

資訊安全管理系統 驗證機構認證規範

(ISO/IEC 27006:2007)



財團法人全國認證基金會
中華民國九十六年八月

「資訊安全管理系統驗證機構認證規範」(文件編號 ICC-01)
係參照 ISO/IEC 27006:2007 訂定，惟全文中所引用之相關國際標準，如已有轉訂為中國國家標準者，均加註中國國家標準編號，以供參閱。

全文所引用文件如國際標準或中國國家標準等若有新修訂版發行時，請自行參閱。本文件為維持與原文一致性，不作個別修訂。

資訊技術－安全技術－資訊安全管理系統稽核及驗證機構之規定

目錄

前言	iv
介紹	v
1. 範圍	1
2. 引用標準	1
3. 名詞及定義	1
3.1 證書	1
3.2 驗證機構	1
3.3 驗證文件	1
3.4 標誌	1
3.5 組織	1
4. 原理	2
5. 一般要求	2
5.1 法律及合約事務	2
5.2 公正性之管理	2
5.3 責任及財務	2
6. 架構要求	3
6.1 組織架構及最高管理階層	3
6.2 保護公正性委員會	3
7. 資源要求	3
7.1 管理階層及人員的能力	3
7.2 參與驗證活動人員	3
7.3 外部稽核員與外部技術專家之使用	6
7.4 人員記錄	6
7.5 外包	6
8. 資訊要求	6
8.1 可公開取得的資訊	6
8.2 驗證文件	6
8.3 已驗證客戶之目錄	7
8.4 驗證之引用及標誌的使用	7
8.5 機密性	7
8.6 驗證機構與其客戶間之資訊交換	7
9. 流程要求	7
9.1 一般要求	7
9.2 初次稽核及驗證	11
9.3 追查活動	15
9.4 重新驗證	16
9.5 特別稽核	16
9.6 暫時終止、終止、或減列驗證範圍	16
9.7 申訴	16
9.8 抱怨	16
9.9 申請者及客戶之記錄	17
10. 驗證機構之管理系統要求	17
10.1 選項方式	17
10.2 選項方式 1—依照 ISO 9001 管理系統規定	17
10.3 選項方式 2—一般管理系統要求	17
附件 A (參考) 客戶組織複雜度及特定產業面分析	18
附件 B (參考) 稽核員能力領域範例	21
附件 C (參考) 稽核時間	23
附件 D (參考) 執行 ISO/IEC 27001:2005 附件 A 控制項之審查指引	29

前言

ISO (國際標準組織) 及 IEC (國際電子技術委員會) 組成全球性標準化的特別系統。ISO 及 IEC 會員的國家機構，透過相關組織所設立的技术委員會，參與國際標準的制定，以處理技術性活動的特定領域。ISO 及 IEC 技術委員會在共同關切的領域合作。其它國際組織、政府及非政府組織也協同 ISO 及 IEC 參與這項工作。在資訊技術領域，ISO 及 IEC 已設立一個共同技術委員會 – ISO/IEC JTC 1。

國際標準的擬定係依據 ISO/IEC 指令第 2 部所述規則。

共同技術委員會的主要工作為編製國際標準。技術委員會所擬定國際標準草案，分發給會員機構表決。發佈為國際標準則需有至少 75% 的會員團贊成。

請注意，本文件中有些內容可能係專利權的題材。ISO 不負責指出任何或所有該專利權。

ISO/IEC 27006 是由共同技術委員會 ISO/IEC JTC 1，資訊技術，次級委員會 SEC 27，IT 安全技術，所編制。

介紹

ISO/IEC 17021 係一國際標準，載明對組織之管理系統進行稽核及驗證之機構的標準。若該機構欲取得 ISO/IEC 17021 之認證，以便依據 ISO/IEC 27001:2005 執行稽核及驗證資訊安全管理系統(ISMS)，則 ISO/IEC 17021 另需額外的規定及指引由本國際標準提供。

本國際標準的內容遵循 ISO/IEC 17021 的結構，且有關 ISMS 驗證所採用之 ISO/IEC 17021 的 ISMS 專用規定及指引，標示為"IS"。

本國際標準內容中，使用"應"一詞用，以表示反映 ISO/IEC 17021 及 ISO/IEC 27001 之規定是強制性條文。使用"須"一詞用以表示雖然構成規定應用之指引方針，但期待由驗證機構採用之條文。

本國際標準之目的在於使認證機構更有效地調和其用以評鑑驗證機構之標準的應用。在此情況下，驗證機構之指引方針而生之變動，是為例外。該變動僅能在驗證機構向認證機構證明，該例外情事以同樣符合 ISO/IEC 17021、ISO/IEC 27001 之相關規定，以及本國際標準之用意後，依個案許可之。

註：本國際標準中，"「管理系統」及"「系統」"二詞可交互使用。管理系統之界定見 ISO 9000:2005。本國際標準所使用的管理系統不得與其它系統混淆，例如 IT 系統。

資訊技術－安全技術－資訊安全管理系統稽核及驗證機構之規定

1. 範圍

除 ISO/IEC 17021 及 ISO/IEC 27001 所述規定外，本國際標準對資訊安全管理(ISMS)稽核及驗證機構另指定一些要求並提供指引。它的主要目的在支援 ISMS 驗證機構的認證工作。

本國際標準所述要求，必須由提供 ISMS 驗證的任何機構，以能力及可靠度的名詞予以展現之，並且本國際標準所述指引，提供給任何提供 ISMS 驗證機構有關這些要求的其它解釋。

註 本國際標準可當作認證、同儕評估、或其它稽核程序的標準文件。

2. 引用標準

以下參考文件為使用本文件所不可或缺。註明日期的參考文件中，僅引用的版本適用之。未註明日期的參考文件，則適用該文件的最新版本(包含任何修訂文)。

ISO/IEC 17021:2006，*符合性評鑑－管理系統稽核及驗證機構的要求*

ISO/IEC 27001:2005，*資訊技術－安全技術－資訊安全管理系統－要求*

ISO/IEC 19011，*品質及/或環境管理系統稽核指引*

3. 名詞及定義

就本文件目的而言，ISO/IEC 17021, ISO/IEC 27001 所述名詞及界定，以及下述適用之。

3.1

證書

驗證機構依其認證條件所核發，並載有認證標誌或聲明的證明書。

3.2

驗證機構

為客戶組織的 ISMS，針對相關之公佈 ISMS 標準，以及該系統所需任何補充文件，進行評鑑及驗證的第三者。

3.3

驗證文件

顯示客戶組織的 ISMS 符合特定 ISMS 標準及該系統所需任何補充文件之文件。

3.4

標誌

依認證機構或驗證機構規則所核發之法定註冊商標或其它保護標誌，顯示對該機構所運作之系統具有充分信心，或相關產品或個人符合特定標準之要求。

3.5

組織

具有本身功能及管理並且能確保執行資訊安全之公司、法人、商號、企業、機關或機構，或其部份單位或其集團，無論其是否設立為公司、公營或私營。

4. 原理

ISO/IEC 17021:2006, 第 4 條所述原則適用之。

5. 一般規定

5.1 法律及合約事務

ISO/IEC 17021:2006, 第 5.1 條之規定適用之。

5.2 公正性之管理

ISO/IEC 17021:2006, 第 5.2 條之規定適用之。此外，以下之 ISMS-特別規定及指引亦適用之。

5.2.1 IS 5.2 利益衝突

驗證機構可執行下列工作，而不被視為諮詢或有潛在的利益衝突：

- a) 驗證活動，其中包括資訊會議、計劃會議、文件檢查、稽核(非內部 ISMS 稽核或內部安全審查)與不符合情事之追蹤；
- b) 以講師身份安排及參與訓練課程，惟此等課程與資訊安全管理有關、或有關於管理系統或稽核，驗證機構須只限於提供公眾領域可自由取得的一般資訊及建議；即，不須提供與下款 c)所述規定相互抵觸之對公司的特定建議；
- c) 根據要求，提供或發佈驗證機構對驗證稽核標準的解釋資訊；
- d) 完全為決定驗證稽核是否就緒的稽核前活動；但該活動不須造成提供與本條相互抵觸的意見或建議，並且驗證機構須確認該活動不會與此等要求抵觸，且不會被作為減列最終驗證稽核時間的理由；
- e) 根據非認證範圍之標準或規章而執行之第二或第三者稽核；
- f) 增加驗證稽核及追查訪查時的價值；例如在稽核時對發現的事項，指出改善的機會，但不提供特定的解決建議。

驗證機構應獨立於為客戶組織 ISMS 驗證事宜提供內部 ISMS 稽核的任何機構(包括個人)之外。

5.3 責任及財務

ISO/IEC 17021:2006 第 5.3 條之規定適用之。

6. 架構需求

6.1 組織架構及最高管理階層

ISO/IEC 17021:2006 第 6.1 條之需求適用之。

6.2 保護公正性委員會

ISO/IEC 17021:2006 第 6.2 條之需求適用之。

7. 資源需求

7.1 管理階層及人員之能力

ISO/IEC 17021:2006 第 7.1 條之規定適用之。此外，以下 ISMS 特別規定及指引亦適用之。

7.1.1 IS 7.1 管理階層的能力

執行 ISMS 驗證所需之能力要件為選擇、提供及管理對在稽核活動與有關資訊安全事項有適當技能及統合能力之人員。

7.1.1.1 能力分析與合約審查

驗證機構應確保對所評鑑客戶組織之 ISMS 相關技術及法律沿革的知識。

驗證機構在運作的所有技術領域，應具備有效的資訊安全管理能力分析之系統。

對各客戶而言，驗證機構應能證明它在進行合約審查前，已針對各相關環節的要求，進行能力分析(反應被評估需求之技能評鑑)。然後，驗證機構應與客戶組織依據能力分析的結果，審查合約。驗證機構尤其應能證明具有完成下列活動之能力：

- a) 瞭解客戶組織的活動領域以及相關業務風險；
- b) 界定驗證機構在進行已識別的活動及對資產威脅相關的資訊安全，客戶組織之脆弱性及對其之衝擊方面之驗證而所需具備的能力；
- c) 確認具有所需之能力。

7.1.1.2 資源

驗證機構管理階層應有必要的程序及資源，以判斷稽核員是否能勝任於執行驗證範圍內所需要的工作。稽核員的能力，可藉由背景經驗及特定訓練或簡歷(另請參考附件 B)而建立。驗證機構應能有效地對其服務之所有客戶溝通。

7.2 參與驗證活動人員

ISO/IEC 17021:2006 第 7.2 條之規定適用之。此外，以下 ISMS 特別要求及指引也適用之。

7.2.1 IS 7.2 驗證機構人員的能力

驗證機構應有具備下述能力的人員

- a) 選擇並確認 ISMS 稽核員的能力以組成適合稽核之稽核小組；
- b) 向 ISMS 稽核員簡報並安排任何必要的訓練；
- c) 決定驗證的授與、維持、終止、暫時終止、增列、或減列；
- d) 申訴及抱怨程序之制定與處理。

7.2.1.1 稽核小組的訓練

驗證機構應有訓練稽核小組的規範，以確保

- a) 對 ISMS 標準以及其它相關規範文件的知識；
- b) 對資訊安全的了解；
- c) 從商業觀點，對風險評估及風險管理的了解；
- d) 對受稽核活動的技術知識；
- e) 對有關 ISMS 法規要求的一般知識；
- f) 對管理系統的知識；
- g) 瞭解基於 ISO 19011 的稽核原則；
- h) 對 ISMS 之有效性審查及控制項有效性之評量的知識。

這些訓練要求適用於稽核小組的所有成員，惟 d)除外，稽核小組成員可彼此分享之。

7.2.1.1.1 在選任稽核小組進行特定驗證稽核工作時，驗證機構應確保各項工作所需技能都是適當。該小組應

- a) 對於進行驗證的 ISMS 範圍內之特定活動，具備適當的技術知識，若相關時，包含有關程序及其潛在資訊安全風險之技術知識(非稽核員的技術專家可符合此項功能)；
- b) 對於客戶組織有相當程度的瞭解，以便針對其 ISMS 在活動、產品及服務的資訊安全層面管理，進行可靠的驗證稽核；
- c) 對於適用於客戶組織 ISMS 的相關法規要求有適當的瞭解。

7.2.1.1.2 如有必要，稽核小組能以可證明在稽核工作相關技術領域具有特定能力的技術專家補強。但須當注意，技術專家不得取代 ISMS 稽核員，但對被稽核的管理系統，可針對技術適當性的事項向稽核員建議。驗證機構應有下述程序

- a) 依據能力、訓練、資格及經驗，選擇稽核員及技術專家；

- b) 先在驗證稽核期間評鑑稽核員及技術專家的作為，後續再監督稽核員及技術專家的績效。

7.2.1.2 決策程序之管理

管理階層應具有技術能力及能力管理決策程序，其決策是有關於授予、維持、增列、減列、暫時終止及終止 ISO/IEC 27001 的 ISMS 驗證。

7.2.1.3 ISMS 稽核員必備之教育程度、工作經驗、稽核員訓練及稽核經驗

7.2.1.3.1 下述規範應適用於 ISMS 稽核小組的每位稽核員。稽核員應

- a) 具備中等教育程度；
- b) 在資訊技術方面至少具有四年的全職實務職場經驗，其中至少有兩年擔任資訊安全相關的角色或職位；
- c) 已成功完成五天的訓練，包含 ISMS 稽核及稽核管理的訓練範圍等應被認為適當；
- d) 在履行稽核員職責前，已獲得評估資訊安全之完整過程的經驗。此經驗之獲得須為參與至少四次共計至少 20 天的驗證稽核工作，其中包括文件及風險分析的審查、執行評鑑及稽核報告撰寫；
- e) 具備合時宜的經驗；
- f) 能宏觀地觀察複雜的作業，並且瞭解各單位在大客戶整體組織中的角色。
- g) 透過持續專業的提昇，保持在資訊安全及稽核方面的最新知識及技能。

技術專家應符合 a)、b)、e)、及 f) 的規範。

7.2.1.3.2 除了 7.2.1.3.1 的要求外，稽核小組長應符合下列條件。這些條件應在指導及監督下所進行的稽核工作中證明之：

- a) 具備管理驗證稽核程序的知識及特質；
- b) 至少已擔任過三件完整 ISMS 稽核工作的稽核員；
- c) 已展現具備有效的口頭或書面的溝通能力。

7.3 外部稽核員與外部技術專家之使用

ISO/IEC 17021:2006 第 7.3 條的規定適用之。另外，下述 ISMS 特別要求及指引也適用之。

7.3.1 IS 7.3 使用外部稽核員或外部技術專家作為稽核小組的成員

使用外部稽核員或外部技術專家，作為稽核小組的成員時，驗證機構應確認他們具備能力，並且符合本文件所適用相關條文之原則，並且他們不會以直接或透過其雇主，參與 ISMS 或相關管理系統的設計、執行或維持等方式而使公正性有損害。

7.3.1.1 技術專家的使用

具備影響客戶組織之程序及資訊安全議題及法律等有關特定知識，但不符合 7.2 所有規範的技術專家，得擔任稽核小組成員。技術專家應在稽核員的督導下工作。

7.4 人員記錄

ISO/IEC 17021:2006 第 7.4 條的規定適用之。

7.5 外包

ISO/IEC 17021:2006 第 7.5 條的規定適用之。

8. 資訊要求

8.1 可公開取得的資訊

ISO/IEC 17021:2006 第 8.1 條的規定適用之。此外，以下 ISMS 之特別規定及指引亦適用之。

8.1.1 IS 8.1 驗證之授與、維持、增列、減列、暫時終止及終止的程序

驗證機構應要求客戶組織具有符合 ISO/IEC 27001 的書面及已執行的 ISMS，以及驗證所需其它文件。

驗證機構應具有下列的書面程序

- a) 依據 ISO 19011, ISO/IEC 17021 條文及其它相關文件，對客戶組織 ISMS 進行的初次驗證稽核；
- b) 依據 ISO 19011 及 ISO/IEC 17021 定期對客戶組織之 ISMS 進行追查及重新驗證，以確定其持續地符合相關規定，且查證及記錄客戶組織是否針對所有不相符事項及時地採取矯正措施。

8.2 驗證文件

ISO/IEC 17021:2006 第 8.2 條之規定適用之。此外，以下 ISMS 之特別規定及指引亦適用之。

8.2.1 IS 8.2 ISMS 驗證文件

驗證機構應提供已驗證 ISMS 之各客戶組織驗證文件，例如經指定負責人員簽署的信件或證書。若為證書所涵蓋的客戶組織及其資訊系統，這些文件應指出給予驗證的範圍以及 ISMS 所驗證的 ISMS 標準 ISO/IEC 27001。此外，證書須包含適用性聲明的特定參考版本。

8.3 已驗證客戶之目錄

ISO/IEC 17021:2006 第 8.3 條之規定適用之。

8.4 驗證之引用及標誌的使用

ISO/IEC 17021:2006 第 8.4 條之規定適用之。下述 ISMS 特別要求及指引也適用之。

8.4.1 IS 8.4 驗證標誌的管制

驗證機構應適當管制其 ISMS 驗證標誌的所有權、使用及顯示。若驗證機構給予使用標誌之權利，以顯示 ISMS 之驗證時，驗證機構須確保客戶組織只能依驗證機構書面授權的範圍使用特定標誌。驗證機構不應授權客戶組織將該標誌用於產品上，或以任何方式使其可解讀為指稱產品合格。

8.5 機密性

ISO/IEC 17021:2006 第 8.5 條之規定適用之。另外，下述 ISMS 特別要求及指引也適用之。

8.5.1 IS 8.5 組織記錄的使用

在驗證稽核前，驗證機構應詢問客戶組織，是否有任何含有機密或敏感資訊，而不能提供審查的 ISMS 記錄。驗證機構應判斷，沒有這些記錄時，可否適當稽核 ISMS。如果驗證機構的結論是如未經審查該機密或敏感記錄，則不可能適當稽核 ISMS 時，驗證機構將告知客戶組織，在獲得適當的使用同意前，不能進行驗證稽核。

8.6 驗證機構與其客戶間之資訊交換

ISO/IEC 17021:2006 第 Clause 8.6 條之規定適用之。

9. 流程要求

9.1 一般要求

ISO/IEC 17021:2006 第 9.1 條之規定適用之。另外，以下 ISMS 特別規定及指引也適用之。

9.1.1 IS 9.1.1 一般 ISMS 稽核規範

9.1.1.1 驗證稽核標準

稽核客戶之 ISMS 所採用的標準，應為 ISMS 標準 ISO/IEC 27001 及進行驗證相關功能時所需之其它文件。若將此等文件用於特定之驗證計畫上，則需說理由，且此說明應由與公正性有關之委員會或由具有必要技術能力的人員提出，並由驗證機構公佈之。

9.1.1.2 政策及程序

驗證機構的文件化應包含執行驗證作業的政策及程序，其中包括檢查 ISMS 驗證時所用文件的使用及應用，及稽核驗證客戶組織 ISMS 的程序。

9.1.1.3 稽核小組

稽核小組應經正式委派，並提供其適當的工作文件。稽核計劃及日期，應經客戶組織同意。稽核小組的委派令應清楚界定，並告知客戶組織，且應要求稽核小組檢查客戶組織的結構、政策及程序，並確認上述全部符合相關驗證範圍的要求，且程序已被執行，以至於對客戶組織的 ISMS 有信心。

9.1.2 IS 9.1.2 驗證範圍

稽核小組應稽核客戶組織所界定範圍的 ISMS 是否符合所有相關的驗證規定。驗證機構應確保客戶組織 ISMS 的範圍及界限已依據其業務特性、組織、位置、資產及技術等，已明確界定。驗證機構應確認，在其 ISMS 範圍內，客戶組織符合 ISO/IEC 27001：2005 第 1.2 條所述之規定。

驗證機構應確保，客戶組織的資訊安全風險評鑑及風險處理已適當反映其活動，及在 ISMS 標準 ISO/IEC 27001 中所界定的活動界限內。驗證機構應確認，上述已反映在客戶組織的 ISMS 範圍及適用性聲明中。

驗證機構應確保，不完全在 ISMS 範圍內之服務或活動的介面，已列在 ISMS 驗證事項內，並納入客戶組織的資訊安全風險評鑑中。此種情況的一個例子是與其它組織共用設施(例如，IT 系統、資料庫及通訊系統)。

9.1.3 IS 9.1.3 稽核時間

驗證機構應允許稽核員有充分時間，進行有關初次稽核、追查稽核及重新驗證稽核的所有活動。分配的時間須考慮以下因素，例如

- a) ISMS 範圍的大小(例如，使用資訊系統的數目，雇員人數)；
- b) ISMS 的複雜度(例如，資訊系統的重要性，ISMS 的風險狀況)，另參閱附件 A；
- c) ISMS 範圍內所進行的業務種類；
- d) 執行各 ISMS 項目(例如執行的控制項、文件化及/或作業控制，矯正/預防措施等)時所採技術的範圍及多樣性；
- e) 場區的數目；
- f) 先前已展現的 ISMS 績效；
- g) 在 ISMS 範圍內，外包的範圍及所使用的第三者協議；
- h) 適用於驗證的標準及規章。

附件 C 提供稽核時間的指引。驗證機構應準備好將任何初次稽核、追查稽核及驗證稽核中所使用的時間量，予以證明或合理解釋。

9.1.4 IS 9.1.4 多場區

9.1.4.1 ISMS 驗證領域中的多場區採樣決策比品質管理系統的相同決策更為複雜。若客戶組織有符合以下 a)至 c)所述標準之場區時，驗證機構可考慮使用採樣法，以進行多場區驗證稽核：

- a) 所有場區都採用相同 ISMS 作業，由中央管理及稽核，並由中央進行管理審查；
- b) 所有場區都納入客戶組織的內部稽核計劃中；
- c) 所有場區都納入客戶組織的 ISMS 管理審查計劃中。

9.1.4.2 希望使用採樣法的驗證機構，應有適當的程序以確保以下：

- a) 在初次的合約審查中，盡可能辨識出各場區之間的差異處，以決定足夠的樣品數。
- b) 驗證機構已基於以下考量，採樣代表性的場區數目
 - 1) 總部及各場區之內部稽核結果，
 - 2) 管理審查之結果，
 - 3) 各場區大小之差異，
 - 4) 在場區業務目的之差異性，
 - 5) ISMS 的複雜度，
 - 6) 不同場區所資訊系統之複雜度，
 - 7) 工作實務之差異，
 - 8) 所從事的活動之差異，
 - 9) 關鍵資訊系統或處理敏感資訊之資訊系統的互動，
 - 10) 任何不同的法律規定。
- c) 從所有場區選出客戶組織 ISMS 範圍內之代表性樣品；此項選擇須基於可以反映以上 b)項要素和隨機等所代表的因素。
- d) 納入 ISMS 的場區中之各個具有重大風險之場區，由驗證機構在發證前已先稽核。
- e) 追查計劃已依上述規範設計，並在合理時間內，包含客戶組織中或 ISMS 驗證範圍中的所有場區。
- f) 若於總部或單一場區發現不符合事項時，矯正措施程序適用於總部以及證書所涵蓋的所有場區。

以下 IS 9.1.5 所述之稽核應針對客戶組織的總部活動，以確保單一 ISMS 適用於所有場區，並在作業層面表現中央管理。稽核應針對以上列舉的所有事項。

9.1.5 IS 9.1.5 稽核方法

驗證機構應有程序，以要求客戶組織能證明已安排內部 ISMS 稽核的時間，並且計劃及程序均可運作，且能被證明為可運作。

驗證機構的程序不須預設執行 ISMS 的特定方式，或文件及記錄的特定格式。驗證程序的重點應在於證實客戶組織的 ISMS 是否符合 ISO/IEC 27001 標準的要求，與客戶組織的政策及目的。

稽核計劃須標明稽核時，在適當情況下利用的網路輔助稽核技術。

註 網路輔助稽核技術得包含，例如電信會議、網路會議、互動式網路通訊，與遠距存取 ISMS 文件及/或 ISMS 作業。該技術的重點須在於加強稽核有效性及效率，且須保持稽核作業的完整性。

9.1.6 IS 9.1.6 驗證稽核報告

9.1.6.1 驗證機構得採用適合其需要之報告程序，但程序至少應確保

- a) 離開客戶組織場區前，稽核小組與客戶組織管理階層召開會議，會中稽核小組提供
 - 1) 有關客戶組織 ISMS 是否符合特定驗證要求之書面或口頭說明，
 - 2) 客戶組織對各項發現及其依據，有詢問問題之機會；
- b) 稽核小組提供驗證機構一分有關客戶組織 ISMS 是否符合所有驗證要求之發現的稽核報告。

9.1.6.2 稽核報告須提供以下資訊：

- a) 包含文件審查彙整的稽核紀錄；
- b) 客戶組織資訊安全風險分析的驗證稽核紀錄；
- c) 所使用之稽核總時間，以及分別用於文件審查、風險分析評鑑、現場稽核，及以及稽核報告之詳細時間；
- d) 已被追蹤之稽核項目之詢問，其選擇的合理性，與所採用的方法。

9.1.6.3 提供給驗證機構的稽核發現報告應詳盡，並有助於與支持驗證決定，其應包含

- a) 稽核所涵蓋之領域(例如驗證的要求及被稽核場區)，包含重要稽核軌跡，及使用的稽核方法(參閱 IS 9.1.5)；
- b) 正面(例如值得注意之特點)及負面(潛在的不符合事項)的觀察；
- c) 所發現之任何不符合事項之細節，並以客觀證據證明，與參考此等不符合事項所引用的

ISMS 標準 ISO/IEC 27001 規定或驗證所需其它文件。

- d) 對客戶組織 ISMS 符合驗證要求之意見，其中包含對不符合事項清楚說明、所引用的適用性聲明版本，與在適用情況下，在與客戶組織的驗證稽核結果前之任何有用對照。

完成的問卷表、查檢表、觀察紀錄、日誌、或稽核員筆記等可構成完整稽核報告的一部份。若使用這些方法，上述文件應提供給驗證機構，作為支持驗證決定之證據。有關稽核期間被評估樣本的資訊須納入稽核報告或其它驗證文件中。

報告應考量由客戶組織所採用之內部組織及程序的適當性，以達到對 ISMS 有信心。

除了 ISO/IEC 17021:2006 第 9.1.10 條之報告規範外，報告也須包含

- 對內部 ISMS 稽核及管理審查之信賴程度；
- 關於 ISMS 執行與有效性之最重要的正面與負面觀察之彙整；
- 稽核小組對於客戶組織 ISMS 是否須授予驗證之建議，以及支持該建議之資訊。

9.2 初次稽核及驗證

ISO/IEC 17021:2006 第 9.2 條之規定適用之。此外，以下 ISMS 特別要求及指引也適用。

9.2.1 IS 9.2.1 稽核小組的能力

除了第 7.2 所列要求外，以下要求也適用於驗證評鑑。對追查活動而言，僅對已排訂追查活動的相關要求適用之。

以下要求適用於整個稽核小組。

- a) 在每個以下領域中，至少應有一位稽核小組成員，對符合驗證機構的標準，在小組內負起責任：
- 1) 小組之管理，
 - 2) 適用於 ISMS 之管理系統及程序，
 - 3) 在特定資訊安全領域之法律與法規規定的知識，
 - 4) 識別出資訊安全有關威脅及事故趨勢，
 - 5) 識別出客戶組織的脆弱性，並瞭解其發生的可性能，其影響及其減緩措施及和控制項，
 - 6) ISMS 控制項及其執行的知識，
 - 7) ISMS 有效性審查及控制項量測的知識，
 - 8) 相關之 ISMS 標準、業界最佳實務、安全政策及程序，
 - 9) 事故處理方法與營運持續性的知識，

- 10) 有關有形及無形資訊資產及衝擊分析的知識，
 - 11) 可能相關於安全性或成為安全性議題之目前技術的知識，
 - 12) 風險管理的程序及方法的知識。
- b) 稽核小組應有能力追蹤客戶組織 ISMS 中安全事故的指標並回溯至適當 ISMS 項目。
- c) 稽核小組在上述項目，應有適當的工作經驗及實務應用(這不表示稽核員在資訊安全所有領域需有全面的經驗，但整個稽核小組在被稽核的 ISMS 範圍內，須有充分的瞭解及經驗)。

稽核小組得由一人組成，但該員必須符合以上 a)所述規範。

9.2.1.1 IS 9.2.1.1 稽核員能力的展現

稽核員應能藉由以下，展現其在以上列舉的知識及經驗，例如

- a) 認可的 ISMS 特定資格；
- b) 登錄為稽核員；
- c) 被認可的 ISMS 訓練課程；
- d) 最新的持續專業發展記錄；
- e) 經由見證稽核員在進行實際客戶系統之稽核作業，而予以展現。

9.2.2 IS 9.2.2 初次稽核的一般準備事項

驗證機構應要求客戶組織為驗證稽核進行所有必要的安排，其中包括提供檢驗文件及查閱所有區域、記錄(包括內部稽核報告及資訊安全獨立審查報告)、及安排驗證稽核、重新驗證稽核及解決抱怨等目的之所需人員。

客戶在現場驗證稽核前，至少應提供以下資訊：

- a) 有關 ISMS 及其活動所涵蓋的一般資訊；
- b) ISO/IEC 27001:2005 第 4.3.1 條所要求的 ISMS 文件影本，及必要的相關文件。

9.2.3 IS 9.2.3 初次驗證稽核

9.2.3.1 IS 9.2.3.1 第 1 階段稽核

在本階段的稽核中，驗證機構應取得 ISMS 之設計方面且 ISO/IEC 27001 第 4.3.1 條所要求的文件。

第 1 階段稽核的目的，是藉由客戶組織 ISMS 政策及目的背景下，瞭解其 ISMS，特別是客戶組織準備稽核的狀態，而提供給規劃第 2 階段的重點。

第 1 階段稽核包括，但不須限制於文件審查。驗證機構應與客戶組織對文件審查的時間及地點達成同意。在所有情況下，文件審查應在開始第 2 階段稽核前完成。

第 1 階段稽核的結果，應作成書面報告。驗證機構在決定進行第 2 階段稽核前，應審查第 1 階段稽核報告，以便選擇有必要能力的第 2 階段稽核小組成員。

驗證機構應讓客戶組織知道，第 2 階段中詳細檢視時，可能需要的其它資訊及記錄種類。

9.2.3.2 IS 9.2.3.2 第 2 階段稽核

9.2.3.2.1 第 2 階段稽核總是在客戶組織場區進行。驗證機構依據第 1 階段稽核報告中的書面發現，擬定進行第 2 階段稽核的稽核計劃。第 2 階段稽核的目的為

- a) 確認客戶組織遵守其本身的政策、目的及程序；
- b) 確認 ISMS 符合 ISMS 標準 ISO/IEC 27001 的所有要求，並達成客戶組織的政策目的。

9.2.3.2.2 為達此目的，稽核應將重點放在客戶組織的

- a) 資訊安全相關風險的評鑑，並且其評鑑產生可比較及可再現的結果；
- b) ISO/IEC 27001:2005 第 4.3.1 條所列之文件化要求；
- c) 依據風險評鑑及風險處理作業，選擇控制目標與控制項；
- d) ISMS 有效性之審查，及資訊安全控制項效率性之量測，ISMS 目的之報告及審查；
- e) 內部 ISMS 稽核及管理審查；
- f) 資訊安全政策的管理責任；
- g) 所選擇及執行的控制項、適用性聲明，與風險評鑑及風險處理作業的結果，與 ISMS 政策及目的等相互間關聯性；
- h) 控制項之執行(參閱附件 D)，考慮組織的控制項有效性量測[參閱以上 d)]，以判斷控制項之執行及有效性是否達成所述目標；
- i) 計劃、作業、程序、記錄、內部稽核、及 ISMS 有效性審查等，以確保前述都可追蹤到管理階層的決定，與 ISMS 政策及目的。

9.2.3.3 IS 9.2.3.3 ISMS 稽核的特定元素

驗證機構的主要角色在於確認，客戶組織鑑別、檢驗及評估資訊安全事項中相關資產威脅、脆弱性及對客戶組織之影響的程序，在其制定及維持面是否一致。驗證機構應

- a) 要求客戶組織展現，相關威脅之安全分析對客戶組織運作，是有關且足夠的；

註 客戶組織應負責界定標準，依該標準鑑別在客戶組織相關風險之資訊安全中被視為重要者，並依該標準制定其程序。

- b) 確認客戶組織中關於資訊安全相關資產威脅、脆弱性及衝擊之程序的鑑別、檢驗及評

估，以及其執行結果，是否符合客戶組織的政策、目的及目標。

驗證機構也應證實重要性分析所採用的程序是否健全與適當地執行。如果資訊安全相關資產的威脅、脆弱性、或對客戶組織的衝擊，經鑑別為重要時，其應納入 ISMS 管理。

9.2.3.3.1 法律及法規遵循

法律及法規遵循的維持及評估，為客戶組織的責任。驗證機構應限制自己進行檢查及採樣，僅是為了達到建立 ISMS 功能的信心之目的。驗證機構應證實，客戶組織有一個管理系統，可達成適用於資訊安全風險及衝擊之相關法律及法規的遵循。

9.2.3.3.2 ISMS 文件及其它管理系統文件的整合

只要是 ISMS 可以清楚鑑別，並且與其它系統有適當的介面，客戶組織就可結合 ISMS 文件及其它管理系統文件(例如品質、衛生與安全、與環境)。

9.2.3.3.3 結合管理系統稽核

驗證機構可提供其他與 ISMS 有關之管理系統的驗證，或僅提供 ISMS 驗證。

ISMS 稽核可結合其它管理系統的稽核。若可展現該稽核符合 ISMS 驗證的所有要求，則此項結合則有可能。在稽核報告中，應清楚呈現 ISMS 的所有重要要項，並且很容易識別。稽核品質不應該因結合稽核而受到負面影響。

註 ISO 19011 提供執行結合管理系統稽核的指引。

9.2.4 IS 9.2.4 給予初次驗證的資訊

為提供驗證決定的基礎，驗證機構應要求明確的報告，以提供作此決定的充分資訊。

各階段驗證稽核作業，都需有稽核小組提供給驗證機構的報告。為結合現存檔案中的資訊，報告至少須含有 IS 9.1.6 所要求的資訊。

9.2.5 IS 9.2.5 驗證決定

驗證機構中作出給予/終止驗證決定的單位或個人，須在全領域具備相當程度的知識及經驗，以評估稽核過程與稽核小組的相關建議。

驗證機構應依據驗證作業中所搜集的資訊，與任何其它相關資訊，作出是否驗證客戶組織 ISMS 的決定。作出驗證決定者，不應參與稽核。該決定應依據稽核小組在其驗證稽核報告中所提供的發現及驗證建議(參閱 IS 9.1.6)，以及驗證機構可利用的任何其它相關資訊。

決定給予驗證的單位，正常情況下不須推翻稽核小組的負面建議。若發生此情況，驗證機構應以書面方式說明推翻該建議的基礎。

就有關驗證決定事項，ISO/IEC 17021 並未提到客戶組織的 ISMS 至少應進行一次完整的內部 ISMS 稽核，與一次的管理審查的特定期間。驗證機構得指定該期間。無論驗證機構是否選擇指定最低頻率，驗證機構應訂定衡量方式，以確保客戶組織管理審查及內部 ISMS 稽核作業的有效性。

除非有足夠證據證明，管理審查及內部 ISMS 稽核的安排，都已被執行及有效性，並且將被維持，不應核發驗證給客戶組織。

9.3 追查活動

ISO/IEC 17021:2006 第 9.3 條之規定適用之。此外，以下 ISMS 特別規定及指引也適用之。

9.3.1 IS 9.3 追查稽核

9.3.1.1 追查稽核程序應與本標準中有關客戶組織 ISMS 驗證稽核的規定一致。

追查之目的在於，證實所通過的 ISMS 將被繼續執行，考量因客戶組織的作業變動可能對原系統造成的改變，並確認對驗證規範的繼續遵循。追查計劃通常須包含

- a) 內部 ISMS 稽核、管理審查、與預防及矯正措施等系統維持要項；
- b) ISMS 標準 ISO/IEC 27001 所要求的與外部人士溝通，以及驗證所需要的其它文件；
- c) 文件化系統的變動；
- d) 變動的領域；
- e) 選擇 ISO/IEC 27001 中的項目；
- f) 適當時，其它選擇的領域。

9.3.1.2 驗證機構的追查至少應審查以下各項：

- a) 有關達成客戶組織資訊安全政策目的之 ISMS 有效性；
- b) 定期評估及審查是否遵循相關資訊安全法律及法規的程序運作；
- c) 針對前次稽核中發現的不符合事項，所採取的措施。

9.3.1.3 驗證機構的追查，至少須包含 ISO/IEC 17021 對追查稽核所要求的項目。此外，以下問題也須考慮。

- a) 驗證機構須能調整其追查計劃，以因應有關客戶組織對資產威脅、脆弱性與衝擊等資訊安全問題，並且使該計劃具正當性。
- b) 驗證機構的追查計劃須由驗證機構決定。特定的訪視日期，可與被驗證的客戶組織達成協議。
- c) 追查稽核可結合其它管理系統的稽核。報告應清楚指示各管理系統的相關部分。
- d) 驗證機構必須監督證書的適當使用。

在追查稽核中，驗證機構應檢查向驗證機構提出的申訴及抱怨記錄，且若有有不符合事項，或不符合驗證要求，客戶組織已調查其本身之 ISMS 及程序，並已採取適當的矯正措施。

追查報告應包含，特別是對先前揭示的不符合事項的排除資訊。追查所衍生的報告，至少須

包含以上第 a) 點之全部要求。

9.4 重新驗證

ISO/IEC 17021:2006 第 9.4 條之規定適用之。此外，以下 ISMS 特別要求及指引也適用之。

9.4.1 IS 9.4 重新驗證稽核

重新驗證稽核程序應與本國際標準中有關客戶組織 ISMS 驗證稽核一致。

驗證機構應有清楚的程序，規定維持驗證的環境及條件。如果在追查或重新驗證稽核中，發現有不合事項時，該不合事項於與驗證機構同意的時間內，應有效地矯正。若未能於同意的時間內矯正，驗證範圍應予以減列，或該驗證將被暫時終止或終止。允許進行矯正措施的時間，須與不合事項的嚴重性及風險相當，以確保客戶組織的產品或服務，能符合特定規定。

9.5 特別稽核

ISO/IEC 17021:2006 第 9.5 條之規定適用之。此外，以下 ISMS 特別要求及指引也適用之。

9.5.1 IS 9.5 特殊案例

若具有 ISMS 驗證的客戶組織，對其系統作出重大修改，或發生會影響其驗證基礎的其它變更時，追查活動應依特別規定辦理。

9.6 暫時終止、終止、或減列驗證範圍

ISO/IEC 17021:2006 第 9.6 條之規定適用之。

9.7 申訴

ISO/IEC 17021:2006 第 9.7 條之規定適用之。

9.8 抱怨

ISO/IEC 17021:2006 第 9.8 條之規定適用之。此外，以下 ISMS 特別要求及指引也適用之。

9.8.1 IS 9.8 抱怨

抱怨代表可能不符合事項的資訊來源。驗證機構須要求客戶組織在收到抱怨後，被驗證的客戶組織須確定抱怨的原因，並於適當時報告，其中包括客戶組織 ISMS 內的任何預先設想(或預先排除)因素。

驗證機構須對於客戶組織使用調查以為制定補救/矯正措施而感到滿意；其中須包括對以下措施之衡量

- a) 如法規要求時，通知適當的權責機關；
- b) 恢復符合性；

- c) 防止再發生；
- d) 評估並減小任何負面的安全事故，及其相關衝擊；
- e) 確保與其它 ISMS 項目有滿意的互動；
- f) 評鑑所採補救/矯正措施的效率。

驗證機構應要求每一被驗證 ISMS 的客戶組織，在被要求時，提供所有抱怨及依據 ISO/IEC 27001 所採矯正措施的記錄。

9.9 申請者及客戶之記錄

ISO/IEC 17021:2006 第 9.9 條之規定適用之。

10. 驗證機構之管理系統要求

10.1 選項方式

ISO/IEC 17021:2006 第 10.1 條之規定適用之。

10.2 選項方式 1—依照 ISO 9001 管理系統要求

ISO/IEC 17021:2006 第 10.2 條之規定適用之。

10.3 選項方式 2—一般管理系統要求

ISO/IEC 17021:2006 第 10.3 條之規定適用之。此外，以下 ISMS 特別要求及指引也適用之。

10.3.1 IS 10.3 ISMS 執行

建議驗證機構依據 ISO/IEC 27001 執行。

附件 A (參考)

客戶組織複雜度及特定產業面分析

A.1 組織的潛在風險

在決定稽核時間及稽核員能力時，必須考慮 ISMS 範圍的複雜度。本附件提供針對本目的分析客戶組織複雜度的範例。

可對 ISMS 範圍指定其複雜度類別，以決定

- a) ISMS 稽核的稽核員能力要求(附件 B 提供其範例)；
- b) ISMS 稽核的稽核時間要求(附件 C 提供其範例 C)。

表 A.1 為決定 ISMS 範圍複雜度時可能考慮因素的一般說明。在適當情況下，它可能需要依特定環境調整或納入任何的特別因素。

若分別採用複雜度標準(表 Table A.1)時，ISMS 範圍的複雜度層面，可使用一些不同因素而歸類為三個類別："高"、"中"、及"低"。複雜度的整體有效類別，可作為所有考慮因素的最高類別，並且結果為類別"「高」"、"「中」"「低」。

Table A.1 — Criteria for ISMS 範圍複雜度的標準

複雜度 因素	類別			重大性
	高	中	低	
雇員+契約人員 的人數	≥1,000	≥200	<200	<ul style="list-style-type: none"> • ISMS 執行等級 • 管理資訊系統 • 生產管理相關系統 • 銷售/經銷/一般服務的相關系統 • 資訊技術/資訊服務與相關系統 • 建築/造船/工廠工程的相關系統
使用者人數	≥1 百萬	≥200,000	<200,000	<ul style="list-style-type: none"> • 金融系統 • 政府、學校、醫學/醫院系統
場區數目	≥5	≥2	1	<ul style="list-style-type: none"> • ISMS 執行等級 • 實體及環境安全(ISO/IEC 27001:2005, A.9)
伺服器數目	≥100	≥10	<10	<ul style="list-style-type: none"> • ISMS 執行等級 • 實體及環境安全(A.9) • 存取控制 (ISO/IEC 27001:2005, A-11) • 電信及作業管理(ISO/IEC 27001:2005, A-10)
工作站+PC+膝 上型電腦數目	≥300	≥50	<50	<ul style="list-style-type: none"> • 存取控制 (ISO/IEC 27001:2005, A-11)
應用開發及維護 人員人數	≥100	≥20	<20	<ul style="list-style-type: none"> • 資訊系統取得、開發及維護 (ISO/IEC 27001:2005, A-12)
網路及加密技術	外部/網際網路連線，有加密/數位簽名/PKI 規定	外部/網際網路連線，有使用標準設施的內建加密，無數位簽名/PKI 規定	外部/網際網路連線，無數位簽名/PKI 規定	<ul style="list-style-type: none"> • 電信及作業管理(ISO/IEC 27001:2005, A-10) • 存取控制 (ISO/IEC 27001:2005, A-11)
法律遵循之重要性	不遵循導致可能之起訴	不遵循導致嚴重之財務罰款或商譽損害	不遵循導致輕微之財務罰款或商譽損害	<ul style="list-style-type: none"> • 法律及準則(ISO/IEC 27001:2005, A-15)
特定產業風險之適用性（資訊安全風險之產業特定分類範例請參照 A.2）	適用特定產業之法律規章	不適用特定產業的法律規章，但適用特定產業的風險	不適用特定產業之法律規章，並且不適用特定產業的風險	<ul style="list-style-type: none"> • ISMS 執行等級 • 法律及準則(ISO/IEC 27001:2005, A-15)

A.2 資訊安全風險的特定產業類別

所考慮的資訊種類或組織從事的產業，各有特定的資訊風險。以下例子說明不同的風險類別。

適用於所有組織的特定類別：

- 薪資、退休金、衛生及安全、組織記錄、內部及部門間資訊等；
- 任何其它個人身份資訊；
- 任何其它商業敏感/重要資訊，例如研發資訊、設計資訊、客戶詳細資料、財務結果及預測，業務計劃、智慧財產權、製造加工等。

政府敏感/重要資訊：

- 公共資訊；
- 電子政府應用；
- 有關公民所持有的資訊(例如衛生、福利、稅務、記錄等)；
- 政府供應商及製造商所處理的資訊，例如 ICT 設計、設施、產品、服務等。

適用於組織級別的特定類別：

- 公司治理— 上市公司(也可適用其它大型企業)。

適用於產業的特定類別：

- 醫療；
- 教育；
- 航太；
- 電信；
- 金融服務；
- 慈善及非營利組織。

附件 B (參考)

稽核員能力領域範例

B.1 一般能力考量

稽核員可藉由一些方式，證明他們的知識及經驗。例如，可使用認可的資格來證明知識及經驗。註冊，例如 IRCA 或其它認可的稽核員註冊，也可用來證明所需要的知識及經驗。稽核小組所需要的能力水準，須依據組織的產業/技術領域及複雜度因素而決定。

B.2 特定能力考量

B.2.1 ISO/IEC 27001:2005 附件 A 控制項的知識

以下說明有關 ISMS 稽核的一般知識。除了下表所列的 ISO/IEC 27001:2005 附件 A 控制項領域外，稽核員也須知道 27000 系列標準中的其它標準。

資訊安全政策及業務要求的知識及經驗	安全政策
業務作業、實務、及組織架構的一般知識及經驗	資訊安全組織
資產評價、存貨、分類、及可接受使用政策的知識	資產管理
人力資源部門採用的作業及程序的一般知識及經驗	人力資源管理
實體及環境安全的知識	實體及環境安全
資訊安全所使用的標準、作業、技術及方法的最新知識及經驗，包括管理量測以及適當水準的技術專業。這包括一些通用業務實務的目前知識。	通訊及作業管理
	存取控制
	資訊系統取得、開發及維護
事件管理作業及程序的最新知識及經驗。	資訊安全事件管理
營運延續的標準、作業、計劃及測試程序的最新知識及經驗	營運持續管理
業務合約問題及 ISMS 相關的一般法律及規章的最新知識	遵循

B.2.2 有關 ISMS 的一般知識

稽核員須具備知識並瞭解以下稽核及 ISMS 事項：

- 稽核計劃及規劃，
- 稽核種類及方法，
- 稽核風險，
- 資訊安全作業分析，
- 繼續改善的戴明(Deming)週期(PDCA)，
- 資訊安全的內部稽核。

稽核員須具備知識並瞭解以下法規要求：

- 智慧財產權，
- 組織記錄的內容、保護及保留，
- 資料保護及隱私，
- 密碼控制的法規，
- 反恐怖，
- 電子商務，
- 電子及數位簽名，
- 職場監督
- 電信攔截及資料監控(例如電子郵件)，
- 電腦濫用，
- 電子證據搜集，
- 滲透測試，
- 國際及國內特定產業的要求(例如銀行業)。

稽核員須具備知識並瞭解以下管理要求：

- 資訊安全風險處理，
- ICT 委外安全風險，
- 供應鏈資訊安全風險。

附件 C (參考)

稽核時間

C.1 介紹

本附件包含有關 ISO/IEC 17021:2006 第 9.1、9.2、9.3 及 9.4 條的其它資訊。它須連同本國際標準第 IS.9.1.2、IS 9.1.3、IS 9.1.5、IS 9.1.6、IS 9.2.3.1、IS 9.2.3.2 及 IS 9.2.3.3 條一起閱讀。本附件提供驗證機構，發展其本身程序之指引，以決定驗證客戶組織的 ISMS 之不同規模與在各種活動的範圍內複雜度之所需的時間量。

驗證機構需確定其用於初次驗證、追查及重新驗證各客戶及被驗證 ISMS 的稽核時間量。在稽核規劃階段使用本附件，可導致決定適當稽核時間的一致方法。同時，本指引也可因稽核中所發現的事項而有彈性，尤其是在第 1 階段稽核期間與考慮 ISMS 範圍複雜度。

C.2 決定稽核時間的程序

經驗顯示，ISMS 範圍與其雇員人數(如以下 C.3 的稽核時間表所示)、大小、特性、複雜度與潛在資訊安全風險重大性(如以下更詳細的說明)，將支配任何 ISMS 稽核所需的時間量。在決定所需稽核時間量時，須考慮第 IS 9.1.3 條以及第 IS 9.2.3.1、IS 9.2.3.2 及 IS 9.2.3.3 條所列的標準。驗證機構進行合約審查作業期間，需要檢驗這些及其它因素對分派的稽核時間量的潛在影響。

決定稽核時間時，須考慮這些因素是很重要的，而以下 C.3 的稽核時間表不能單獨使用。以下例子說明會影響稽核時間的因素，並將第 IS 9.1.3 條所述因素列在表上。

- 有關 ISMS 範圍大小的因素(例如，使用資訊系統的數目，處理資訊的數量、使用者人數、特權使用者人數、IT 平台數量、網路數目、及它們的大小)；
- 有關 ISMS 複雜度的因素(例如，資訊系統的臨界性、ISMS 的風險狀況、處理及作業的敏感及重要資訊數目及種類、電子交易的數目及種類、任何開發專案的數目及大小、發生遠端工作的內容、ISMS 文件的內容)；
- ISMS 範圍內進行的業務種類，以及有關這種業務的安全、法律、法規、契約及業務要求；
- 執行各種 ISMS 元件時所利用的技術範圍及差異(例如執行控制項、文件及/或作業控制、矯正/預防行動、資訊系統、IT 系統、網路，亦即，這些是否為固定、移動、無線、外部、內部)；
- ISMS 範圍內的場區數目，這些場區有何相似或不同，以及是稽核全部場區還是採樣；
- 先前已證明的 ISMS 績效；
- ISMS 範圍內使用委外及第三者合約的範圍，以及對些服務的依賴度；

- 適用於驗證的標準、法律及法規，以及任何可能適用的特定產業要求。

由於對資訊安全管理系統透過特定的 ISMS 需求，例如 ISMS 政策、風險管理、ISMS 控制目標、及控制項，而有更多的要求，所以 ISMS 驗證所需的時間通常比品質管理系統或環境管理系統多。驗證機構須

- a) 稽核客戶組織決定其資訊安全風險及影響重大性所採方法的健全性及一致性；
- b) 確認被設計需遵循（相關法律及適用於 ISMS 的其它要求）的系統可以做到，並且該系統已被執行及維持；
- c) 確認控制目標及控制項已被正確地選擇及執行，其效果已被衡量，且"預防及適當反應安全失效"之程序已達到健全並且被遵守；
- d) 確認客戶組織 ISMS 所需文件已實現；
- e) 回應第一階段稽核衍生的更多需求。

C.3 稽核時間表

C.3.1 概述

以下提供的稽核員時間表，指出初次稽核的平均天數(在此及爾後，數目包含第 1 階段稽核及第 2 階段稽核的天數)，經驗顯示它適合所述雇員人數的 ISMS 範圍。經驗也證明，類似大小的 ISMS 範圍，有些需較多的時間，有些則較少。

各驗證所需的時間，依大小、稽核範圍、後勤協助、組織複雜度及稽核準備狀況等因素，各有不同(另參閱以上 C.2)。在驗證機構的合約審查過程中，須檢驗這些及其它因素，以發現其對分派的稽核時間量的潛在影響。因此，稽核員時間表不可單獨使用。

以下稽核員時間表提供一個架構，藉此依據所有工作時間的雇員總人數鑑別為起點而規劃稽核工作，並依適用於及被稽核之 ISMS 範圍的重要因素而調整之，並給每個因素加或減的權重，而修正基數。本表所使用的名詞在以下 C.3.2 說明之。

稽核時間表

雇員人數	QMS 稽核員的初次稽核時間(稽核員天數)	EMS 稽核員的初次稽核時間(稽核員天數)	ISMS 稽核員的初次稽核的時間(稽核員天數)	增加及減少 的因素	稽核員的總 時間
1-10	2	3	5	參閱附件 C.2	
11-25	3		7	參閱附件 C.2	
26-45	4	6	8.5	參閱附件 C.2	
46-65	5		10	參閱附件 C.2	
66-85	6		11	參閱附件 C.2	
86-125	7	8	12	參閱附件 C.2	
126-175	8		13	參閱附件 C.2	
176-275	9		14	參閱附件 C.2	
276-425	10		15	參閱附件 C.2	
426-625	11	12	16.5	參閱附件 C.2	
626-875	12		17.5	參閱附件 C.2	
876-1,175	13		18.5	參閱附件 C.2	
1,176-1,550	14		19.5	參閱附件 C.2	
1,551-2,025	15	18	21	參閱附件 C.2	
2,026-2,675	16		22	參閱附件 C.2	
2,676-3,450	17		23	參閱附件 C.2	
3,451-4,350	18		24	參閱附件 C.2	
4,351-5,450	19		25	參閱附件 C.2	
5,451-6,800	20		26	參閱附件 C.2	
6,801-8,500	21		27	參閱附件 C.2	
8,501-10,700	22		28	參閱附件 C.2	
>10,700	按上述進度		按上述進度	參閱附件 C.2	

C.3.2 名詞解釋

稽核員時間表中之“雇員”係指其工作活動與 ISMS 範圍有關之所有個人。所有輪班之雇員總人數是決定稽核時間的起點。

有效雇員人數包含將於稽核期間在場之非長期性(季節性、臨時性及分包)職員。驗證機構須與被稽核組織商議出，最能展現整個組織範圍的稽核時機。此考量可包含的季節、月份、天數/日期及若情況適當之輪班。

兼職雇員須視同如全職雇員。這將依據與全職雇員相較的工作時數而決定。

“稽核員時間”包括稽核員或稽核小組在第 1 階段稽核、第 2 階段稽核及規劃(包括現場外文件審查，如適當時)；接觸組織、人員、記錄、文件及作業；以及撰寫報告所需的時間。預期牽涉該規劃及報告書寫兩者加起來的“稽核員時間”，須通常使現場“稽核員時間”不低於稽核員時間表所顯示的時間的 70%。如需要增加規劃及/或報告撰寫的時間，則這一點不得做為

減少現場稽核員時間的正當理由。稽核員交通的時間不計算在內，並且是外加於該表所述的稽核員時間。

註 1 70%是依據 ISMS 稽核經驗的係數。

若利用互動式網路合作、網路會議、電訊會議及/或組織作業的電子驗證等遠距稽核技術，與組織互動時，這些活動須在稽核計劃中標示(參閱 IS 9.1.5)，並可視為對總"現場稽核時間"之部分。

若驗證機構規劃的稽核計劃中，遠距稽核活動佔規劃的現場稽核時間 30%以上時，驗證機構須合理化該稽核計劃，並在執行前先取得認證機構的特別核准。

註 2 現場稽核員時間是指分配到各場區的現場稽核員時間。即使電子稽核實際上是在組織的場區執行，遠距場區的電子稽核仍視為遠距稽核。

表所述"稽核員時間"是以需在稽核的"稽核員天數"表示。"稽核員天數"通常是整個正常的工作天。

初次驗證稽核週期中，對某組織的追查時間須與在初次稽核的時間成比例，每年需在追查的總時間大約為初次稽核時間的 1/3。規劃的追查時間須隨時檢討，以因應組織變更、系統成熟度等，並且至少應在重新驗證稽核時檢討之。

執行重新驗證稽核的總時間量，將依本國際標準第 IS 9.1.6 以及 ISO/IEC 17021:2006 第 9.4 條所界定的審查發現而定。重新驗證稽核的時間量須與在同一組織的初次稽核時間量成比例，並且重新驗證須大約為同一組織初次驗證稽核所需時間量的 2/3。重新驗證稽核所需時間超過定期追查的時間，但重新驗證稽核若以規劃中定期追查相同之時間執行，則重新驗證稽核也將符合追查之規定。無論結論如何，IS 9.1.2 的指引仍適用之。

對一般 ISMS 範圍依據顯示僱員人數而決定所需稽核員時間是一般的起點，一些調整必需予以考慮，以因應除 C.2 所列者外，可能影響有效稽核特定 ISMS 所需實際時間的其它變動因素。

需增加稽核員時間的因素有以下例子

- 在 ISMS 範圍內涉及超過一棟或一個地點的複雜後勤協助；
- 說一種語言以上的職員(要求口譯人員或預防稽核人員獨立工作)；
- 高度的法規規章；
- ISMS 包含高複雜度的作業或較多數量或獨特的活動；
- 涉及硬體、軟體、作業、及服務結合的作業；
- 活動需要訪視臨時性場區以確認被驗證之管理系統的永久場區所的活動(參閱以下註 3)。

允許較少稽核員時間的因素有以下例子

- 無/低風險產品/程序；

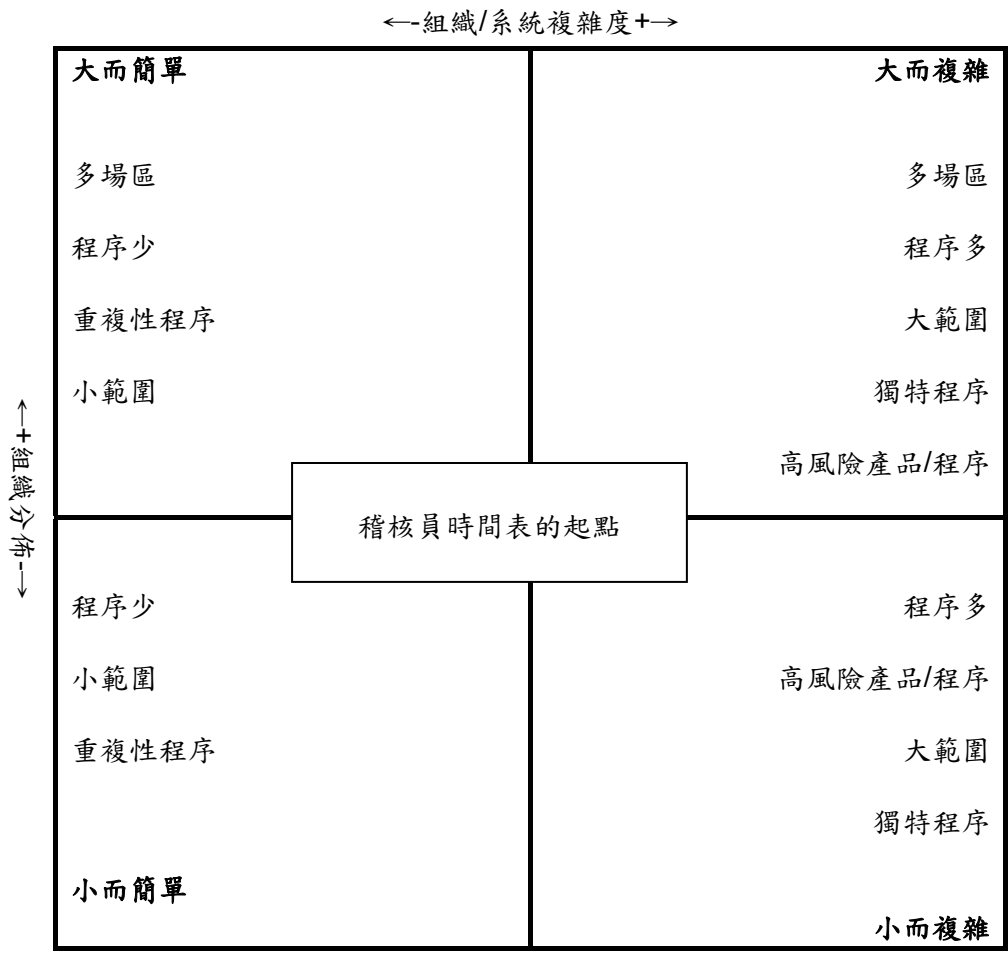
- 先前已瞭解該組織(例如，若該組織已由相同驗證機構驗證為符合其它標準時)；
- 客戶已針對驗證作好準備 (例如，已被驗證或被第三者機構之計劃所認可)；
- 涉及單一一般性活動的程序(例如，只有服務)；
- 已有成熟的管理系統；
- 執行相同的簡單工作之僱員佔高比例。

註 3 當驗證客戶或被驗證組織在臨時場區提供其產品或服務時，將該場區的評估納入驗證稽核及追查計劃，是很重要的事。

臨時場區係指驗證文件所載明的場區/位置以外的位置，驗證範圍內的活動於特定期間在該處執行。這些場區的範圍可從大型專案管理場區至小型服務/安裝場區。訪查該場區的必要性，以及抽樣的程度，須依據因產品或服務得失敗導致不能滿足需求/預期而造成系統不符合的風險的評估。被選擇的樣本場區須當代表組織能力需求及不同服務的範圍，並已考慮活動大小及種類，以及專案進展中各階段。

ISMS 範圍、作業、及產品/服務的所有屬性須被考慮，且此等因素之公平調整，可或多或少調整稽核人員時間，達到有效的稽核。增加性因素可以是現場外的減少性因素。在稽核員時間表有調整情況之所有案例，應保持充分的證據及記錄以合理解釋其變動。

下表說明稽核員時間在上表中的增加及減少因素兩者的潛在互動。



附件 D (參考)

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，事件解決的記錄，正確的授權職員所簽署的處理授權，管理層階(或其它)的會議記錄等)。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記錄的審查、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				

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.7.2.2	資訊標示及處置	X				名稱：目錄、檔案、印刷記錄、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	製作出入記錄檔案
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				

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.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、 開道器
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					

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.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	應用系統的正确處理					
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

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
						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	包括資訊安全之發展及實行持 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

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.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		

財團法人全國認證基金會

台北辦公室：台北市中正區 100 南海路二十號八樓

電 話 ： (02) 2391-4626

電 傳 ： (02) 2397-1744

E-mail ： service@taftw.org.tw

Web Site ： <http://www.taftw.org.tw>