● 管理系統標準化簡述－根基於資訊安全管理系統

摘要：

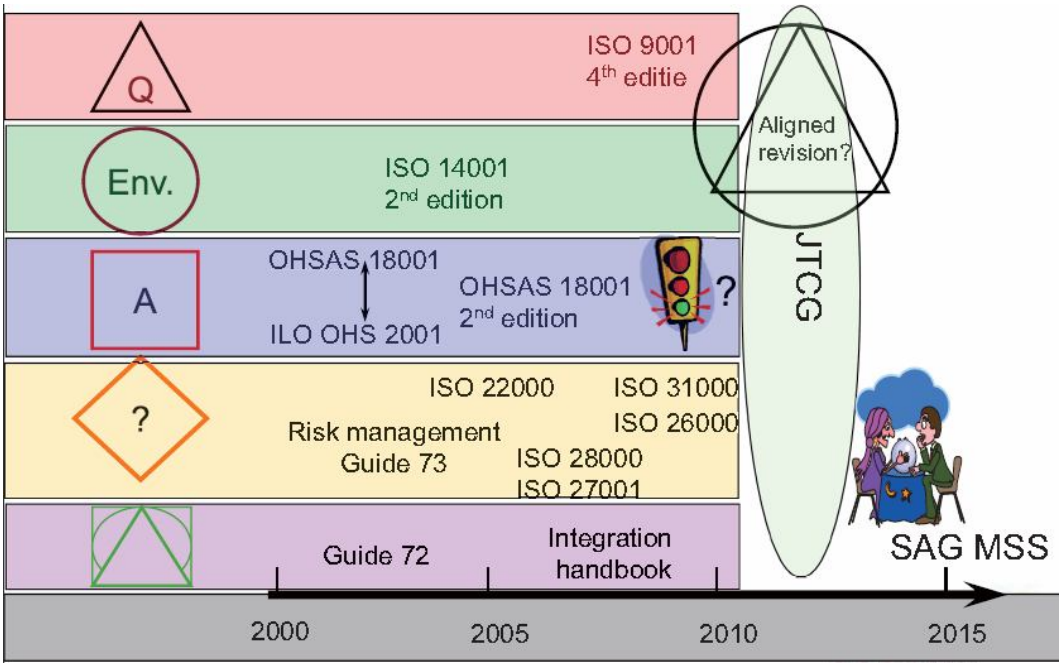
標準可以累積知識與經驗，標準化則是冀求以系統的、共同協調一致之方法來強化標準實作的知識以供傳承。鑑於管理系統日益增多，其標準系列宜加以規範，國際標準組織(International Standardization for Organization，簡稱ISO)自2000年起即分3階段進行管理系統標準(Management System Standards，簡稱MSS)之標準化工作項目，期能在2015年完成各個管理系統要求事項的調合，ISO/IEC 27001標準系列已遵循MSS逐步建立中。根基於此，本文以ISO/IEC 27001標準系列爲源地，陳述MSS及其與台灣地區建立以及驗證資訊安全管理系統(Information Security Management System，簡稱ISMS)之概況。

關鍵詞：

1. 資訊安全管理系統(Information Security Management System)。
2. 管理系統標準(Management System Standards)。
3. 標準化(Standardization)。

一、前言：

國際標準組織(International Standardization for Organization，簡稱ISO)爲求索管理系統要求事項之一致性以符合社會大眾的利益，於2001年先行出版ISO Guide 72 (Guidelines for the justification and development of management system standards)作爲準備[1]，並在2008-06~2012-12於能源管理(Energy Management)爲標的試行[2]。ISO技術管理委員會(Technical Management Board，簡稱TMB)主責之如圖1.1所示的管理系統標準(Management System Standards，簡稱MSS)於2010年已完成第2階段之共同用語(Term)與核心定義(Core Definitions)的標準化作業，ISO/IEC 27001新版亦將遵循[3~7]。根基於此，本文先於第2節及第3節分別說明遵循ISO Guide 72之資訊安全管理系統(Information Security Management System，簡稱ISMS)的ISO/IEC 27001標準系列的現況以及已公布之MSS結構[3~9]；在第4節是本文的結論[9~11]。



資料來源：Waumans, R. (2010) JTCG Introduction, Buenos Aires, May 2010。
圖 1.1：管理系統之校準(Alignment)－未來：2010~?

二、ISMS標準系列：

自1995年之ISO DIS 14980起，資訊安全管理系統標準化之進程已逾15年，隨著電子科技的一日千里，資訊安全之議題已成爲數位社會安全的基石。「讓過去與現在爭執不下，將錯失未來」，ISO/IEC JTC1/SC27主席Walter Fumy先生，在世界資訊高峰會之邀請下，於2004年09月24日公布了ISO之深度防禦(Defense in Depth)的資訊安全管理模型觀點；其標準組件ISO 27001標準系列之ISO/IEC 27003已於2010年2月1日正式發行，ISMS標準化的第一階段工作已樹立第1座里程碑。

各管理系統的國際標準提供了一項建立與維持管理系統時得以遵循的模型。本模型之特色乃包含了本領域中各專家就現有國際水準所達成的共識。ISO/IEC JTC1/ SC27維持專家委員會，致力於資訊安全國際管理系統標準之發展，此外也以資訊安全管理系統(ISMS)標準系列著稱。爲反映出ISMS標準系列在不同領域的實作宜進行之變更，ISO 27799與ISO/IEC 27011已分別頒布成爲健康(Health)及電信(Telecommunication)領域控制措施實作變更之規範。

ISMS標準系列遵循ISO/IEC Guide 72之規範由互相關聯的標準組成，不是已發行就是在發展中，且包含依些重要的結構化組件。這些組件強調描述ISMS要求事項(CNS 27001)規定的標準與驗證CNS 27001遵循性的驗證機構要求事項(CNS 27006)。其它標準提供ISMS實作之各個層面指引、提出概括性過程、控制相關的指導綱要以及特定部分之指引。圖2.1說明ISMS標準系列的關係。

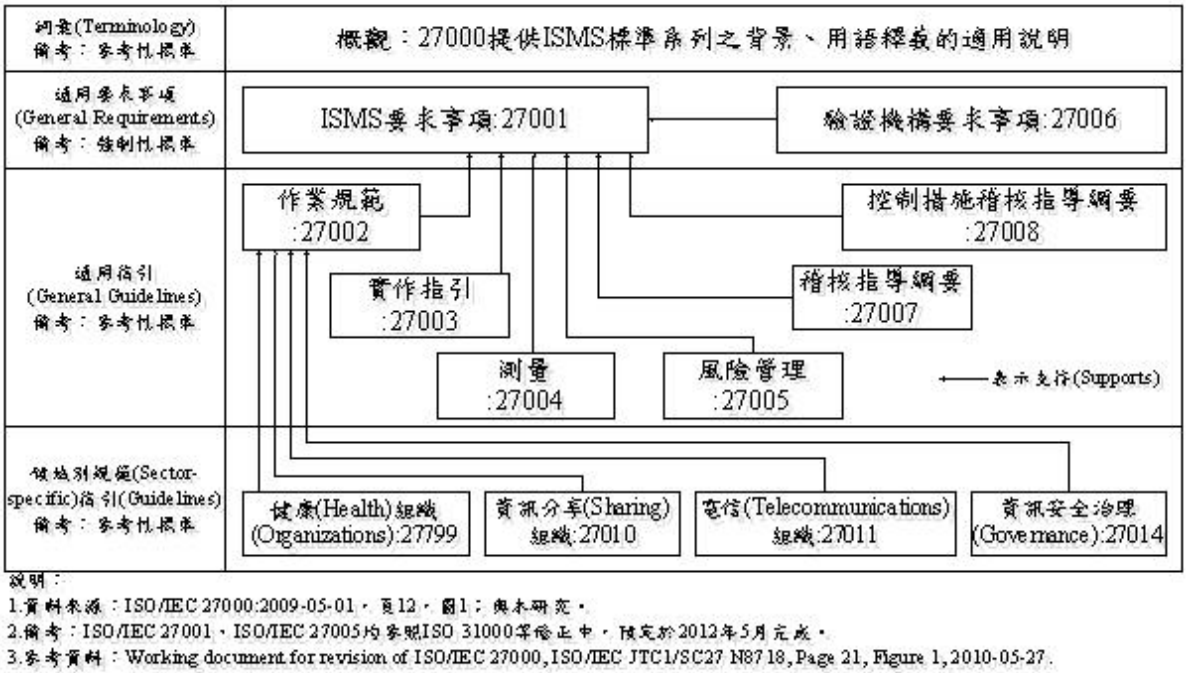


圖 2.1：資訊安全管理系統(Information Security Management System，簡稱 ISMS)標準系列(ISO/IEC 27001 屬別(Family))框架

提供直接支援、詳細指引及/或整體規劃-執行-檢查-行動(Plan-Do-Check-Act，簡稱PDCA)過程之解譯與ISMS 27001所規定要求的標準有：CNS 27000、CNS 27002、CNS 27003、CNS 27004、CNS 27005、CNS 27007與CNS 27008。CNS 27006因應提供ISMS驗證機構之要求事項。ISO/IEC 27010、ISO/IEC 27011、ISO/IEC 27014與ISO 27799因應ISMS特定部分的指引。ISMS標準系列維護與許多其它ISO和ISO/IEC標準的關係，並且分類及進一步描述爲下列之一：

1.描述概觀和詞彙的標準。

2.規定要求的標準。

3.描述一般指導綱要的標準。

4.描述特定部分指導綱要的標準。

分述如後：

2.1 描述概觀與詞彙的標準：

2.1.1 CNS 27000：資訊技術－安全技術－資訊安全管理系統－概觀與詞彙

範圍：本標準提供給組織及個人：

(a) ISMS標準系列的概觀。

(b) 資訊安全管理系統(ISMS)的簡介。

(c) 規劃-執行-檢查-行動(Plan-Do-Check-Act，簡稱PDCA)過程的簡短描述。

(d) 整個ISMS標準家族使用的用語及定義。

目的：CNS 27000描述資訊安全管理系統的基本原理，形成ISMS標準家族主體並定義相關的用語。

2.2 規定要求事項的標準：

2.2.1 CNS 27001：資訊技術－安全技術－資訊安全管理系統－要求事項

範圍：本標準規定在組織全景內的整體營運風險下建立、實作、運作、監控、審查、維護和改進正式的資訊安全管理系統(ISMS)。本標準規定實作就個別組織或其中部分客製化安全控制措施的要求。本標準對所有型式的組織(例如：商業企業、政府機構及非營利組織)均是通用的。

目的：CNS 27001提供控制措施及減輕與組織藉由運作其ISMS尋求保護的資訊資產相關風險規定的要求。運作ISMS的組織可稽核與驗證其符合性。應選擇來自附錄A (CNS 27001)適切的控制目標和控制措施作爲ISMS過程的一部分以涵蓋已識別的要求。表A.1 (CNS 27001)所列的控制目標和控制措施是直接源自於CNS 27002所列的第5到第15條款並與之調校一致。

2.2.2 CNS 27006：資訊技術－安全技術－提供資訊安全管理系統稽核與驗證機構之要求事項

範圍：本標準規定除包含於ISO/IEC 17021內的要求外，依據CNS 27001稽核及ISMS驗證組織之要求事項並提供指引。其主要意圖爲支援依據CNS 27001提供ISMS驗證之驗證機構的認證。

目的：CNS 27006輔助ISO/IEC 17021提供認證驗證機構合格之要求，以准許這些機構能一致性地以CNS 27001所提出的要求驗證其遵循性。

2.3 描述一般指導綱要的標準：

2.3.1 CNS 27002：資訊技術－安全技術－資訊安全管理之作業規範

範圍：本標準提供爲達成資訊安全，在選擇和實作控制措施時一共同接受的控制目標和可使用之最佳實務控制措施以作爲實作指引的清單。

目的：CNS 27002提供實作資訊安全控制措施的指引。特別是第5到第15條款支持CNS 27001 A.1到A.15條款中具體指定的控制措施，在最佳實務上提供特定的實作建議和指引。

2.3.2 CNS 27003：資訊技術－安全技術－資訊安全管理系統實作指引

範圍：本標準將提供實際的實作指引和依據CNS 27001在建立、實作、營運、監控、審查、維護和改進ISMS上提供更進一步資訊。

目的：CNS 27003將依據CNS 27001對成功的實作ISMS提供過程導向(作法)。

2.3.3 CNS 27004：資訊技術－安全技術－資訊安全管理－量測

範圍：本標準將提供爲評鑑ISMS有效性、控制目標和CNS 27001規定用以實作和管理資訊安全之控制措施等的量測之發展和使用上提供指引和建議。

目的：CNS 27004將提供量測框架以期能依據CNS 27001評鑑ISMS的有效性。

2.3.4 CNS 27005：資訊技術－安全技術－資訊安全風險管理

範圍：本標準提供資訊安全風險管理之指導綱要。本標準內描述的作法支援規定於CNS 27001內之一般概念。

目的：CNS 27005提供在合意地(Satisfactorily)實作和實現CNS 27001的資訊安全風險管理要求上實作過程導向之風險管理作法的指引。

2.3.5 CNS 27007：資訊技術－安全技術－資訊安全管理系統稽核指導綱要

範圍：本標準將提供ISMS稽核，以及適用於一般管理系統、包含於CNS 14809內的指引之外之資訊安全管理系統稽核員資格指引。

目的：CNS 27007將提供組織需要就CNS 27001所規定之要求執行ISMS內部或外部稽核或管理ISMS稽核計畫的指引。

2.3.6 CNS 27008：資訊技術－安全技術－資訊安全管理系統控制措施之稽核員指南

範圍：本標準將提供所有類型組織之ISMS控制措施的稽核員稽核工作之指南。

目的：CNS 27008提供所有類型組織實現CNS 27001附錄A的指引對其稽核之工作指南。

2.4 描述特定部分指導綱要的標準：

2.4.1 CNS 27010：資訊技術－安全技術－領域間與組織間之資訊安全管理

範圍：本標準提供建立領域間與組織間交換及分享敏感性資訊之資訊安全管理的要求事項以及指導綱要。

目的：CNS 27010提供跨領域與跨組織交換敏感資訊、除實現CNS 27001、附錄A的要求之外，採用CNS 27002於資訊交換/分享的獨特之資訊安全管理的指導綱要。

2.4.2 CNS 27011：資訊技術－安全技術－資訊安全管理系統－植基於CNS 27002之電信組織資訊安全管理指導綱要

範圍：本標準提供支援電信組織資訊安全管理(ISM)實作的指導綱要。

目的：CNS 27011提供電信組織，除實現CNS 27001、附錄A要求的指引外，採用ISO 27002對其工業領域(Industry Sector)獨特之資訊安全管理的指導綱要。

2.4.3 CNS 27014：資訊技術－安全技術－資訊安全治理

範圍：本標準提供所有類型之組織，CNS 27001中的ISMS過程中治理機制之控制的指導原則。

目的：CNS 27014提供於實現CNS 27001之過程中，於治理面向獨特之資訊安全管理控制的指導原則。

2.4.4 CNS 27799：健康資訊學－使用CNS 27002之健康資訊安全管理

範圍：本標準支援醫療組織資資訊安全管理(ISM)實作的指導綱要。

目的：CNS 27799提供採用CNS 27002健康組織除實現CNS 27001、附錄A要求的指引外，採用ISO 27002對其工業領域獨特之資訊安全管理的指導綱要。

2.4.5 備考：CNS 27008、CNS 27010與CNS 27014目前均由ISO/IEC SC27/WG 1制定標準中。

三、管理系統標準：

ISMS標準系統之每一文件本身並未具備強制任何人遵循該文件的義務。然而，該義務仍可能因如立法或契約而成爲強制的。爲能聲明文件遵循性，使用者需能識別需要符合之要求事項。使用者亦需能區分這些要求事項與其他有相當選擇自由的建議。ISMS標準系列遵循如表3.1所示之ISO之TMB爲澄清ISO標準文件中的要求事項及/或建議根據字面表示如何解譯的規範。

表 3.1：標準之條款表示之用語釋義

表示	解釋
要求	“應”(shall)和“不得”(shall not)用語表示嚴格遵循以符合文件，且不允許有所誤差的要求
建議	“宜”(should)和“不宜”(should not)用語表示在數個可能中有一個被建議爲特別合適的，沒有提及或排除其它，或較偏好某行動做法但不一定必須，或(以否定形式)某種可能或一行動做法被聲明不贊成但不禁止
許可	“可”(may)和“不需”(need not)用語表示一行動做法在該文件範圍內是允許的
可能	“得”(can)和“不能”(cannot)用語表示某事發生的可能性

同前所述，ISMS標準系列已遵循如圖3.1所示之執行ISO理事會的TMB如圖1.1中之第1階段管理系統標準(Management System Standards，簡稱MSS)建立如圖2.1所示之ISMS標準系列的框架。

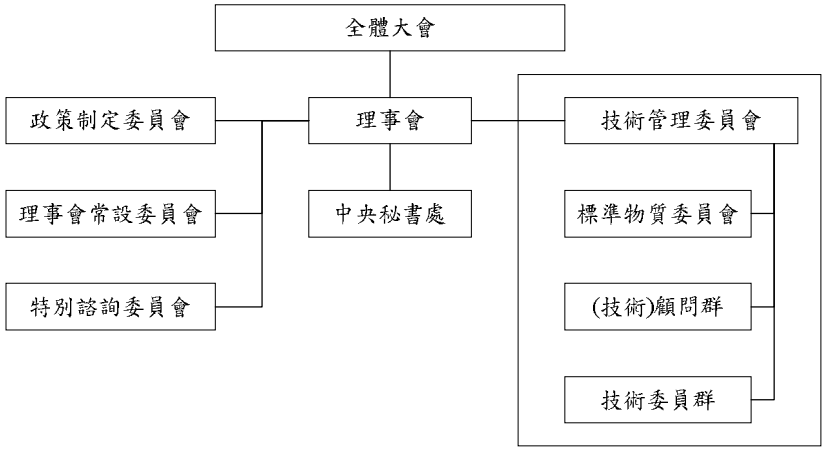


圖 3.1：國際標準組織技術工作框架

分3階段進行之MSS已進入第3階段的工作項目，其進程如後：

1. 源起：國際標準組織(International Organization for Standardization，簡稱ISO)技術管理委員會(Technical Management Board，簡稱TMB)爲求索管理系統要求事項之一致性，於2001年先行出版ISO Guide 72 (Guidelines for the justification and development of management system standards)作爲準備，並於2008-06~2010-12以能源管理(Energy Management)爲標的試行。自2006年起組建MSS之策略顧問群(Strategic Advisory Group，簡稱SAG-MSS)，要求其第13技術顧問群(Technical Advisory Group，簡稱TAG)亦即JTCG (Joint Technical Co-ordination Group)發展各個管理系統之共同願景(Joint Vision)並校準現有的MSS與任一新MSS。
2. JTCG於2008年完成草案後，在2009-04-10，提出MSS之建議書：ISO/TMB/TAG13-JTCG/TG3/N034，請各個相關之技術委員會等審查，期能在2010年完成MSS。
3. 2009-04-23，ISO/IEC JTC1/SC27以N7616號文件轉發MSS之建議書。
4. JTCG於2010-05-17提出MSS之「高階管理系統結構以及一致性文句與共同名詞(Draft high level management system structure with draft identical text and common terminology)」草案：JTCG/TF1/N28&JTCG/TF3/ N086，請各個標準化機構研究並提供意見(Study and comment)。
5. ISO/IEC JTC1/SC27於2010-07-15提出：「ISO/IEC 27001與MSS前景白皮書(WHITEPAPER FUTURE OF ISO/IEC 27001 AND MANAGEMENT SYSTEM STANDARDS (MSS))」。

TMB制定前述第2階段之MSS時，先提出分如圖3.2、圖3.3、圖3.4及圖3.5的概念圖及其說明，交付各ISO技術委員會(Technical Committees)審查(例：JTC1/SC27、TC 8、TC 34、TC 46、TC 176、TC 207、TC 223、TC 241、TC 242、TMB風險管理工作群、CASCO (Conformity Assessment)等)。

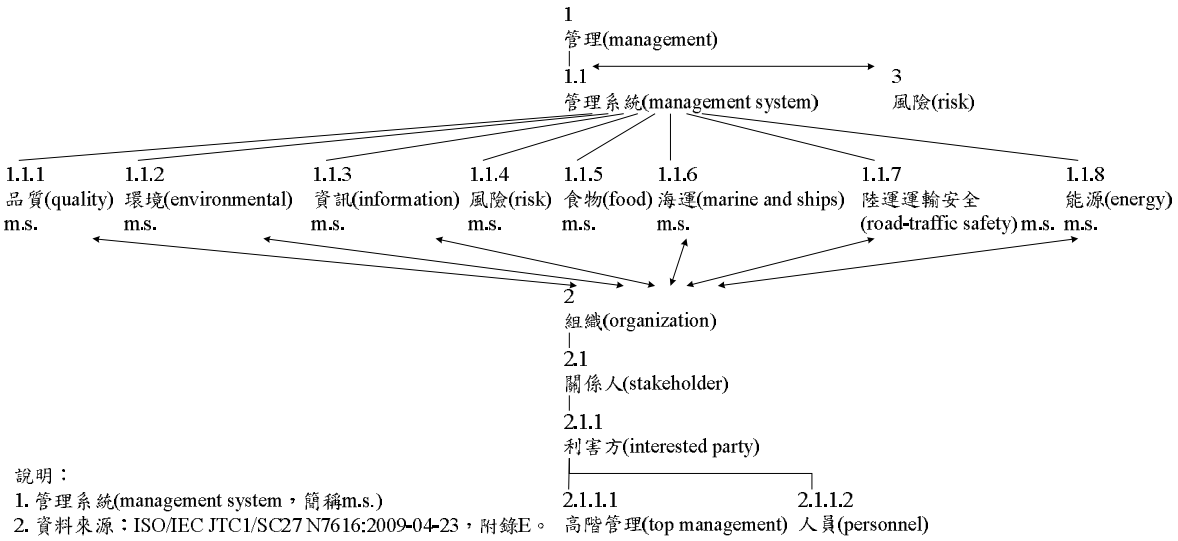
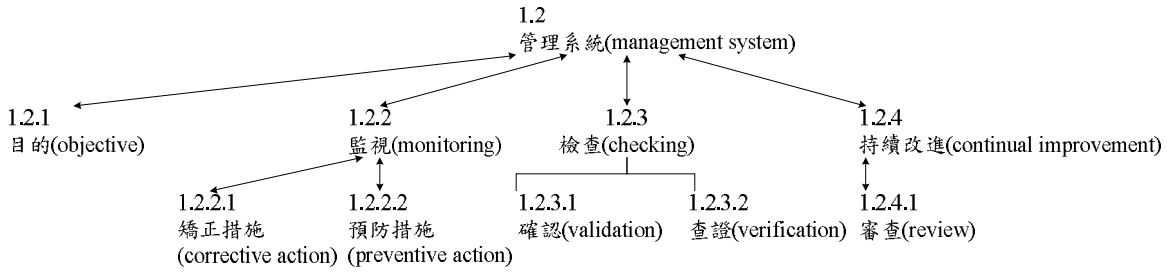
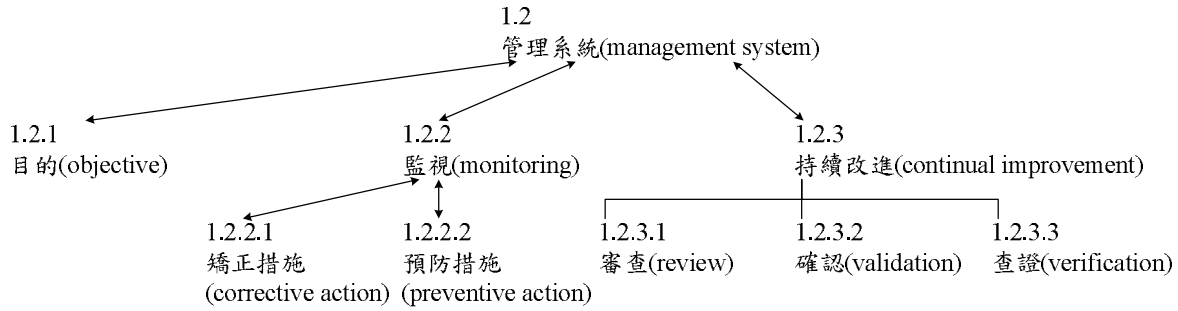


圖 3.2：管理系統標準核心概念(Core concepts)－概念圖(Diagrams)之 1



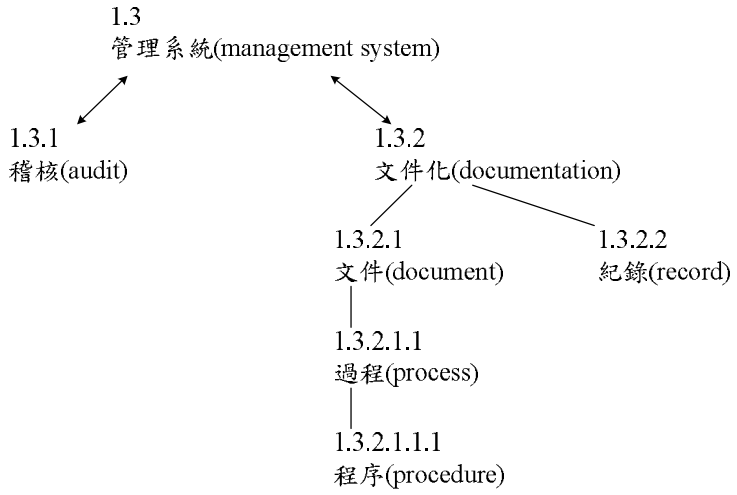
資料來源：ISO/IEC JTC1/SC27 N7616:2009-04-23，附錄E。

圖 3.3：管理系統標準核心概念(Core concepts)－概念圖(Diagrams)之 2 (方案 A)



資料來源：ISO/IEC JTC1/SC27 N7616:2009-04-23，附錄E。

圖 3.4：管理系統標準核心概念(Core concepts)－概念圖(Diagrams)之 2 (方案 B)



資料來源：ISO/IEC JTC1/SC27 N7616:2009-04-23，附錄E。

圖 3.5：管理系統標準核心概念(Core concepts)－概念圖(Diagrams)之 3

目前TMB提出之MSS規範所有管理系統要求事項(例：ISO 9001、ISO 14001、ISO 27001、ISO 28001、ISO 50001等)的至次節之高階結構(High Level Structure)，其章節如後：

1. 第1章：適用範圍(Scope)。
2. 第2章：引用標準(Normative references)。
3. 第3章：用語釋義(Terms and definitions)。
4. 第4章：組織全景(Context of the organization)。
5. 第5章：統禦力(Leadership)。
6. 第6章：規劃(Planning)。
7. 第7章：支持(Support)。
8. 第8章：運作(Operations)。
9. 第9章：績效評估(Performance evaluation)。
10. 第10章：改進(Improvement)。
11. 資料來源：：ISO/IEC JTC1/SC27 N7616:2009-04-23，附錄B。

遵循MSS之規範，於ISO/IEC 4th 27001:2010-11-15中已調整如前所述之條款結構，於第5.3節中從新定義ISMS政策與資訊安全政策如表3.2中的備考1所述[1,5~7,10]。

表 3.2：資訊安全管理系統(Information Security Management System，簡稱 ISMS)與資訊安全管理過程

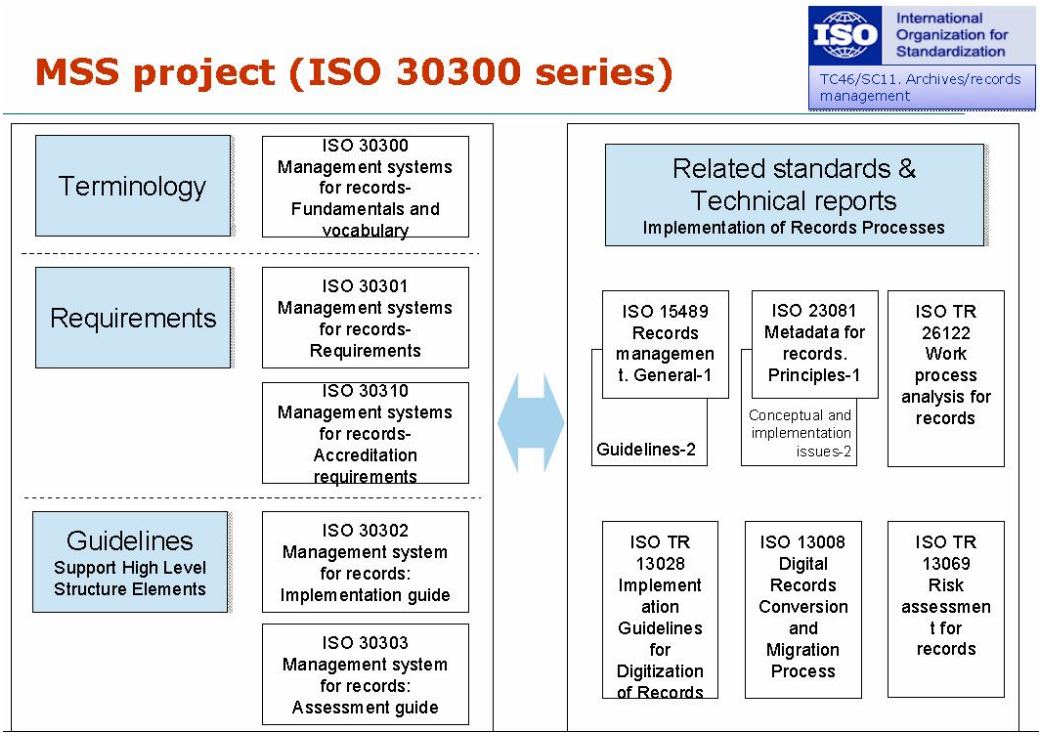
<table>
<tr><td>管理</td><td>運作</td><td>技術</td></tr>
<tr><td rowspan="2">創建 ISMS 政策</td><td colspan="2">監視(Monitor)與測度(Measure))</td></tr>
<tr><td>資訊安全政策</td><td>資訊安全(系統)政策</td></tr>
<tr><td>建立目標(Goals)</td><td colspan="2">發展資訊安全管理剖繪(Profile)</td></tr>
<tr><td>識別標的(Targets)</td><td colspan="2">資訊安全管理評鑑合規</td></tr>
<tr><td colspan="3">稽核：
1. ISMS 里程碑與改進計畫。
2. ISMS 有效性之實作計畫。
3. ISMS 持續改進之查證結果的回饋機制。</td></tr>
<tr><td colspan="3">資料來源：</td></tr>
</table>

1. ISO/IEC 27001 標準系列。
2. ISO/IEC 15408 標準系列。
3. 本研究。

備考：

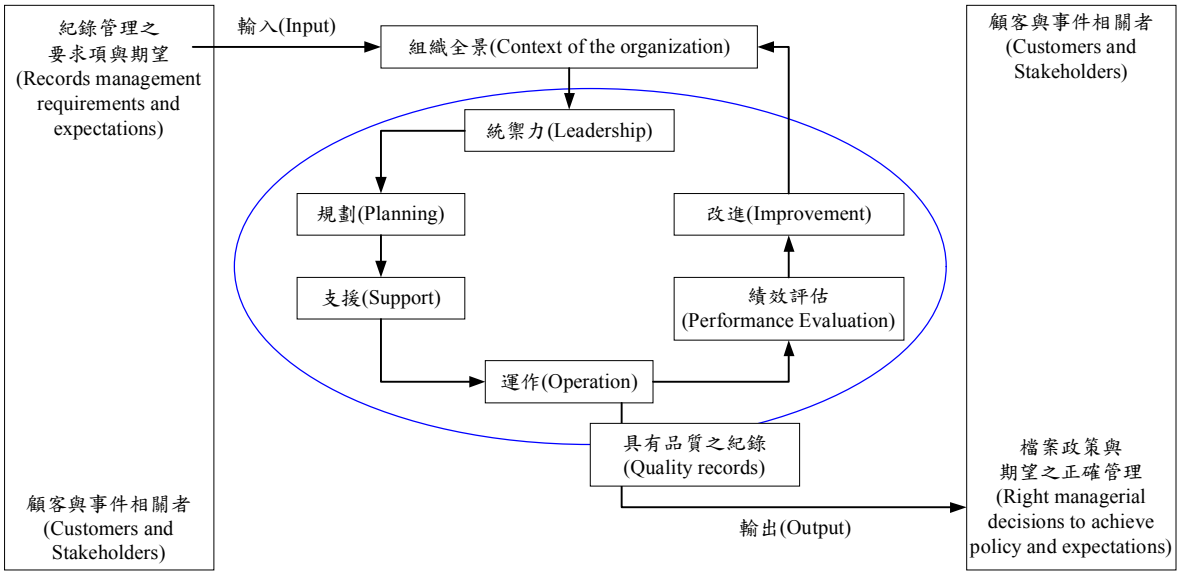
1. 遵循管理系統標準(Management System Standards)之進程，於 ISO/IEC 4th WD 27001:2010-11-15「ISMS 政策」已改名「資訊安全政策」，「資訊安全政策」改名「資訊安全特定政策(Information Security Specific Policy)」。
2. 於 ISO/IEC 4th WD 27001 中，規範資訊安全風險管理取徑(Approach)與資訊安全規則(Rules) 2 資訊安全特定政策之文件化。
3. 資訊安全(系統)政策係本研究之用語。

前述管理系統標準之之高階結構對ISMS具有攸關性的影響，以ISO/IEC 27002第15.1.3節引用的組織紀錄保護宜參照的ISO/IEC 15408-1:2001爲例，如圖3.6、圖3.7與圖3.8所示，已對ISMS實作之可操作性產生直接的衝擊。



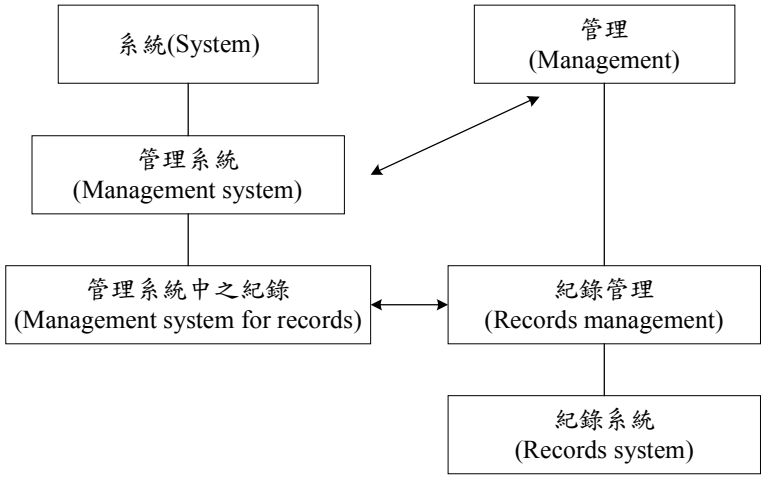
資料來源：Bustelo, C. (2010) Update ISO TC46/SC1 Current MSS Project, Buenos Aires, May 2010。

圖 3.6：管理系統標準(Management System Standards，簡稱 MSS)標準化(2001~2015?)與紀錄管理計畫



資料來源：ISO (2010) Information and documentation – Management system for records – Fundamentals and vocabulary, ISO DIS 30300:2010-05-21, Figure 3, p. 7.

圖 3.7：根基於過程導向之管理系統的紀錄模型(Process-based MSR model)



資料來源：ISO (2010) Information and documentation – Management system for records – Fundamentals and vocabulary, ISO DIS 30300:2010-05-21, Figure 3, p. 7.

圖 3.8：管理系統與管理中之紀錄的關係

安全就像空氣，原本毫無價值，失去時才會痛苦覺察其存在，私密資訊外流，爲數位台灣投下了空前的威脅；查證費時，鑑識困難，甚至傳出犯罪集團已握有台灣民眾戶籍、兵籍、稅務等資料。在網路社會生活型態快速普及，資安威脅不斷使得人人自危之際，必須能讓社會大眾充分認知，惟有落實與時俱進的ISMS於日常生活中，才能成功邁向優質網路社會，確保人民生活之便利與安全；如何善用MSS第3階段工作項目的契機，塑建如表3.2及表3.3之ISMS作業與法規的框架以落實ISMS標準化之實作，是建立與驗證ISMS宜面對的議題。

表 3.2：資訊與資訊系統分類分級作業比較表

國家 機構別	美國	大陸
權責機構	商務部(政府機構)	公安部(政府機構)
認證機構(管理)	國家標準與技術研究院	國家認證認可監督管理委員會
驗證機構	政府、公益法人、一般法人共同參與	指定公營機構
法源	1. 聯邦資訊安全管理法 2. 重要關鍵基礎建設資訊法	信息系統安全保護條例
測試實驗室	1. 密碼模組測試實驗室 2. 共同準則測試實驗室	1. 信息安全產品測評認證中心 2. 涉密信息系統安全保密測評認證中心 3. 信息安全測評認證中心
強制性標準	1. FIPS 199 2. FIPS 200	GB 17859
範疇	1. 產品 2. 系統 3. 人員	1. 產品 2. 系統 3. 人員
電子政務安全等級劃分	以「資訊」之潛在風險劃分安全等級	原以網路之業務性質劃分安全等級，2006 年 1 月 20 日起同美國之方式劃分等級

表 3.3：資訊安全管理法制作業框架初探－以大陸爲例

法源位階	大陸	中華民國
法律、條例或通則	1. 計算機信息系統安全保護條例(1994-02-28)。 2. 警察法(1995-02-18)。	
法規命令	1. 計算機信息安全專用產品和銷售許可證管理辦法(1997-12-12)。 2. 信息安全等級保護管理辦法(2007-06-22)。 3. 通信網絡安全防護管理辦法(2010-03-01)。	
行政規則	1. 關于開展全國重要信息系統安全等級保護定級工作的通知(2007-07-16)。 2. 關于部分信息安全產品實施強制性認證的公告 (2008-02-28)。 3. 關于調整信息安全產品強制性認證實施要求的公告(2009-04-	1. 政府機關(構)資訊安全責任等級分級作業施行計畫(2005-09-28)。 2. 政府機關(構)資訊安全責任等級分級作業施行計畫(2009-

	29)。	06-01)。
強制性國家標準或規範	1. 計算機信息系統安全保護等級劃分準則:GB17859-1999(1999-09-13 發布，2001-01-01 實施)。 2. 「網路安全隔離卡與線路選擇器產品」及「安全隔離與信息交換產品」等 13 項信息安全產品之強制性認證檢測規範(2009-04-29)。	
資料來源： 1. 行政機關法制作業實務，行政院法規委員會編印 2005 年 12 月。 2. 本研究。		

四、結論：

研究「標準」是需要「同情」與「推理」能力，「同情」是制定「標準」的人有相同之情，那樣體驗的「標準」自然是立體、多元的。「同情」加上「推理」，則「標準」是活的，每一份「標準」之頒布是因或是果，是一個趨勢的契機或是成績，「標準」是無數之偶然形成，但是亦絕非偶然，「標準」從長遠的角度來看，便可以體察出是有一股流勢，有無法阻擋的推移之力；資訊安全的「標準」更需整合自然科學及社會科學之脈絡來解讀、推理，方能溶入文化與數位台灣混然為一體，MSS標準化的進程僅為一端。

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。2006年6月16日，遵循ISO/IEC 27001之資訊安全管理系統的驗證等之國家標準已正式公布，成為創建可信賴資訊作業環境的指引，建立ISMS並通過驗證，自2002年起，已成為臺灣地區資訊安全之工作項目的主軸之一。

標準(Standard)：係指經由共識與某一公認的機構核准，提供一般或重複使用以提供各項活動或結果有關的規則、指導綱要或特性所建立之文件，期使在某一情況下獲致秩序的最佳程度；而標準化(Standardization)：係指在一定的範疇內，針對實際或潛在的問題，建立共同而經常使用的條款之活動，以期達成秩序的最佳程度，此標準化活動，特別包括標準之制定、發行及實施等過程。換言之，標準是標準化的源池，標準化是標準之實踐；標準的發展宜以科學、技術與實踐之綜合成果為基礎，以促進最佳的共同效益為目的。根基於管理系統標準(MSS)標準化之進程與臺灣地區的環境，參酌MSS的發展軌跡等，以為探討制定ISMS各類人員實作宜建立之能力的基石，已是ISMS領域內之重要議題。

參考文獻：

[1] ISO (2001) Guidelines for the justification and development of management system standards, ISO Guide 72:2001(E).

[2] ANSI et al. (2007) Justification study for a new work item proposal for a energy management standard ad guidance document.

[3] ISO/TMB (2009) Request for feedback and comment on proposed identical sub-classes titles for management system standards, 2009-04-10.

[4] ISO/TMB (2009) Request for feedback and comment on proposed common terms and core definitions for management system standards, 2009-04-20.
[5] ISO/IEC JTC 1/SC 27 (2010) Text for ISO/IEC 4th WD 27001 – information technology – Security techniques – Information security management systems – Requirements, 2010-11-15.
[6] ISO/IEC JTC 1/SC 27 (2010) Whitepaper future of ISO/IEC 27001 and management system standards (MSS), ISO/IEC JTC 1/SC 27 N8662, 2010-07-15.
[7] ISO (2009) Risk management – principles and guidelines, ISO 31000:2009(E).
[8] Fumy, W. (2004) IT security standardization, Network Security, December 2004, pp. 6-11.
[9] ISO (2009) Information technology – security techniques – information security management systems – overview and vocabulary, ISO/IEC 27000:2009(E).
[10] ISO/IEC (2005) Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2005(E).
[11] ISO (2009) Risk management – risk assessment techniques: IEC/ISO 31010 Edition 1.0, 2009-11.
[12] 樊國楨等(2010) 資訊安全管理系統標準化之實然應然問題探微，資訊安全通訊，第16卷，第4期，頁1~31。

(本文由國立交通大學資訊管理研究所/樊國楨教授、國立臺灣大學資訊管理學研究所/黃健誠、新竹市稅務局/廖菊芳 提供)