

第二章 文獻探討

文獻探討的部分，首先瞭解組織教育訓練之目的及政府組織之訓練需求，並探討資訊安全在國際及國內的防護要求，作為本教材內容之參考。其次，探討數位學習所面臨的挑戰，並分析成人學習及教學之特性，最後探討運用學習科技於數位教材設計之重點，以作為本研究之教材設計的參考。

第一節 組織之教育訓練

一、教育訓練之目的

AECT對教育的定義是：在每個人生活的社會中，所有能讓個人在能力、態度方面發展，或能產生積極的價值觀和行為的各種活動和過程（朱湘吉，1994）。資訊知識時代，人成為組織重要的資源。組織訓練之目的在使員工擔任某項職務或工作時能具備應有的知識、技能及態度（蕭錫錡，2001）。組織通常將教育和訓練兩者並用，稱為「教育訓練」。對組織而言，教育訓練是培育人力的最主要方式（鄭錫鏞，2004）。訓練係指有計劃性、系統性的透過學習過程，以發展知識、技術或態度，並培養達成績效的行動能力，在工作領域中，訓練在使個人獲得應有的能力，使其完成工作任務。其目的在於強化員工的工作知能及工作效率，以達成組織的政策目標或重要任務，為一種具有目的性及意圖性的行為，企圖透過系統性的安排以改變或培養成員對工作的認知、態度與觀念，以符合組織的要求，達成組織的期望。（鄭錫鏞、陳定銘，2002）。簡言之，組織之教育訓練的目的

的在於提供學習後所產生的相關經驗，以達成某種行為及心理上的改變。

組織社會化為員工學習適應新工作、角色及工作文化的過程。Klein (2000) 的研究內容針對新進員工擬定認識組織之訓練計畫，透由政治、組織沿革、組織目標、組織成員、組織效能、組織術語共6個角度擬定訓練計畫，該計畫對116位新進員工進行2個月的訓練，研究結果發現：對新進員工進行訓練後，員工在了解組織目標、組織沿革及組織成員等3部分，有具體成效。訓練對協助新進員工融入組織文化，是不可缺之過程。

政府對於公務員文官體制的考訓，一直有一套既定的制度，85年成立之「公務人員培訓暨保障委員會」負責公務人員訓練進修政策。行政院人事行政局所屬之「公務人力發展中心」於85年1月成立運作，辦理行政院所屬各機關公務人員之管理發展訓練。各政府組織內，亦多由人事單位辦理內部專業訓練。隨著知識經濟時代的環境衝擊，訓練的急迫性及管道相對的多元。政府組織的訓練管道增加了數位學習方式。根據行政院主計處94年7月對221個政府組織所作的調查顯示，94年7月前已推動數位學習之機關佔64%，預計至民國96年推動數位學習之機關將會達到76%。透過數位學習的方式進行訓練，已成為公務人員訓練進修的另一種管道。

二、政府組織之訓練需求

2002年「數位台灣計畫」全力推動「600萬戶寬頻到家」、「e化生活」、「e化

商務」、「e化政府」、「e 化交通」等五大構面計畫，整合產官學研各界資源，以建設台灣成為高科技服務島。於此目標下，需著重政府組織內人力的訓練培養，並普及公務人員資訊能力。此外，處於21世紀知識領航的新經濟時代，運用高度資訊科技，加速知識的蒐集、整理、傳播與應用，顯然已經成為公私部門提升競爭力的重點管理策略。政府組織之訓練，除既有的管道之外，近年來亦建置網路學習專屬網站，例如文官 e 學苑、網路文官學院及公務人員終身學習入口網，提供公務員工數位學習管道。

訓練的需求形態大略可分為三類型：(1)、明定的需求：如政府法令或組織政策；(2)、推論的需求：依據組織或個人特殊狀況衍生；(3)、感受的需求：來自心理感覺(簡建忠，83)。近年來由於資訊科技的發展，網路及電腦的高度運用，政府積極推動電子化服務，資訊的可用性、完整性及安全性受到更高的重視，資訊安全成為全民生活及工作上會觸及的問題。電腦駭客藉由網路非法侵入政府系統竊取資料或破壞系統的不法行為時有所聞，雖然政府組織大多已運用資訊科技作為防護工具，惟資訊安全問題涉及範圍頗為廣泛，除了需對資訊安全管理對象施予專業訓練之外，員工的資訊安全概念訓練亦不可缺。

並非所有駭客均透過電腦技能或惡意程式進行竊取主機名稱、使用者登入帳號、密碼及機敏資料。駭客通常只需要透過電話詢問即可取得上述資料(Gaudin,2002)。Infotex公司指出：員工缺乏資訊安全概念是資訊安全體系最脆弱之部分。組織須訂定資訊安全政策，依循此政策進行員工資訊安全概念訓練。

美國國家電腦網路安全策略(The National Strategy To Secure Cyberspace)列出的安全重點為：1.國家網路安全回應系統；2.國家網路安全威脅及弱點降低系統；3.國家網路安全意識及訓練計畫；4.加強政府機關的網路安全；5.國家及國際間的網路安全合作；其中第3項「國家網路安全意識及訓練計畫」之重點又分為「概念」及「訓練及教育」。在概念部分，主要為建立全民的電腦網路安全概念，以確保電腦網路安全；在訓練及教育的部分，則以支持國家電腦網路安全之需要為基準，提供充分的訓練及教育，並提升既有的聯邦電腦網路安全訓練課程之效率（Yoran,2004）。

我國由行政院國家資通會報於民國九十年起啟動第一期資通安全機制計畫，針對3,713個重要政府機構建立一個完整的資通安全整體防護體系，並對二十個影響國家安全、社會安定的國家重要基礎建設資訊系統實施嚴格管制。本階段於資通安全軟硬體の建置、教育訓練の實施、資通安全管理制度的推廣等作業已具成效。因資訊通訊發展快速，新的資訊安全的議題及問題不斷產生，故必要加強實施資安作業，並於九十三年三月由行政院頒布實施第二期資通安全機制計畫，該計畫期間為九十四年至九十七年。資訊安全教育訓練必需於組織內進行，提高人員資訊安全概念，降低資訊安全脆弱程度。各組織執行資訊安全計畫，首要在於製定組織安全政策，在政策之下製定各項規範，強化組織成員的認同感與參與感，進而要求遵守規範內容，提升組織內部資訊安全等級。規範內容因組織政策而異，故有其獨特性，惟需包括安全概念、組織安全規範、社交工程等內容，

由上而下進行資訊安全概念訓練，以提昇組織成員資訊安全概念。為達到快速及一致性的傳播，組織可以透過數位學習的方式，將資訊安全政策內容、相關規範及應具備之資訊安全概念內容傳達予員工。

三、數位學習之運用及挑戰

Allen(2002)認為數位教材設計應從簡單的觀念和工作做起。對大多數人而言，先提出挑戰的任務，會使得學習更有效，假如學習者能完成挑戰，那就不必再告訴他已經知道的內容，假如學習者不能完成挑戰，他會尋求幫助，也更加珍視所獲得的資訊協助，也能更深刻體會到內容和任務的相關性。另外，數位教材應能提供學習者立即的回饋。

2005 年美國的訓練市場朝向數位學習的方式進行，數位學習的訓練方式自 2002 年至 2005 年，有巨幅的成長(Bersin,2004)。雖然如此，Bersin 的調查亦指出 E-Learning 的九大挑戰，其分別為：1·使用者接受度；2·品質；3·工具及範本；4·基礎架構；5·數位學習發展技術；6·資源；7·管理者的支持；8·教材及內容專家；9·速度／時間 (圖 2.1)。其中 rapid e-learning 的教材開發方式，被視為解決數位教材發展費時的方式。

E-Learning Challenges

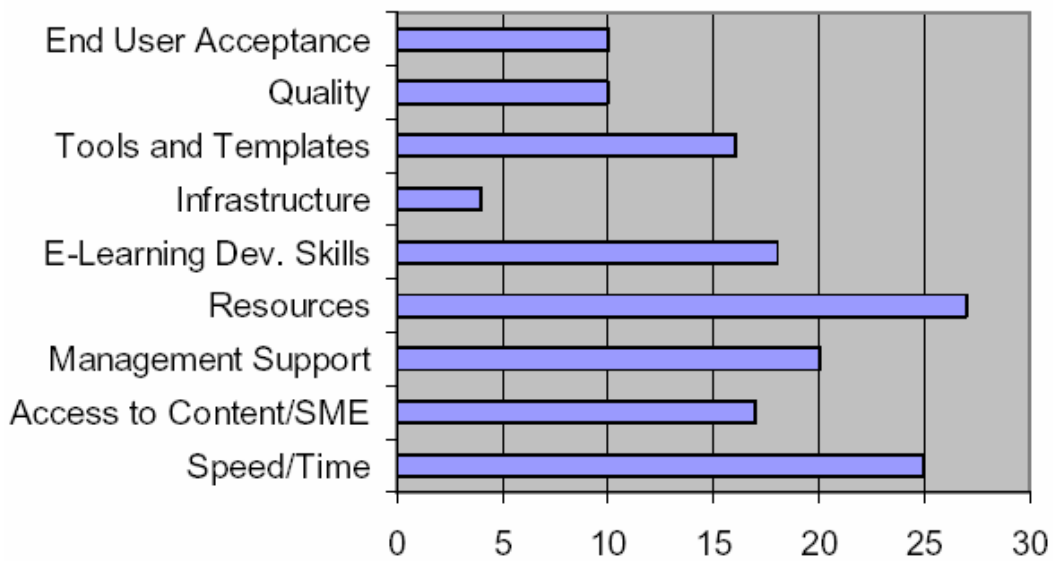


圖 2.1 Top E-Learning Developer Challenges(Bersin,2004,p4)

公務機構因業務之推動而需進行教育訓練，對於數位教材需求的急迫性高，由於各單位之業務性質各有其特殊性，除固定性如資訊、語文類之教材外，其餘之教材的共通性及再使用性並不高，變動性也很大。行政院主計處於94年9月1日公布221個公務單位之「政府機關數位學習推動情形」調查報告指出：至民國96年，預期有76%的公務機關推動機關內的數位學習，已採用數位學習之機關，所使用之教材內容與業務相關者佔71%。有關教材的來源，15%的單位未擁有教材，45%的單位之教材來源為自製，43%的單位的教材來源為購買。組織若能改善數位教材的製作方式，必能提高自製教材的比例，解決教材更換快速之問題。

第二節 成人學習

一、成人學習

美國成人教育大師Knowles認為二十世紀後，有些文化革命發生，且步調加速，個人在二十歲所獲的知識及技能，在四十歲時大多已過時。成人的學習皆源於一種需要，因此學習動機必與個人的生活角色有密切的關係。Knowles 指出二十世紀前成人與兒童均同等適用於一種學習理論，然而對於成人之學習應提出新的學習理論，以解釋成人的學習過程。成人學習比較獨立，其學習動機和需求較為明確。Knowles主張五個基本假設：一、成人具有自我導向的學習觀念，能夠為自己作決定及負責；二、成人具有豐富而多樣的生活經驗，為其學習的重要資源，但經驗也可能是學習的阻力；三、成人的學習準備與發展任務的改變有密切相關，亦即成人學習是以解決問題為考量；四、成人的學習以生活、任務及問題為中心，即學習動機的強度與學習結果是否有益於解決問題或工作表現存有密切關係，故課程設計應以環繞生活情境為中心；五、成人的學習動機大多來自個體的內在力量，例如想將工作做好（引自黃富順，民78）。Lee & Owens（2000）指出：成人學習理論應用在開發多媒體訓練課程有兩方面啟示：一、教材不能超越成人所理解的範圍；二、設定的目標必須符合成人樂於學習的程度。故組織進行教育訓練時，教學內容及教學方式應考量成人學習特質，於課程訓練後運用於實務作業，以獲得預期目標。當教材內容改以數位化的方式呈現時，則需根據教材內容的特性決定教學策略。

二、一般學習理論與成人教學

公務機構員工均為成人，故透過數位教材進行教學的過程宜以成人學習的角度進行設計。以下探討行為學派、認知學派、人本學派三大學習理論中與成人學習相關之部分理論，以符合本研究之教材設計。

(一) 行為學派：學習是在刺激環境下出現的適當反應行為，即所謂「刺激-反應的聯結」學習歷程。由行為結果來塑造及持續學習效果，也相當重視學習或訓練的遷移效果（張春興，民85）。在學習過程安排上，必須營造能夠刺激學習之環境，以及針對學習結果加以增強，使學習效果遷移至工作上（Bloom,1971，引自蕭錫錡，民90）。

(二) 認知學派：認知學派認為學習是個體對事務經由認識、辨別、理解，從而獲得新知識的歷程（蕭錫錡，民90）。當學習者發現教材內容之間或教材與其他事物之間存在有意義的關聯，並把握住此一關聯結構時，才真正產生了學習（張春興，民85）。故在教材內容設計，應善加利用成人已具有的各種經驗及先備知識，使學習與過去經驗產生連結。訊息處理理論說明人類在環境中，經由感官知覺、注意、辨識、轉換、記憶等心理活動，以吸收並運用知識的歷程（張春興，民85）。適當運用訊息處理於教學，可以滿足教學上的需求，例如「引起注意」是將感官收錄轉入短期記憶的重要歷程，訊息儲存於短期記憶後再經編碼訊息轉入長期記憶。

(三) 人本學派：成人參與學習是自發性的，也能夠決定自己想要的學習內容，

故需提供各種學習管道。此外，人本學派以學習者為中心，將生活中真實問題作為教材，讓學習者去面對問題、了解事實真相。同時使用學習契約，學習者被允許自己設定學習目標和計劃（張春興，民85）。

第三節 學習科技之運用

一、教材設計

教材的撰寫分為三個階段：1.規畫階段：決定教材的範圍與目的，亦即要知道誰要用這教材、如何用、使用時有何限制，以及撰寫時有何困難。2.撰寫階段：撰擬組織、採用簡明的文字及適切的圖表呈現內容。3.編輯階段：安排讀者試用，依試用結果修訂，以改善教材（Felker,1980,引自蕭錫錡，民90）。發展好教材需包括下列步驟：1.教學目標確認；2.教學內涵分析；3.學員者特質認定；4.行為目標的編寫；5.試題的發展；6.教學策略的分析；7.教材的編纂；8.教材的形成性評量；9.教材的修正。此外，教材應含有測驗，測驗的方式則分為形成性評量及總結性評量(蕭錫錡，民90)。系統化教學設計步驟可以分為分析、設計、發展、及評鑑，分析的階段應包括三個步驟：1.界定教學目的，即決定學習者在完成學習後應有的表現；2.分析教學內容，亦即界定學習內容的種類及下層，據以繪製內容架構圖；3.分析學習者特性。設計階段包含二個步驟：1.分析教學資源，即找出環境中的資源與限制；2.訂定教學目標：依據內容架構，撰寫學習者在完成學習後應有的表現。發展階段包括三個步驟：1.發展教學策略，即擬訂達到學習目

標之策略，例如引發學習動機、安排教學順序、選擇教學方法；2.製作教材：依教學策略發展教材；3.發展學習成果評量工具：依教學目標及內容，設計學習成果評量工具。評鑑階段的目的是在於改善課程不完美之處，可分為教學前實施的形成式評鑑及教學後的總結性評鑑。其中形成性評鑑係針對教材的原型(prototype)進行測試，以改善不完美之處。總結性評鑑則於教學結束後，針對整體教學效果作評鑑。(朱湘吉 民83)。

XIA公司則對於數位教材之發展提出另一套方式(圖2.2)，以達到製作出高品質數位教材為目標，做法上採取結合系統化教學設計步驟及運用工具軟體，以雛型化為中心，讓教材設計者及學習者能於教材發展的每一個階段均能看到教材的全貌。主要步驟強調：於教材發展過程之每一個階段均能看到最後的課程內容，亦即於設計階段即能解決結構、格式等問題，在設計階段運用彈性的重組及編排素材方式，而不影響進度及成本，並強調不需繁複的 Programming 程序，即可於教材內增加 interactive 功能。

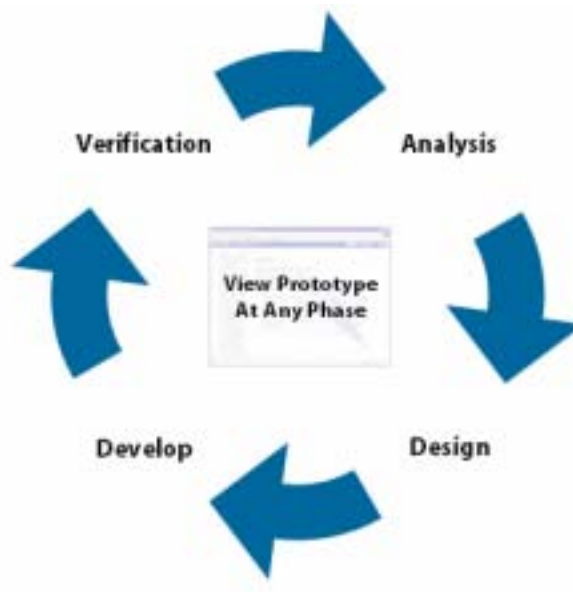


圖 2.2 Rapid e-Learning Development Process(資料來源:<http://www.xiasystems.com>)

二、學習者介面設計

數位教材之製作採取多媒體設計型式傳達教材內容，需考量教學訊息傳達策略，以期達到教學目的，故多媒體的訊息設計應以達到學習者最大的學習效果為原則。學習者透過數位教材進行學習之過程可能發生中斷學習(drop out)的情形，Jun(2005)的研究指出成人於數位學習過程發生中斷之原因為：1.缺乏時間；2.缺乏管理上的監督；3.缺少動機；4.使用科技的問題；5.缺少支援；6.個別學習的效率問題；7.不佳的課程設計。運用多媒體於數位教材，可以達到豐富教材內容的效果，但應著重設計方式，避免成為不佳的課程設計。

Lee 和Owens(2000)指出：多媒體的介面設計應能表現出採用的佈景主題、學習者特色,以及組織的環境。其要素如下:1.愈簡單愈好,適當的留白；2.重複出現在螢幕上的項目,例如:標題、回饋、連結、選單或提示等，要出現在固定的位置，

以保持一致性；3.要有一個固定一致的瀏覽介面設計，讓使用者在這個學習或績效支援環境內能操作自如；4.安排螢幕的各個項目要考慮以Z字型模式排列，圖形放左上方，文字及補充放右邊，提示及瀏覽放在下面，最常用的瀏覽放在右下方；5.要有標示，讓使用者知道離結束還有多遠；6.要有離開、目錄、往前、往後的按鈕，以利瀏覽；7.暫停記號(bookmarking)，學習者可以重返課程並瀏覽。8.字彙(Glossary)按鈕，因為學習者可能不熟悉課程中所用到的詞彙；9.說明(Help)按鈕，提供瀏覽摘要提示、補充資訊；10.重播(Repeat)按鈕，讓使用者可以在任一幕都可以重聽聲音；11.詳全文(More info)按鈕，可以取得更多詳細的說明；12.列印(Print)按鈕13.單元目錄(Lesson and Topic)按鈕，幫助使用者在單元複雜的課程中瀏覽。此外，圖像設計則應維持簡單的風格，不應分散對於文字內容的注意力。所有圖像的大小和出現位置應該一致，若圖像內有文字時，必須清晰能讀。多媒體的互動能吸引使用者的注意力，引發動機，幫助建立學習關聯。問題的回饋應該是立即的、資訊的，並且是正面而鼓勵的內容。

第四節 資訊安全管理

一、資訊安全管理系統

ISMS(Information Security Management System, 資訊安全管理系統)標準條文指出「資訊對於組織而言就是一種資產，其與其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營

運，將營運損失降到最低，得到豐厚的投資報酬」。為了確保資訊安全，我國國家資通安全會報要求3,713個政府單位於2003-2004年達成相關資安要求，故許多政府機構積極導入BS7799 資訊安全管理系統。

BS7799 最早由英國標準協會(British Standards Institute, BSI)於1999年發行，當時的版本為BS7799 Part-1 及 Part-2；2000年ISO通過Part-1為ISO 17799：Information technology – Code of practice for information security management。2002年BS7799 Part-2修訂為Information Security Management Systems – Specification with guidance for use。2005年ISO通過BS7799 Part-2成為ISO 27001，成為資訊安全管理國際標準。ISO 17799為ISMS系統實施指南，其說明ISMS之實作方式及執行時的建議。ISO 27001為陳述與驗證的依據，亦為通過ISMS系統驗證之依循要求。如表2.1所示，ISO 17799包含11大管控項目，39個管控目標及133個管控措施，目的是建立一套完整的資訊安全管理系統，以達到組織的資訊安全目標。

表 2.1 ISO 17799 11 大管控項目

Security Policy (資訊安全政策)			
Organization of information security(資訊安全組織)			
Asset management(資產管理)			
Human re- source security (人力資源安 全)	Physical and envi- ronmental secu- rity(實體與環境安 全)	Communications and operations management (通訊 與作業管理)	Information systems acqui- sition, development and maintenance(資訊系統取 得、開發及維護)
Access control (存取控制)			
Information security incident management (資訊安全事件管理)			
Business continuity management(營運持續管理)			
Compliance (遵循性)			

ISO 17799所列之11大管控項目為大方向，為達成這些管控項目，故定義了39個管控目標(Control Objectives)分別屬於這些管控項目。39個管控目標由133個管控措施(Controls)運作。11個管控項目與39個管控目標如表2.2所示。

表 2.2 IS17799:2005 NEW Structure

11 大管控項目	39 個管控目標
安全政策 (Security Policy)	提供管理階層對資訊安全的指示與支持，以符合組織需求及相關規定。
資訊安全組織 (Organization of information security)	1. 在組織中管理資訊安全 2. 維護組織資訊的安全及外部團體存取通訊或管理資訊處理設施之安全。
資產管理 (Asset management)	1. 達成組織資產適切的保護。

gement)	2. 確保資訊資產獲得適當之保護層級。
人力資源安全 (Human resources security)	<ol style="list-style-type: none"> 1. 確保員工、約聘人員及第三方使用者認知其責任及應扮演之角色及降低竊盜、詐欺、或誤用設施之風險。 2. 確保員工、約聘人員及第三方使用者對資訊安全威脅之認知及責任、義務，於工作中應具備能力以支持組織資訊安全政策，減少人員錯誤之風險。 3. 確保員工、約聘人員及第三方使用者離職或更換人員依正常程序辦理。
實體與環境安全 (Physical and Environmental Security)	<ol style="list-style-type: none"> 1. 避免營運場所及資訊遭未經授權存取、損害與干擾。 2. 避免資產遺失、毀壞或受損，並避免營運活動中斷。
通訊與作業管理 (Communications and operations management)	<ol style="list-style-type: none"> 1. 確保正確與安全地操作資訊處理設施。 2. 實施及維護資訊安全等級及維護由第三者傳遞之服務內容之一致性。 3. 降低系統失效之風險。 4. 保護軟體及資訊完整性。 5. 維護資訊處理與通訊服務之完整性及可用性。 6. 確保網路內資訊之安全，並保護支持之基礎建設。 7. 避免非授權之洩露、更改、刪除或破壞資產而損及企業活動中斷。 8. 維護組織內或外單位之間交換資料之安全性。 9. 確保電子商務服務機密性及安全的使用。 10. 偵測非授權之資料存取活動。
存取控制 (Access Control)	<ol style="list-style-type: none"> 1. 管制資訊之存取行為。 2. 避免資訊錯誤、遺失，確保授權者對於資訊系統之存

	<p>取權，並避免非經授權者存取資訊系統。</p> <ol style="list-style-type: none"> 3. 避免未獲授權之使用者存取、破壞、偷竊資訊及其作業之設備。 4. 防止未經授權之網路服務。 5. 防止未經授權的電腦存取。 6. 防止未經授權存取資訊系統內之資訊。 7. 確保使用行動式電腦作業與遠距工作設施時之資訊安全。
資訊系統取得、開發及維護 (information systems acquisition, development and maintenance)	<ol style="list-style-type: none"> 1. 確保安全為資訊系統不可缺乏的部分。 2. 避免資訊發生錯誤、遺失，未經授權修改或誤用。 3. 以密碼控制措施，保護資訊之機密性、真實性及完整性。 4. 確保系統檔案之機密性。 5. 維護應用系統軟體及資訊之安全性。 6. 降低已知之技術弱點之風險。
資訊安全事件管理 (Information security incident management)	<ol style="list-style-type: none"> 1. 報告資訊安全事件及弱點，確保與資訊系統有關之資訊安全事件及弱點得以及時改善。 2. 管理資訊安全事件並改進，確保資訊安全事件持續及有效之方式管理。
營運持續管理 (Business Continuity Management)	<p>防治營運活動的中斷，保護重要營運過程不受重大故障或災害的影響。</p>
遵循性(Compliance)	<ol style="list-style-type: none"> 1. 避免違反所有刑、民法、行政命令、管理規定或合約義務及所有安全要求。 2. 確保系統遵守組織安全政策與標準。

	3. 使系統稽核過程得到最大成效，並將稽核過程產生或受到之干擾降到最低。
--	--------------------------------------

組織導入ISMS（資訊安全管理系統）之際，會成立資訊安全組織，包含資訊安全管理委員會、資訊安全執行委員會(其下分為執行小組、內部稽核小組、文管小組)，並定義資訊安全政策與執行範圍，該政策及執行範圍經由管理委員會審核通過並行公告予員工了解。資訊安全管理系統之落實，需由全體員工共同遵循，故於ISO 27001條文A8.2.2規定，組織需進行資訊安全概念教育訓練。

建置資訊安全管理系統之始，需定義組織資產，進行資產評估，計算資產的價值，評估資產所存在的脆弱、威脅及風險的高低，對此資產所存在之風險的發生原因進行審核，並運用管控措施使風險降低或轉移。在此目標之下，管理及技術需同時並行。資訊安全的風險只能降低，無法完全去除，不同組織所能接受的風險程度亦不同，故採取的降低風險措施也不相同，故在進行ISMS資訊管理系統導入時，需依組織需求的差異性而採用不同的方式。例如，本研究對象所處機構訂定之存取控制(Access Control)採取以ID/Password的辨識方式；其他機構或許因為所能接受之風險等級極低，故採取更嚴格的指紋辨識機制作為存取控制之方式。

組織存在的環境會改變，故其所面對的風險也會改變。同樣的，組織的員工可能異動，資產可能變更、故當風險或資產有改變或有發生重大衝擊事件時，則須重新審查與調整資產評鑑內容。資產評鑑工作應視情況而執行，非僅進行一次。

經過資產建立、風險評鑑之後，需撰寫適用性聲明，即依據資產評鑑結果，

由133個管控措施逐一比對是否適用，若適用某控制措施，則相對需提出對應的四階文件資料，故適用性聲明是組織選擇適合其營運需求目標與管控措施的文件。

四階文件包含第一階的安全手冊(Security Manual)、第二階的程序書(Procedure)、第三階的作業指導書(Work Instructions, Checklists)、及第四階的表單紀錄(Records)。導入ISMS資訊安全管理系統後，所有相關作業均需留下紀錄，以作為稽核的憑據，供內部稽核與外部稽核查驗。

將PDCA (Plan,Do,Check,Act) 模式應用至ISMS (資訊安全管理系統) 之建置，即含蓋5個階段，如圖2.3所示，即：1.Plan:Establish ISMS； 2.Do: Implement and operate the ISMS； 3.Check : Monitor and review the ISMS； 4.Act: Maintain and improve the ISMS。

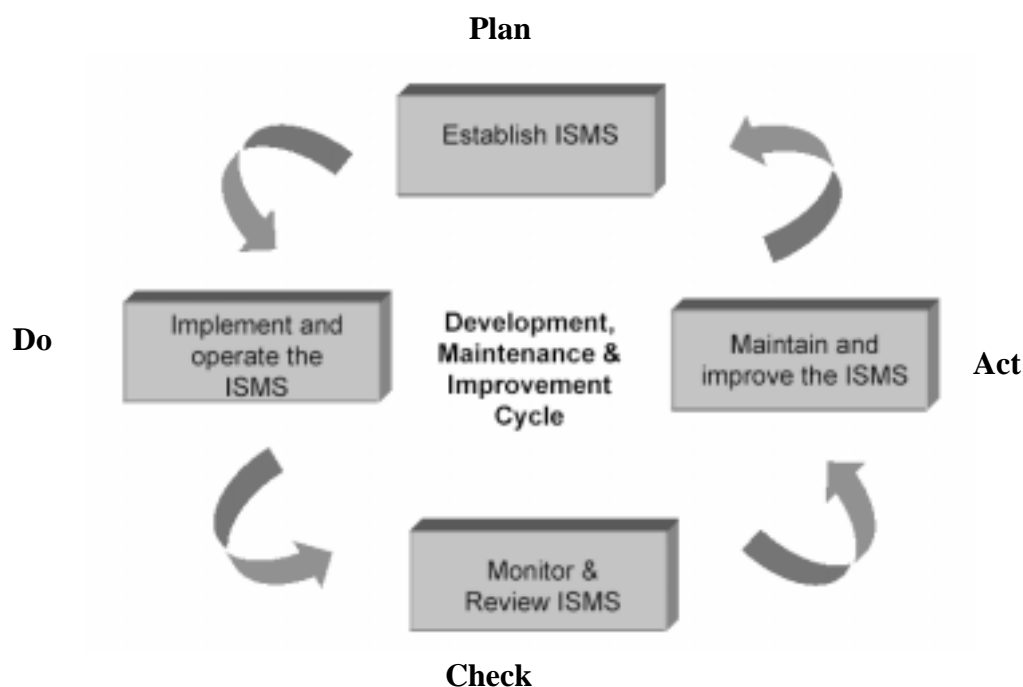


圖 2.3 PDCA model applied to ISMS processes(資料來源：ISO/IEC 27001)

二、資訊安全概念教育訓練

資訊安全最大的漏洞已經不是單純的技術問題，雖然組織導入ISMS系統，但一旦某一員工違反規定，而導致資訊安全漏洞，則可能讓組織受到損害。資訊安全的最大挑戰在於必須面對未知的人，其可能使用無法預知的方法、在未知的時間對組織進行侵入性行為。故除了安全管控措施之外，經由資訊安全概念教育訓練，使員工充分了解資訊安全的意涵及管理制度的重要性，積極協助制度的實施，尤其在提高安全認知的教育訓練，更必須全面推展至組織每位員工，該項工作需持續辦理，不可間斷。組織製定之ISMS四階文件內容，對於資訊安全實施之教育訓練對象，通常區分為一般員工、系統維護人員及管理階層。對於不同角色所施行之教育訓練內容應有所區分，以員工而言，必須使其能對組織之資訊安全政策產生認知意識，學會各基本操作技巧，並能保護組織資訊。系統維護人員則需提升其資通安全之基本技能、了解駭客入侵方式、資訊安全威脅種類、組織之弱點及進行系統弱點補強等相關作業。管理階層則須接受資訊安全基礎課程，扮演防範政策制定角色，支持資訊安全管理系統之建置。

員工為組織資訊之使用者及生產者，然而員工亦是組織資訊安全最大的防範漏洞。許多資訊安全事件之發生或因員工故意或無意的行為。實施資訊安全教育訓練則可減少員工無意的行為所引發之資訊安全漏洞。

第五節 結語

在知識經濟時代環境的衝擊及「數位台灣計畫」願景之下，公務機構必須著重人力的訓練培養，普及公務人員資訊能力及增強運用資訊科技方法，以加速知識的蒐集、整理、與傳播應用，方足以提升競爭力，故訓練需求的急迫性亦隨之增高。藉由數位學習方式，則能提供便捷、快速的訓練管道。數位學習除了考量學習平台，數位教材內容亦是影響訓練成效之要素。根據Bersin的調查指出E-Learning的九大挑戰，其分別為：1.使用者接受度；2.品質；3.工具及範本；4.基礎架構；5.數位學習發展技術；6.資源；7.管理者的支持；8.教材及內容專家；9.速度／時間。其中發展數位學習所需的資源及數位教材發展之速度／時間為影響數位學習的前兩大因素。為解決數位學習發展速度緩慢之問題，故提出由行業專家以簡易工具發展數位教材之rapid e-Learning的作法。由於公務單位業務特性殊異，故數位教材的共通性及再使用性並不高，變動性也很大，故本研究探討rapid e-Learning教材發展方式，考量成人學習特性及多媒體教材設計原則，希望在有限的經費及時間下發展合適公務單位使用之數位教材。

網路的蓬勃發展及電腦的快速運用，衍生了資訊安全問題，美國國家電腦網路安全策略將國家網路安全意識及訓練納入重點工作，而我國則由行政院國家資通會報啟動資通安全機制計畫，藉著建立 ISMS系統保護資訊不受各種威脅，確保持續營運，在此政策之下，使員工充分了解資訊安全的意涵及管理制度的重要

性，積極協助制度的實施，成為公務機構需推廣之重點，故提高安全認知的教育訓練，必須全面推展至組織每位員工。由於該項工作需持續辦理，不可間斷，故可透過數位教材進行訓練。本研究透過上述理論，據以發展資訊安全概念訓練數位教材，希望能建立公務機構發展數位教材之模式。