第二十九章

BS 7799內涵與驗證

Discover What BS7799 is and How It Validate

李殷

Yin-Lee

檔案管理局檔案資訊組 科長

Section Chief, Archives Information Division,

National Archives Administration

壹、資訊安全的定義

由於資訊技術運用範圍的不斷擴展，利用資訊技術所伴隨的安全重要性也隨之日益突顯。而什麼是資訊安全呢？依照英國標準協會BSi定義，資訊安全爲「保護的資訊機密性(Confidentiality)、 完整性(Integrity)及可用性(Availability)」（簡稱CIA），其三要素內容分述如下：

1. 機密性(Confidentiality)：確保只有經授權的人才能存取資訊。
2. 完整性(Integrity)：保護資訊與處理方法的正確性和完整性。
3. 可用性(Availability)：確保經授權的使用者在需要時可以存取資訊及相關資產。

貳、ISMS 的定義

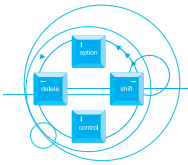
資訊安全管理系統（Information Security Management System, ISMS）的目標就是追求上述三要素的達成，當然組織在設定資訊安全三要素的優先順序及比重時，可視組織的保護資訊流程設計，賦予不同的資訊安全等級。完善的資訊安全管理系統是結合人員、政策與技術的規範準則。要確保資訊安全，則需建置金字塔式的管理架構。在金字塔底層爲資訊安全產品的提供，包含針對主

機、應用系統、資料庫、網站及電子郵件伺服器等加強技術的防護。而資訊安全政策爲由上而下的管理方式，負責教育、監控、稽核及接受回報等責任範圍。資訊安全管理系統是一個管理的流程，雖有一部分是在技術解決的方案，但管理仍是系統的本質。經由資訊安全管理系統的政策導入，再配合資訊安全方案的提供，以收管理及技術的完美整合。建置一套完整的資訊安全管理系統，藉由人員參與的過程中建立起所有使用者對資訊安全的認同感及警覺意識的提高，降低資訊安全事件對資訊的衝擊及發生的機率，大大提昇內部資訊安全等級。

參、資訊安全標準沿革

鑒於今日有關資訊安全可信賴性的策略，常在不完整的資訊內容的條件下決定，制定的標準可以減輕因不完整資訊所引發的困難，因爲標準可以減少選擇的範圍，進而簡化可信賴性供給與需求決策的過程。因此，近年國際各資訊安全管理標準相應而生，簡述如下：

1. 1990年：世界經濟合作開發組織(Organization for Economic Cooperation and Development， 簡稱OECD)轄下之資訊、電腦與通訊政策組織開始草擬「資訊系統安全指導方針」。
2. 1992年：OECD於1992年11月26日正式通過「資訊系統安全指導方針。
3. 1993年：英國工業與貿易部頒布「資訊安全管理實務準則」。
4. 1995年：英國訂定「資訊安全管理實務準則」之國家標準BS 7799第一部分，並提交國際標準組織(International Organization for Standardization， 簡稱ISO)成爲ISO DIS 14980 。
5. 1996年：BS 7799第一部分提交國際標準組織(ISO)審議之結果，於1996年2月24日結束6個月的審議，參與投票之會員國未超過三分之二。
6. 1997年：OECD於1997年3月27日公布密碼模組指導原則；英國正式開始推動資訊安全管理認證先導計畫。



7. 1998年：英國公布BS 7799第二部分「資訊安全管理規範」並爲資訊安全管理認證之依據；歐盟於1995年10月公布之「個人資料保護指令，自1998年10月25日起正式生效，要求以「適當標準(Adequacy Standard)」保護個人資料。
8. 1999年：增修後之BS 7799再度提交ISO審議。
9. 2000年：增修後之BS 7799第一部分於2000年12月1日通過ISO審議，成爲ISO/IEC 17799國際標準。
10. 2002年：英國公布增修之BS 7799第二部分。

肆、BS 7799 建置模式

BS 7799分成第一部分和第二部分，第一部分係資訊安全管理之作業要點，提供資訊安全管理的建議，但不是資訊安全管理認證之依據。BS 7799因第一部分已通過ISO審議，成爲ISO/IEC 17799國際標準，也是國際上最知名的資訊安全管理組織實施規則及系統規範最佳的準則。同時，也使得以做爲資訊安全管理認證之依據的第二部分廣爲國際所採用。BS 7799第一部分和第二部分皆已被我國標準檢驗局納爲國家標準，編號分別爲17799與17800。

BS 7799資訊安全管理驗證規範之理念與架構和ISO 14001等國際標準相同，均秉持重點要求、目標管理、風險預防、法規遵循、持續改善之制度化安全理念，執行P-D-C-A(Plan-Do-Check-Action)的工作循環。惟其風險鑑別因涵蓋所有組織、所有部門、地區、人員與活動，且其評估的合理性與一致性仍是研究的課題，相較於ISO 14001 較爲困難。

組織採用PDCA過程模式建立資訊管理系統時，PDCA流程如下：

1. 計畫（建立ISMS）：建立安全政策、目標、標的、過程及相關程序以管理風險及改進資訊安全，使結果與組織整體政策與目標相一致。
2. 執行（實施與操作ISMS）：安全政策、控制措施、過程與流程之實施與操作。
3. 檢查（監控與審查ISMS）：依據安全政策、目標與實際經驗，以評鑑及測量(適當時)過程績效，並將結果回報給管理階層加以審查。

4. 行動（維持與改進ISMS）：依據管理階層審查結果採取矯正與預防措施，以達成持續改進資訊安全管理系統。

伍、BS 7799 控制內容

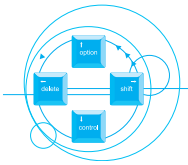
修訂的BS 7799第二部分資訊安全管理系統規範內容包含10 個管理領域、36 個控制目標及127個控制要點，10 個管理領域如下：

1. 安全政策
2. 安全組織
3. 資產分類與控制
4. 人員安全管理
5. 實體及環境安全管理
6. 通訊及作業管理
7. 存取控制
8. 系統開發及維護
9. 營運持續管理
10. 符合性

BS 7799-2:2002/ CNS 17800 標準目錄如下：

表一　BS 7799-2:2002/ CNS 17800 標準目錄如下

BS 7799-2:2002/ CNS 17800 標準目錄		
0 簡介		5 管理階層責任
0.1 概說		5.1 管理階層承諾
0.2 過程導向		5.2 資源管理
0.3 與其他管理系統之相容性		5.2.1 資源提供



1 適用範圍		5.2.2 訓練、認知與能力
1.1 概論		6 ISMS 管理階層審查
1.2 應用		6.1 概述
2 引用標準		6.2 審查輸入
3 名詞及定義		6.3 審查輸出
4 資訊安全管理系統		6.4 ISMS 內部稽核
4.1 一般要求		7 ISMS 之改進
4.2 建立及管理 ISMS		7.1 持續改進
4.2.1 建立 ISMS		7.2 矯正措施
4.2.2 實施與操作 ISMS		7.3 預防措施
4.2.3 監控與審查 ISMS		附錄 A 管制目標與控制措施
4.2.4 維持及改進 ISMS		附錄 B 標準使用指引
4.3 文件要求		附錄 C 與不同管理系統標準之關係
4.3.1 一般要求		
4.3.2 文件管制		
4.3.3 紀錄管制		

BS 7799-2:2002/ CNS 17800標準附錄A控制目標與控制措施(規範性附錄)屬強制性要求，組織應選擇適用者加以實施，對不適用之項目亦應於「適用性聲明書」文件中對不適用理由加以說明。

BS 7799-2:2002/ CNS 17800標準附錄B標準使用指引（參考性附錄）屬參考性質，相關內容並不列入驗證範圍僅供標準使用者參考。

BS 7799-2:2002/ CNS 17800標準附錄A 控制目標與控制措施(規範性附錄)雖屬強制性要求，然而也非絕對完整，組織應考慮增加其他必要的控制目標及

控制措施。CNS 17799〔ISO/IEC 17799〕條款3至條款12可提供BS 7799-2:2002/ CNS 17800標準附錄A.3至A.12所列各項控制措施在實施上協助最佳實務之建議與指導。茲摘錄BS 7799-2:2002/ CNS 17800標準附錄A.3至A.12所列各項控制措施如下：

表二 A.3 安全政策

			CNS 17799 節次
A.3.1 資訊安全政策 控制目標：提供管理階層對資訊安全的指示與支持			3.1
控制措施			
A3.1.1	資訊安全政策文件	政策文件應由管理階層核准，並以適當方式向所有員工公布與宣導。	3.1.1
A3.1.2	審查與評估	政策應定時以及有重大改變時審查，以確保合乎時宜。	3.1.2

表三 A.4 安全組織

			CNS 17799 節次
A.4.1 資訊安全基礎架構 控制目標：在組織中管理資訊安全			4.1
控制措施			
A.4.1.1	管理階層資訊安全會報	管理階層資訊安全會報可確保有明確方向，且管理階層能表現對與資訊安全有關計畫之支持。	4.1.1
A.4.1.2	資訊安全協調工作	大型組織中，應有相關單位代表組成之跨部門管理的會報，負責協調資訊安全控制措施之執行。	4.1.2
A.4.1.3	資訊安全責任的配置	個別資產之保護責任及執行特定安全程序之責任應明確劃分。	4.1.3
A.4.1.4	資訊處理設施的授	新資訊處理設施應有管理人員授權程序。	4.1.4

	權作業		
A.4.1.5	資訊安全專家的建議	向全公司內部人員或專業諮詢人員徵詢、協調資訊安全建議。	4.1.5
A.4.1.6	組織間的合作	與執法機關、主管機構、資訊服務廠商及電信公司維持適當溝通管道。	4.1.6
A.4.1.7	獨立的資訊安全審查	資訊安全政策執行狀況應獨立審查。	4.1.7
A.4.2 第三方（Third-Party）存取之安全 控制目標：爲維護資訊處理設施及資訊資產提供給第三方存取時之安全。			4.2
控制措施			
A.4.2.1	鑑別來自第三方存取之風險	第三方存取組織資訊處理設施之風險應予評鑑，並實施適當安全控制措施。	4.2.1
A.4.2.2	第三方合約中之安全要求	第三方存取組織資訊處理設施之相關事宜應有正式合約，規定所有必要安全要求。	4.2.2
A.4.3 委外作業 控制目標：當資料處理工作委外其他組織時，維持資訊安全。			4.3
控制措施			
A.4.3.1	委外合約之安全要求	組織將所有或部分資訊系統、網路、桌上電腦環境等之管理及控制工作委外時，其安全要求應於兩造合約中提出並獲同意理。	4.3.1

表四 A.5 資產分類與控制

			CNS 17799 節次
A.5.1 資產可歸責性 控制目標：爲維護組織資產適切的保護。			5.1
控制措施			
A.5.1.1	資產清冊	應製作所有與每一資訊系統相關重要資產之清冊並維護。	5.1.1

A.5.2 資訊分類 控制目標：確保資訊資產獲得適當之保護層級。			5.2
控制措施			
A.5.2.1	分類指引	資訊分類與相關保護控制措施應考量企業分享或限制資訊之需求，以及與該需求有關之業務衝擊。	5.2.1
A.5.2.2	資訊標示與處理	應制訂一套與組織採用之分類方式相符之資訊標示與處理流程。	5.2.2

表五　A.6 人員安全

			CNS 17799 節次
A.6.1 工作說明及資源分配的安全 控制目標：降低人爲錯誤、竊盜、詐欺、或誤用設施之風險			6.1
控制措施			
A.6.1.1	將安全列入工作職掌中	組織資訊安全政策中規定之安全角色與職務應於工作職掌中適當地予以文件化。	6.1.1
A.6.1.2	人員篩選及政策	正職員工在申請工作時即應進行背景檢查。	6.1.2
A.6.1.3	保密協議	員工應簽署保密合約，作爲聘僱首要條件與限制之一部分。	6.1.3
A.6.1.4	聘用條件與限制	聘僱條件與限制應說明員工對資訊安全之責任。	6.1.4
A.6.2 使用者訓練 控制目標：確保使用者了解資訊安全的威脅與問題，且有能力在日常工作中支持組織安全政策。			6.2
控制措施			
A.6.2.1	資訊安全教育與訓練	組織內所有員工及相關第三方之使用者皆應接受適當訓練以及有關組織政策及程序之例行修訂。	
A.6.3 安全及失效事件的反應處理 控制目標：將安全及失效事件所造成的損害降至最低，並監督這類事故並從中學習。			6.3

控制措施			
A.6.3.1	通報安全事件	安全事件應循適當管理途徑儘快通報。	6.3.1
A.6.3.2	通報安全弱點	應要求資訊服務之使用者在注意到系統或服務有任何明顯或可疑安全弱點或威脅時逕行通報。	6.3.2
A.6.3.3	通報軟體失效	應建立軟體失效通報程序。	6.3.3
A.6.3.4	從事件中學習	建立機制，以便量化且監控事件與失效的類型、數量與成本。	6.3.4
A.6.3.5	懲罰處理	違反組織資訊安全政策與程序之員工，應以正式懲罰處理。	6.3.5

表六 A.7 實體與環境安全

			CNS 17799 節次
A.7.1 安全區域 控制目標：避免營運場所及資訊遭未經授權存取、損害與干擾。			7.1
控制措施			
A.7.1.1	實體安全邊界	組織應採用安全邊界以保護存放資訊處理設施之區域。	7.1.1
A.7.1.2	實體進入控制措施	安全區域應有適當進入控制措施，確保只有授權人員方可進出。	7.1.2
A.7.1.3	辦公處所及設施之保護	應設立保全區域，以提供特殊安全需求，保護辦公室、房間及設施。	7.1.3
A.7.1.4	在保全區域內工作	在保全區域內工作時應採取額外控制措施及指引，以強化該保全區域之安全性。	7.1.4
A.7.1.5	隔離的收發與裝卸區	裝卸區應予管制，若可能，應與資訊處理設施隔離，避免遭未授權進入。	7.1.5
A.7.2 設備安全 控制目標：避免資產遺失、毀壞或受損，並避免營運活動中斷。			7.2
控制措施			

A.7.2.1	設備安置及保護	設備應被安置或保護以降低來自環境之威脅及災害，以及未授權存取之機會。	7.2.1
A.7.2.2	電源供應	應保護設備不受電力故障及其他電力異常影響。	7.2.2
A.7.2.3	纜線的安全	傳送資料或支援資訊服務之電源與通訊纜線應予保護，以防止竊聽或破壞。	7.2.3
A.7.2.4	設備維護	設備應正確維護，使其持續可用與完整。	7.2.4
A.7.2.5	場外設備之安全	組織場所外設備應使用安全流程及控制措施，以保護其安全。	7.2.5
A.7.2.6	設備之安全報廢或再使用	設備在報廢或再使用前應將資訊清除。	7.2.6
A.7.3 一般控制措施 控制目標：避免資訊及資訊處理設施受危害或遭竊。			7.3
控制措施			
A.7.3.1	桌面淨空與螢幕淨空政策	組織應有一桌面及螢幕淨空政策，以降低資訊未授權存取、遺失及毀損之風險。	7.3.1
A.7.3.2	財產攜出	組織之設備、資訊或軟體未經授權禁止移動。	7.3.2

表七 A.8 通訊與作業管理

			CNS 17799 節次
A.8.1 作業程序與責任 控制目標：確保正確與安全地操作資訊處理設施。			8.1
控制措施			
A.8.1.1	書面的作業程序	安全政策所規定之作業程序應製作文件記錄並維護。	8.1.1
A.8.1.2	操作變更之管制	資訊處理設施與系統之變更應予管制。	8.1.2
A.8.1.3	事件管理程序	應建立事件管理責任與程序以確保回應安全事件時迅速、有效、有條理。並收集事件相關數據資料例如稽核軌跡與檔	8.1.3

		案(logs)。	
A.8.1.4	職責區隔	職務與責任範圍應予區分，以降低資訊或服務遭未授權修改或誤用之機會。	8.1.4
A.8.1.5	分隔開發與作業設施	開發與測試用設施應與作業設施分開。軟體從開發狀態轉移至作業狀態之規則應加以界定並文件化。	8.1.5
A.8.1.6	外部設施的管理	使用外部設施管理服務前，應鑑別風險並制訂適當控制措施，並與承包商協議後併入合約。	8.1.6
A.8.2 系統規劃與驗收 控制目標：降低系統失效的風險。			8.2
控制措施			
A.8.2.1	容量規劃	應監控系統容量需求，並預估未來需求，以確保有充分處理能量與儲存空間。	8.2.1
A.8.2.2	系統驗收	應建立新資訊系統、系統升級與新版本之驗收標準，且驗收前應有適當之測試。	8.2.2
A.8.3 惡意軟體的防範 控制目標：保護軟體及資訊完整性免於受惡意軟體損害。			8.3
控制措施			
A.8.3.1	對抗惡意軟體的控制措施	應實施防備惡意軟體之偵測及預防控制措施與適當之使用者認知程序。	8.3.1
A.8.4 日常事務管理 控制目標：維護資訊處理與通訊服務之完整性及可用性。			8.4
控制措施			
A.8.4.1	資料備份	重要營運資訊及軟體應定期備份。	8.4.1
A.8.4.2	操作員日誌	操作人員應維持其活動日誌。操作員日誌應予接受定期及獨立之檢查。	8.4.2
A.8.4.3	錯誤事件登錄	錯誤應予通報，且採取矯正措施。	8.4.3
A.8.5 網路管理 控制目標：確保網路內資訊之安全，並保護支持之基礎建設。			8.5
控制措施			
A.8.5.1	網路控制措施	應實施一套控制措施，達成並維護網路	8.5.1

		安全。	
A.8.6 儲存媒體的處理與安全 控制目標：避免資產毀損及企業活動中斷。			8.6
控制措施			
A.8.6.1	可攜式電腦儲存媒體之管理	可攜式電腦儲存媒體（如磁帶、磁碟、卡帶與印出之報表等）之管理方式應有控制措施。	8.6.1
A.8.6.2	儲存媒體之報廢	儲存媒體不再使用時應以保護與安全方式報廢。	8.6.2
A.8.6.3	資訊處理程序	應建立資訊之處理及儲存程序，以防止資訊被未授權揭露或誤用。	8.6.3
A.8.6.4	系統文件之安全	系統文件應受保護，避免未授權之存取。	8.6.4
A.8.7 資訊及軟體交換 控制目標：避免組織間交換資料時遭遺失，竄改、或誤用。			8.7
控制措施			
A.8.7.1	資訊與軟體交換協議	組織間交換資訊與軟體之行爲（無論是電子或是實體交換）應有協議規範，某些協議則應制訂正式合約。	8.7.1
A.8.7.2	儲存媒體運送過程之安全	運送之儲存媒體應予保護，防止未授權遭存取、誤用或毀損。	8.7.2
A.8.7.3	電子商務安全	應防止電子商務遭詐欺行爲、合約爭議及資訊遭揭漏或竄改等情事。	8.7.3
A.8.7.4	電子郵件安全	應制定電子郵件使用政策，且執行控制措施以降低電子郵件產生之安全風險。	8.7.4
A.8.7.5	電子化辦公系統之安全	應擬定並實施政策及指引，以管制與電子辦公系統有關之企業與安全風險。	8.7.5
A.8.7.6	公共系統	資訊對外開放前應有正式授權程序，且該資訊之完整性應予保護，以避免未授權之竄改。	8.7.6
A.8.7.7	其他資訊交換形式	以語音、傳真及視訊通訊設施交換資訊時應有保護流程與控制措施。	8.7.7

表八 A.9 存取控制

			CNS 17799 節次
A.9.1 存取控制之營運要求 控制目標：管制資訊之存取行爲。			9.1
控制措施			
A.9.1.1	存取控制政策	存取控制之企業要求應予鑑定及文件化，存取行爲應僅限於存取控制政策內規定之範圍。	9.1.1
A.9.2 使用者存取管理 控制目標：確保資訊系統之存取權限適切地授權、配置及維持。			9.2
控制措施			
A.9.2.1	使用者註冊	核准存取多人使用資訊系統及服務時，應制定正式使用者註冊及註銷流程。	9.2.1
A.9.2.2	特權管理	特許權限之分配與使用應受限制與控管。	9.2.2
A.9.2.3	使用者通行碼管理	通行碼之分配應以正式管理程序控管。	9.2.3
A.9.2.4	使用者存取權限審查	管理階層應定期執行正式程序審查使用者存取權限。	9.2.4
A.9.3 使用者責任 控制目標：避免未獲授權之使用者存取。			9.3
控制措施			
A.9.3.1	通行碼之使用	選擇及使用通行碼時，應要求使用者遵守良好安全方式。	9.3.1
A.9.3.2	無人看管之資訊設備	應要求使用者確保無人看管之資訊設備有適當保護措施。	9.3.2
A.9.4 網路存取控制措施 控制目標：保護網路服務。			9.4
控制措施			
A.9.4.1	使用網路服務的政策	使用者只能直接存取被明確准許使用之服務。	9.4.1
A.9.4.2	強制存取路徑	從使用者終端機至電腦服務之存取路徑應予控管。	9.4.2

A.9.4.3	外部連線之使用者身份鑑別	遠端使用者之存取應有身份鑑別。	9.4.3
A.9.4.4	結點鑑別	連線至遠端電腦系統應有鑑別作業。	9.4.4
A.9.4.5	遠端診斷埠保護	診斷埠之存取行爲需嚴密控管。	9.4.5
A.9.4.6	網路區隔	網路應有控制措施，將資訊服務、使用者及資訊系統群組區隔。	9.4.6
A.9.4.7	網路連線控管	使用者連線能力應僅限於共享網路，以符合存取控管政策。	9.4.7
A.9.4.8	網路路由控管	共享網路應有路由控制措施，以確保電腦連線與資訊流不至破壞企業應用系統之存取控管政策。	9.4.8
A.9.4.9	網路服務之安全	組織對使用之所有網路服務其安全特性應提供一份清楚說明。	9.4.9
A.9.5 作業系統存取控制措施 控制目標：防止未經授權的電腦存取。			9.5
控制措施			
A.9.5.1	自動終端機識別功能	應考慮自動終端機識別功能，以鑑別連線至指定地點及可攜式設備。	9.5.1
A.9.5.2	終端機登錄流程	存取資訊服務應使用安全登錄程序。	9.5.2
A.9.5.3	使用者識別與身份鑑別	所有使用者應有專屬識別符碼（使用者識別序號），以便追蹤責任歸屬。應選擇一適切的身分鑑別技術已證實使用者宣稱之身分。	9.5.3
A.9.5.4	通行碼管理系統	通行碼管理系統應提供有效、互動功能，以確保通行碼品質。	9.5.4
A.9.5.5	系統公用程式之使用	系統公用程式之使用應予限制並嚴密控管。	9.5.5
A.9.5.6	保護使用者的反脅迫警報器	可能遭脅迫之使用者，應提供反脅迫警報器。	9.5.6
A.9.5.7	終端機自動關機時間	終端機若置於危險場所或所登入之系統風險極高，則閒置時應於一定時間後自動關機，避免遭未經授權存取。	9.5.7
A.9.5.8	連線時間的限制	高風險之應用系統，應設定連線時間限制，以提供多一層安全。	9.5.8
A.9.6 應用系統之存取控制			9.6

控制目標：防止資訊系統中之資訊遭未經授權存取。			
控制措施			
A.9.6.1	資訊存取限制	根據存取控制政策應限制對資訊及應用系統功能之存取。	9.6.1
A.9.6.2	敏感性系統的隔離	敏感系統應有專屬（隔離）電腦作業環境。	9.6.2
A.9.7 監控系統之存取與使用 控制目標：偵測未經授權的活動。			9.7
控制措施			
A.9.7.1	事件記錄	應製作記錄異常事件及其他安全相關事件之稽核日誌記錄，並保留至規定期間，以便有助於存取控制之監及未來之調查。	9.7.1
A.9.7.2	監控系統之使用	應建立監控資訊處理設施之使用程序，且應定期審查監視活動的結果。	9.7.2
A.9.7.3	時鐘同步	電腦系統時鐘應予同步，以使紀錄正確。	9.7.3
A.9.8 行動式電腦作業（mobile computing）與遠距工作（teleworking） 控制目標：確保使用行動式電腦作業與遠距工作設施時之資訊安全。			9.8
控制措施			
A.9.8.1	行動式電腦作業	應制訂正式政策及適當控制措施，以預防行動式電腦設施，尤其在無保護之環境下運作之風險。	9.8.1
A.9.8.2	遠距工作	應發展各項政策、流程及標準，以授權及管制遠距工作活動。	9.8.2

表九 A.10 系統開發及維護

			CNS 17799 節次
A.10.1 系統之安全要求 控制目標：確保資訊系統已建置安全機制。			10.1
控制措施			
A.10.1.1	安全要求分析	爲新系統或現有系統提升之營運要求	10.1.1

	及規格	中，應詳述各項控制措施之要求。	
A.10.2 應用系統之安全 控制目標：預防應用系統中之使用者資料遺失、遭修改或誤用。			10.2
控制措施			
A.10.2.1	輸入資料之確認	輸入應用系統之資料應予確認，以確保其正確且適當。	10.2.1
A.10.2.2	內部處理之控制	系統內應有確認檢查機制，以偵知所處理資料之塗改。	10.2.2
A.10.2.3	訊息鑑別	對於有保護訊息內容完整性之安全要求的應用程式，應採用訊息鑑別機制。	10.2.3
A.10.2.4	輸出資料之確認	應用系統資料輸出應經確對，以確保所儲存資訊之處理程序正確且合乎實際情況。	10.2.4
A.10.3 密碼控制措施 控制目標：保護資訊之機密性、鑑別性及完整性。			10.3
控制措施			
A.10.3.1	使用密碼控制措施之政策	應發展使用密碼控制措施以保護資訊之政策。	10.3.1
A.10.3.2	加密	應使用加密以保護敏感或重要資訊之機密性。	10.3.2
A.10.3.3	數位簽章	應採用數位簽章以保護電子資訊之鑑別性與完整性。	10.3.3
A.10.3.4	不可否認服務	應使用不可否認服務，以解決某事件或行爲是否發生之爭議。	10.3.4
A.10.3.5	金鑰管理	以一套公認之標準、流程及方法爲基礎之（金鑰管理系統），應加使用以支援密碼技術之運作。	10.3.5
A.10.4 系統檔案之安全 控制目標：確保資訊技術專案及支援活動以安全方式執行。			10.4
控制措施			
A.10.4.1	作業系統軟體之控制	對作業系統上軟體的實施應備有各程序以管制之。	10.4.1

A.10.4.2	系統測試資料之保護	測試資料應予保護及控制。	10.4.2
A.10.4.3	原始程式庫之存取控制	原始程式庫的存取應維持嚴謹的控制措施。	10.4.3
A.10.5 開發及支援作業的安全 控制目標：維護應用系統軟體及資訊之安全性。			10.5
控制措施			
A.10.5.1	變更管制程序	應採取正式變更管制程序以嚴格控制變更作業之實施。	10.5.1
A.10.5.2	作業系統變更的技術審查	應用系統若有變更，應審核與測試。	10.5.2
A.10.5.3	套裝軟體變更之限制	應阻止修改套裝軟體，有必要的修改應嚴格管制。	10.5.3
A.10.5.4	隱密通道及特洛依木馬程式	軟體之採購、使用及修改應予管制及檢查，以防止可能之隱密通道及特洛依木馬程式。	10.5.4
A.10.5.5	軟體開發委外	應採取控制措施以保護軟體開發委外工作的安全。	10.5.5

表十 A.11 營運持續管理

			CNS 17799 節次
A.11.1 營運持續管理之考量面 控制目標：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。			11.1
控制措施			
A.11.1.1	營運持續管理過程	全組織持續營運措施之制訂與維護作業，應有管理之過程。	11.1.1
A.11.1.2	營運持續及衝擊分析	爲整體的達成營運應根據適當風險評鑑制訂持續，一份策略計畫。	11.1.2
A.11.1.3	持續計畫之撰寫及實施	應擬訂計畫以在重要企業過程中斷或失效時，維護或即時恢復企業營運。	11.1.3
A.11.1.4	營運持續規劃框架	應維持單一營運持續計畫之框架，以確保所有計畫皆一致，並鑑別測試及	11.1.4

		維護之優先順序。	
A.11.1.5	營運持續計畫之測試、維護及重新評鑑	營運持續計畫應定時測試，並藉定期審查加以維護，以確保維持最新且有效。	11.1.5

表十一 A.12 符合性

			CNS 17799 節次
A.12.1 遵守法規要求 控制目標：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。			12.1
控制措施			
A.12.1.1	適用法令之鑑別	清楚鑑別所有與資訊系統有關之法規、管理規定及合約要求，並予文件化。	12.1.1
A.12.1.2	智慧財產權	應實施適當流程，以確保遵守（有關智慧財產權）資料之使用及專利軟體產品使用之法律限制。	12.1.2
A.12.1.3	組織記錄之保護	組織重要記錄應予保護，以防止遺失、毀損及僞造。	12.1.3
A.12.1.4	個人資訊的資料保護及隱私	應根據相關法令採取控制措施保護個人資訊。	12.1.4
A.12.1.5	預防資訊處理設施遭誤用	資訊處理設施之使用需經管理階層授權，且應採取控制措施防止該設施之不當使用。	12.1.5
A.12.1.6	密碼控制措施之規定	應有控制措施以確保符合國家協議、法律規範，或以其他工具管制密碼控制措施之存取或使用。	12.1.6
A.12.1.7	蒐證	若個人或組織行爲牽涉法律，不論民法或刑法，則提出之證據應符合相關法律規定之證據規則，或該案審理法庭之規定。此應包含符合任何公告的標準或生產規範可採納的證據。	12.1.7
A.12.2 安全政策及技術符合性之審查 控制目標：確保系統遵守組織安全政策與標準。			12.2

控制措施			
A.12.2.1	安全政策之符合性	管理者應確保其責任範圍內所有安全流程執行方式皆正確，且組織內所有區域皆應定期審查，以確保遵守安全政策及標準。	12.2.1
A.12.2.2	技術符合性的檢查	應定期檢查資訊系統是否符合安全實施標準。	12.2.2
A.12.3 系統稽核的考量 控制目標：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。			12.3
控制措施			
A.12.3.1	系統稽核控制措施	作業系統之稽核應謹慎規劃且一致，以降低企業過程中斷之風險。	12.3.1
A.12.3.2	系統稽核工具之保護	系統稽核工具之存取應加保護，以防止任何可能之誤用或破解。	12.3.2

陸、BS 7799 建置過程

依照BS 7799第二部分要求，建置資訊安全管理系統過程的關鍵要項如下：

1. 依據業務、組織、所在位置、資產及技術等特性，定義資訊安全管理系統之範圍
2. 依據業務、組織、所在位置、資產及技術等特性，定義資訊安全管理系統之政策
3. 定義風險評鑑之系統化方法
4. 鑑別各項風險
5. 評鑑各項風險
6. 鑑別並評估風險處理之選項作法（風險管理）
7. 選擇控制目標與控制措施以處理風險
8. 擬定一份適用性聲明書
9. 所提出之殘餘風險應取得管理階層之核准，資訊安全系統亦須獲得授權才能實施與操作。

在建置資訊安全管理系統的過程中，應至少有下列書面化文件：

1. 安全政策。
2. 資訊安全管理系統之範圍及支援資訊安全管理系統之各程序及控制措施。
3. 風險評鑑報告。
4. 風險處理計畫。
5. 組織爲確保有效規劃、操作與控制資訊安全過程所需之書面程序。
6. 標準要求之各紀錄。
7. 適用性聲明書。
8. 文件管制程序。

柒、BS 7799 驗證

若組織的資訊安全管理系統要通過BS 7799國際資訊安全標準驗證，則有下列六項執行步驟：

1. 建立資訊安全架構：根據BS 7799-2要求，建立適合組織需求的資訊安全架構；資訊安全架構包含安全政策、範圍、安全小組、風險評鑑、文件系統等。
2. 審查與評估：驗證機構審查組織提供的資料，評估驗證所需人天、費用及時程安排。
3. 提出申請資料：組織滿意驗證機構的報價資料後，提出一份正式的驗證申請文件。
4. 執行書面審查：驗證機構按照報價時程，執行第一階段的「書面審查」。這階段由主導稽核員審查組織資訊安全管理系統的核心要素，如「驗證範圍」、「資訊安全政策」、「風險評鑑」、「適用性聲明」及相關程序文件，用以鑑別組織資訊安全管理系統之弱點和疏漏，提供改善和解決方案。
5. 現場稽核：由驗證機構一位主導稽核員及其他稽核員所組成的稽核小組依協調的時間至受驗證單位處所實施現場稽核，稽核範圍涵蓋

「驗證範圍」內的人、事和物，審查政策、程序和目標的有效性，並確保書面和實施的一致性。

6. 驗證完成：驗證機構在完成階段審查作業後，將發出有效期間爲三年的證書。於證書有效期間內，驗證機構每半年現場稽核一次，以確保證書的有效性。在證書有效期到達時，則需透過一次重審活動來驗證和延續其有效性。

捌、結語

根據經驗顯示，組織的資訊安全能否落實，下列常爲關鍵因素：

1. 能反應營運目標的安全政策、目標及活動。
2. 與組織文化一致之實施安全保護的方法。
3. 來自管理階層的實際支持和承諾。
4. 對安全要求、風險評鑑以及風險管理的深入了解。
5. 向全體管理人員和雇員有效推廣安全的觀念。
6. 向所有雇員和承包商宣傳資訊安全政策的指導原則和標準。
7. 提供適切的訓練和教育。
8. 一個全面與平衡的量測系統，用以評估資訊安全管理的績效及回饋建議，以便進一步改善