資訊安全管理系統稽核初論：根基於資安健診與標準化

樊國楨[1]、季祥[2]、韓宜蓁[3]
[1]臺灣網路防護協會
[2]趨勢科技股份有限公司
[3]中國文化大學資訊管理學研究所

摘要

隨著政府機關對資通安全的重視，我國整體資安防護體系之建立與資安防護能力之提升已見初步成效；今(2013)年行政院資通安全稽核作業計畫於 2013 年 9 月 2 日至 10 月 31 日，正式將「資安健診」的資訊安全技術項目控制措施之實作納入評分，開啟我國資訊安全管理系統(Information Security Management System，簡稱 ISMS)稽核工作的新姿，並納入 2013 年 12 月 15 日「國家資通訊安全發展方案（102 年至 105 年）」的「行動方案」之中。

ISMS 稽核遵循(ISO/IEC 27006)要求項目中之技術控制與系統測試已涵蓋前述「資安健診」的範疇，根基於此，本文期以中國大陸師法美國，所進行之資訊安全等級保護標準化作業與推動法規規範，闡述其運作過程、技術測評要求等；探討我國 ISMS 稽核工作項目中「系統測試」的全景，作為完善我國「資安健診」宜建立機制的參考。

關鍵詞：稽核、能力、資訊安全管理系統、標準化、測評

備考：2013 年 11 月 21 日，本文初稿已收錄於資安人科技網（www.informationsecurity.com.tw/article/article_detail.aspx?t2id=3&tv=24&aid=7705）。

壹、前言：

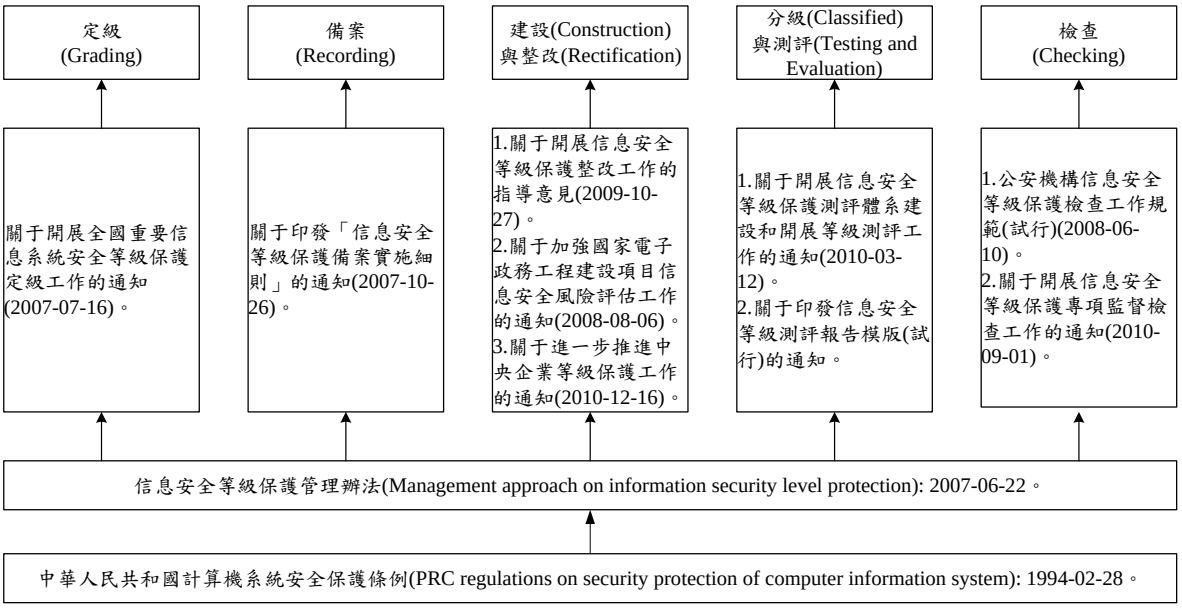
2013 年 9 月 6 日，行政院臺字第 1020146262 號函要求於「102 年度政府機關（構）資通稽核作業計畫（2013-09-02~2013-10-31）」之評分納入「資安健診」，佔總分的 40%[8]。

中國大陸 2007 年 6 月 22 日發布施行之「信息安全等級保護管理辦法」第 16 條規定，第三級以上信息系統於備案時應提供：「測評後符合系統安全保護等級的技術檢測評估報告」；第 18 條規定第三級信息系統每年，第四級信息系統每半年至少由公安機關、國家指定的專門部門對「系統安全等級測評是否符合要求」進行檢查。「他山之石，可以攻玉」，本文在第二節闡明中國大陸之「技術測評」的運作機制

[11][12][13][14][15][16][17]，於第三節敘述今（2013）年「資安健診」之概況及其與 ISMS 稽核要求事項中的「技術測試」工作項目之關連，第四節簡析美國此項工作的取徑並提出本文之結論。

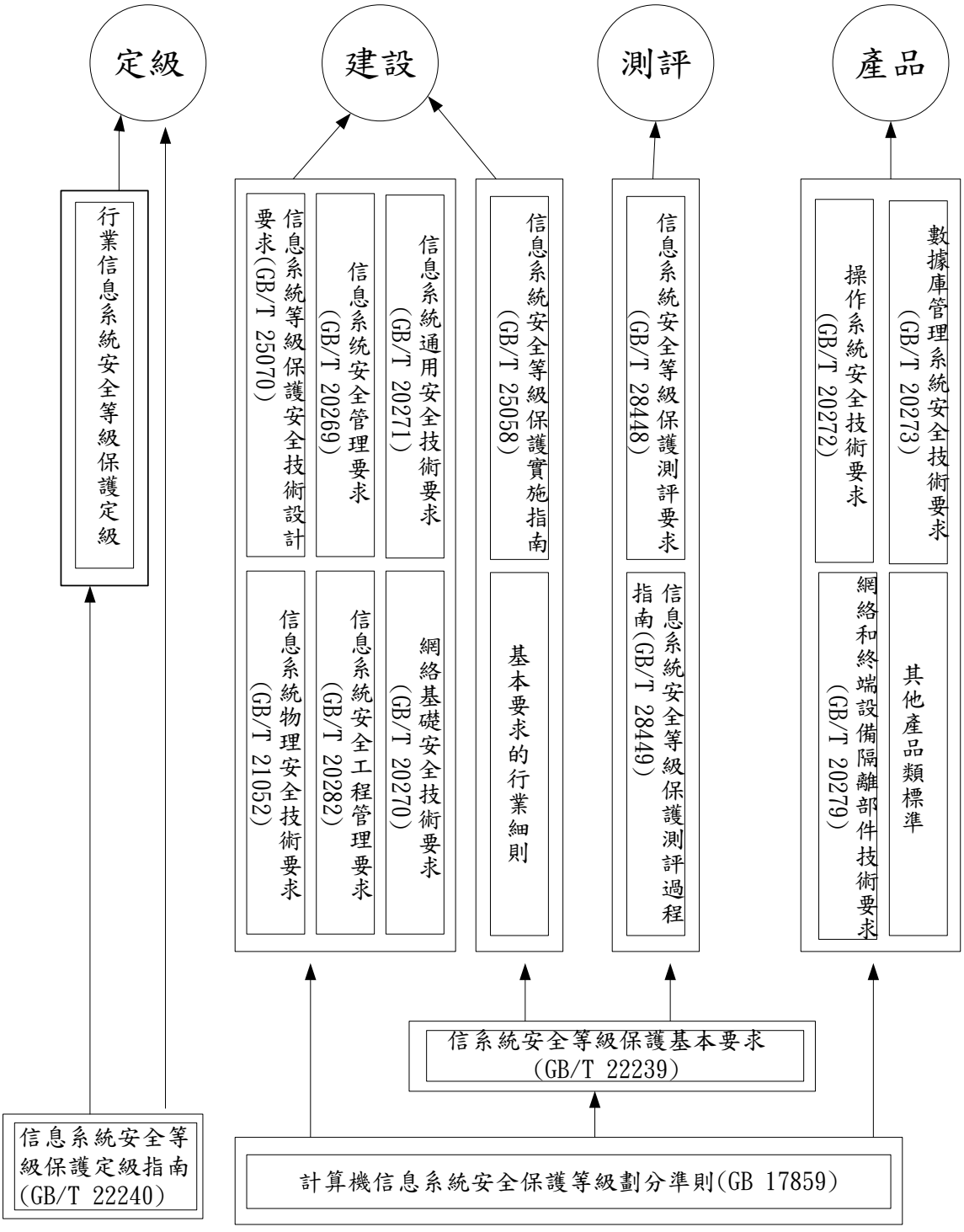
貳、中國大陸等級測評運作機制初探

自 2010 年起，中國大陸正式開展其「信息安全等級保護管理辦法」要求，如圖 2.1 所示之等級測評工作項目，至 2012 年 3 月 16 日，中國大陸已有 108 家測評機構通過其測評能力評鑑，其中 22 家並通過 ISO/IEC 17020 的檢驗機構之能力評鑑，22 家亦通過 ISO/IEC 17025 的測試實驗室之能力評鑑；其目的在於經由資訊（信息）系統安全等級之測評，使資訊系統安全保護態勢逐步達到等級保護的要求；圖 2.2 是其信息安全等級保護之標準體系。



說明：
1. 資料來源：Haohao Song, Zhen Lu, And Jian Gu (2011) Chinese general techniques requirements for important information systems (Presentation), 2011-09-27 in 12th ICCC, 2011-09-27/29，與本研究。
2. 中國大陸信息安全等級3之要求界於ISO/IEC 15408的EAL (Evaluation Assurance Level) 4 ~ EAL 5之間，等級4的要求界於EAL 6 ~ EAL 7之間。

圖 2.1：中國大陸信息安全等級保護工作歷程



備考：GB/T 28448與GB/T 28449於2012-07-12發布，2012-10-01正式實施。

圖 2.2：中國大陸信息安全等級保護相關標準體系框架

等級測評的實施過程由單元測評和整體測評兩部分構成。《信息系統安全等級保護基本要求》(GB/T 22239-2008)中對安全控制點的符合性測評稱為單元測評。單元測

評是等級測評工作的基本活動，即針對測評指標，完成測評實施並進行結果判定。其中，測評指標來源於《信息系統安全等級保護基本要求－GB/T 22239－2008》第四級目錄下的各個要求項目，測評實施對測評活動輸入、測評對象、測評步驟和方法提出了要求，結果判定對測評人員執行測評實施並產生各種測評輸出數據後，如何依據這些測評輸出數據來判定被測系統是否滿足測評指標要求給出了原則和方法。《測評要求》已開發測評單元總數為264項，其中，一級48項、二級66項、三級73項、四級77項，如表2.1所示；表2.2是其等級保護分級簡析，表2.3是其第三級系統測評之基本要求的時間量之估算。

表 2.1：單元測評統計表

技術/管理	安全分類	單元測評數			
		一級系統	二級系統	三級系統	四級系統
安全技術測評	物理安全	7	10	10	10
	網絡安全	3	6	7	7
	主機安全	4	6	7	9
	應用安全	4	7	9	11
	數據安全及備份恢復	2	3	3	3
安全管理測評	安全管理制度	2	3	3	3
	安全管理機構	4	5	5	5
	人員安全管理	4	5	5	5
	系統建設管理	9	9	11	11
	系統運維管理	9	12	13	13
合計		48	66	73	77
總計		264			

表 2.2：中國大陸信息安全等級保護分級簡析

等級	**對象**	**侵害客體**	**侵害程度**	**監管強度**	**評估保證等級 (Evaluation Assurance Level，簡稱 EAL)要求**
第一級	一般系統	合法權益	損害	自主保護	
第二級		合法權益	嚴重損害	指導、備案	
		社會秩序與公共利益	損害		
第三級	重要系統	社會秩序與公共利益	嚴重損害	指導、監督、檢查、備案、測評、整改	EAL 4 ~ EAL 5
		國家安全	損害		
第四級		社會秩序與公共利益	特別嚴重損害	指導、強制監督、強制檢查、備案、測評、整改	EAL 6 ~ EAL 7
		國家安全	嚴重損害		
第五級	極端重要系統	國家安全	特別嚴重損害	指導、專門監督、專門檢查、備案、專門測評、整改	

資料來源：
1. 信息安全等級保護管理辦法（2007-06-22）。
2. Haohao Song, Zhen Lu, and Jian Gu (2011) Chinese general techniques requirements for important information systems (Presentation), 2011-09-27 in 12th ICCC, 2011-09-27/29。
3. 本研究

表 2.3：中國大陸信息安全等級保護之三級系統技術測評(資安健診)基本要求(GB/T 22239-2008)時間量估算

序號	測評對象	時間	序號	測評對象	時間
1	網路結構	1 小時	6	資料庫管理系統	1 小時
2	路由器	40 分鐘	7	應用平臺	40 分鐘
3	交換機	40 分鐘	8	應用軟體	1 小時
4	防火牆	1 小時	9	管理系統文件集	32 小時
5	服務器作業	1 小時	10	系統管理人員	2 小時
資料來源：公安部信息安全等級保護評估中心(2011)信息安全等級測評師培訓教程(中級)，表 3-18，頁 196，電子工業出版社。					

中國大陸公安部於資訊系統安全等級測評工作標準化作業準備工作告一段落後，便開始開展其初級、中級與高級之測評人員的培訓工作，其培訓工作之通過率約為 80%。

資訊安全專業人員之培訓是資訊安全等級測評人員等的源池，中國大陸「中國信息安全測評中心」，自 2002 年起開展之註冊信息安全專業人員（Certified Information Security Professional，簡稱 CISP），分為信息安全工程師（CISP-Engineering，簡稱 CISP-E 或 CISE）與信息安全管理師（CISP-Officer，簡稱 CISP-O 或 CISO），上課內容一樣如表 2.4 所示，惟考試試題不同；中國大陸主責之公安部建議其等級測評機構的 CISP-E 及 CISP-O 之人員比例為 4：1，要求是 3：1 以上；此外，CISP 尚有完成三天的 CISE/CISO 之初階課程並通過考試的註冊信息安全員（CISP-Member，簡稱 CISP-M 或 CISM）及 CISE/CISO 再完成四天擴增課程並通過考試之註冊信息安全審計（稽核）師（CISP-Auditor，簡稱 CISP-A 或 CISA），以及註冊信息安全講師（CISP-Instructor，簡稱 CISP-I 或 CISI）的系列人員培訓機制，表 2.5 是其已註冊之 CISP 的專業發展活動計分表列說明。

表 2.4：CISP（CISE / CISO）課程大綱

時間	課程名稱	課程內容
第一天	資訊安全保證之基礎實踐	◎資訊安全保證基本知識 ◎資訊安全保證原理 ◎資訊安全系統保證模型及框架 ◎資訊安全保證工作概況以及其基本內容
	資訊安全工程之原理與實踐	◎資訊安全工程基本知識 ◎資訊安全工程能力成熟度模型 ◎資訊安全工程之實作、實踐與監理
第二天	密碼學基礎	◎密碼學基本知識 ◎密碼學演算法 （對稱、非對稱與碎映（Hash）函數）

	密碼學應用	◎虛擬專用網路技術 ◎公開金鑰基礎建設與其系統	
第三天	網路協定及其架構之安全	◎TCP/IP 協定安全 ◎無線／移動通訊安全 ◎網路架構安全	
	網路安全技術	◎防火牆技術 ◎入侵偵測／預防技術 ◎網路隔離技術	
第四天	資訊安全漏洞、脆弱性與惡意程式碼	◎惡意程式碼基本知識 ◎資訊安全防禦技術 ◎美國國家脆弱性資料庫 ◎資訊安全漏洞 ◎脆弱性之攻防基礎	
	資訊安全攻防	◎標的資訊蒐集 ◎密碼破譯原理與實踐 ◎緩衝區溢位原理及實踐 ◎電子詐欺攻擊原理與實踐 ◎拒絕服務攻擊原理與實踐 ◎網頁腳本攻擊原理與實踐	
第五天	作業系統及其應用安全	◎作業系統基礎及其安全機制 ◎UNIX 安全實踐 ◎Windows 安全實踐 ◎資料庫基礎知識及其安全機制 ◎資料庫管理系統安全管理及其繫結軟體安全 ◎Web 服務基礎及其安全,電子郵件與 FTP 安全 ◎常用軟體（例：Adobe,Office 等）安全	
	資訊安全法規與標準化	◎資訊安全法規與政策 ◎個人資料保護 ◎資訊安全管理系統標準系列 ◎共同準則標準系列等	
第六天	存取控制與稽核及程式安全	◎存取控制模型 ◎存取控制技術 ◎稽核與監控技術 （含安全作業中心（Security Operation Center）） ◎軟體安全生命週期 ◎如何撰寫安全程式	
	資訊安全風險管理	◎資訊安全風險評鑑 ◎資訊安全風險處理等	
第七天	資訊安全管理要求項目	◎組織全景 ◎統禦力 ◎規劃 ◎技援	◎運作 ◎績效評估 ◎改進

	資訊安全管理控制措施	◎安全政策 ◎通訊／溝通安全 ◎資訊安全組織 ◎資訊系統之獲取 ◎人力資源安全 ◎開發與維護 ◎資產管理 ◎供應商關係 ◎存取控制 ◎資訊安全事故管理 ◎密碼技術 ◎營運持續管理 ◎實體與環境安全 ◎符合性 ◎運作安全
第八天	領域（Sector）與服務（Services）資訊安全管理	◎健康（Health care）、能源及公用事業（Energy & Utility）、金融（Finace）與電信（Telecommunication）領域 ◎個人資料保護及雲端運算服務
	CISP 測驗	100 題單選題，考試時間：兩小時

備考：此課程大綱參照 CISP 知識體系大綱-V2.3:2013-07-28 訂定，2013 年 12 月 03 日已獲得中國信息安全測評中心 CISP 培訓主責單位之同意。

表 2.5：中國大陸註冊信息（資訊）安全專業發展活動計分（三年內完成 60 分以上）方式

序號	活動項目	應予說明之內容	計分方式
1	訓練班或講座	內容、名稱、時間、地點與舉辦者	1~2 分／8 小時
2	自學	自學課程說明（報告）	1~5 分／課程
3	學術會議	內容、名稱、地點與舉辦者	1~2 分／8 小時
4	學術研究	從事與參與之活動內容及承擔的工作	5~10 分／項目（計畫）
5	論文	題目與發表方式	1~2 分／篇
6	著作	作品標題與發表方式	10~20 分／本
7	諮詢或服務	項目說明 備考： 此活動項目不適用於諮詢機構之工作人員	1 分／工作日，最高以 10 分為限
資料來源：中國信息安全測評中心（2002）註冊信息安全專業人員認證程序，信息安全標準與法律法規，頁 279~285，中國郵電出版社，2003。			

前述 CISP 之訓練課程，方進行於中國大陸大專院校的信息安全專業課程（3 學分）之開設項目，期能創造 CISP 的價值與增加其效能。

參、「資安健診」實作初探：

行政院研考會於 94 年度「國家資通安全技術服務與防護管理計畫」中，曾提出資安規範整體發展藍圖，規劃發展一系列的資安規範與參考指引，以提供組織基本的安全要求水準。更於今年為了從技術面瞭解政府機關(構)資安防護狀況，規劃資安健診（以下簡稱健診）專案，希望藉由檢測結果提升目前政府機關資安防護能量，並作為

訂定與調整資安政策之參考。在初次辦理此次資安健診的專案中，首先挑選較為重要，並處理大量機敏業務之政府機關，透過專案委託，由國內幾家專業資安廠商負責執行健診專案。而因為是初次執行之專案，且礙於專案經費有限的情況下，專案內容僅能依據近年案例中，駭客較常利用之資安防護脆弱點，執行重點項目的檢測，健診項目表 3.1 所示，大致分為六類：包含網站安全檢測、網路架構檢視、有線網路惡意活動偵測、使用者電腦檢測、伺服器主機檢測、安全設定檢測，以期綜整健診結果能夠呈現機關資安政策與防護狀態之完整性。

表 3.1：2013-09-02~2013-10-31 資安健診執行項目說明（備考：2013-08-09 PM20:48，張善政政務委員電子郵件中說明「資安健診項目為避免讀者誤會是經過仔細斟酌最完備之組合」，要求加註「初稿，持續修訂中」)

項次	檢測方式	檢測類別	檢測項目	檢測範圍	執行方式	配合事項	對應 ISO/IEC27001:2005(E) 附件 A 控制項	對應 ISO/IEC27001:2013(E) 附件 A 控制項之節碼
1	外部檢測 (15 分)	網站安全 (10 分)	網站安全防護檢測	主要對外網站	針對主要對外網站進行弱點項目 (OWASP TOP10)掃描	請提供受測網站 IP 及 Domain Name 等網站資訊	A.10.6.2 網路服務安全 A.12.2.1 輸入資料確認 A.12.6.1 技術脆弱性控	A.13.1.2 網路服務之安全 A.12.6.1 技術脆弱性管理
2		網路檢測 (5 分)	防火牆服務埠檢測	外層防火牆開啟埠	針對防火牆是否開啟具有安全性風險或非必要服務埠進行檢測	請協助提供外層防火牆 IP 及受測 DMZ 掃描網段位置	A.10.6.1 網路控制措施 A.10.6.2 網路服務安全 A.11.1.1 存取控制政策	A.13.1.1 網路控制措施 A.13.1.2 網路服務之安全 A.9.1.1 存取控制政策

3	現場檢測(85分)	網路架構檢視(15分)	網路架構設計邏輯檢視(6分)	網路架構	針對網路架構設計、網路安全設計及備援機制進行檢測	請機關協助提供網路架構圖請機關協助安排網管人員參與檢測及訪談	A.9.2.3 佈纜的安全 A.10.6.1 網路控制措施 A.10.6.2 網路服務安全	A.11.2.3 佈纜安全 A.13.1.1 網路控制措施 A.13.1.2 網路服務之安全
4			網路區域配置檢視(6分)		針對防火牆管理及網路區域存取管理進行檢測		A.9.2.3 佈纜的安全 A.10.6.1 網路控制措施 A.10.6.2 網路服務安全	A.11.2.3 佈纜安全 A.13.1.1 網路控制措施 A.13.1.2 網路服務之安全
5			主機位置配置檢視(3分)		針對各網路區域電腦主機設備配置進行檢測		A.9.2.3 佈纜的安全 A.10.6.1 網路控制措施 A.10.6.2 網路服務安全	A.11.2.3 佈纜安全 A.13.1.1 網路控制措施 A.13.1.2 網路服務之安全

6		有線網路惡意活動檢視(10分)	封包監聽與分析(5分)	至少6小時的封包側錄	針對有線網路架設側錄設備，觀察是否有異常連線或DNS查詢，並比對是否連線已知惡意中繼站或符合惡意網路行為之特徵	請機關協助提供側錄所需使用IP位置	A.10.6.1 網路控制措施 A.10.6.2 網路服務安全 A.11.4.2 外部連線的使用者鑑別 A.11.4.6 網路連線控制 A.11.4.7 網路選路控制	A.13.1.1 網路控制措施 A.13.1.2 網路服務之安全
7			網路設備記錄檔分析(5分)	至少半年內的紀錄檔或100M Bytes	針對防火牆紀錄檔中異常連線紀錄、異常流量紀錄，及入侵偵測/防禦系統紀錄中，特徵比對紀錄與異常偵測紀錄進行檢測	請機關協助提供防火牆連線與流量紀錄，以及入侵偵測/防禦系統的異常偵測紀錄	A.10.10.1 稽核存錄 A.10.10.3 日誌資訊的保護	A.12.4.1 事件存錄 A.12.4.2 日誌資訊之保護
8		使用者電腦檢視(25分)	使用者電腦惡意程式檢測(15分)	150台使用者電腦	針對使用者電腦中是否存在木馬後門、蠕蟲或駭客工具等惡意程式進行檢測	請機關協助安排人員陪同進行檢測 每台使用者電腦的檢測時間預估需要30分鐘	A.10.4.1 對抗惡意碼的控制措施 A.10.4.2 對抗行動碼的控制措施 A.10.10.1 稽核存錄 A.10.10.5 失誤日誌	A.12.2.1 防範惡意軟體之控制措施 A.12.4.1 事件存錄

9			使用者電腦更新檢視(10分)		針對使用者電腦之作業系統及應用程式更新情況進行檢測		A.12.5.1 變更控制程序 A.12.5.2 作業系統變更後的應用系統技術審查 A.12.6.1 技術脆弱性控制	A.14.2.2 系統變更控制程序 A.14.2.3 運作平台變更後，應用之技術審查 A.12.6.1 技術脆弱性管理
10		伺服器主機檢視(25分)	伺服器主機惡意程式檢測(15分)	20台伺服器主機	針對伺服器主機中是否存在木馬後門、蠕蟲或駭客工具等惡意程式進行檢測	請機關協助安排人員陪同進行檢測 每台伺服器主機的檢測時間預估需要30分鐘	A.10.4.1 對抗惡意碼的控制措施 A.10.4.2 對抗行動碼的控制措施 A.10.10.1 稽核存錄 A.10.10.5 失誤日誌	A.12.2.1 防範惡意軟體之控制措施 A.12.4.1 事件存錄
11			伺服器主機更新檢視(10分)		針對伺服器主機之作業系統、應用程式及資料庫軟體更新情況進行檢測		A.12.5.1 變更控制程序 A.12.5.2 作業系統變更後的應用系統技術審查 A.12.6.1 技術脆弱性控制	A.14.2.2 系統變更控制程序 A.14.2.3 運作平台變更後，應用之技術審查 A.12.6.1 技術脆弱性控制

12		安全設定檢視(10分)	AD伺服器群組原則安全檢測(5分)	1台AD伺服器設定	檢視AD伺服器群組原則安全性項目，如: (1)稽核原則 (2)密碼原則 (3)帳戶鎖定原則 (4)螢幕保護原則 (5)AD伺服器安全管理	請機關協助安排AD伺服器管理人員陪同執行相關群組原則安全性項目檢視	A.10.10.6 鐘訊同步 A.11.5.1 安全登入程序 A.11.5.2 使用者識別與鑑別 A.11.5.3 通行碼管理系統 A.11.5.5 連線階段逾時 A.11.6.1 資訊存取限制 A.11.6.2 敏感性系統的隔離 A.12.3.1 使用密碼控制措施政策 A.12.4.1 作業軟體的控制 A.12.5.1 變更控制程序	A12.4.4 鐘訊同步 A.9.4.2 保全登入程序 A.9.2.1 使用者註冊及註銷 A.9.2.2 使用者存取權限之配置 A.9.4.3 通行碼管理系統 A.9.4.2 保全登入程序 A.9.4.1 資訊存取限制 A.10.1.1 使用密碼控制措施之政策 A.12.5.1 對運作中系統之軟體安裝 A.12.6.2 對軟體安裝之限制 A.14.2.2 系統變更控制程序
13			DB伺服器安全設定檢視(5分)	1台DB伺服器設定	檢視DB伺服器群安全設定項目，如: (1)資料加密 (2)存取控制	請機關協助安排DB伺服器管理人員陪同執行相關安全性項目檢視	A.10.5.1 資訊備份 A.11.5.1 安全登入程序 A.11.5.2 使用者識別與鑑別 A.11.5.3 通行碼管理系統 A.11.5.5 連線階段逾時 A.11.6.1 資訊存取限制 A.11.6.2 敏感性系統的隔離 A.12.3.1 使用密碼控制措施政策 A.12.3.2 金鑰管理 A.12.4.1 作業軟體的控制 A.12.5.1 變更控制程序	A.12.3.1 資訊備份 A.9.4.2 保全登入程序 A.9.2.1 使用者註冊及註銷 A.9.2.2 使用者存取權限之配置 A.9.4.3 通行碼管理系統 A.9.4.2 保全登入程序 A.9.4.1 資訊存取限制 A.10.1.1 使用密碼控制措施之政策 A.10.1.2 金鑰管理 A.12.5.1 對運作中系統之軟體安裝 A.12.6.2 對軟體安裝之限制 A.14.2.2 系統變更控制程序

說明：1.於 ISO/IEC 27006:2011(E)中，A.10.4.1、A.10.5.1、A.11.4.2、A.11.4. 6、A.11.4.7、A.11.5.1、A.11.5.2、A.11.5.3、A.12.2.1、A.12.3.2，與 A.12.6.1 技術脆弱性管理均闡明系統測試是必要之稽核工作項目。

2.表列之 ISO/IEC 27001:2005(E)附件 A 控制項中，僅 A.12.5.1 及 A.12.5.2 於 ISO/IEC 27006:2011(E)列為「組織控制」。

3.對應 ISO/IEC 27001:2005(E)及 ISO/IEC 27001:2013(E)之附件 A 控制項，為本文作者自行處理。

以上項目為本次資安健診的重點項目，共計 13 項，但與 94 年資安規範整體發展藍圖相比較，發現雖然這次健診的項目屬於技術性的評測，但是仍有部分項目未包含

在資安健診中，未包含項目為資訊作業委外安全、電子郵件安全、控制措施建議、無線網路、可攜式媒體。在此次健診專案中技術性評測面向，雖然包含了資安規範整體發展藍圖中執行與檢查兩個構面的部分項目，扣除偏向資安管理的項目後，僅占45%，詳細的比較項目列於表 3.2 中。

表 3.2：資安健診執行項目與資安規範整體發展藍圖比較表

構面	資安規範整體發展藍圖	資安健診
規劃	資安管理要點	△
	資安管理規範	△
	實務導入指引	△
	資安產品選擇	△
	資訊系統風險評鑑	△
執行	資訊作業委外安全	╳
	電子資料庫保護	◎
	電子郵件安全	╳
	網頁程式安全	◎
	控制措施建議	╳
	檢查表發展指引	△
檢查	作業系統	◎
	入侵偵測	╳
	網頁伺服器	◎
	防火牆	◎
	無線網路	╳
	可攜式媒體	╳
	營運持續管理	△
	資安事故通備應變作業	△
	資安事故通報應變規範	△
維持與改進	指引審查	△
	教育訓練機構認證作業	△
	資安人員驗證機構認證作業	△
	資安人員驗證作業	△
	第三方驗證機構認證作業	△
	第三方驗證稽核驗證作業	△

△：該項目為政策管理面的評核項目。

◎：已包含或部分包含在資安健診專案。

╳：未包含在資安健診專案中的項目。

健診專案中對於執行人員的資格要求是參照健診項目，而認定方式以國際認證的取得為依據，因此分為四個主要能力的認證作為資安廠商人員資格評核項目，包括：惡意程式檢測能力、封包分析能力、AD（Active Directory）管理能力，以及整體資安技術能力，如表 3.3 所示；而健診項目中包含的防火牆安全、資料庫安全、網站安全等項目，因未定義應取得之國際認證，因此執行該健診項目時的技術能力較無法一致。

表 3.3：資安健診專案成員技術要求參考資料

技術項目	要求技術證照	數量
網路管理	CCNA(Cisco Certified Network Associate)以上	2
惡意程式檢測能力	CEH(Certified Ethical Hacker) 或 CHFI(Computer Hacking Forensic Investigation) 或 GSNA(GIAC Systems and Network Auditor Certification)	2
封包分析能力	NSPA(Network Security Packet Analysis) 或 GCIA(GIAC Certified Intrusion Analyst)	1
AD 管理能力	MCTS(Microsoft Certified Technology Specialist)：Windows Server 2008 Active Directory 或 MCSE(Microsoft Certified Solutions Expert)	1
整體資安技術能力	CISSP(Certified Information Systems Security Professional)或 ISO/CNS 27001 Lead Auditor	1

在健診專案計畫中，專案從起始到結束所給予的時程為十日。如表 3.4 所示，扣除起始會議一日，結束會議一日，僅能在八個工作日完成所規定進行技術評核項目。健診之項目中，可由工具執行的項目為掃描主網站弱點、掃描防火牆、側錄封包分析，但在健診專案中並未明確規範使用之工具，各資安廠商在執行資安健診時，所用的判斷標準無法一致的情況下，各政府機關所因應健診結果所採取的矯正措施也將會不一；須由資深顧問到場檢視的項目為網路架構訪談、資料庫安全檢視、AD 設定檢視與防火牆設定檢視，這三項的訪談與檢視，為此健診專案中的重點項目，因為在伺服器端的錯誤設定可能造成用戶大規模的資安弱點，但由於顧問能夠投入的時間有限，僅能在一至兩日內完成檢查，對這三個項目之瞭解深度可能會不足以呈現真實資安風險；而必須由大量一般資安工程師進行的項目為惡意程式檢測，由於此項目涵蓋範圍較大，包含 20 台重要伺服器與 150 台一般使用者電腦，以五個工作日完成資料的

蒐集，平均一天就要蒐集 30 台以上之主機資訊，本項目人力就需要安排 20 人天，若是多個檢診專案在同一時段進行，可能會讓資安廠商面臨人力調配困難，以及符合此技術能力的人力資源不足。

表 3.4：2013-09-02~2013-10-31 資安健診專案執行示意甘特圖

項次	工作名稱	期程	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10
1	起始會議	1 日	■									
2	工作計畫書交付	2 日		■	■							
3	網路架構訪談	1 日				■						
4	掃描主網站弱點	1 日					■					
5	掃描防火牆	1 日					■					
6	封包側錄設備架設	1 日						■				
7	資料庫安全檢視	1 日						■				
8	AD 設定檢視	1 日						■				
9	防火牆設定檢視	1 日						■				
10	惡意程式檢測	5 日					■	■	■	■	■	
11	結案會議	1 日										■

前述「資安健診」亦推展至地方政府，以「新竹市稅務局」為例，於 2013 年 11 月 21 日接受「行政院國家資通安全會報技術服務中心」2 人次之如表 3.5 所示的「伺服器主機安全檢測」，惟範疇與工作項目均較表 3.4 精簡，宜強化之。

表 3.5：2013-11-21 之「新竹市稅務局」資安健診作業-伺服器主機安全檢測配合事項

1. 請完成基本資料調查表內容填寫。
   - 請確認受測主機的 IP 及相關主機資訊。
2. 請協助提供內部掃描 IP，以利主機弱點掃描作業進行。
   - 請確認所提供的內部掃描 IP 可連線至受測主機。
   - 請於檢測前完成檢測 IP 準備。
3. 請協助安排陪同人員參與伺服器主機檢測作業。
   - 伺服器主機檢測期間需請單位協助安排陪同人員及伺服器管理員。
   - 伺服器主機檢測需以系統管理員權限登入，每台伺服器檢測時間約為 1~3 小時，包含安全項目檢測及惡意程式檢測。
   - 檢測期間若發現疑似惡意程式樣本，需將樣本攜回技服中心進行後續分析作業。

「居安思危，思則有備，有備無患，敢以此規」，已納入如表 3.6 所示之「2013 年資訊安全重點工作項目」的年度政府機關（構）資通稽核作業 40%之如表 3.1 所示的「資安健診」，開啟我國資訊安全管理系統（Information Security Management System，簡稱 ISMS）技術項目稽核之新頁，惟於 ISMS 的 ISO/IEC 27000 系列標準中之 ISO/IEC 27006 之附件 D，規範技術控制與系統測試的範疇已超越表 3.1；此外，在 2011 年已公佈之相關標準（ISO/IEC 27007 與 TR 27008 Guidelines for auditors on ISMS Controls）宜予以參考，俾規範「資安健診」的標準化作業，表 3.6 中之「推動政府資訊安全組態基準」及「ISMS 驗證的工作項目」亦同[3][4][5]。

表 3.6：2013 年資訊安全重點工作項目[資料來源：行政院資通安全辦公室，http://www.npl.ly.gov.tw (2013-10-23 檢索)]

1. 行政院國家資通安全會報技術服務中心(Information and Communication Security Technology Center，簡稱 ICST)改以「二線監控」為主；此外，ICST 亦將扮演政府資訊安全服務辦公室(Security Project Management Office，簡稱 SPMO)角色。
2. 推動政府資訊安全組態基準(Government Configuration Baseline，簡稱 GCB)。
3. 推動網域名稱安全延伸(Domain Name System Security Extensions，簡稱 DNSSEC)。
4. 推動以全機關為範疇之資訊安全管理系統之驗證。
5. 規劃資安健診作業。
6. 規劃辦理網路攻防演習。

前述「資安健診」開展我國資訊安全管理稽核之新姿，惟其與 ISMS 稽核要求事項中之「系統測試」工作項目的有效性之關連等，均存在持續修訂之空間。

肆、結論：

中國大陸師法美國，中國大陸公安部於進行資訊(信息)安全等級的保護之標準化作業並適時發布法規規範如圖 4.1 所示的相關工作；以伺服機為例，表 4.1 是其遵循標準技術要求舉隅，表 4.2 是其 3 級系統技術測評之基本要求舉隅。

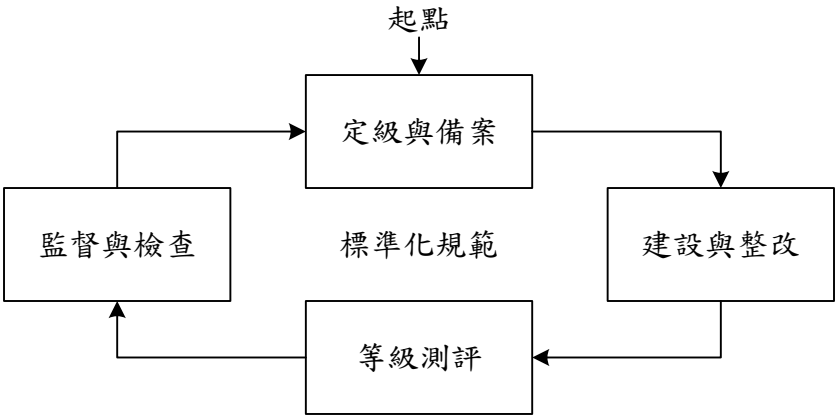


圖 4.1：中國大陸之資訊安全管理實作路徑示意

表 4.1：中國大陸資訊系統分級之伺服機技術要求舉隅

	第二級	第三級	第四級
鑑別	通行碼	雙因子(例：通行碼與符記)	同第三級，惟要求其中 1 因子不可偽造(例：生物識別)
安全標記	無	無	建議安裝
存取控制	自主性存取控制(DAC)	強制性存取控制(MAC)	同第三級
可信路徑	無	無	必須具備
稽核存底	稽核檔	必須具備稽核分析工具	必須安裝集中處理之稽核分析工具
殘留資訊保護	無	必須具備刪除工具	同第三級
完整性檢查	無	時須具備完整性檢查工具	同第三級
電磁防護	電磁干擾之防護	關鍵設施之屏蔽防護	關鍵區域之屏蔽防護(例：必須位於屏蔽室內)

說明：

1. DAC: Discretionary Access Control。
2. MAC: Mandatory Access Control。
3. 參考資料：GB/T 22239-2008，信息安全技術－信息系統安全等級保護基本要求。

表 4.2：中國大陸信息安全等級保護測評之 3 級系統技術測評的基本要求 (GB/T22239-2008)舉隅

《基本要求》項	工具測試方法
7.1.2.1 結構安全(G3)c) 應在業務終端與業務伺服器之間進行路由控制建立安全的存取路徑；	利用追蹤路徑(Traceroute)等指令，跟蹤路由資訊，查看網路之間的路由情況。
f) 應避免將重要網段部署在網路邊界處且直接連接外部資訊系統，重要網段與其他網段之間採取可靠的技術隔離手段；	利用多點掃描結果對比分析
7.1.2.2 存取控制(G3)b) 應能根據會話狀態資訊為資料流程提供明確的允許/ 拒絕存取的能力，控制粒度為埠級；	利用多點掃描結果對比分析
c) 應對進出網路的資訊內容進行過濾，實現對應用層 HTTP、FTP、TELNET、SMTP、POP3 等協議命令級的控制；	利用埠、漏洞掃描及滲透測試工具，驗證是否具備命令級別的檢測及阻斷能力
7.1.2.5 入侵防範(G3)a) 應在網路邊界處監視以下攻擊行為：埠掃描、強力攻擊、木馬後門攻擊、拒絕服務攻擊、緩衝區溢出攻擊、IP 碎片攻擊和網路蠕蟲攻擊等；	在入侵防範設備監控範圍內，針對入侵防範設備策略配置情況，進行漏洞掃描以及滲透測試等手段，發送攻擊資料，查看入侵防範設備的回應情況。
b) 當檢測到攻擊行為時，記錄攻擊源 IP、攻擊類型、攻擊目的、攻擊時間，在發生嚴重入侵事件時應提供報警。	在入侵防範設備監控範圍內，針對入侵防範設備策略配置情況，進行漏洞掃描以及滲透測試等手段，發送攻擊資料，查看入侵防範設備的回應情況。
7.1.2.7 網路設備防護(G3)a) 應對登錄網路設備的用戶進行身分鑒別；	利用掃描器弱口令探測功能探測網路設備弱口令
e) 身分鑑別資訊應具有不易被冒用的特點，口令應有複雜度要求並定期更換；	利用掃描器發現網路設備漏洞，嘗試利用滲透工具進行驗證測試
7.1.3.2 存取控制(S3)d) 應嚴格限制預設帳戶的存取許可權，重命名系統預設帳戶，並修改這些帳戶的預設密碼；	利用掃描器探測伺服器是否存在預設帳戶，利用掃描器探測系統是否存在弱密碼
7.1.3.5 入侵防範(G3)a) 應能夠檢測到對重要伺服器進行入侵的行為，能夠記錄入侵的源 IP、攻擊的類型、攻擊的目的、攻擊的時間，並在發生嚴重入侵事件時提供報警；	利用掃描器、滲透工具，對目標伺服器進行漏洞掃描及類比攻擊操作，查看目標伺服器報警及日誌情況
c) 作業系統應遵循最小安裝的原則，僅安裝需要的元件和應用程式，並透過設置升級伺服器等方式，保持系統修補及時得到更新。	利用掃描器漏洞掃描功能，探測目標系統所開啟的服務及漏洞情況
7.1.4.9 資源控制(A3)f) 應能夠對系統服務水平降低到預先規定的最小值進行檢測和報警。	檢查應用系統，查看其服務水平最小值之設定及其檢測以及報警的功能，並測試之
說明：中國大陸 GB/T 22239-2008 中之基本要求分成技術要求與管理要求兩大類，其技術要求再進一步細分成資訊安全類要求(簡記為 S)、服務保證類要求(簡記為 A)及通用安全保護類要求(簡記為 G) 3 種類型。	

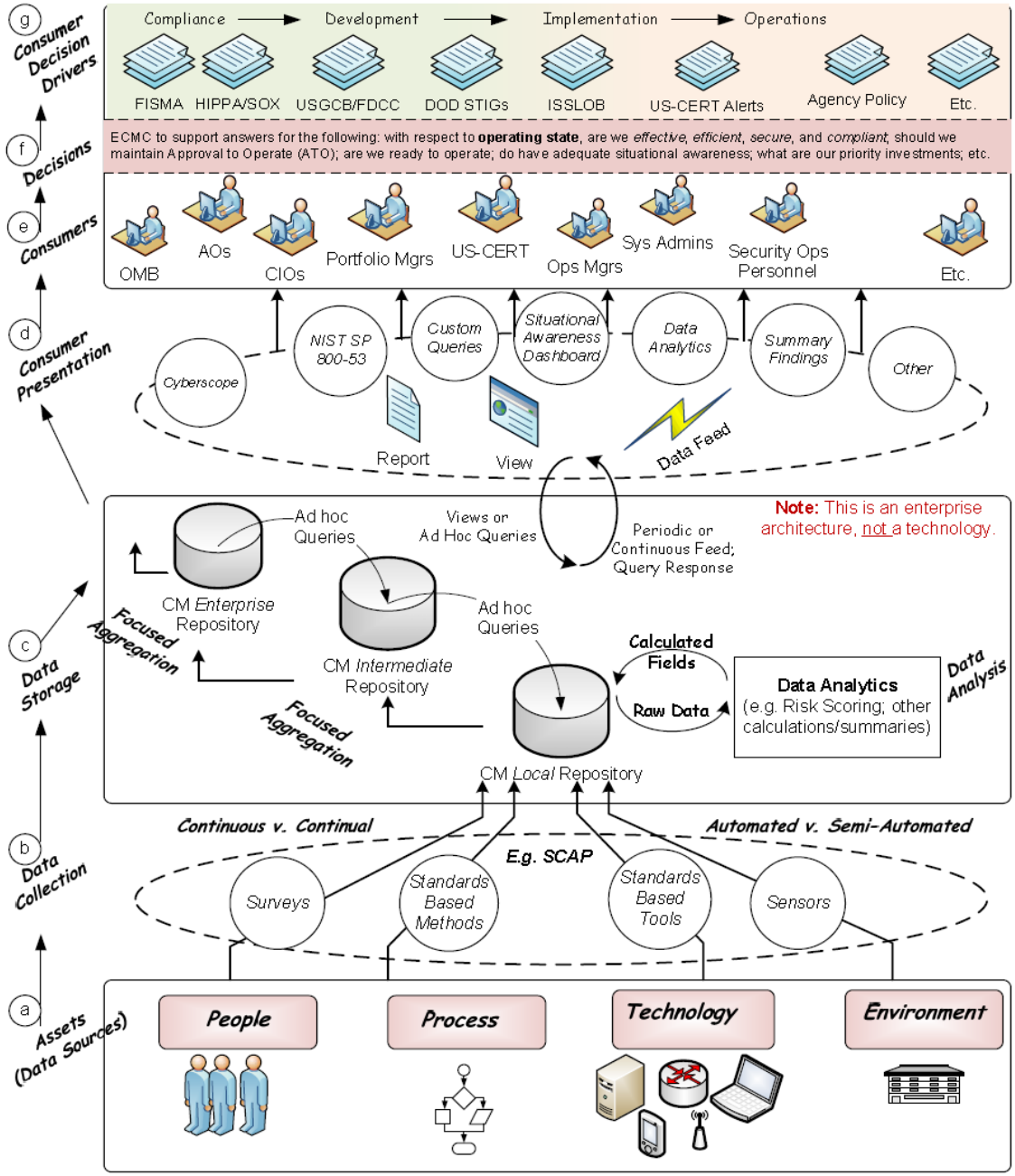
資訊系統涉及公共與國家安全已是事實，如何確保機敏性資訊及其資訊系統不受未經授權之存取、使用、揭露、破解、修改與毀壞，以提供機密性、完整性與可用性之應用，已是各國政府宜面對的問題。標準化是法規遵循之普同理解的形塑過程，中國大陸資訊安全等級保護測評等標準化之歷程，值得開展更深入的思考與討論，以塑建我國 ISMS 之「資安健診」事實及規範間的反思機制[4][5][9][10][2][18]。

2014 年 01 月 03 日，行政院以：「院臺護字 1020158918 號函」要求加速推動 Windows 7 與 IE8 環境導入 GCB 設定，並由資安辦（行政院資通安全辦公室）持續掌握及督促各部會推動辦理 GCB 之設定導入（請參見表 3.6）。

美國 FISMA（Federal Information Security Management Act）實作計畫於 2010 年之 FISMA 2.0 方使用 USGCB / FDCC 的名稱，之前，在 FISMA 1.0 僅使用 FDCC（Federal Desktop Core Configuration）的名稱；FISMA 實作計畫於 FDDC 之標準化工作項目告一段落並於 435,000 部個人電腦的先導計畫獲得：「降低一半以上之資訊安全的風險，減少四分之三以上的成本。」之結果後，在 2007 年 06 月 22 日以 M-07-11 號備忘錄要求使用經 SCAP（Security Content Automation Protocol）確認的 FDCC（相似於前述之 GCB）；USGCB（FISMA 2.0）除 FDCC 外，尚包含伺服機（例：UNIX）、網路(例：CISCO 路由器)、資料庫管理系統（例：ORACLE）等。

根基於 FDCC 之技術性及其目的，於準備工作完成後，2009 年，使用：「連續性監視（Continuous Monitoring，簡稱 CM）」之名稱開展 FISMA 2.0 的計畫；2010 年 04 月 21 日，以 M-10-15 號備忘錄將 CM 列為 FISMA 實作計畫之核心工作項目，同時提出「連續性監視即服務（Continuous Monitoring as a Services，簡稱 CMaaS）」並於「雲端運算」編列 US$440,000,000 的採購預算。推展 CMaaS，於成本面向，美國估計將節省三分之二以上。2013 年 8 月 23 日，美國國土安全部公布應 2010 年 7 月 6 日，OMB（US Office of Management and Budget）遵循 FISMA 的要求，實作 CMaaS 之 M-10-28 號備忘錄的 CDM（Continuous Diagnostics and Mitigation）/ CMaaS 之 US$6,000,000,000 預算的三階段（Phase）之 CDM 計畫（Program）的 17 家工業夥伴（Industry Partners），將 CMaaS 擴增至關鍵基礎設施、州、地方政府、保留區等的服務，期以 3 年（2014 年～2016 年）之努力提昇包含人力資源在內的美國全國之 15 項資訊安全連續性監視的能力（Capabilities）。

「他山之石，可以攻玉」，FISMA 實作計畫要求使用 SCAP 取徑（CyberScope），如圖 4.2 所示，CM 已建立表 3.1 的「資安健診」工作項目之自動化作業，圖 4.3 是其量測的示意說明[18][1][19]。

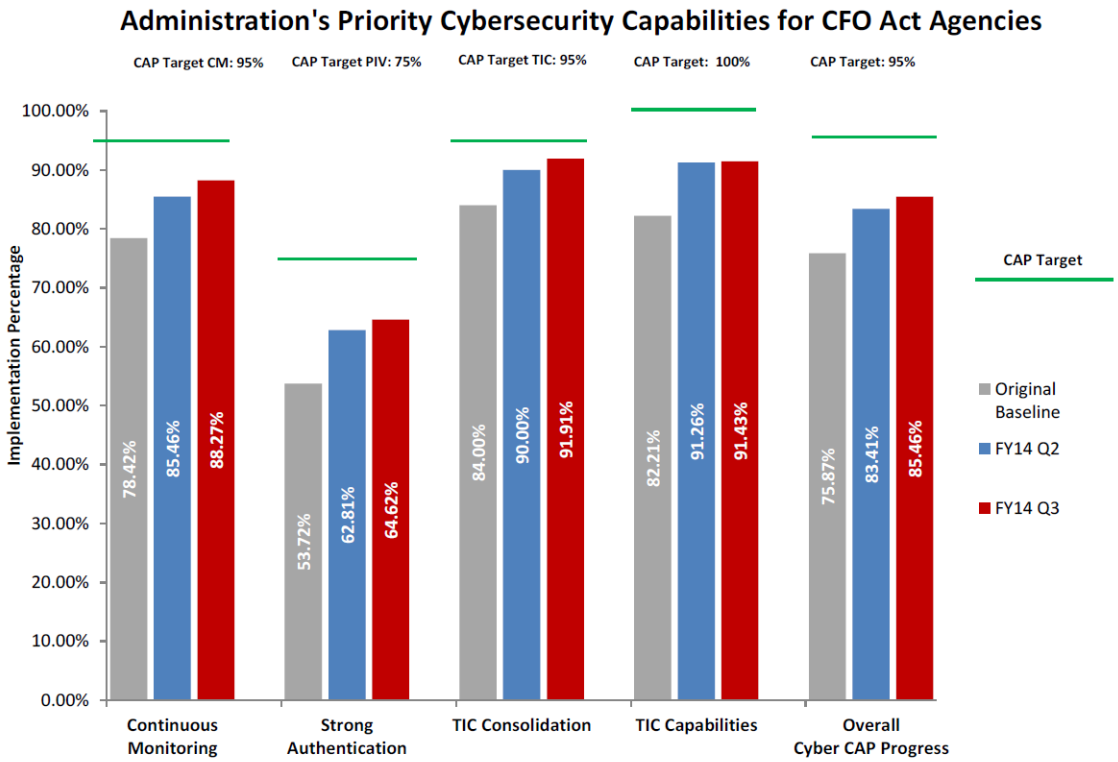


資料來源：NIST Interagency Report (IR)7756 (2nd Draft), CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model, January 2012。

備考：囿於篇幅，此圖之闡明，將另文敘明，有興趣之讀者可以先行參閱：

1. NIST IR 7799 (Draft):Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specification, January 2012。
2. NIST IR 7800 (Draft):Applying Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains, January 2012。
3. NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM)for Federal Information Systems and Organizations, September 2011。

圖 4.2：連續性風險評鑑（Continuous Asset Evaluation Situational Awareness, and Risk Scoring, CAESARS)之參考架構(Reference Architecture View)



The implementation percentages of the CAP cybersecurity priority capabilities from the FISMA reporting in CyberScope for Q3 FY2014.

Agency	Continuous Monitoring Average	Automated Asset Management	Automated Configuration Management	Automated Vulnerability Management	PIV Local Acces	TIC 2.0 Capabilities	TIC Traffic Consolidation	CAP Average
DHS	88	92	83	90	55	92	97	85
DOC	76	68	86	74	60	72	77	73
DOD	85	98	66	92	81	N/A	N/A	84
DOE	91	93	94	86	34	92	69	78
DOI	80	98	69	74	0	85	99	71
DOJ	99	99	99	99	43	88	100	88
DOL	99	100	98	98	0	100	100	83
DOT	88	95	90	78	13	85	99	77
ED	94	100	92	90	72	95	84	89
EPA	53	33	96	31	0	90	95	57
GSA	98	100	95	100	94	98	99	98
HHS	92	95	83	97	66	100	82	87
HUD	94	94	100	87	0	85	100	78
NASA	96	99	91	99	56	88	100	89
NRC	92	88	95	94	0	100	100	79
NSF	95	100	86	100	7	100	100	82
OPM	97	95	100	95	0	74	100	77
SBA	100	100	100	100	0	100	99	83
SSA	98	100	93	100	85	93	100	95
State	88	86	88	91	1	92	100	76
Treasury	98	99	98	97	11	99	99	84
USAID	93	90	100	90	0	100	100	80
USDA	85	100	100	55	2	82	71	68
VA	96	94	100	94	12	93	44	73

**The Continuous Monitoring average is the average of Asset, Configuration, and Vulnerability Management. The CAP average is the average of PIV, TIC 2.0 Capabilities, TIC Consolidation, and Asset, Configuration, and Vulnerability Management.*

圖 4.3：美國 FY14Q2 到 FY14Q3 之跨部機關優先（Cross-Agency priority , CAP）目標績效與 FY14Q3 財務總監（Chief Financial Officers ，CFO）的機關 FISMA 計分卡[1]

為落實 ISMS，自 2008 年起 FISMA 實作計畫提出包含前述 15 項 CM 宜具備能力之資訊技術的（Information Technology，簡稱 IT）的如表 4.3 所示之資訊（技術）安全基礎知識（IT Security Essential Body of Knowledge，簡稱 EBK）及其與 ISMS 之角色關連框架，期能自義務教育起，養成 ISMS 的執行能力[18][1][19][6][7]。

表 4.3：資訊安全基礎知識與角色關連表列[6]

IT Security EBK：能力與功能框架 功能觀點 M：管理 Manage D：設計 Design I：實作 Implement E：評估 Evaluate		資訊技術安全角色(IT Security Roles)																			
		經營管理階層(Executive)						功能執行階層(Functional)								基本必然階層(Corollary)					
		資訊長 Chief Information Officer		資訊安全官 Information Security Officer		資訊技術安全合規官 IT Security Compliance Officer		數位鑑識專業人員 Digital Forensics Professional		資訊技術系統操作維護專業人員 IT Systems Operations and Maintenance Professional		資訊技術安全專業人員 IT Security Professional		資訊技術安全工程師 IT Security Engineer		實體安全專業人員 Physical Security Professional		隱私權專業人員 Privacy Professional		採購專業人員 Procurement Professional	
資訊技術安全能力領域	資料安全 Data Security	M		M	D							M	D		D				D		
					E		E			I	E		E		E				E		
	數位鑑識 Digital Forensics			M	D			M	D												
							E	I	E	I											
	企業營運持續 Enterprise Continuity	M		M							D						D				
							E			I			E			I					
	事件管理 Incident Management	M		M							D		D					M	D		
							E	I		I	E		E			I		I	E		
	IT 安全教育訓練 IT Security Training and Awareness	M		M									D						D		
							E					I	E						E		
	IT 系統營運與維護 IT Systems Operations and Maintenance								D	M	D				D						
							E	I	E	I	E			I							
	網路與通訊安全 Network and Telecommunications Security								D	M	D				D						
							E	I		I	E			I							
	人員安全 Personnel Security	M		M									D						D		
							E						E				E	I			
	實體與環境安全 Physical and Environmental Security	M		M									D			M	D				
							E						E			I	E				
	設備採購	M		M																M	D

	Procurement						E		E		E						E			I	E
	法規與標準遵循 Regulatory and Standards Compliance	M	D	M			D											M	D		
					I		E					I						I	E		
	安全風險管理 Security Risk Management	M		M									D					M	D		
			E		I		E	I		I		I	E	I		I		I	E		
	策略安全管理 Strategic Security Management	M	D	M																	
			E	I			E														
	系統與應用程式安全 System and Application Security	M		M											D						
							E			I				I	E						

綜上所述，「借箸代籌」，於「短程（2014 年至 2016 年）」宜要求我國 ISMS 之驗證，稽核時應遵循 ISO/IEC 27006 之要求事項履行「技術控制」的「系統測試」[2]；「中程（2016 年至 2018 年）」宜遵循 ISO/IEC TR 27008 之規範，建立我國「資安健診」的「單元測試」之要求事項標準，並參照表 4.3 修訂表 3.2 的內容[8][14][4]；「長程（2018 年至 2020 年）」宜制定我國 ISMS 之行政管理的核心能力之標的（Target），並建立如圖 4.3 所示的績效量測機制[18][1][19][6][7]。

[誌謝]：本文作者謹在此向審稿者對增進本文品質之貢獻與黃健誠先生協助整理資料的辛勞，致衷心的謝忱！

參考文獻：

[1] Daniel, M., A. Mayorkas and B. Work (2014) Cybersecurity : Cross Agency Priority Goal Quarterly Progress Update (FY 2014 Quarter 3).

[2] ISO (2011) Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems, 2011-12-01。

[3] ISO (2011) Information technology – Security techniques – Guidelines for information security management systems auditing, ISO/IEC 27007:2011-11-15.

[4] ISO (2011) Information technology – Security techniques – Guidelines for auditors on information security controls, ISO/IEC TR 27008:2011-10-15.

[5] ISO (2013) Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013-10-01.

[6] U.S. Department of Homeland Security (DHS) (2008) Information Technology (IT) Security Essential Body of Knowledge (EBE), September 2008.

[7] U.S. DHS (2014) FY15 CIO Annual FISMA Metrics, 2014-09-12.
[8] 行政院 (2013) 院臺資字第 1020146262 號函，2013-09-06。
[9] 行政院資通安全辦公室 (2013) 我國如何因應網軍與駭客攻擊並強化資訊安全措施，http://npl.ly.gov.tw/do/www/FileViewer?id=3667 (2013-10-23 檢索)。
[10] 行政院(2013)院臺護字第 1020157911 號函，2013-12-15。
[11] 中國大陸全國等級保護測評機構推荐目錄，http://www.djbh.net (2013-10-19 檢索)。
[12] 中華人民共和國公安部(2010)信息安全等級保護測評工作管理規範(試行)，公信安[2010]303 號函，2010-03-02。
[13] 中華人民共和國公安部(2009)關于開展信息安全等級保護安全建設整改工作的指導意見，公信安[2009]1429 號函，2009-10-27。
[14] 公安部信息安全等級保護評估中心編著(2010)信息安全等級測評師培訓教程(初級)，電子工業出版社，2010-10。
[15] 公安部信息安全等級保護評估中心編著(2011)信息安全等級測評師培訓教程(中級)，電子工業出版社，2011-01。
[16] 計算機信息系統 安全保護等級畫分準則，GB/17859-1999，中華人民共和國國家標準。
[17] 樊國楨等 (2013) 中國大陸資訊安全政策發展要情研析(未發表研究報告)。
[18] 樊國楨等(2012)論美國資訊安全管理政策－從「數位空間國際策略」中之供應鏈風險管理標準化進程談起，前瞻科技與管理，第 2 卷第 2 期，頁 15~34。
[19] 樊國楨、黃健誠與林樹國 (2013) 完備我國資訊安全管理法規初論，前瞻科技與管理，第 3 卷，第 1 期，頁 97~147。

附件：ISO/IEC 27006:2011(E)之附件 D（參考：依據 ISO/IEC 27001：2013 之 ISO/IEC 27006 新版，於 2014 年 11 月 18 日方進入 DIS 登錄(40.40)階段）。

執行 ISO/IEC 27001:2005 附件 A 控制項的審查指引

D.1 目的

本附件提供有關 ISO/IEC 27001:2005 附件 A 所列控制項的執行情形的審查指引，以及在初次稽核及後續追查訪查時，如何搜集有關其執行情形的稽核證據的指引。客戶組織為 ISMS 而選定的所有控制項(如適用性聲明)的執行情形，需在初次稽核的第 2 階段，與追查或重新驗證活動期間審查。

驗證機構所收集的稽核證據必須充分，以便作出控制項是否有效的結論。控制項如何被預期地執行，將在客戶組織在適用性聲明中或由其參考引述之程序及政策中說明。顯然地，ISMS 範圍以外的控制項將不被稽核。

D.1.1稽核證據

最佳品質的稽核證據，是收集自稽核員的觀察(例如：上鎖門已上鎖，人們確已簽署保密協議，有資產登記簿並且觀察到資產，系統設定適當等)。證據可收集自執行控制項結果的查 閱(例如：由正確授權職員所簽名而給予存取權的人員印出資料，事件解決的紀錄，正確的授權職員所簽署的處理授權，管理層階(或其它)的會議紀錄等)。證據可以是稽核員直接測試(或再執行)控制項的結果(例如：企圖執行為控制項所禁止的工作，判斷是否安裝並更新防護惡意碼的軟體在機器上，被賦予的權限(在檢查授權後)等)。證據可藉由面談雇員/承包商有關處理及控制事項，並判斷其是否正確收集之。

D.2 如何使用表 D.1

D.2.1“組織控制”及“技術控制”欄

各欄中的“X”表示該控制項是組織控制項或技術控制項。因為某些控制項是組織也是技術者，所以在兩欄中都有登錄。

執行組織控制項的證據，可透過執行控制項的紀錄的審查、面談、觀察、及實體檢查而搜集。 執行技術控制項的證據，通常可經由系統測試(參閱以下)，或經由專業的稽核/報告工具而搜集。

D.2.2“系統測試”欄

“系統測試”是指直接的系統審查(例如：系統設定或型態的審查)。稽核員的問題，可在系統控制台，或藉由測試工具結果的評估，而得到答案。如果稽核員知道客戶組織有使用電腦工具時，可用它來支援稽核工作；或對客戶組織(或其次承包商)的評估結果之審查。

對技術控制項的審查有兩種：

- 「可能」：系統測試可能被用來評估控制項的執行，但通常不需要；
- 「建議」：系統測試通常是必要的。

D.2.3 “「虛擬檢驗」”欄

“虛擬檢驗”是指這些控制項通常需要現場的虛擬檢驗，以評估其效能。這表示，相關書面文件的審查或透過面談並不足夠－稽核員須在執行地點驗證控制項。

D.2.4 “「稽核審查」指引”欄

稽核特定控制項時如有指引將會有所幫助，“意見”欄提供評估該控制項的可能重點，做為稽核員的進一步指引。

表 D.1－控制類別

ISO/IEC 27001:2005 附件 A 的控制項		組織控制	技術控制	系統測試	虛擬檢驗	稽核審查指引
A.5	安全政策					
A.5.1	資訊安全政策					
A.5.1.1	資訊安全政策文件	X				
A.5.1.2	資訊安全政策之審查	X				管理審查記錄
A.6	資訊安全組織					
A.6.1	內部組織					
A.6.1.1	管理階層對資訊安全的承諾	X				管理會議記錄
A.6.1.2	資訊安全協調工作	X				管理會議記錄
A.6.1.3	資訊安全責任的配置	X				
A.6.1.4	資訊處理設施的授權過程	X				
A.6.1.5	機密性協議	X				從檔案中取樣
A.6.1.6	及權責機關的聯繫	X				
A.6.1.7	及特殊利害相關團體的聯繫	X				
A.6.1.8	資訊安全的獨立審查	X				閱讀報告
A.6.2	外部人士					
A.6.2.1	及外部人士相關的風險之識別	X				
A.6.2.2	與顧客交涉時注意到安全	X				
A.6.2.3	在第三方協議中注意到安全	X				檢驗一些合約條件
A.7	資產管理					
A.7.1	資產責任					
A.7.1.1	資產清冊	X				鑑別資產
A.7.1.2	資產的擁有權	X				
A.7.1.3	資產之可被接受的使用	X				
A.7.2	資訊分類					

A.7.2.1	分類指導綱要	X				
A.7.2.2	資訊標示及處置	X				名稱：目錄、檔案、印刷紀錄、記錄媒體(例如磁帶、磁碟、CDs)、電子訊息及檔案傳輸。
A.8	人力資源安全					抽查一些人力資源檔案
A.8.1	聘雇之前					
A.8.1.1	角色及責任	X				
A.8.1.2	篩選	X				
A.8.1.3	聘僱條款及條件	X				
A.8.2	聘雇期間					
A.8.2.1	管理階層責任	X				
A.8.2.2	資訊安全認知、教育及訓練	X				問職員是否知道一些他們須知道的特定事情
A.8.2.3	懲處過程	X				
A.8.3	聘僱的終止或變更					
A.8.3.1	終止責任	X				
A.8.3.2	資產的歸還	X				
A.8.3.3	存取權限的移除	X	X	建議		
A.9	實體及環境安全					
A.9.1	安全區域					
A.9.1.1	實體安全周界	X				
A.9.1.2	實體進入控制措施	X	X	可能	X	製作出入紀錄檔案
A.9.1.3	保全辦公室、房間及設施	X			X	
A.9.1.4	對外部及環境威脅的保護	X			X	
A.9.1.5	在安全區域內工作	X			X	
A.9.1.6	公共進出、收發及裝卸區	X			X	
A.9.2	設備安全					
A.9.2.1	設備安置及保護	X	X	可能	X	
A.9.2.2	支援的公用設施	X	X	可能	X	
A.9.2.3	佈纜的安全	X			X	
A.9.2.4	設備維護	X				
A.9.2.5	場所外設備的安全	X	X	可能		可攜式裝置加密
A.9.2.6	設備的安全汰除或再使用	X	X	可能	X	
A.9.2.7	財產的攜出	X				
A.10	通訊及作業管理					
A.10.1	作業之程序及責任					
A.10.1.1	文件化作業程序	X				
A.10.1.2	變更管理	X	X	建議		
A.10.1.3	職務的區隔	X				
A.10.1.4	開發、測試及運作設施的分隔	X	X	可能		

A.10.2	第三方服務交付管理					
A.10.2.1	服務交付	X				
A.10.2.2	第三方服務的監視及審查	X	X	可能		
A.10.2.3	第三方服務變更的管理	X				
A.10.3	系統規劃及驗收					
A.10.3.1	容量管理	X	X	可能		
A.10.3.2	系統驗收	X				
A.10.4	防範惡意碼及行動碼					
A.10.4.1	對抗惡意碼的控制措施	X	X	建議		抽樣伺服器、桌上電腦、閘道器
A.10.4.2	對抗行動碼的控制措施	X	X	可能		
A.10.5	備份					
A.10.5.1	資訊備份	X	X	建議		嘗試復原
A.10.6	網路安全管理					
A.10.6.1	網路控制措施	X	X	可能		
A.10.6.2	網路服務的安全	X				SLA's、安全特性
A.10.7	媒體的處置					
A.10.7.1	可移除式媒體的管理	X	X	可能		
A.10.7.2	媒體的汰除	X				
A.10.7.3	資訊處置程序	X				
A.10.7.4	系統文件的安全	X	X	可能	X	
A.10.8	資訊交換					
A.10.8.1	資訊交換政策及程序	X				
A.10.8.2	交換協議	X				
A.10.8.3	輸送中的實體媒體	X	X	可能		加密或實體保護
A.10.8.4	電子傳訊	X	X	可能		確認樣本訊息符合政策/程序
A.10.8.5	業務資訊系統	X				
A.10.9	電子商務服務					
A.10.9.1	電子商務	X	X	可能		
A.10.9.2	線上交易	X	X	建議		檢查：信用、存取授權
A.10.9.3	公眾可用的資訊	X	X	可能		
A.10.10	監視					線上或列印
A.10.10.1	稽核存錄	X	X	可能		
A.10.10.2	監控系統的使用	X	X	可能		
A.10.10.3	日誌資訊的保護	X	X	可能		
A.10.10.4	管理者及操作者日誌	X	X	可能		
A.10.10.5	失誤存錄	X				
A.10.10.6	鐘訊同步		X	可能		
A.11	存取控制					
A.11.1	存取控制的營運要求					

A.11.1.1	存取控制政策	X				
A.11.2	使用者存取管理					
A.11.2.1	使用者註冊	X				抽選雇員/承包商被授權所有系統的存取權
A.11.2.2	特權管理	X	X	可能		職員的內部轉移
A.11.2.3	使用者通行碼管理	X				
A.11.2.4	使用者存取權限的審查	X				
A.11.3	使用者責任					
A.11.3.1	通行碼的使用	X				證實在適當處所有使用者使用之準則/政策
A.11.3.2	無人看管的使用者設備	X				證實在適當處所有使用者使用之準則/政策
A.11.3.3	桌面淨空及螢幕淨空政策	X			X	
A.11.4	網路存取控制					
A.11.4.1	網路服務的使用政策	X				
A.11.4.2	外部連線的使用者鑑別	X	X	建議		
A.11.4.3	網路設備識別		X			
A.11.4.4	遠端診所及組態埠保護		X	建議		
A.11.4.5	網路區隔	X	X	可能		網路圖：WAN、LAN、VLAN、VPA、網路物件、網路區隔(例如 DMZ)
A.11.4.6	網路連線控制	X	X	建議		不尋常分享網路
A.11.4.7	網路選路控制	X	X	建議		防火牆、路由器/開關：原則依據、ACL's、存取控制政策
A.11.5	作業系統存取控制					
A.11.5.1	保全登入程序	X	X	建議		
A.11.5.2	使用者識別及鑑別	X	X	建議		
A.11.5.3	通行碼管理系統	X	X	建議		
A.11.5.4	系統公用程式的使用	X	X	建議		
A.11.5.5	會談期逾時	X	X	可能	X	
A.11.5.6	連線時間的限制	X	X	可能	X	
A.11.6	應用系統及資訊存取控制					
A.11.6.1	資訊存取限制	X	X	建議		
A.11.6.2	敏感性系統的隔離	X	X	可能		
A.11.7	行動計算及遠距工作					
A.11.7.1	行動計算及通信	X	X	可能		
A.11.7.2	遠距工作	X	X	可能		
A.12	資訊系統獲取、開發及維護					
A.12.1	資訊系統的安全規定					
A.12.1.1	安全要求分析及規格	X				
A.12.2	應用系統的正確處理					

A.12.2.1	輸入資料的確認	X	X	建議		軟體開發準則、SW 測試；在抽樣的營運應用中確認，且是在使用者所需要的控制項實際存在情況下。
A.12.2.2	內部處理的控制措施	X	X	可能		軟體開發準則、SW 測試；在抽樣的營運應用中確認，且是在使用者所需要的控制項實際存在情況下。
A.12.2.3	訊息完整性		X	可能		
A.12.2.4	輸出資料的確認	X	X	可能		軟體開發準則、SW 測試；在抽樣的營運應用中確認，且是在使用者所需要的控制項實際存在情況下。
A.12.3	密碼控制措施					
A.12.3.1	使用密碼控制措施之政策	X	X	可能		若適當，亦檢查政策執行
A.12.3.2	金鑰管理	X	X	建議		
A.12.4	系統檔案之安全					
A.12.4.1	作業軟體的控制	X	X	可能		
A.12.4.2	系統測試資料之保護	X	X	可能	X	
A.12.4.3	程式源碼的存取控制	X	X	建議		
A.12.5	開發及支援程序的安全					
A.12.5.1	變更控制程序	X				
A.12.5.2	作業系統變更後的應用系統技術審查	X				
A.12.5.3	套裝軟體變更之限制	X				
A.12.5.4	資料洩漏	X	X	可能		未知服務
A.12.5.5	委外的軟體開發	X				
A.12.6	技術弱點管理					
A.12.6.1	技術弱點之控制	X	X	建議		批次分佈
A.13	資訊安全事故管理					
A.13.1	通報資訊安全事故及弱點					
A.13.1.1	通報資訊安全事故	X				
A.13.1.2	通報安全弱點	X				
A.13.2	資訊安全事故及改進之管理					
A.13.2.1	責任及程序	X				
A.13.2.2	從資訊安全事故中學習	X				
A.13.2.3	證據之收集	X				
A.14	營運持續性管理					
A.14.1	營運持續性管理之資訊安全層面					管理審查記錄
A.14.1.1	將資訊安全納入營運持續性管理程序中	X				
A.14.1.2	營運持續及風險評鑑	X				

A.14.1.3	包括資訊安之發展及實行持續計畫	X	X	可能	X	依據風險評鑑及相關法律/法規之 DR 現場檢驗、DR 現在距離
A.14.1.4	營運持續計畫架構	X				
A.14.1.5	營運持續計畫之測試、維護及重新評鑑	X				
A.15	符合性					
A.15.1	對法規之遵守					
A.15.1.1	找出適用之法條	X				
A.15.1.2	智慧財產權(IPR)	X				
A.15.1.3	組織紀錄的保護	X	X	可能		
A.15.1.4	個人資料保護及個人資料之隱私及	X	X	可能		
A.15.1.5	防止資訊處理設施的誤用	X				
A.15.1.6	密碼控制措施的規定	X				
A.15.2	安全政策及標準之遵守以及技術符合性					
A.15.2.1	安全政策及標準的符合性	X				
A.15.2.2	技術符合性查核	X	X			存取過程及追蹤
A.15.3	資訊系統稽核考量					
A.15.3.1	資訊系統稽核控制	X				
A.15.3.2	資訊系統稽核工具之保護	X	X	可能		