# 資訊安全管理系統驗證作業的研究
# A Study on the Certification of Information Security Management Systems


樊國楨
鈺松國際資訊股份有限公司顧問
北市敦化南路 2 段 38 號 4 樓之 1
kjf@iss.com.tw

方仁威
交通大學資訊管理研究所博士研究生
新竹市大學路 1001 號管理二館
u8834811@cc.nctu.edu.tw

林勤經
國防部通信電子資訊局　局長
台北郵政 90019 號信箱
abelin01@yahoo.com

黃景彰
交通大學資訊管理研究所　教授
新竹市大學路 1001 號管理二館
jjhwang@spring.iim.nctu.edu.tw



## 摘要

今日有關資訊安全可信賴性的策略，均是在不完整的資訊內容下做決定的，標準可以減輕因不完整資訊所引發的困難，因為標準可以減少選擇的範圍而簡化可信賴性供給與需求決策的過程。本文植基於經濟部標準檢驗局依據國際標準及其相關組織已頒佈之規範，於資訊安全管理系統及其驗證作業加以探討，並研提可作為我國與國際接軌之資訊安全管理系統不同等級之驗證要求構想。



**關鍵詞：**
1.驗證(Certification)
2.符合性評鑑程序(Conformity Assessment Procedure)
3.資訊安全管理系統(Information Security Management System)
4.標準(Standard)
5.信賴(Trust)

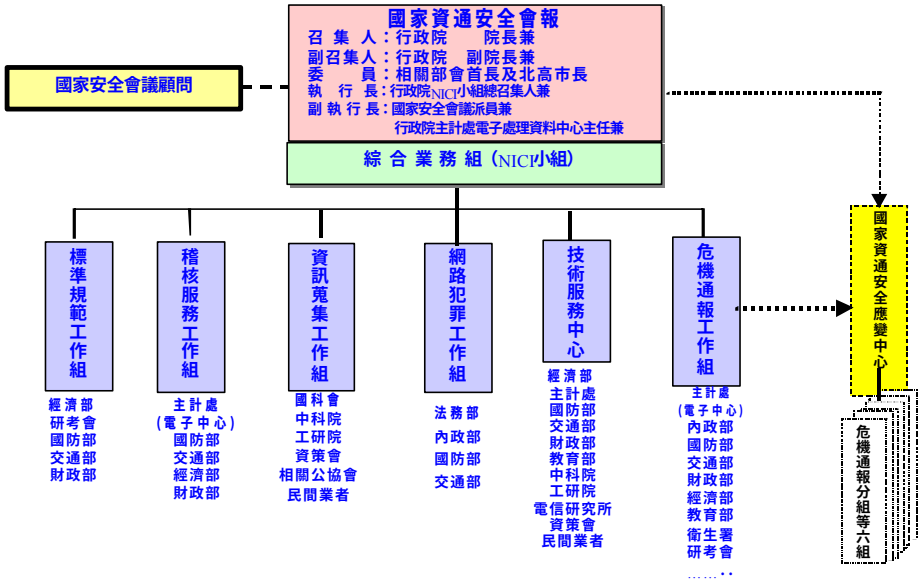

## 一、前言

2001 年 2 月 5 日，行政院以「台九十經字第 00 七四三一號函」，函送「建立我國資通訊基礎建設安全機制計畫」至行政院各部會行處局署暨省市政府、各縣市政府，請切實配合辦理[3]，正式開啟我國資訊安全發展的新頁。

1999 年春季，有關單位鑑於通資訊基礎建設安全對國家的重要性，著手規劃「我國通資訊基礎建設安全機制」中，並於去(2000)年 3 月 27、28、30、31 日舉辦 4 天之討論會[9]。由於我國現有之通資訊安全措施均侷限於局部性，並無整體防護、識別及回復能力等，國家安全會議於去年 5 月奉 總統指示研提「建立我國通資訊基礎建設安全機制」建議書，並經 總統於同年 8 月 30 日核定。2000 年 9 月 15 日，行政院以「台九十科字第二七一七九號函」，函請行政院國家資訊通信基本建設專案推動(簡稱 NII(National Information Infrastructure))小組規劃辦理；經審慎研擬，於今(2001)年 1 月 2 日面報行政院院長後，1 月 9 日經行政院院長核定同意辦理，1 月 17 日並經行政院第 2718 次院會通過，1 月 31 日召開「國家資通安全會報」第一次會議，期以 4 年的時間，完成「建立我國通資訊基礎建設安全機制計畫」[4~ 6]。

前述計畫在行政院正式成案之前，動員人數之多、牽涉層面之廣、民間互動之深等各方面，於我國資訊安全領域均屬空前[1][4][8]，未來對資訊安全方面之科技專案研發方向，可能亦將產生深遠的影響。根據今(2001)年 4 月 24 日奉行政院院會核定修訂辦理之前述計畫版本[4]國家通資安全會報組織運作架構如圖 1.1 所示，其中標準工作規範組由經濟部主責、研考會、國防部、交通部、財政部配合協辦，職掌如下：

1. 訂定資通安全技術標準。
2. 訂定各機關辦理資通安全有關作業規範。
3. 規劃建置資通安全檢測技術。
4 規劃建置資通安全驗證方法。
5. 規劃建置資通安全認證程序。




NICI：**行政院資訊通信發展推動小組**(National Information and Communication Initiative)。

**圖** 1.1：**國家資通安全會報組織運作架構**

**為達成前述計畫之工作計畫目標，標準檢驗局已根基於世界貿易組織烏拉圭回合多邊貿易談判協定**(The Results of The URUGUAY Round of Multilateral Trade Negotiations)**技術性貿易障礙協定**(Agreement of Technical Barriers to Trade，**簡稱** TBT)**附件** 1~3(Annex 1~3)**之規範，分以：**

1. **資訊技術安全評估共通規範**(ISO/IEC 15408)**系列、資訊安全管理**(ISO/IEC 17799)、**軟體處理評估**(ISO/IEC TR 15504)**等標準之制定。**
2. ISO/IEC 15408 **系列標準中針對不同產品(例：存取管制、密碼模組、金鑰憑證發行及管理)之保護剖繪**(Protection Profile)**與其之共通性檢測技術之建置。**
3. **將** BS7799-2(Information Security Management Part 2：Specification for Information Security Management)**轉定為國家標準，建置我國通資訊安全之管理系統驗證作業體系。**
4. **符合** ISO/IEC Guide 62、ISO/IEC Guide 65 **與** ISO/IEC 17025 **之要求，分別建置通資訊安全管理系統認證、產品驗證認證以及實驗室認證之認證程序。**

**推動相關工作中。**

**本文植基於資訊安全管理系統驗證作業，分別在第二節與第三節簡析其與諸如品質管理系統、環境管理系統的異同以及於我國相關認驗證作業之準備工作並提出風險分級之驗證基準構想，第四節是本文的結論。**

## 二、資訊安全管理相關規範簡述

**國際間建立數位社會資訊安全管理認證的工作，可以上溯至** 1988 **年** 11 **月，針對資訊安全專業人員應有的基本知識**(Common Body of Knowledge，**簡稱**CBK)**如何認證呢？專門認證資訊安全專業人員的機構：國際資訊系統安全授證公會**(International Information System Security Certification Consortium，**簡稱**$(ISC)^2$)**在英國的索爾斯伯利**(Selisbury)**正式成立了，通過**$(ISC)^2$ **包含如表** 2.1 **所示十大類** CBK **的測驗(通常是** 6 **小時的時間對** 250 **題選擇題作答)**[6]，**答對** 70%**常模分配且已從事三年以上之資訊安全相關工作的人，方取得資訊安全師**(Certified Information Systems Security Professionals，**簡稱** CISSP)**的資格。**CISSP **的頭銜並非終身擁有，每三年必須重新評核，通過後方再授證。**CIPS(Canadian Information Processing

Society)、CSI(Computer Security Institute)、ISSA(Information Systems Security Association)等機構均承認 CISSP 的證書。(ISC)$^2$ 之外，SANS 等機構針對資訊安全專業技術(例：UNIX Security、Instrusion Detection Systems 等)亦有系列認證測試；除了資訊安全專業人員的授證外，資訊系統安全管理規範的國際標準制定工作也在持續推動之中[10][14]，表 2.2 是其發展簡史，表 2.3 是其增修後正式提交 ISO 審議之內容概述。

表 2.1：美國(ISC)$^2$ International Information Systems Security Certification Consortium 舉辦之資訊安全師證照認證考試範疇

1. 執權控制(Access control)。
2. 應用程式安全(Application Program Security)。
3. 通訊安全(Communications Security)。
4. 電腦結構與系統安全(Computer Architecture and System Security)。
5. (電腦)操作安全([Computer] Operations Security)。
6. 密碼學(Cryptography)。
7. 法律、調查與倫理(Law, Investigations and Ethics)。
8. 實體安全(Physical Security)。
9. 政策、標準與組織(Policy, Standards and Organization)。
10. 風險管理與業務持續運作規範(Risk Management and Business Continuity Planning)。

表 2.2：資訊安全管理認證簡史

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)成為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個月的審議後，參與投票之會員國未超過三分之二。
6. 1997年：
   6.1 OECD於1997年3月27日公布密碼模組指導原則。
   6.2 英國正式開始推動資訊安全管理認證先導計畫。
7. 1998年：
   7.1 英國公布BS 7799第二部分：「資訊安全管理規範」並為資訊安全管理認證之依據。
   7.2 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，成為ISO/IEC 17799國際標準。。
10. 2001年(？)：資訊安全管理認證正式成為ISO 17799國際標準。

註：目前英國之外，已有荷蘭、丹麥、挪威、瑞典、芬蘭、澳洲、紐西蘭、南非同意使用BS 7799，日本、瑞士、盧森堡等表示對BS 7799的興趣。

**表 2.3：BS7799 內容增修概述**

| | 內容 | 1999年增修部分 |
|---|---|---|
| 一 | 安全政策 | 強化評估鑑核章節。 |
| 二 | 安全組織 | 1.強化第三者存取控管事項。2.增加委外安全管理章節。 |
| 三 | 資產分類與控制 | 增加安全標號管理章節。 |
| 四 | 人員安全 | 增加重大事故學習章節。 |
| 五 | 實體與環境安全 | 加強辦公室與員工安全的注意事項，同時減少強調專用電腦房的應注意事項。 |
| 六 | 電腦與網路管理 | 1.詳細規範開放系統安全事項。2.增加公眾可用系統安全章節。<br>3.改名為通訊與操作管理。 |
| 七 | 系統存取控制 | 1.強化系統監控事項。2.增加可攜式資訊使用安全章節。 |
| 八 | 系統開發與維護 | 1.增加密碼技術控管章節。2.增加可信賴資訊系統章節。 |
| 九 | 業務持繼運作規劃 | 詳細規範安全衝擊分析與計畫撰寫方式。 |
| 十 | 遵行 | 1.強化法規事項。2.增加事件蒐集方式章節。3.增加密碼控管法規章節。 |

**資料來源：**Parkin, R. (1999) BS 7799, in Web Sec'99

資訊安全管理驗證規範之理念與架構和 ISO 14001 等相同，均秉持如圖 2.1 所示之。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，執行如圖 2.2 所示之 P-D-C-A(Plan -Do- Check-Action)的工作循環，唯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[7]，相較於 ISO 14001 較為困難，圖 2.3 是資訊安全管理風險評估過程之圖示與說明，圖 2.4 是風險分析、風險鑑別與風險管理關係之示意說明[11~12]。

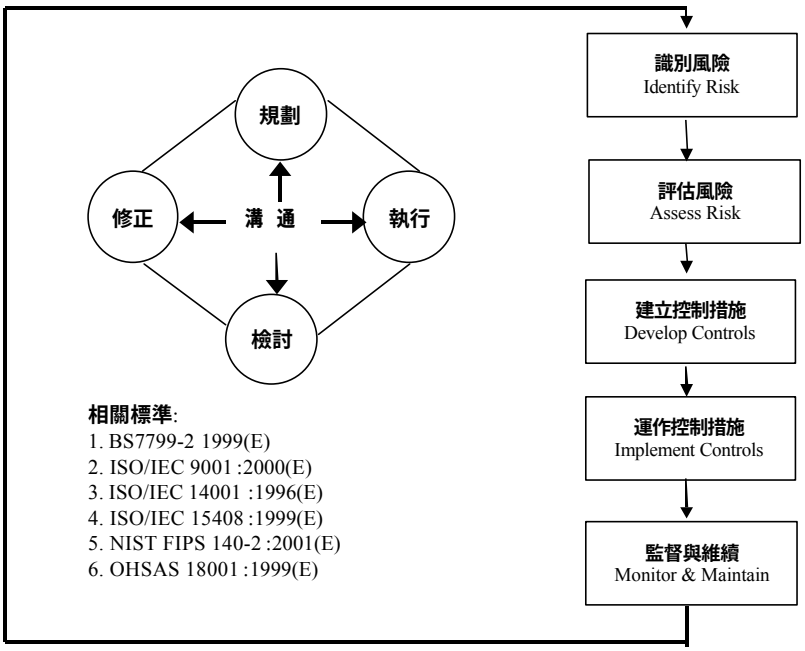



**圖 2.1：制度化的安全管理**

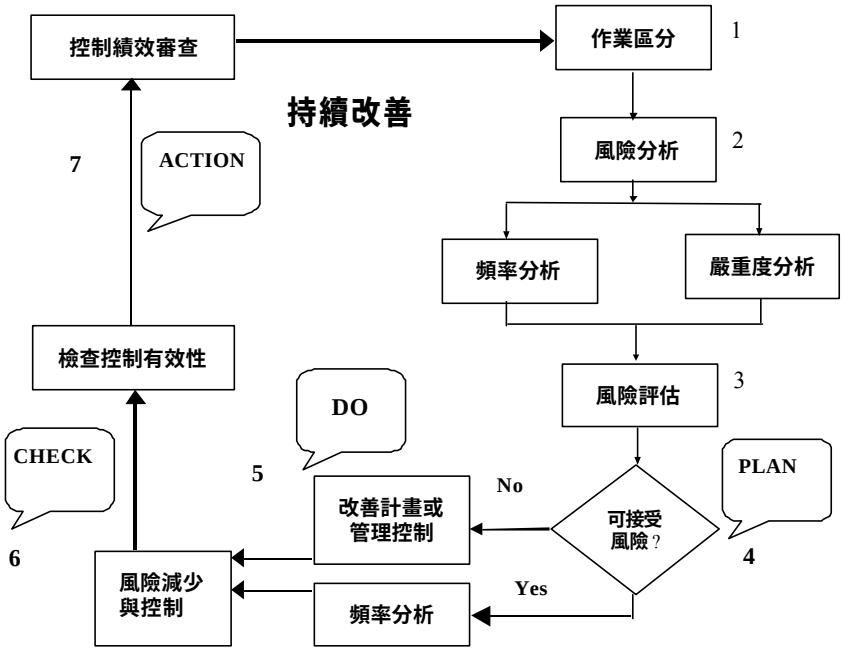



**圖** 2.2：**資訊安全管理系統風險管理步驟示意說明**

| 下面任何一個威脅會透過右邊的脆弱性發生嗎？ | 所透過之脆弱性 |
|---|---|
| 資訊遭未經授權的外洩、變更或損毀<br>資訊因粗心而遭變更損毀<br>資訊未被傳遞或傳遞不當<br>服務被阻絕或退步 | 人事<br>設施及設備<br>應用<br>通訊<br>環境軟體及作業系統 |
| | 產生下面任何一個風險嗎？ |
| | 金錢損失<br>生產力損失<br>困窘 |

威脅：與任何營運機能、過程及活動有關的資訊安全性可從許多方式受到威脅。銀行業已辨識出其發生將會損弱對一營運機能產品服務之信心或其整體性，或是驚擾營運永續性的 4 個特定威脅。

下表針對這 4 個威脅逐一說明。

| 威脅 | 說明 |
|---|---|
| 資訊遭未經授權的外洩、變更或損毀 | 此威脅為人於正常職責執行中存取或未存取工作過程而使資訊遭意外或故意釋出及遭故意之添補、變更或損毀。 |
| 資訊因粗心而遭變更或損毀 | 此威脅為資訊因不小心、疏忽或意外而遭漏失、添補、變更或損毀。此威脅的發生可能來自人們的行為或不行為、硬體、軟體或通訊故障及天災。 |
| 資訊未被傳遞或傳遞不當 | 此威脅為紙張或電子格式的資訊遭意外刪除及不當傳遞。此包括硬體、軟體及通訊故障與天災。 |
| 服務被阻絕或退步 | 此威脅為整個工作過程或某工作部份發生了出乎計畫外的短期或長期退步表現或可用性不足。 |

**圖** 2.3:**風險評估過程圖示及其說明**

**脆弱性：脆弱性為威脅發生所透過之方法。**
**下表逐一說明這些脆弱性。**

| 脆弱性 | 說明 |
|---|---|
| 人事 | 此脆弱性說明員工、廠商及約聘人員。此處理了員工訓練及對部門運作程序及控制之瞭解與遵守度。 |
| 設施及設備 | 此脆弱性說明工作區域及設備的實體安全，及對工作區域及設備的存取。 |
| 應用 | 此脆弱性說明一事業機能所用的資訊處理方法。應用牽涉到對輸入的處理以產生輸出。 |
| 通訊 | 此脆弱性說明資訊在兩個端點之間的電子移動。 |
| 環境軟體及作業系統 | 此脆弱性說明應用程式被研發及執行所在的作業系統軟體及子系統。 |

**風險分類：在進行風險評估時，有三個主要風險一定要被考慮。**
**下表逐一說明這些風險分類。**

| 風險分類 | 說明 |
|---|---|
| 金錢損失 | 金錢損失的定義為有價值物損失或成本、支出增加。金錢損失風險越高或損失的潛在價值越高，事業機能風險的分類也越高。<br>舉例：<br>有價值物－現金<br>－債券<br>－資金轉移<br>增加成本：－發行債券<br>－遭竊<br>－不利的法律判決等 |
| 生產力損失 | 當職員無法繼續執行其指定職責或當職責執行須被重複時，生產力損失就會發生。當事業機能無法可用或當結果不正確時，就會發生工作中斷或努力重複。 |
| 對機構的困窘 | 此風險分類考慮影響公信度的情況。機密性、精確性及一致性應亦被考慮。 |

**圖** 2.3:**風險評估過程圖示及其說明(續)**

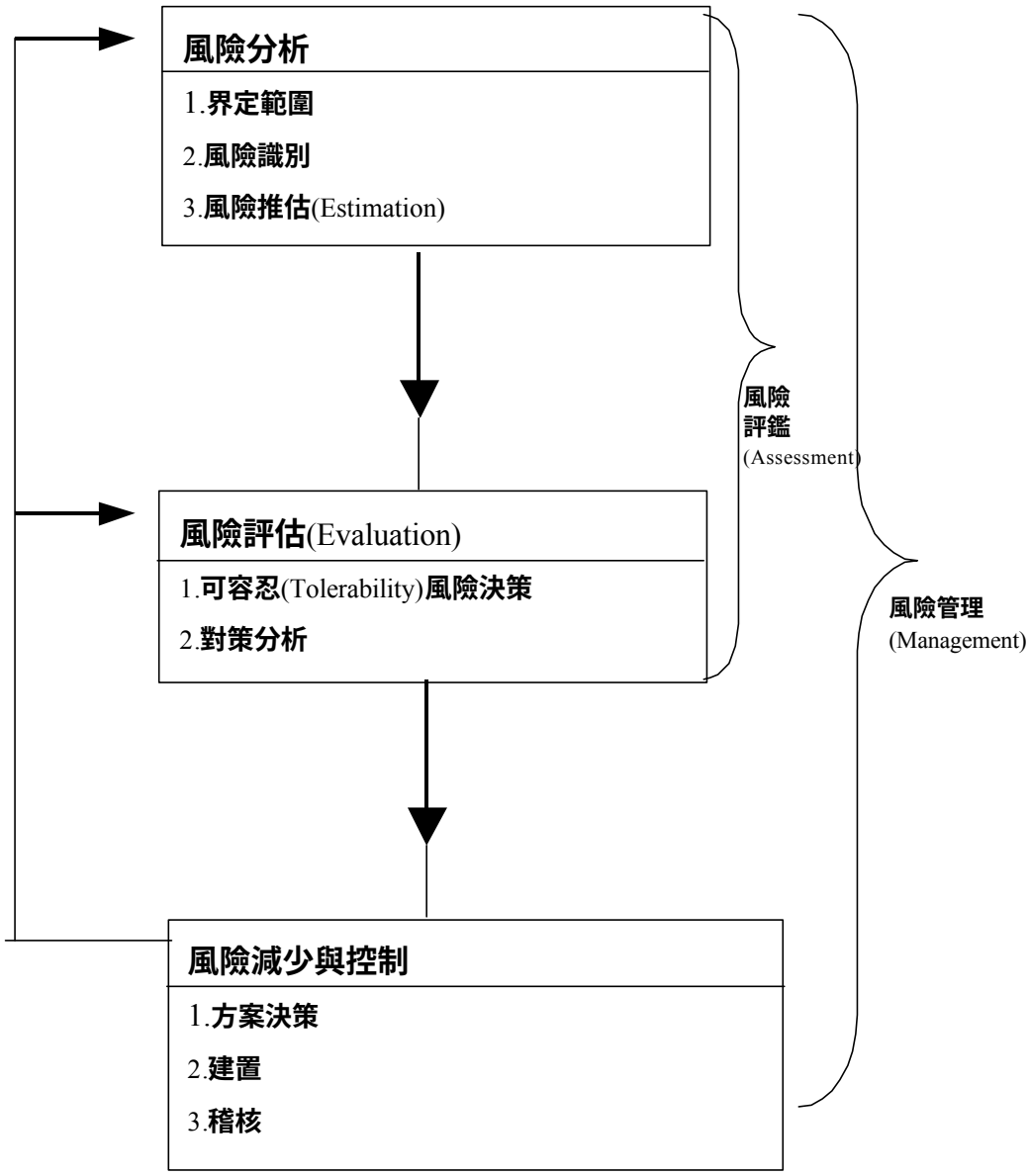



**圖 2.4：風險分析、風險評鑑與風險管理關連示意說明**

## 三、資訊安全管理系統認、驗證機制

鑑於我國品質管理及環境管理方面之驗證發展迅速，蔚為風潮，唯發證品質良莠不齊，易對貿易產生負面影響，經濟部特於 1997 年 3 月 5 日以經濟部商檢字第 86350708 號令訂定發布「中華民國品質管理及環境管理認證制度實施辦法」，並於同年 3 月 26 日以經濟部商檢字第 86260244 號令訂定發布「中華民國品質管理及環境管理認證委員會設置要點」，設置中華民國品質管理及環境管理認證委員會專責辦理相關認證業務，並自 1998 年 7 月 30 日起正式受理相關驗證機構與稽核員訓練機構之認證申請。根基於前述辦法第四條之用詞定義：

1. 認證：指主管機關給予書面正式承認驗證或訓練機構有能力執行規定工作之過程或活動。
2. 驗證：指驗證機構授予書面保證稽核員、產品、程序或服務符合規定要求之過程或活動。

為因應諸如職業安全衛生、消防安全設備、資訊安全管理系統等驗證作業之需求，於 2001 年 3 月 14 日以經濟部經(90)認字第 0900460122 號令訂定發布「中華民國認證辦法」，除原有之品質管理及環境管理外，一般性之驗證機構(例：資訊安全管理系統驗證機構等)以及產品驗證、檢驗(Inspection)機構之認證工作均由中華民國認證委員會(Chinese National Accreditation Board，簡稱 CNAB)負責；並於中華民國 90 年 3 月 2 日以經濟部經(90)認字第 09003504120 號函修正下達：「中華民國認證委員會設置要點」，公佈周知。換言之，如圖 3.1 所示，自關稅暨貿易總協定(General Agreement on Tariff and Trade，簡稱 GATT)體系之技術性貿易障礙協定中要求各國為安全、衛生、環保或保護消費者等因素，而訂定之技術法規或標準，以及證明相關產品符合這些技術法規或標準之符合性評鑑程序(Conformity Assessment Procedure，簡稱 CAP)，不應對國際貿易造成沒有必要的障礙後。鑑於沒有真確性(Integrity)等安全可靠性質的資訊，電子商務與電子化/網路化政府等均將遙不可及，虛擬世界仍將跳不出文娛和廣告的格局；國際間建立電子化/網路化社會資訊安全機制之認、驗證、檢驗之業務已於今年 3 月 2 日起，由「中華民國認證委員會」主管；根據標準檢驗局的規劃，預定於 2002 年 1 月正式起動如圖 3.2 所示之資訊安全管理系統認驗證作業。

資訊系統常因作業形態之不同而對相關安全的要求也不同，譬如：美國聯邦存款保險公司(Federal Deposit Insurance Corporation，簡稱 FDIC)之監理部門(Division of Supervision，簡稱 DOS)提出之「電子銀行安全與穩健檢查程序」(Electronic Banking Safety and Soundness Examination Procedures，簡稱 S&S Exam.)中，針對金融機構所提供電子銀行業務性質及所面臨風險程度之不同，明定分成如表列所示之三種不同等級，根基於「風險分級管理」管理之概念與參照其他國家的辦法[13][15~16]，在我們推動資訊安全管理系統驗證工作時，可以分成如表 3.2 所示之四級，第三級以上與國際 BS7799-2 之驗證接軌，第四級則除 BS7799-2 之要求外，尚需考慮資訊安全管理系統與品質管理系統、環境管理系統等之整合性。

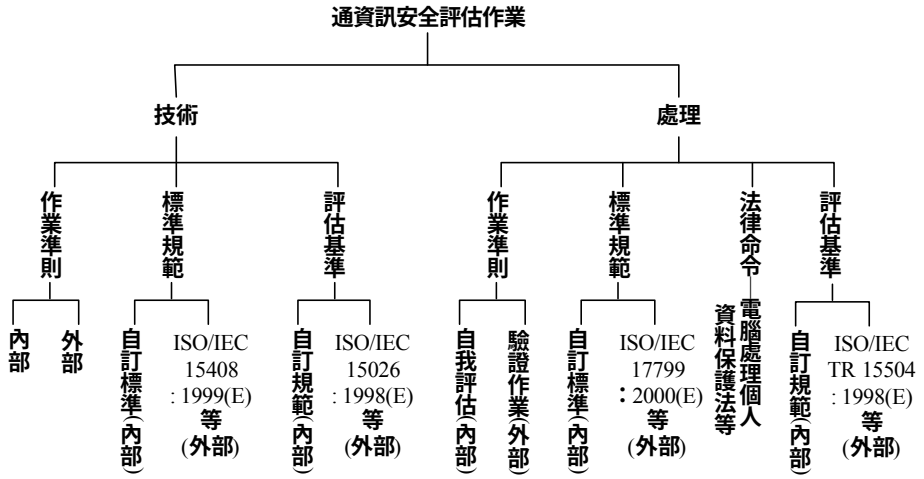



圖 3.1：通資訊安全評估作業示意說明

**表** 3.1：**美國聯邦存款保險公司監理部門「電子銀行安全與穩健**(Safety and Soundness)**檢查程序」分級示意說明**

| 級　別 | 電　子　銀　行　功　能　說　明 |
|---|---|
| 1 | **單純提供資訊的系統**(Information-only Systems) |
| 2 | **電子資訊轉移系統**(Electronic Information Transfer Systems) |
| 3 | **完全交易資訊系統**(Fully Transactional Information Systems) |

**資料來源：**U.S.A. Federal Deposit Insurance Corporation, Division of Supervision(1998) Electronic Banking：Safety and Soundness Examination Procedures, June 1998。

| | |
|---|---|
| **資訊安全管理系統之一般性要求事項：**<br>4.1　**資訊安全政策。**<br>4.2　**資訊安全組織。**<br>4.3　**資訊資產分類管理。**<br>4.9　**業務持續性管理。**<br>4.10 **遵循法律要求。** | **人員的要求事項：**<br>4.4　**人員安全。**<br>4.5　**實體與環境的安全。**<br>4.8　**開發與支援過程的安全。** |
| **實體與環境的要求事項：**<br>4.5　**實體與環境的安全。** | **資訊技術的要求事項：**<br>4.6　**通信與操作管理。**<br>4.7　**存取控制的管理。**<br>4.8　**開發與支援過程的安全。** |

**圖** 3.2：**資訊安全管理系統驗證**(BS7799-2)**要求事項**

**表** 3.2：**資訊安全管理系統驗證分級要求構想**

| 級　別 | 驗　證　要　求 |
|---|---|
| 1 | 1. **法律之遵循**(BS 7799-2：1999, 4.10.1)。<br>2. **資訊安全政策**(BS 7799-2：1999, 4.1)。<br>2. **資訊資產分類管理**(BS 7799-2：1999, 4.3)。<br>3. **惡意軟體的控制**(BS 7799-2：1999, 4.6.3)。<br>4. **開發與支援過程的安全**(BS 7799-2：1999, 4.8.5)。 |
| 2 | 1. **第一級的要求。**<br>2. **資訊安全之遵循性**(BS 7799-2：1999, 4.10)。<br>3. **資訊安全組織**(BS 7799-2：1999, 4.2)。<br>4. **資訊安全的教育與訓練**(BS 7799-2：1999, 4.4.2)。<br>5. **資訊安全事件與故障的處理**(BS 7799-2：1999, 4.4.3)。<br>6. **業務持續性管理**(BS 7799-2：1999, 4.9)。 |
| 3 | BS 7799-2：1999 **之要求。** |
| 4 | **全面品質**(**含** BS 7799-2)**經營**(Total Quality Management，**簡稱** TQM)**之要求。** |

## 四、結論

國際上標準化的主要目的在於創造下列各項能促進物品交換、技術移轉的貿易環境：

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。

自 1906 年起由電氣技術開始，至 1946 年 10 月 14 日在英國倫敦召開以「促進工業標準的國際統一和調整」為主要宗旨之國際性會議正式成立國際標準組織(International Organization for Standardization，簡稱 ISO)，ISO 於 1947 年 2 月 23 日正式開始運作；因此，10 月 14 日又稱為世界標準日[2]。

所謂標準就是基於公平、公正、便利等觀點做好統一規範、單純化時之必要條件，對於物件、性能、配置、狀態、動作、操作手續、使用方法、工作程序、責任義務、權限概念等均應有一測度判斷的基準；而通稱的規格就是這些標準中直接或間接的有關產品或服務品質之技術上的規範事項。一般而言，規格或標準常因不同組織層級而有不同的要求，圖 4.1 是其示意說明。

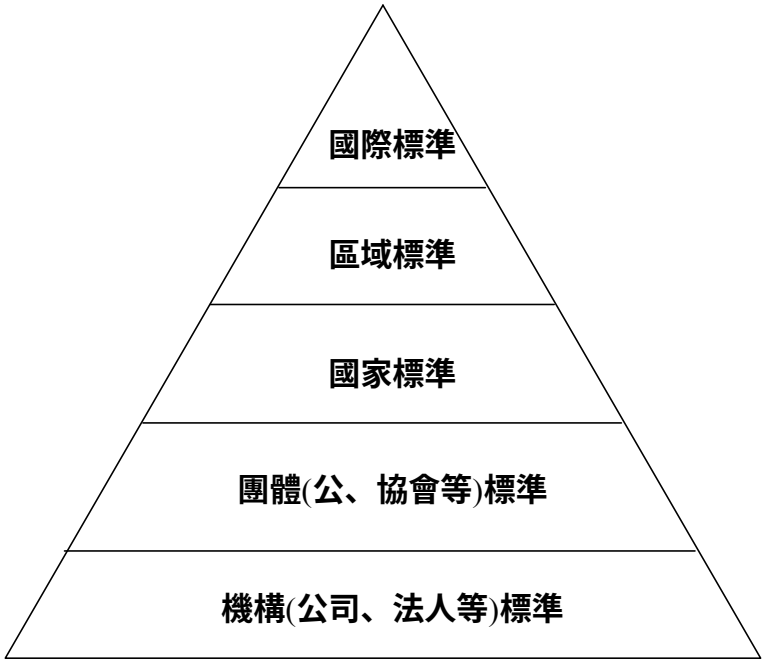



**圖 4.1：標準化層次示意**

在第三節中，本文提出了資訊安全管理系統我國(1~4 級)能與國際(3~4 級)接軌之驗證規範，符合圖 4.1 之層次要求，在不同層次中有關資訊技術驗證規範之要求等尚待進一步的研究。

九十年代全球文明歷經了重大的轉變，品質、環境和安全衛生管理逐漸朝向一致化與標準化，而相關的國際標準也影響了許多國家經濟的發展和組織管理與經營的方式，ISO 9000 品質管理和 ISO 14000 環境管理系列標準的遵從，是最佳的佐證。二十世紀最後一個月，資訊安全管理的國際標準已正式頒佈，成為創建可信賴資訊作業環境的指引，若善加運用，不僅可以提昇資訊系統的安全性，亦有助於品質文化之塑造。

誌謝詞：

本文作者謹在此對 BSi 大中國區資訊安全產品鄧永基經理對表 3.3 之建議致謝。

## 參考文獻


[1] 中華民國電腦稽核協會(2001)經濟部標準檢驗局九十年度委託計畫書，中華民國電腦稽核協會。

[2] 朱樹德(1990)國家標準國際化之研究，經濟部中央標準局。

[3] 行政院(2001)中華民國九十年二月五日，台九十經字第OO七四三一號函。

[4] 行政院(2001)建立我國資通訊基礎建設安全機制計畫，行政院(目前已有奉九十年一月九日行政院院長核定同意辦理及奉九十年四月二十四日行政院院長核定修訂辦理等兩個版本)。

[5] 行政院資訊與通信基本建設專案推動(National Information Infrastructure，簡稱NII)小組(2001)國家資通安全會報第一次會議(會議資料)，行政院資訊與通信基本建設專案推動小組。

[6] 國家安全局(2000)建立我國通資訊基礎建設安全機制(本文與參考資料)國家安全局。

[7] 經濟部標準檢驗局(2001)APEC-SBS 研討會論文集，2001 年 9 月 22 日，台北市，經濟部標準檢驗局。

[8] 樊國楨(2001)資訊安全工作初始方向芻議，電腦與通訊，第 95 期，頁 72~81。

[9] 樊國楨與胡信靈編輯(2000)我國通資訊基礎建設安全機制討論會背景景說明資料，工業技術研究院電腦與通訊工業研究所。

[10] BSi(British Standard Institute) (1999) Information Security Management—Part 2: Specificatoin for Information Security Management Systems, BS7799-2:1999, BSi。

[11] IEC (1995) Dependability Management—Part 3: Application Guide—Section 9: Risk Analysis of Technology Systems, IEC 300-3-9:1995, IEC。

[12] ISO (1997) Banking, Securities and Other Financial Services—Information Security Guidelines, ISO TR 13569:1997(E), ISO。

[13] ISO (2000) Information Technology —Guidelines for the Management of IT Security, ISO/IEC TR 13335(All Parts), ISO。

[14] ISO (International Organization for Standardization)/IEC(International Electrotechnical Commission) (2000) Information Technology—Code of Practice for Information Security Management , ISO/IEC 17799:2000 (E), ISO。

[15] SEI(Software Engineering Institute) (1999) The Systems Security Engineering Cability Model v2.0, Carnegie Mellon SEI。

[16] Solms, B. and R. Solms (2001) Incremental Information Security Certification, Computer and Security, Vol.20, No.4, pp. 308~310。