簡介BS7799 資訊安全管理標準

作者／謝德望 中校・鄭福三 中校

提要

一、「兩國論」論點的提出造成海峽兩岸間的爭論與危機，彼此的電腦駭客們更是競相出招，互相攻擊對方的網頁，甚至國家級機關網站都遭入侵，造成兩岸間全面性撼動，國家安全議題伴隨資訊戰攻防作爲突顯而出。

二、資訊安全技術爲確保組織資訊安全重要的防護機制，且以往資訊安全議題的研究，大都著重於確保資訊安全相關技術的應用爲主，然資訊安全防範，非僅靠技術就可確保。資訊安全不僅爲技術問題，並且也是一門管理的問題。再者，資訊犯罪方法日新月異，層出不窮，資訊單位及保防部門實無能力獨自承擔；相較之下，「管理制度」就成爲協助「人」的工具，透過有效健全的資訊安全制度，不僅可大幅降低不利因素，且可降低損失到最小的目標。

三、運用BS7799資訊安全管理標準建構一套資訊安全風險管理模式，明確定義資訊安全項目與範圍，藉由科學的方法，進行評估並予以量化，提供單位資產、人員、威脅及安全弱點等風險管理，以改善國軍組織安全上的缺失。

前言

1999年8月，兩國論論點的提出造成海峽兩岸間的爭論與危機，彼此的電腦駭客們更是競相出招，互相攻擊對方的網頁，甚至國家級機關網站都遭入侵，造成兩岸間全面性撼動，國家安全議題伴隨資訊戰攻防作爲突顯而出，全面性資訊安全議題甚囂塵上，資訊之於國家安全的重要性亦趨明顯。「兩國論」期間，中國大陸的駭客族，單單在8月間，就對臺灣發動了高達72,000次的攻擊，其中有165次成功。因此，如未來無法充分發揮防護功能的國家系統，則政府運作與戰爭行動，都將受到嚴重的影響。

鑑於資訊安全技術爲確保組織資訊安全重要的防護機制，且以往對於資訊安全議題的研究，大都著重於確保資訊安全相關技術的應用爲主，如資料加(解)密、電腦病毒、防火牆技術等安全機制議題。然資訊安全防範，非僅靠技術就可確保。因資訊安全層面涵蓋甚廣，所以不僅爲技術問題，並且是管理的問題。再者，資訊犯罪方法日新月異，層出不窮，資訊單位及保防部門實無能力獨自承擔。相較之下，「管理制度」就成爲協助「人」的工具，透過有效健全的資訊安全制度，不僅可大幅降低不利因素，且可達到降低損失到最小的目標。換言之，若能從政策面管理與實體上控制著手，則能更具成效。

面對資訊安全方面的種種威脅，提出以國際資訊安全管理標準「BS7799」之驗證機制來建構國軍資訊安全風險管理模式，使評選模式發揮其功能，得以遴選具安全性之資訊系統或組織架構，增進國軍資訊系統安全之機密性、完整性及可用性。

資訊安全

一、資訊安全的意義

資訊，不僅僅是電腦、網路等相關的數據及資料，也包括資訊資產、實體資產、軟體資產、服務資產、文件、人員及國軍形象等資訊：

㈠資訊資產

包括資料庫、資料檔案、系統文件、使用手冊、教育訓練教材、操作或支援程序、緊急應變計畫、備份資訊等。

㈡實體資產

包括電腦設備（伺服器、主機等）、通訊設備（橋接器、集線器等）、儲存媒體（磁帶機、光碟等）及其他技術設備（不斷電系統、發電機等）等。

㈢軟體資產

有應用及系統軟體、開發工具、套裝軟體及公用程式等。

㈣服務資產

包含網路及語音通訊服務、公共設施（空調及電力）等。

㈤文件

有合約、財務報告等。

㈥人員

如組織編裝、人員基本資料、名冊等。

㈦國軍形象

國軍機密資料攸關國家安全，其保密作業更甚於民間企業；一旦機密外洩，有損國軍形象，更甚而危及國家安全。

在「資訊安全」作爲上，是指防止非法存取、竄改、偷竊及對資訊系統造成傷害的一些政策、程序和技術方法。①因此，對資訊安全而言，所應考量範圍包含電腦軟、硬體、網路及環境的安全技術與人員的教育訓練及安全操作觀念之養成，有關「技術」與「人」等二大因素週全的資訊安全措施，可維繫組織資訊機密性、完整性及可用性等三大目標：②

㈠機密性(confidentiality)

即資料或資訊，僅在授權時間、有授權的行爲下，公開給授權的人員、物件及過程運用。

㈡完整性(integrity)

即資料或資訊確保其精確性及完全性。

㈢可用性(availability)

即資料、資訊及資訊系統在需要用的時間中，都能使用及存取。

二、資訊所面臨的威脅

美國財星1000大企業中因爲專屬資訊遭竊，損失金額超過450億美元。在國內依國家資通安全會報技術服務中心(2002年)所做「政府機關資訊安全問卷調查」報告，內容針對國內232個公家機關、事業單位及學校所做的調查，對於資訊安全所發生災害的歸類，電力中斷佔62%、病毒感染佔56%、天然災害佔25%、駭客入侵佔18%及人爲疏失佔19%，僅有5%的單位沒有發生資訊安全事件。因此，可以瞭解資訊安全所扮演角色日趨重要。

資訊所面臨的威脅可區分爲二個方向，

① 周宣光，管理資訊系統，東華書局，2000年。

② http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD,"OECD Guidelines for the Security of Information Systems, Information Security Objective", 2001.

表一　資訊安全威脅分析表③

問題類別		原因	說明		後果
天然因素	災害	外部來的自然現象。	水災、火災、地震、打雷及溫濕度異常。		無法正常服務。
	故障	本身系統發生故障。	硬體、軟體、網路故障。		
人為因素	過失	人為錯誤或怠慢造成的故障。	疏失	・操作疏失。 ・維護疏失。 ・管理疏失。	資訊資產濫用。
	故意	人為惡意或蓄意造成之故障。	破壞	・電腦系統破壞。 ・資訊設備破壞。 ・資料程式破壞。 ・資料程式竄改。	
			不當使用	・擅自使用電腦設備。 ・未經授權使用，不當使用資料、媒體、程式。	
			隱私權	・不當蒐集資料。 ・不當使用資料。 ・不當公開資料。	

一爲天然因素；另一爲人爲因素，資訊安全威脅分析表，如表一：

㈠人爲因素

人爲的威脅可區分爲病毒與非病毒因素，病毒的來源可能爲公司外部的駭客或公司內部懷有惡意或圖謀不軌的員工；非病毒的威脅如公司員工的操作錯誤。

㈡天然因素

如硬體的損害、軟體的漏洞、網路連線或電力供應的中斷；水災、火災及地震等。

以BS7799建構資訊安全風險管理模式

一、「BS7799」資訊安全管理標準介紹

㈠標準的好處

所謂標準就是基於公平、公正、便利等觀點做好統一規範、單純化之必要條件，對於物件、性能、配置、狀態、動作、操作程序、使用方法、工作流程、責任義務、權限概念等均應有一判斷的基準。國際上標準化的主要目的在於創造下列各項可促進物品交換、技術轉移的貿易環境：④

1.產品品質及信賴性與價格相符。

2.保障使用者的安全並促進資源的再利用。

3.物品、技術與服務的互運性以及彼此之間的接續性。

4.單純化以減少塑模數，期能擴大生產規模以降低成本。

5.強化維修保養的便利性與配銷的效率性。

其中有關各國際資訊安全管理標準評估如表二⑤所示。

㈡「BS7799」簡介

「BS7799」是英國國家標準，由英國國家標準協會所制定，此項標準之主要目的在於定義及提供組織作爲保護自身或客戶關鍵資訊之私密性、眞確性及可利用性的管制方法。

㈢「BS7799」沿革

1993年英國頒佈國家的「資訊安全管

③ 黃慶堂，「我國行政機關資訊安全管理之研究」，政治大學公共行政系碩士論文，1999年。

④ 林勤經等，「網際網路發展與應用環境之安全標準芻議」，國防通信電子及資訊季刊，第2期。

⑤ Karin Hone and J.H.P. Eloff "Information security policy-what do international information security standards say?," Elsevier Science Ltd. 2002, pp.402-409.

表二　各國際資訊安全管理標準評估表

資訊安全政策特點	BS7799	BSI	COBIT	GASSP	GMITS	ISF'S
資訊安全範圍	X	X	X	X		X
資訊安全目的	X	X				
資訊安全定義	X					
資訊安全管理授權	X	X		X		X
資訊安全認可(簽署)						
資訊安全政策目標						
資訊安全政策原則	X	X				X
一法律、管理及契約承諾	X				X	X
一使用者警覺與教育	X	X			X	
一病毒預防及偵測	X					
一企業永續經營規劃	X				X	
一系統發展與採購					X	
一風險管理					X	X
一人事議題					X	X
一委外管理					X	
一事件控制					X	
一資訊分類		X				X
一存取控制		X				
角色與責任	X	X	X	X	X	X
資訊安全政策違犯與訓練	X	X	X		X	
監控與審核		X				
使用者聲明與確認						
交叉驗證	X					
共同要件						
一作者						
一資訊安全制訂日期						
一資訊安全修訂日期						
篇幅		X				
樣式		X				
版式	X	X				X
複審	X	X				X
分配	X	X				X

註：X表該標準具有此特點。

理實務準則」，1995年2月，英國標準協會即訂定「資訊安全管理實務準則」之國家標準「BS7799」第一部分，1998年2月公布「BS7799」第二部分「資訊安全管理規範」，1999年4月提出修訂版「BS7799:1999」，為目前國際上知名的安全規範；採用「BS7799」規範的國家包括挪威、荷蘭、丹麥、瑞典、芬蘭、澳州、紐西蘭及南非等國家；日本、瑞士及盧森堡等國亦對「BS7799」深表興趣。BSI於2000年3月將「BS7799」提交ISO於東京舉行之年會中審議，將其標準編號訂為ISO-17799(DIS)，由ISO/IECJTC1/SC27工作委員會進行發展與協調，其中「BS7799」第一部分已在2000年12月1日成為ISO/IEC17799國際標準。

㈣「BS7799」安全驗證標準

內容主要可分成兩個部分：

1. Part 1

為1999年版的資訊安全管理實施規則，設立產業最佳化與全面性的資訊安全管理準則，是系統規範要求的最佳應用指南，內文共分為12個章節。

2. Part 2

是1999年版的資訊安全管理系統規範，為資訊安全管理系統詳細說明書。它詳述一個資訊技術安全應用與稽核所應遵循的

架構，以做爲整個組織或部分單位資訊安全管理系統評估的基準，並可做爲一個正式驗證的標準。此規範包含4個章節與10個控管要點，36項控管目標及127項控管與評審要項來確保目標的達成。

㈤「BS7799」10個主要控管要點與控管目標

1.安全政策(Security Policy)

主要目標在於提供管理的方向與對資訊安全之保障。

2.安全組織(Security Organization)

⑴企業內部資訊安全之管理。

⑵處理組織資訊設施與資訊資產及第三者所存取的相關安全之維護。

⑶資訊處理外包予其他組織時的安全責任之維護。

3.資產分類與管制(Asset Classification and Control)

⑴對企業資產維持適當的保護。

⑵確保資訊資產可得到一個相當層級的保障。

4.人員安全(Personnel Security)

⑴降低人爲錯誤、竊取、欺騙及誤用相關設施的風險。

⑵確認使用者知道資訊安全的威脅與相關利害關係，並灌輸在常態工作程序中支持單位的資訊安全政策。

⑶降低安全意外事件與故障之損害，並從事件中監控與學習相關經驗。

5.實體與環境安全(Physical and Environmental Security)

⑴避免未授權之存取、破壞與影響企業的實體資產與資訊。

⑵避免損失、傷害或對資產的破壞與阻礙企業活動的進行。

⑶避免對資訊及其處理設施的破壞或竊取。

6.通訊與操作管理(Communications and Operations Management)

⑴確保資訊處理設備之正確與安全運作。

⑵降低系統誤失的風險。

⑶保護軟體和資訊的完整性。

⑷維持資訊處理與通訊服務的整體性與有效性。

⑸確保資訊在網路上的安全防護與相關支援的基本設施之保護。

⑹避免對資產的損害與對企業活動之阻斷。

⑺避免資訊在組織間傳遞時的漏失、竄改與誤用。

7.存取控制(Access Control)

⑴資訊存取之管制。

⑵防止對資訊系統未授權之存取。

⑶防止未授權使用者之存取。

⑷網路服務的保護。

⑸防止未授權電腦之存取。

⑹防止對資訊系統所存有之資訊作未授權之存取。

⑺偵測未獲授權之活動。

⑻確保行動運算與電信網路設施運作之資訊安全。

8.系統開發與維護(Systems Development and Maintenance)

⑴確保安全被內建在運作的系統中。

⑵防止使用者資料在應用系統中之漏失、竄改與誤用。

⑶保護資訊的機密性、確實性與完

整性。

⑷確保所有的資訊技術專案與相關支援活動都在安全考量下進行。

⑸維護應用系統軟體與資訊的安全。

9.企業永續運作管理(Business Continuity Management)

主要控管目標是要消除對企業活動的阻礙與保護關鍵性之企業活動免於嚴重障礙或災害的影響。

10.遵行(compliance)：達成目標包括

⑴避免違反民、刑事法律、法令、規範或任何安全要求之契約義務。

⑵確保系統運作遵循組織的安全政策與標準。

⑶透過系統稽核過程使效能極大化與干擾影響最小化。

二、「BS7799」安全評審驗證實施步驟

㈠安全評審驗證要項表

資訊安全管理系統規範中明確詳細的訂定控管評審目標與要項，以利評審之依據遵行，內容含括資訊安全政策、安全組織、資產分類與管制、人員安全、實體與環境安全、通訊與操作管理、存取控制、系統開發與維護、企業永續運作管理及遵行等十大範圍之細部控管評審要項計127項，經採用總加量表法，以四等級模式將評審要項內容文件格式化成爲四分量表，⑥內容分述如下：

1.資訊安全政策評審要項

⑴資訊安全政策文件：資訊安全政策文件是否建立，並有效的管理、公開與適切的與員工溝通，獲致認可。

⑵檢討與評估：資訊安全政策是否定期檢討，如果發生影響改變，是否確認政策仍然適切有效。

2.安全組織評審要項

⑴資訊安全基礎設施

A.資訊安全管理討論：資訊安全管理是否實施座談討論，以確保管……理之明確方向及獲得明顯適當管理的初始支持。

B.資訊安全協調：組織相關部門資訊安全管制之執行，是否經常實施交叉討論與協調。

C.資訊安全責任之歸屬：個別資產之保護及實行特殊的安全程序的資訊安全責任歸屬是否明確。

D.資訊處理設備之授權程序：資訊安全處理設備之管理授權程序是否明確建立。

E.專家顧問之資訊安全建議：是否遍詢組織內部與專家顧問對於資訊安全提供相關建議。

F.組織間之相互合作：是否與法律執行機構、管理機構、資訊服務提供者、電信業者等組織維持適當的合作。

G.資訊安全之個別檢核：資訊安全政策的執行是否個別獨立的檢核評估。

⑵第三者存取使用之安全

A.第三者存取資料之風險鑑定：第三者存取組織資訊處理設備所衍生之風險是否經過鑑定並適當之執行安全管制。

B.第三者契約之安全要件：第三者存取組織資訊處理設備是否簽訂包含所有安全要件之正式契約。

⑶外包

⑥ 李慶民，「以BS7799爲基建構資訊安全評選模式之研究—以虛擬私有網路系統爲例」，國防管理學院國防資訊研究所碩士論文，2000年。

委外契約之安全要件：組織之資訊系統、網路及硬體設備環境之全部或一部分委外管理與控制的安全需求，是否註明於雙方認可之委外契約中。

3.資產分類與管制評審要項

⑴資產責任

資產清單：重要資產是否詳列清單並持續維護。

⑵資訊分類

A.分類指導方針：資訊的分類與相關之保護管制是否與企業對資訊分配與限制之需求，及因此需求產生關聯之影響相稱。

B.資訊歸類與處理：按組織採用的分類方案而實施的資訊歸類與處理程序是否明確界定。

4.人員安全評審要項

⑴工作職掌定義與辦法之安全

A.職務責任之安全內涵：組織資訊安全政策中之安全角色與責任是否在工作職掌中適當地界定。

B.人事查核與政策：固定性員工之人事遴選安全查核是否在工作申請之同時完成。

C.保密切結：員工是否簽署任職保密切結。

D.員工任期與環境：對員工任職的期限與環境中是否明示其資訊安全之責任。

⑵使用者訓練

A.資訊安全教育訓練：對組織員工與相關之第三單位使用者，是否就組織政策與常規實施教育訓練及定期之在職訓練。

B.安全事件與障礙之回應

C.安全事件回報：安全事件之發生是否能經由適當的管理管道迅速回報。

D.安全弱點回報：資訊服務之使用者是否對發現足以影響系統或服務之安全弱點予以紀錄並回報。

E.軟體故障回報：軟體故障回報程序是否建立並遵行。

F.事件經驗學習：對事件與故障可能之形式、大小與耗費是否建立適當的量化與監管機制。

G.懲戒處理：對於違反組織安全政策與常規之員工，是否建立正式懲戒處理程序。

5.實體與環境安全評審要項

⑴安全範圍

A.實體安全領域：組織是否利用安全領域以保護包含資訊處理設備在內的區域。

B.實體入口管制：安全區域是否採取適當地入口管制保護，以確保僅有經過授權人員允許進入存取資料。

C.安全辦公空間與設施：是否建立安全區域以因應特殊安全需求之辦公室、房間及設備之保護。

D.安全區域之工作：是否建立安全區域工作附加管制與指導方針，以藉由安全區域之實體管制保護增強安全性。

E.輸運與裝卸區域之區隔：輸運與裝卸區域是否建立管制措施，並儘可能與資訊處理設備分隔，以避免未經授權之接近與存取。

⑵設備安全

A.裝備定位與保護：裝備是否定位並予以保護，以減低環境威脅與危險以及

未經授權接近存取機會的風險。

B.電源供應：裝備是否建立對電源誤失及其他電力異常的安全保護措施。

C.電纜線安全：傳輸資料與提供資訊服務的電源及電信網路纜線，是否建立防止竊取竊聽與損害之保護措施。

D.裝備維護：裝備維護是否依據製造廠商之指示或文件化程序，以確保裝備之持續可用性與整合性。

E.房舍外部設施安全：對組織房舍外部之裝備是否建立安全程序與管制，以維安全。

F.裝備的安全處置或再使用：裝備汰除處置或重新使用時，是否建立資訊清除措施。

⑶一般管制

A.清理桌面與螢幕策略：組織是否設立並執行清理桌面與電腦螢幕策略以減低對資訊未經授權之存取、漏失與損害之風險。

B.資產之遷移搬動：組織之裝備、資訊或軟體是否未經授權即可遷移搬動。

6.通訊與操作管理評審要項

⑴操作程序與責任

A.作業程序文件化：在資訊安全政策文件詳載確認之作業程序，是否建立文件並維護。

B.操作異動管制：對資訊處理設備與系統之異動更改，是否訂定管制措施。

C.事件管理程序化：是否建立事件管理之責任與處理程序，以確保對安全事件快速、效率與有次序的回應。

D.職責區隔：責任之義務與範圍是否明確區隔，以減低對資訊或服務未經授權之竄改、誤用的機會。

E.開發與作業設備之區隔：研發測試設備是否與一般設備區隔。

F.外部設備管理：優先使用外部設備管理服務，是否先與承包商確認獲致共識並適當地管制安全風險，且納入合約中。

⑵系統規劃與接受

A.生產能量規劃：生產能量需求是否建立監管與未來能量需求規劃的機制，以確保可行的適當處理能力與庫存。

B.系統接受：新建立、更新與升級版本之資訊系統，是否建立接受標準並於系統接受之前進行適當地測試。

C.惡意軟體入侵之防護

D.惡意軟體防備管制：對惡意軟體偵測與預防管制之保護防衛，以及適當的使用者認知規範是否建立並執行。

⑶內部行政

A.資訊備份：企業必要資訊與軟體之備份存檔作業是否定期執行。

B.作業日誌：作業人員是否建立作業紀錄日誌。

C.缺失紀錄：作業缺失是否紀錄並採取改正作業。

⑷網路管理

網路管制：是否採取相當範圍的管制以確保並維護網路安全。

⑸媒體處理與安全

A.移動式電腦媒體管理：磁帶、磁碟、卡帶及列印報表等可移動式電腦媒體之管理是否建立管制措施。

B.媒體處置：當媒體不再需要時，是否採取安全與可靠的汰除處置措施。

C.資訊操作處理程序：資訊處理

與儲存程序是否建立，以保護資訊免於未經授權之外露與誤用。

D.系統文件安全：系統文件是否對未授權之存取採取保護措施。

⑹資訊與軟體之交流

A.資訊與軟體交流協定：組織間之資訊與軟體的電子或人工交流是否建立協議，或是正式之協定，以利憑據。

B.媒體傳送安全：媒體傳送輸運是否採取保護措施，以防止未經授權之存取、誤用或訛用。

C.電子商務安全：電子商務是否建立保護措施，以防止欺詐、契約抗辯與資訊外洩及竄改等行爲。

D.電子郵件安全：電子郵件使用策略是否開發並適當地管制，以降低電子郵件導致的安全風險。

E.電子辦公室系統安全：電子辦公室系統之策略與指導原則是否備妥並執行，以管制因建置系統產生相關聯之企業與安全風險。

F.公用系統：公用資訊是否經過正式的授權程序，並且資訊之完整是否建立保護措施以防止未經授權之竄改。

G.其他形式之資訊交流：聲音、傳眞與視訊通訊器材產生的資訊交流，是否建立適當程序與管制措施，以確保安全。

7.存取控制評審要項

⑴企業資訊存取控制之需求

存取管制策略：企業存取管制需求是否建立定義與文件，且相關存取是否受限於存取管制策略中之定義規範。

⑵使用者資訊存取之管理

A.使用者登記：是否建立正式之使用者登記與登出程序，以對所有使用者資訊系統與服務授予同意存取作業。

B.特權管理：特權之使用與配置是否限制與管制。

C.使用者密碼管理：密碼配置是否透過正式的管理程序建立管制

D.使用者存取權限檢討：使用者存取權限是否建立正常程序並定期檢討。

⑶使用者責任

A.密碼使用：使用者是否依據正確的安全常規選擇與使用密碼。

B.無人看管之使用者裝備：建立無人看管之使用者裝備適當保護措施，以確保安全。

⑷網路資訊存取控制

A.網路服務使用策略：使用者是否依據其所明確授權，僅僅的直接存取網路服務。

B.執行路徑：對從終端使用者到電腦連線之路徑是否採取管制措施。

C.外部連線之使用者認證：遠端使用者之存取是否服從認證管制。

D.節點認證：遠端電腦系統的連結是否建立認證。

E.遠端診斷埠保護：遠端診斷埠之存取是否建立安全管制。

F.網路區隔：是否建立網路管制以區隔資訊服務、使用者以及資訊系統等不同群組。

G.網路連結管制：使用者網路連結權限是否依據存取管制策略所規範限制於網路資源分享。

H.網路路徑管制：網路分享是否建立路徑管制，以確保電腦連結與資訊流不

致違反4.7.1.1詳述之企業適用存取管制策略。

I.網路服務安全：組織所有網路服務之安全特性是否提供明確清楚之說明。

⑸作業系統存取控制

A.自動終端識別：自動終端識別是否建立，以對特定位置與手提式電腦裝備之連結實施驗證確認。

B.終端開機程序：資訊服務的存取是否運用安全之開機程序。

C.使用者識別與認證：所有使用者是否使用個人唯一之識別碼並單獨使用，以利所有記錄活動均可追溯至可信賴之個體。

D.密碼管理系統：密碼管理系統是否適當地提供有效且互動式之工具，以確保密碼品質。

E.系統工具使用：系統公用程式的使用是否建立限制與緊密的管制措施。

F.保護使用者之禁制警示：禁制警示是否建立，以提供警告可能成爲強制目標之使用者。

G.終端暫停：在高風險位置之閒置終端機或使用於高風險之系統，是否建立於規定之閒置時間及自行關閉之措施，以防止未經授權人員之存取。

H.連結時間限制：對高風險性應用，是否建立連結時間之限制，以提供附加之安全性。

⑹應用軟體存取控制

A.資訊存取限制：對於資訊與應用系統功能之存取，是否依據 4.7.1.1詳述之存取管制策略建立限制措施。

B.精密系統隔離：精密系統是否建立專屬隔離之運算環境。

⑺監控系統之存取與使用

A.事件記錄：評審日誌所記錄的異常與其他安全相關事件，是否彙整並保存一段協議的期間，以利未來複檢與存取管制督核之輔助。

B.監控系統使用：運用資訊處理設備實施監控之程序是否建立，且監控所獲得之結果是否定期實施檢討。

C.同步計時：電腦計時器是否同步運作，以有效精確計時。

⑻行動運算與電信網路

A.行動運算：是否建立具體策略並實施適切適當地管制，以防範行動運算裝備運作之風險，特別是在未受防護的環境。

B.電信網路：是否開發建立策略與程序以授權與管制電信網路的運作。

8.系統開發與維護評審要項

⑴系統之安全需求

安全需求分析與清單：企業對新系統或提昇現有系統的需求，是否也具體詳述對安全管制之要件。

⑵應用系統之安全

A.輸入資料確認：應用系統的資料輸入是否建立確認措施，以確保作業之正確與適切。

B.內部處理控制：確認檢查是否與系統結合，以偵測資料處理的誤用。

C.信息認證：應用上是否建立信息認證機制，以基於安全需求保護信息內容的完整。

D.輸出資料確認：應用系統的資料輸出是否建立確認措施，以確保資訊儲存程序對環境的正確與適切。

⑶加密控制

A.加密管制使用策略：加密管制使用策略是否開發建立並遵行，以有效保護資訊。

B.加密：是否使用加密機制以保護敏感或重要資訊之機密性。

C.數位簽章：是否應用數位簽章機制以保護電子資訊之確實性。

D.不可否認服務：是否使用不可否認服務以解決有關事件或動作的發生或未發生之爭辯。

E.密鑰管理：是否建立一套基於共識的標準、程序與方法的密鑰管理系統，用以支持密碼技術的使用。

⑷系統檔案之安全

A.作業軟體管制：作業系統軟體是否建立執行管制措施。

B.系統測試資料保護：測試資料是否予以保護與管制。

C.原始程式庫存取管制：原始程式庫的存取使用是否建立嚴格管制措施。

⑸開發與支援程序之安全

A.變更管制程序：程序變更作業是否按正式的變更管制程序建立嚴格之管制，以減少資訊系統的誤用。

B.作業系統變更之技術性檢討：應用系統之變更使用是否建立檢討評估與測試措施。

C.套裝軟體更動限制：套裝軟體的修改是否勸阻，並且必要之變更修改是否予以嚴格管制。

D.隱藏途徑與特洛伊病毒碼：軟體的獲得、使用與修改是否建立管制與檢查措施，以保護防止可能的隱藏途徑與特洛伊病毒碼。

E.委外軟體開發：委外軟體開發是否建立管制措施，以維安全。

9.企業永續運作管理評審要項

⑴企業永續運作管理程序：是否建立適當的管理程序，以開發與維護企業組織全面永續運作。

⑵企業永續運作與衝擊分析：是否開發建立一個根基於適當風險評估後之策略規劃，以利全面達到企業之永續運作。

⑶撰寫與執行永續運作計畫：是否開發與建立一個辦法，以將企業在運作中斷、操作疏失或緊要處理程序時之及時處理方式與內容予以維護或儲存。

⑷企業永續運作規劃架構：企業永續運作計畫的單一架構是否建立與維護，以確保所有之規劃具有一貫性，並確認測試與維護之優先權。

⑸測試、維護與重複評估企業永續運作計畫：企業永續運作之計畫是否定期測試與檢討維護，以確保計畫內容之最新與有效。

10.遵行評審要項

⑴合法需求之承諾與遵行

A.適用法規確認：對每一個資訊系統之所有相關的法令、管理與契約要件，是否明確的定義與文件化。

B.智慧財產權：是否建立與執行一個適當的程序，以確保資料與專利軟體使用時尊重智慧財產權。

C.組織紀錄之安全防衛：對於組織重要紀錄是否建立保護措施，以防止遺失、破壞與竄改。

D.資料保護與個人資訊之隱私：

是否應用適當的管制措施，以依照相關之法令保護個人之資訊。

E.資訊處理設備誤用之防範：對於資訊處理設備之使用管理是否建立授權許可機制，並應用適當的管制措施以防止對相關設備的誤用、濫用。

F.加密控制管理：是否建立適當的管制，以確保遵行國家協定、法令、規範或其他儀器之相關管制存取或加密控制之使用。

G.證據採集：牽涉法令之違犯個人或組織之行爲，是否建立對涉案犯刑的判定機制，由所顯示之證據是否符合相關法令對證據之規定或相關司法單位對同樣案件之判例爲依據。此規定也應包含遵行所有已公開之標準或被接受的證據成品之施行法規。

⑵安全政策與技術遵行之檢審

A.安全政策之遵行：管理人是否確保在其責任區內之所有安全規範得以正確的實行，且組織內之所有區域是否都納入定期檢討以確保安全政策與標準的確實遵行。

B.技術的遵行查核：資訊系統是否定期實施安全施行標準之查核。

⑶系統評審相關考量事宜

A.系統評審控制：作業系統評審是否予以規劃並意見一致，以降低企業流程分裂的風險。

B.系統評審工具保護：系統評審工具是否採取保護以防止可能之誤用或損害。

「BS7799」包含了所有企業安全政策，從安全政策的擬定、安全責任的歸屬、風險的評估到定義與強化安全參數及存取控制、防毒策略等，巨細靡遺涵蓋週全。

㈡以「BS7799」建立評選量表

將「BS7799」之評審要項按四等級模式予以格式化爲四分量表(Four-point Bipolar Scale)，建立一套可運用之評選與驗證之資訊模式，以利於資訊系統安全驗證之實施，有效掌握資訊系統安全驗證機制，確保資訊安全之全般建立與完整保障。「BS7799」資訊安全驗證規範就資訊系統應用面歸納分類之十大範圍，並據以擬定細部控制要項計127項，經按總加量表法之四等級模式予以格式化，其相關評量作業標準定義如下：

1.評量方式：實施現地評審，並就評審結果於評審要項表作勾選紀錄。

2.評量原則：評量原則採認證式，其評等方式區分如下：

⑴非常完整：符合評審要項內容精神與作法，並作業完整完善。

⑵尚屬完整：符合評審要項內容精神與作法。

⑶不盡完整：不完全符合評審要項內容精神與作法，有瑕疵但不招致急迫安全顧慮。

⑷完全未提：完全不符合評審要項內容精神與作法，有安全顧慮與缺失。

3.評分值：擬定評審要項表進行量化，明定評分值，區分如下：

⑴非常完整：3分。

⑵尚屬完整：2分。

⑶不盡完整：1分。

⑷完全未提：0分。

4.評量評定：按評量要項內容計127項，每單項評量值之總合即爲評審結果值。如全部單項評審結果均爲「非常完整」的最佳值，即爲3分(127=381分，此即爲本評量

表三　以「BS7799」對目標產品規格評審結果統計總表

項次	控制項目	管控要點	得分			備考
			A產品	B產品	C產品	
一	1.1	安全政策	5	5	3	
二	1.2	安全組織	19	19	19	
三	1.3	資產分類與管制	6	6	5	
四	1.4	人員安全	20	20	20	
五	1.5	實體與環境安全	26	25	26	
六	1.6	通訊與操作管理	49	48	46	
七	1.7	存取控制	63	62	61	
八	1.8	系統開發與維護	37	34	35	
九	1.9	企業永續運作管理	10	9	9	
十	1.10	遵行	22	22	21	
		總計	260	250	245	
		評審結論（合格或不合格）	1 合格	2 合格	3 合格	

表之總分。彙整評量鑑定等級區分如下：

⑴認證特優：381分(滿分)。

⑵認證優等：254~380分。

⑶認證合格：127~253分。

⑷認證不合格：0~126分。

5.實施評選模式實例驗證－以陸軍保修管理系統採購網路設備虛擬私有網路系統產品爲例：隨著電腦網路普及，考量資訊安全因素，假設陸軍保修管理系統擬採購虛擬私有網路系統產品，首先蒐集各式產品價格及功能，並將相關產品按價格高低先行分類，以利評選。考量價格因素，選定同價位等級之相關產品A、B、C等三種。按「BS7799」評審要項內容逐條實施評量，即可得知評選結果，如表三。

結論

BS7799是一套相當複雜的資訊安全應用與稽核的標準，且是一套完整的政策、程序、實施與組織化的架構，用來提供合理的保障使組織目標得以達成，並可避免、偵測或修正無法預期事件所造成的後果。BS7799標準的風險評估包括了兩項系統化的考量：一爲資訊技術安全的破壞造成可能的資訊保密性、眞確性與可用性失效之後果，將會導致對國軍組織的傷害；另一爲對各種威脅的防範與合理的控管都會影響這些破壞發生的實際可能性。

根據過去文獻研究，對資訊安全風險考量，大部分偏重於資訊安全技術方面，鮮少融入組織對選擇資訊安全之行爲及風險的預測，藉由風險管理，對危險預測並預防，以降低危安事件的肇生；運用BS7799資訊安全管理規範建構一套資訊安全風險管理模式，明確定義資訊安全項目與範圍，藉由科學的方法，進行評估並予以量化，提供單位資產、人員、威脅及安全弱點等資訊安全風險，並可建立定性的分析，擬定相關對策，以改善國軍組織資訊安全上的缺失。

作者簡介

謝德望中校，中正理工學院電機系48期、中正理工學院電研所28期。曾任排長、教官、連長、資訊督導官、教官。現於國防大學中正理工學院國科所攻讀博士。

鄭福三中校，國防管理學院資管系31期、國防大學國防管理學院國防資訊研究所7期。曾任資參官、資訊室主任、中端台台長。現任陸軍後勤學校資訊室主任。