考量的軟、硬體設備，通訊與資料庫及人員配置已運作模式爲基礎，而資訊系統的需求發展則以企業策略衡量，如此則倆不互斥。

【參考書目】
1.劉英武老師99MIS講義第一回，第67頁-72頁
2. 《資訊管理：理論與實務》(六版)謝清佳、吳琮璠，智勝出版，第168頁-170頁