

資訊安全管理系統 驗證機構認證規範

(ISO/IEC 27006:2015 AMD1:2020)



財團法人全國認證基金會
中華民國 109 年 10 月

「資訊安全管理系統驗證機構認證規範」(文件編號 MS-IC01) 係參照 ISO/IEC 27006:2015 AMD1:2020 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	v
簡介	vi
1. 範圍	1
2. 引用標準	1
3. 名詞及定義	1
4. 原理	1
5. 一般要求	1
5.1 法律及合約事務	1
5.2 公正性之管理	1
5.2.1 IS 5.2 利益衝突	1
5.3 責任及財務	2
6. 架構要求	2
7. 資源要求	2
7.1 人員之能力	2
7.1.1 IS 7.0 能力之考量	2
7.1.2 IS 7.1.2 能力規範的確認	2
7.2 參與驗證活動人員	6
7.2.1 IS 7.2 稽核員知識和經驗之展現	6
7.3 外部稽核員與外部技術專家之使用	7
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	7
7.4 人員記錄	7
7.5 外包	7
8. 資訊要求	7
8.1 公開的資訊	7
8.2 驗證文件	7
8.2.1 IS 8.2 ISMS 驗證文件	7
8.3 驗證之引用及標誌的使用	7
8.4 機密性	7
8.4.1 IS 4.5 組織記錄的使用	7
8.5 驗證機構與其客戶間之資訊交換	7
9. 流程要求	8
9.1 驗證前活動	8
9.1.1 申請	8
9.1.2 申請審查	8
9.1.3 稽核方案	8
9.1.4 確認稽核時間	9
9.1.5 多場區抽樣	9
9.1.6 多重管理系統	10
9.2 規劃稽核	10
9.2.1 確認稽核目標、範圍與規範	10
9.2.2 稽核小組的遴選與任務	10
9.2.3 稽核計畫	11
9.3 初次驗證	11
9.3.1 IS 9.3.1 初次驗證稽核	11
9.4 執行稽核	12
9.4.1 IS 9.4 一般性	12
9.4.2 IS 9.4 ISMS 稽核的特定要素	12
9.4.3 IS 9.4 稽核報告	13
9.5 驗證決定	13
9.5.1 IS 9.5 驗證決定	13
9.6 維持驗證	14
9.6.1 一般性	14
9.6.2 追查活動	14
9.6.3 重新驗證	14
9.6.4 特別稽核	15
9.6.5 暫時終止、終止、或減列驗證範圍	15
9.7 申訴	15

9.8	抱怨	15
9.8.1	IS 抱怨	15
9.9	客戶記錄	15
10.	驗證機構之管理系統要求	15
10.1	選項方式	15
10.1.1	IS 10.3 ISMS 執行	15
10.2	選項 A：一般管理系統要求	15
10.3	選項 B：依照 ISO 9001 管理系統要求	16
附件 A (參考性)	ISMS 稽核與驗證的知識和技能	17
附件 B (規範性)	稽核時間	19
附件 C (參考性)	稽核時間計算方法	24
附件 D (參考性)	實施 ISO/IEC 27001:2013 附件 A 控制項的審查指引	27

前言

國際標準組織 (ISO) 及國際電工委員會 (IEC) 構成全球標準化特別系統。ISO 或 IEC 之國家會員機構，透過相關組織所成立之技術委員會，處理技術性活動的特定領域，參與制定國際標準。ISO 及 IEC 技術委員會就共同利益事項，協同合作。其它國際組織、政府及非政府組織、ISO 與 IEC 的聯絡單位，也參與此作業。ISO 及 IEC 業就資訊技術領域設立一個聯合技術委員會 – ISO/IEC JTC 1。

制定本文件及進一步維持所使用的程序於 ISO/IEC 指令第 1 部中描述。尤須注意不同類型文件需要不同的核准原則。本文件係根據 ISO/IEC 指令第 2 部的編輯規則草擬 (請參照 www.iso.org/directives)。

請注意，本文件某些要項可能涉及專利權。ISO 及 IEC 不對鑑別任何或全部該項專利權負責。制定本文件期間經鑑別的任何專利權將於簡介及/或收到的 ISO 專利權宣告名單中說明細節(參閱 www.iso.org/patents)。

本文件使用的任何商業名稱係基於使用者方便而提供之資訊，並不構成某種背書。

至於有關符合性評鑑的 ISO 專有名詞及表述之釋義，以及 ISO 遵照 WTO 技術性貿易障礙 (TBT) 原則資訊之相關資訊，請參照下述 URL：

前言 – 補充資料

負責本文件之委員會為 ISO/IEC JTC 1，資訊技術，SC 27, IT 安全技術

ISO/IEC 27006 是由 ISO/IEC JTC 1，/資訊技術聯合技術委員會 SEC 27，IT 安全技術次級委員會所編制。

經技術性修訂後，本第三版即取消並取代第二版 (ISO/IEC 27006:2011)。

本次轉版並非標準版次之轉版，而係針對 ISO/IEC 27006:2015 於特定要求之變更以 AMD1:2020 版識別。

簡介

ISO/IEC 17021-1 係載明對組織之管理系統進行稽核及驗證之機構的準則。若此類機構欲取得 ISO/IEC 17021-1 之認證，以便依據 ISO/IEC 27001:2013 執行稽核及驗證資訊安全管理系統 (ISMS)，除必要的 ISO/IEC 17021-1 外，所需額外規定及指引，由本國際標準提供。

本國際標準的內容遵循 ISO/IEC 17021-1 的結構，且有關 ISMS 驗證運用 ISO/IEC 17021-1 所需的 ISMS 特定規定及指引，標示為 "IS"。

本國際標準內容中，使用 "應" 一詞，以表示 ISO/IEC 17021-1 及 ISO/IEC 27001 之規定為強制性條文。使用 "須" 一詞，以表示建議。

本國際標準之主要目的在於使認證機構更有效地調和其評鑑驗證機構之標準的應用。

本國際標準中，「管理系統」及「系統」二詞可交互使用。管理系統之定義詳見 ISO 9000:2005。本國際標準所稱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 17021-1 及 ISO/IEC 27001 所述規定外，本國際標準對資訊安全管理系統(ISMS) 稽核及驗證機構明定一些要求並提供指引。其主要目的旨在支援 ISMS 驗證機構的認證作業。

本國際標準所述要求，必須由任何提供 ISMS 驗證的機構，以其能力及可靠度予以展現，且本國際標準所述指引，係供任何提供 ISMS 驗證機構有關這些要求的額外解釋。

註：本國際標準可當作認證、同儕評鑑、或其它稽核過程的標準文件。

2. 引用標準

下列文件之全部或部分，係本文引用之標準，且對其應用是不可或缺的。引用文件有標註日期者，僅適用該版本。引用文件未標註日期者，則適用該文件之最新版本(包括任何修正版)。

ISO/IEC 17021-1:2015，符合性評鑑－管理系統稽核及驗證機構的要求－第1部分：要求

ISO/IEC 27000，資訊技術－安全技術－資訊安全管理系統－概述和詞彙

ISO/IEC 27001:2013，資訊技術－安全技術－資訊安全管理系統－要求

3. 名詞及定義

就本文件之目的，ISO/IEC 17021-1, ISO/IEC 27000 所列及下列各項名詞與定義均適用之。

3.1 驗證文件

載明客戶的 ISMS 符合特定 ISMS 標準及其他有關系統之書面化補充規定文件。

4. 原理

ISO/IEC 17021-1，第4條所述原則適用之。

5. 一般要求

5.1 法律及合約事務

ISO/IEC 17021-1，第5.1條之規定適用之。

5.2 公正性之管理

ISO/IEC 17021-2，第5.2條之規定適用之。此外，以下之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) 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可公開取得的一般資訊及建議；即，不須提供與下款 b) 所述規定相互抵觸之對公司的特定建議；
- b) 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(參閱 9.1.3.6)；
- c) 完全為決定驗證稽核是否就緒的稽核前活動；但該活動不應造成提供與本條相互抵觸的意見或建議，並且驗證機構應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；
- d) 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；
- e) 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。

驗證機構不應根據驗證提供客戶 ISMS 內部資訊安全審查。再者，驗證機構應獨立於提供 ISMS 內部稽核機構(包括任何個人)之外。

5.3 責任及財務

ISO/IEC 17021-1，第 5.3 條之規定適用之。

6. 架構需求

ISO/IEC 17021-1，第 6 條之要求適用之。

7. 資源要求

7.1 人員之能力

ISO/IEC 17021-1，第 7.1 條之規定適用之。此外，以下要求和指引亦適用之。

7.1.1 IS 7.1 一般考量

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 一般能力要求

驗證機構應確保充分瞭解有關其評鑑客戶 ISMS 之相關技術、法律和法規發展。

驗證機構應參照 ISO/IEC 17021-1 表 A.1 定義各項驗證功能之能力要求。驗證機構應確將 ISO/IEC 17021-1 及本國際標準第 7.1.2 和 7.2.1 條所有與 ISMS 技術領域相關要求列為驗證機構之要求。

註：附件 A 提供有關特定驗證功能人員能力要求彙總表。

7.1.2 IS 7.1.2 能力規範的確認

7.1.2.1 ISMS 稽核之能力要求

7.1.2.1.1 一般要求

驗證機構應備有確認驗證稽核小組成員背景經驗、特定訓練或簡介之規範，至少確保：

- a) 對資訊安全的知識；
 - b) 對受稽核活動的技術知識；
 - c) 對管理系統的知識；
 - d) 稽核原則的知識；
- 註：有關稽核原則詳細資訊請參照 ISO 19011。
- e) 對 ISMS 監督、評量、分析和評估的知識。

上述 a)至 e)項要求適用於稽核小組之所有稽核員，惟 b)項除外，它可由稽核小組稽核員共同分擔之。

稽核小組應有能力從客戶 ISMS 資訊安全事故指標回溯至適當的 ISMS 項目。

稽核小組應具上列各項的適當工作經驗及其實務應用(這不表示稽核員要有資訊安全各領域之完整經驗，惟整個稽核小組，應具備涵蓋 ISMS 稽核範圍的充分瞭解及經驗)。

7.1.2.1.2 資訊安全管理技能、原則、實務和技術

稽核小組全體成員均應具備下列知識：

- a) ISMS 特定文件結構、層級和相互關係；
- b) 資訊安全管理相關工具、方法，技術及其應用；
- c) 資訊管理風險評估和風險管理；
- d) 適用於 ISMS 之程序；
- e) 可能與資訊安全相關之現有技術或議題。

每一位稽核員都應滿足 a), c) 和 d)項。

7.1.2.1.3 資訊安全管理系統之標準和規範文件

參與 ISMS 稽核之稽核員應具備下列知識：

- a) ISO/IEC 27001 之所有要求。

稽核小組全體成員均應具備下列知識：

- b) ISO/IEC 27002 所有控制項 (若有必要，也可增加特定標準之部分)以及其實務，包含：
 - 1) 資訊安全政策；
 - 2) 資訊安全組織；
 - 3) 人力資源安全；
 - 4) 資產管理；
 - 5) 存取控制，包括授權；
 - 6) 密碼學；
 - 7) 實體和環境安全；
 - 8) 作業安全，包括 IT-服務；
 - 9) 通信安全，包括網路安全管理和資訊傳輸；

- 10) 系統取得、開發和維護；
- 11) 供應商關係，包括外包服務；
- 12) 資訊安全事故管理；
- 13) 與營運持續管理相關之資訊安全層面，包括重複者；
- 14) 符合性，包括資訊安全審查。

7.1.2.1.4 業務管理實務

參與 ISMS 稽核的稽核員應具備下列知識：

- a) 資訊安全業界優良實務及資訊安全程序；
- b) 資訊安全之政策和營運要求；
- c) 一般營運管理理念，實務和政策以及政策、目的和結果間之相互關係；
- d) 管理流程和相關術語。

註 這些流程也包括人力資源管理，內部和外部溝通以及其他相關支援流程。

7.1.2.1.5 客戶之業務

參與 ISMS 稽核之稽核員應該具備下列知識：

- a) 特定資訊安全領域、地域和管轄權之法律和法規要求；

註：法律和法規要求知識並不意味需要深厚的法律背景。

- b) 與業務相關的資訊安全風險；
- c) 與客戶業務相關之通用術語、流程和技術；
- d) 相關業務的實務。

a)項之規範可由稽核小組共同分擔之。

7.1.2.1.6 客戶產品、流程和組織

參與 ISMS 稽核之稽核員全體均應具備下列知識：

- a) 組織型式、規模、治理、架構、功能與 ISMS 發展和實做及驗證活動間關係之影響，包括外包；
- b) 宏觀地觀察複雜的作業；
- c) 產品或服務所適用之法律和法規要求。

7.1.2.2 ISMS 稽核小組長之能力要求

除了 7.1.2.1 條款要求外，稽核小組長應符合下列要求，這些要求應在指導與督導下所做稽核中加以證明：

- a) 管理驗證稽核流程和稽核小組之知識和技能；
- b) 證明在口頭和書面兩方面具有有效溝通之能力。

7.1.2.3 執行申請審查之能力要求

7.1.2.3.1 資訊安全管理系統標準和規範文件

進行申請審查以確定稽核小組必要能力，遴選稽核小組成員及決定稽核時間之人員應具備下列知識：

- a) 驗證流程中所採用之相關 ISMS 標準及其他規範文件。

7.1.2.3.2 客戶業務

進行申請審查以確定稽核小組必要能力，遴選稽核小組成員以及決定稽核時間之人員應具備下列知識：

- a) 與客戶業務相關之通用術語、流程、技術和風險。

7.1.2.3.3 客戶產品、流程和組織

進行申請審查以確定稽核小組必要能力，遴選稽核小組成員以及決定稽核時間之人員應具備下列知識：

- a) 客戶產品、流程、組織型式、規模、治理、架構、功能與 ISMS 發展和實做及驗證活動間之關係，包括外包功能。

7.1.2.4 審查稽核報告並作驗證決定之能力要求

7.1.2.4.1 一般性

審查稽核報告並作驗證決定之人員應具備足供他們查證驗證範圍適當性，與變更範圍及其對稽核有效性的影響，特別是鑑別與持續有效性相關之介面與相依關係及相關風險等之知識。

此外，審查報告並作驗證決定人員應具備下列知識：

- a) 一般管理系統；
- b) 稽核流程和程序；
- c) 稽核原則、實務和技能。

7.1.2.4.2 資訊安全管理術語、原則、實務和技能

審查稽核報告並作驗證決定人員應具備下列知識：

- a) 第 7.1.2.1.2 條款第 a), c) 和 d) 項所列項目；
- b) 與資訊安全相關之法律和法規要求。

7.1.2.4.3 資訊安全管理系統標準和規範文件

審查稽核報告並作驗證決定人員應具備下列知識：

- a) 驗證流程中所採用之相關 ISMS 標準及其他規範文件。

7.1.2.4.4 客戶業務

審查稽核報告並作驗證決定人員應具備下列知識：

- a) 與相關業務實務有關之通用術語和風險。

7.1.2.4.5 客戶產品、流程和組織

審查稽核報告並作驗證決定人員應具備下列知識：

- a) 客戶產品、流程、組織型式、規模、治理、架構、功能和關係。

7.2 參與驗證活動人員

ISO/IEC 17021-1, 第 7.2 條規定適用之。此外，以下要求和指引也適用之。

7.2.1 IS 7.2 稽核員知識和經驗之展現

驗證機構應透過下列各項展現稽核員具備知識和經驗：

- a) 認可的 ISMS-特定資格；
- b) 適用時，登錄為稽核員；
- c) 參加 ISMS 訓練課程並取得相關人員證照；
- d) 最新的專業發展記錄；
- e) 由其他 ISMS 稽核員見證其 ISMS 稽核。

7.2.1.1 遴選稽核員

除了第 7.1.2.1 條款外，稽核員遴選規範應確保各稽核員：

- a) 具備專業教育或與大學教育同等之訓練；
- 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) 已成功完成至少五天的訓練，其範圍包含 ISMS 稽核及稽核管理；
- d) 在履行稽核員職務前，已經有 ISMS 稽核之經驗。這些經驗包括過去 5 年內執行至少 10 天的 ISMS 現場稽核，並且其中應以實習稽核員身份在 ISMS 評估員(見 ISO/IEC 17021-1:2015, 9.2.2.1.4)的監督下，至少執行一次 ISMS 初次驗證稽核(包括第 1 階段與第 2 階段)或重新驗證稽核以及至少一次追查稽核。參與的稽核活動應包括文件與風險評估之審查、執行稽核及稽核報告撰寫。
- e) 具備合宜且及時的經驗；
- f) 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與技能。
- g) 具備依據 ISO/IEC 27001 執行 ISMS 稽核的能力。

技術專家應符合 a)、b)、及 e)的規範。

7.2.1.2 遴選稽核小組長

除了 7.1.2.2 及 7.2.1.1 外，遴選稽核小組長之規範應確保該稽核員：

- a) 積極參與至少 3 件完整的 ISMS 稽核。此之參與應包括初步的範圍界定和規劃，審查文件和風險評鑑，執行評鑑和正式的稽核報告。

7.3 外部稽核員與外部技術專家之使用

ISO/IEC 17021-1，第 7.3 條的規定適用之。另外，下述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

技術專家應在稽核員的督導下工作。技術專家最基本要求列於第 7.2.1.1 條款。

7.4 人員記錄

ISO/IEC 17021-1，第 7.4 條的規定適用之。

7.5 外包

ISO/IEC 17021-1，第 7.5 條的規定適用之。

8. 資訊要求

8.1 公開的資訊

ISO/IEC 17021-第 8.1 條的規定適用之。

8.2 驗證文件

ISO/IEC 17021-1，第 8.2 條之規定適用之。此外，以下規定及指引亦適用之。

8.2.1 IS 8.2 ISMS 驗證文件

組織依據 ISO/IEC 27001:2013 6.1.3 d) 選擇其適用的控制措施 (Statement of Applicability)，驗證文件可以註明組織除了 ISO/IEC 27001 附錄 A 以外所適用的其他國際或國內的控制措施。驗證文件應明確說明這些控制措施僅屬適用性聲明而不是對其驗證。

8.3 驗證之引用及標誌的使用

ISO/IEC 17021-1，第 8.4 條之規定適用之。

8.4 機密性

ISO/IEC 17021-1，第 8.4 條之規定適用之。另外，下述要求及指引也適用之。

8.4.1 IS 4.5 組織記錄的使用

在驗證稽核前，驗證機構應詢問客戶是否有任何 ISMS 相關資訊（諸如 ISMS 記錄或有關控制項之意圖和有效性資訊）因其含有機密或敏感資訊，而不能提供稽核小組審查。

驗證機構應判斷，沒有這些資料時，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資訊，則不可能適當稽核 ISMS 時，驗證機構應告知客戶，在獲得適當的使用同意前，不能進行驗證稽核。

8.5 驗證機構與其客戶間之資訊交換

ISO/IEC 17021-1，第 8.5 條之規定適用之。

9. 流程要求

9.1 驗證前活動

9.1.1 申請

ISO/IEC 17021-1，第 9.1.1 條之規定適用之。另外，以下規定及指引也適用之。

9.1.1.1 IS 9.1.1 申請準備

驗證機構應要求其客戶備妥符合 ISO/IEC 27001 之書面文件，及已執行之 ISMS，以及其他驗證必要文件。

9.1.2 申請審查

ISO/IEC 17021-1,第 9.1.2 條款規定適用之。

9.1.3 稽核計畫

ISO/IEC 17021-1 第 9.1.3 條款規定適用之。此外，以下要求和指引也適用之。

9.1.3.1 IS 9.1.3 一般性

ISMS 稽核之稽核計畫應考量已確認之資訊安全控制項。

9.1.3.2 IS 9.1.3 稽核方法

驗證機構的程序不應預設執行 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的 ISMS 是否符合 ISO/IEC 27001 說明的要求，與客戶的政策及目的。

註：有關稽核的更多指引詳見 ISO/IEC 27007

9.1.3.3 IS 9.1.3 初次稽核的一般準備事項

驗證機構應要求客戶為存取內部稽核報告和資訊安全獨立審查報告做好必要安排。客戶在驗證稽核的第一階段期間，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 所要求的 ISMS 文件影本，及必要的相關文件。

9.1.3.4 IS 9.1.3 審查期間

除非已進行至少一次管理審查和一次涵蓋驗證範圍的內部 ISMS 稽核，否則驗證機構不得驗證其 ISMS。

9.1.3.5 IS 9.1.3 驗證範圍

稽核小組應稽核客戶所界定範圍的 ISMS 是否符合所有驗證規定。驗證機構應確認，在客戶 ISMS 範圍內，客戶符合 ISO/IEC 27001 第 4.3 條款所述規定。

驗證機構應確保客戶的資訊安全風險評鑑和風險處理適切反映其活動，且擴及驗證範圍所界定的活動邊界內。驗證機構應確認上述事項均反映在客戶的 ISMS 範圍及適用性聲明中。驗證機構應查證各驗證範圍至少有一份適用性聲明。

驗證機構應確保不完全在 ISMS 範圍內之服務或活動介面，均已納入 ISMS 驗證事項中，且納入客戶的資訊安全風險評鑑。例如與其他組織共用的設施（例如，IT 系統、資料庫和電信系統或部分業務功能外包）。

9.1.3.6 IS 9.1.3 驗證稽核規範

稽核客戶 ISMS 的規範應是 ISMS 標準 ISO/IEC 27001。執行功能驗證時可能需要其他文件。

9.1.4 確認稽核時間

ISO/IEC 17021-1 第 9.1.4 條款之規定適用之。此外，以下要求和指引也適用。

9.1.4.1 IS 9.1.4 稽核時間

驗證機構應允許稽核員有充分的時間進行所有與初次稽核、追查稽核或重新驗證稽核相關的所有活動。整體稽核時間的計算應包括充份的稽核報告時間。

驗證機構應使用附件 B 來決定稽核時間。

註：附件 C 提供有關稽核時間計算的更多指引和範例。

9.1.5 多場區抽樣

ISO/IEC 17021-1 第 9.1.5 條的規定適用之。此外，以下要求和指引也適用。

9.1.5.1 IS 9.1.5 多場區

9.1.5.1.1 若客戶有符合下列 a) 至 c) 項的數個場區時，驗證機構可以考慮採用抽樣法進行多場區驗證稽核：

- a) 所有場區都在中央管理及稽核的相同 ISMS 下運作，並由中央管理審查；
- b) 所有場區都納入客戶的內部 ISMS 稽核方案內；
- c) 所有場區都納入客戶的 ISMS 管理審查方案內。

9.1.5.1.2 希望採用抽樣法之驗證機構，應備有確保下列事項之程序：

- a) 初步合約審查中，竭盡所能辨識出各場區間的差異，以決定適當的抽樣水準。
- b) 驗證機構採樣場區代表樣本數時，應考慮到：
 - 1) 總部及各場區的內部稽核結果；
 - 2) 管理審查之結果；
 - 3) 場區大小之差異；

- 4) 場區業務目的之差異；
 - 5) 不同場區資訊系統的複雜性；
 - 6) 工作實務之差異；
 - 7) 所從事活動之差異；
 - 8) 控制項設計和操作的差異；
 - 9) 關鍵資訊系統或處理敏感資訊之資訊系統的潛在互動性；
 - 10) 任何不同的法律規定；
 - 11) 地理和文化的觀點；
 - 12) 場區的風險處境；
 - 13) 特定場區的資訊安全事故。
- c) 從客戶的 ISMS 範圍內所有場區選出代表樣本；這項挑選應是基於足以反映上述 b)項所述要素以及隨機元素之判斷所為。
- d) ISMS 範圍內每個面臨重大風險的場區，均要在發證前加以稽核。
- e) 稽核方案已經根據上述規範設計，並在三年期限內涵蓋 ISMS 驗證範圍的代表樣本。
- f) 不論是在總部或單一場區發現不符合事項，矯正措施程序適用於總部和證書所涵蓋的所有場區。

稽核應針對客戶的總部活動，以確保單一 ISMS 適用於所有場區，並在作業層面實施中央管理。稽核應針對上述所有議題。

9.1.6 多重管理系統

ISO/IEC 17021-1 第 9.1.6 條款的規定適用之。此外，以下要求和指引也適用。

9.1.6.1 IS 9.1.6 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，且與其他系統具適當的介面，驗證機構即可接受合併文件（例如有關資訊安全、品質、健康與安全以及環境）。

9.1.6.2 IS 9.1.6 結合管理系統稽核

若可展現稽核符合 ISMS 驗證的所有要求，則 ISMS 稽核可結合其它管理系統的稽核。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。

9.2 規劃稽核

9.2.1 確認稽核目標、範圍和規範

ISO/IEC 17021-1 第 9.2.1 條款的規定適用之。此外，以下要求和指引也適用之。

9.2.1.1 IS 9.2.1 稽核目標

稽核目標應包括管理系統有效性的確定，以確保客戶根據風險評鑑，實做適用的控制項，且達成既定的資訊安全目標。

9.2.2 稽核小組的遴選和任務

ISO/IEC 17021-1 第 9.2.2 條款的規定適用之。此外，以下要求和指引也適用之。

9.2.2.1 IS 9.2.2 稽核小組

稽核小組應經正式指派，並提供其適當的工作文件。給予稽核小組的授權應清楚定義並知會客戶。

稽核小組可以由一人組成，惟此人應符合第 7.1.2.1 條款明載的所有規範。

9.2.2.2 IS 9.2.2 稽核小組的能力

第 7.1.2 條款所列要求適用有關追查和特別稽核活動之要求，僅適用於既定的追查活動及特別稽核活動。

於遴選和管理稽核小組執行特定驗證稽核時，驗證機構應確保其完成各項任務能力之適當性。稽核小組應該：

- a) 對進行驗證的 ISMS 特定活動具備適當的技術知識，若相關時，包括相關程序及其潛在資訊安全風險之適當技術知識 (技術專家可執行此項功能)；
- b) 對客戶充分瞭解，足以對客戶的 ISMS 範圍及組織內部管理其活動、產品和服務的資訊安全層面進行可靠的 ISMS 驗證稽核；
- c) 具備適當瞭解適用於客戶 ISMS 的法律和法規要求。

註：適當瞭解並非意味要有深厚的法律背景。

9.2.3 稽核計畫

ISO/IEC 17021-1 第 9.2.3 條款的規定適用之。此外，以下要求和指引也適用之。

9.2.3.1 IS 9.2.3 一般性

ISMS 稽核的稽核計畫應將已確定之資訊安全控制項列入考慮。

9.2.3.2 IS 9.2.3 網路輔助稽核技術

稽核計畫應鑑別若適當時，在稽核期間將使用的網路輔助稽核技術。

網路輔助稽核技術可包括，例如，電訊會議、網路會議、互動式網路通訊以及電子式遠距存取 ISMS 文件或 ISMS 作業。該等技術應著重在提升稽核效力和效率，且須保持稽核作業的完整性。

9.2.3.3 IS 9.2.3 稽核適當時機

驗證機構應與被稽核組織協議可展現組織全部範圍的最佳稽核時機。適當時，季節、月份、日/日期以及輪班均可列入考慮。

9.3 初次驗證

ISO/IEC 17021-1 第 9.3 條款的規定適用之。此外，以下要求和指引也適用。

9.3.1 IS 9.3.1 初次驗證稽核

9.3.1.1 IS 9.3.1.1 第 1 階段

在此稽核階段，驗證機構應取得 ISMS 設計上的文件，並涵蓋 ISO/IEC 27001 所要求的文件。

驗證機構應獲得充分瞭解有關客戶組織中的 ISMS 設計、風險評鑑和處理（包括確定控制項）、資訊安全政策及目的，尤其是客戶為稽核所做準備程度，使能規劃第 2 階段。

第 1 階段的結果應做成書面報告。驗證機構在決定進行第 2 階段以前應先審查第一階段的稽核報告，並且應確認第 2 階段稽核小組成員所需具備的必要能力；這部份可由領導稽核小組執行第 1 階段的稽核員來決定第 2 階段成員是否勝任與適當。

驗證機構應使客戶知悉，第 2 階段期間可能需要更多形式資訊和記錄以供詳細檢查。

備註 獨立審查(即由驗證機構人員但未涉入該稽核者進行之審查)可以降低決定是否進行第 2 階段稽核以及由誰進行稽核時所涉及的風險。但是，仍可以有其他降低風險的措施達到同樣目標。

9.3.1.2 IS 9.3.1.2 第 2 階段

9.3.1.2.1 驗證機構依據第 1 階段稽核報告所記錄的發現，擬訂執行第 2 階段的稽核計畫。除了評估 ISMS 有效實施外，第 2 階段的目的是：

a) 確認客戶遵循它自己的政策、目的和程序。

9.3.1.2.2 為達此目的，稽核應聚焦於客戶的：

- a) 管理高層領導能力及對資訊安全政策和資訊安全目的之承諾；
- b) ISO/IEC 27001 所列文件化要求；
- c) 資訊安全相關風險評鑑，及若重做評鑑是否產生一致、有效且可比較的結果；
- d) 依據資訊安全風險評鑑和風險處理作業，以確立控制目標與控制項；
- e) 資訊安全績效及 ISMS 有效性，資訊安全目標之評估；
- f) 所選控制項、適用性聲明與資訊安全風險評估、風險處理作業、資訊安全政策和目標間的關聯性；
- g) 實施控制項 (參照附件 D) 時，考量外部和內部背景及其相關的風險，組織的監控、資訊安全作業及控制項之量測與分析，以確認控制項是否實施且有效，並符合其所聲稱的資訊安全目標；
- h) 計畫、作業、程序、記錄、內部稽核和 ISMS 有效性審查；確保上述均可追溯至管理階層決策及資訊安全政策與目標。

9.4 執行稽核

ISO/IEC 17021-1 第 9.4 條款適用之。此外以下要求和指引也適用。

9.4.1 IS 9.4 一般性

驗證機構應具有下列各項書面化程序：

- a) 依據 ISO/IEC 17021-1 規定，對客戶的 ISMS 執行初次驗證稽核；
- b) 依據 ISO/IEC/IEC 17021-1 定期追查及重新驗證客戶的 ISMS 是否持續符合相關要求，並查證與記錄客戶是否及時採取矯正措施以矯正所有不符合事項。

9.4.2 IS 9.4 ISMS 稽核的特定要素

由稽核小組代表的驗證機構，應該：

- a) 要求客戶展現資訊安全相關風險評鑑是與 ISMS 範圍內 ISMS 運作相關且適當；
- b) 確認客戶有關鑑別、檢查和評估資訊安全相關風險的程序，及其實施結果是否與客戶的政策、目的和目標一致。

驗證機構也應確認風險評鑑所用程序是否健全且適當地實施。

9.4.3 IS 9.4 稽核報告

9.4.3.1 除了 ISO/IEC 17021-1 第 9.4.8 條款有關報告規定外，稽核報告應提供下列資訊或可供引用：

- a) 包括文件審查彙總的稽核說明；
- b) 客戶的資訊安全風險分析的驗證稽核說明；
- c) 稽核計畫的偏差 (例如某些預定活動花費時間增多或減少) ；
- d) ISMS 的範圍

9.4.3.2 稽核報告應充份詳細，有助並支持驗證決定。

稽核報告應該包含：

- a) 遵循的重要稽核軌跡及所用稽核方法(請參照第 9.1.3.2 條款)；
- 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) 評論客戶的 ISMS 是否符合驗證要求並清楚說明不符合事項，所引用適用性聲明版本，以及，若適用的話，任何與客戶前次驗證稽核結果有用的對照。

完成的問卷、查檢表、觀察紀錄、日誌或稽核員筆記可以構成稽核報告的一部份。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的樣本資訊應納入稽核報告或其它驗證文件中。

報告應考量客戶所採行之內部組織和程序的適當性，足供信賴 ISMS。

除了 ISO/IEC 17021-1 第 9.4.8 條款有關報告規定外，報告也應涵蓋：

- 總結有關 ISMS 要求及資訊安全控制項實做和有效性之最重要的正面和負面觀察；
- 稽核小組有關客戶的 ISMS 是否應予驗證的建議，及其證明資訊。

9.5 驗證決定

ISO/IEC 17021-1 第 9.5 條款的規定適用之。此外，以下要求和指引也是適用之。

9.5.1 IS 9.5 驗證決定

驗證決定，除應依據 ISO/IEC 17021-1 的規定外，也應依據稽核小組在其驗證稽核報告中所提供之驗證建議（請參照第 9.4.3 條款）

決定給予驗證的個人或委員會，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根據。

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，否則不應核發驗證給客戶。

9.6 維持驗證

9.6.1 一般性

ISO/IEC 17021-1 第 9.6.1 條款的規定適用之。

9.6.2 追查活動

ISO/IEC 17021-1，第 9.6.2 條之規定適用之。此外，以下規定及指引也適用之。

9.6.2.1 追查活動

9.6.2.1.1 追查稽核程序應與本標準中有關客戶的 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持續遵循。追查計畫通常至少應包含

- a) 如資訊安全風險評鑑及持續監控、內部 ISMS 稽核、管理審查、與矯正措施等系統維持要素；
- 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 中的要求事項；
- f) 適當時，其它選擇的領域。

9.6.2.1.2 驗證機構的每次追查至少應審查以下各項：

- a) 有關達成客戶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) 控制項確定的變動，並導致 SoA 的變動；
- d) 根據稽核方案所選控制項之實做與有效性。

9.6.2.1.3 驗證機構應能調整其追查計畫，以因應有關客戶對風險與衝擊等資訊安全問題，並且使該計畫具正當性。

追查稽核可結合其它管理系統的稽核。報告應清楚標示各管理系統的相關部分。

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，且若有不符合事項，或不符合驗證要求，客戶已調查其本身之 ISMS 及程序，並已採取適當的矯正措施。

追查報告應包含，特別是有關先前揭示的不符合事項的排除，以及 SoA 版本與前次稽核後重要變動等資訊。追查所產出的報告，至少應建構在涵蓋前述第 9.6.2.1.1 條款及第 9.6.2.1.2 條款的全部要求。

9.6.3 重新驗證

ISO/IEC 17021-1，第 9.6.3 條之規定適用之。此外，以下要求及指引也適用之。

9.6.3.1 IS 9.6.3 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 ISMS 初次的驗證稽核一致。

允許進行矯正措施的時間，須與不符合事項的嚴重性及有關資訊安全風險相當。

9.6.4 特別稽核

ISO/IEC 17021-1，第 9.6.4 條之規定適用之。此外，以下要求及指引也適用之。

9.6.4.1 IS 9.6.4 特殊案例

有特殊稽核的必要性時，應符合特殊之條件，如若已驗證 ISMS 的客戶，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。

9.6.5 暫時終止、終止、或減列驗證範圍

ISO/IEC 17021-1，第 9.6.5 條之規定適用之。

9.7 申訴

ISO/IEC 17021-1，第 9.7 條之規定適用之。

9.8 抱怨

ISO/IEC 17021-1，第 9.8 條之規定適用之。此外，以下要求及指引也適用之。

9.8.1 IS 9.8 抱怨

抱怨代表潛在的事故，且是不符合事項的可能徵兆。

9.9 客戶記錄

ISO/IEC 17021-1 第 9.9 條款的規定適用之。

10 驗證機構之管理系統要求

10.1 選項方式

ISO/IEC 17021-1 第 10.1 條之規定適用之。此外，以下要求及指引也適用之。

10.1.1 IS 10.3 ISMS 執行

建議驗證機構依據 ISO/IEC 27001 執行 ISMS 驗證。

10.2 選項 A：一般管理系統要求

ISO/IEC 17021-1 第 10.2 條款的規定適用之。

10.3 選項 B：依照 ISO 9001 管理系統要求

ISO/IEC 17021-1 第 10.3 條款的規定適用之。

附件 A (參考性)

ISMS 稽核與驗證的知識與技能

A.1 組概論

表 A.1 彙總提供 ISMS 稽核與驗證的知識和技能，惟僅供參考，因它只鑑別特定驗證功能的知識和技能領域。

本國際標準主文說明各項功能的能力要求，本表則提供特定要求。

表 A.1 — ISMS 稽核與驗證的知識

	驗證功能		
	執行申請審查 (執行申請審查以確定稽核小組必要能力、遴選稽核小組成員及確認稽核時間)	審查稽核報告並作成驗證決定	稽核與領導稽核小組
知識			
資訊安全管理術語、原則、實務和技能		7.1.2.4.2	7.1.2.1.2
資訊安全管理系統標準/規範文件	7.1.2.3.1	7.1.2.4.3	7.1.2.1.3
商業管理實務			7.1.2.1.4
客戶的業務	7.1.2.3.2	7.1.2.4.4	7.1.2.1.5
客戶產品、流程與組織	7.1.2.3.3	7.1.2.4.5	7.1.2.1.6

A.2 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。可供評估的知識與經驗，例如，可使用被認可的資格。人員驗證方案下的登錄紀錄，也可以評估其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 ISMS 複雜度因素而定。

A.3 特定知識和經驗考量

A.3.1 有關 ISMS 的特定知識

除了第 7.1.2 條款的要求外，也應考量下列各項。稽核員須具備並熟悉下列稽核及 ISMS 事項的知識：

- 稽核計畫及規劃；
- 稽核種類及方法；
- 稽核風險；
- 資訊安全處理分析；
- 持續改善；
- 資訊安全的內部稽核。

稽核員應具備並熟悉以下法規要求的知識：

- 智慧財產權；
- 組織記錄的內容、保護及保存；
- 資料保護及穩私；
- 密碼學式控制的法規；
- 電子商務；
- 電子與數位簽章；
- 職場監督；
- 電信截聽及資料監控(例如電子郵件)；
- 電腦濫用；
- 電子證據蒐集；
- 滲透測試；
- 國際及國內特定產業的要求(例如銀行業)。

附件 B (規範性)

稽核時間

B.1 簡介

本附件包含有關 ISO/IEC 17021-1 第 9.1 條的其它要求。本附件提供驗證機構，發展其本身程序之最低要求及指引，以決定驗證客戶的 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。

驗證機構應鑑別每一位客戶及被驗證 ISMS 的初次驗證、追查和重新驗證的稽核時間量。在稽核規劃階段使用本附件達到決定適當的稽核時間的一致性方法。此外，也可根據稽核期間，特別是在第 1 階段期間的發現（例如 ISMS 範圍複雜性，或在範圍內追加場區的不同評鑑）加以調整稽核時間。

本附件提出：

- 用於稽核時間計算的概念 (B.2)；
- 決定不同稽核階段的稽核時間程序之要求 (B.3 至 B.5)；
- 有關多場區稽核之要求 (B.6)；

附件 C 提供有關稽核時間計算以說明附件 B 的應用範例。這個方法的基本假設為決定稽核時間的計算方案應：

- a) 僅能根據可被證實的屬性作決定；
- b) 簡單的足供驗證機構有效應用；
- c) 複雜到能夠充分區別。

稽核時數的決定根據下面表 B.1（「稽核時間表」）內的數字，並應考量會導致修改的影響因素。

B.2 概念

B.2.1 組織控制下的工作人數

確定驗證範圍內組織控制下所有班別的總工作人數是確定稽核時間的起點。

註：「在組織控制下的工作人員」一詞請參照如 ISO/IEC 17021-1 的人員。

在組織控制下兼職工作人員對組織控制下工作人數的計算，係依與在組織控制下全職工作人員相較之比例。這項決定應取決於與全職員工相較之下之工作時數而定。

B.2.2 稽核員天

如圖表中所述「稽核時間」是根據稽核所花費的「稽核員天數」說明之。附件 B 的計算基礎是以一日工作 8 小時為準。

B.2.3 臨時場區

臨時場區係指驗證文件所載明的場區/位置以外的活動處所，驗證範圍內的活動於特定期間在該處所執行。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。

訪查該等場區的需要，以及抽樣程度，應依據臨時場區所產生的不符合事項導致不符合資訊安全目的之風險評估。

所選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。關於一般抽樣請詳見 9.1.5.1。

B.3 確定初次稽核之稽核時間程序

B.3.1 一般性

稽核時間的計算應遵循書面程序文件。

B.3.2 遠距稽核

若係使用諸如互動式網路協作，網路會議，電訊會議及/或電子式查證組織作業等遠距稽核技術做為與組織之介面時，這些活動應該在稽核計畫中予以鑑別 (參照第 9.2.3 條款)並可被視為「現場稽核時間」總時數的一部分。

若驗證機構發展的稽核計畫，其中遠距稽核活動佔已規劃現場稽核時間的 30%以上時，驗證機構應合理化該稽核計畫，並在實施前先取得認證機構明確的核可。

註：現場稽核時間係指分配給各個場區的現場稽核時間。即使電子式稽核實際上是在組織的場所進行，遠端場區的電子式稽核被視為遠距稽核。

B.3.3 稽核時間計算

下面所提供的稽核時間表列出初次稽核平均天數(此處及下述的這個數字包含初次稽核(第 1 階段和第 2 階段)的天數)為起點，根據經驗顯示，它對於所定在組織控制下工作人數的 ISMS 範圍是適當的。經驗也證實對於類似規模的 ISMS 範圍，有些需要較多時間，有些則較少。

下面稽核時間表提供稽核規劃框架，應鑑別組織控制下所有班別工作總人數為起點規劃稽核，及依據適用於被稽核的 ISMS 範圍之重要因素而加以調整，並依各因素所增減加權以修正基數。在考慮影響因素和最大偏差限制之下，應使用此稽核時間表 (參照下面 B3.4 和 B3.5)。本圖表中所用名詞說明於上面 B.2 以及附件 C 提供如何進行規劃範例。

表 B.1 — 稽核時間表

組織控制下之 工作人數	QMS 初次稽核 之稽核時間 (稽核員天數)	EMS 初次稽核之 稽核時間 (稽核員天數)	ISMS 初次稽核 之稽核時間 (稽 核員天數)	增加和減少的因 素	總計稽核時間
1~10	1.5-2	2.5-3	5	參照 B.3.4	
11~15	2.5	3.5	6	參照 B.3.4	
16~25	3	4.5	7	參照 B.3.4	
26~45	4	5.5	8.5	參照 B.3.4	
46~65	5	6	10	參照 B.3.4	
66~85	6	7	11	參照 B.3.4	
86~125	7	8	12	參照 B.3.4	
126~175	8	9	13	參照 B.3.4	
176~275	9	10	14	參照 B.3.4	
276~425	10	11	15	參照 B.3.4	
426~625	11	12	16.5	參照 B.3.4	
626~875	12	13	17.5	參照 B.3.4	
876~1175	13	15	18.5	參照 B.3.4	
1176~1550	14	16	19.5	參照 B.3.4	
1551~2025	15	17	21	參照 B.3.4	
2026~2675	16	18	22	參照 B.3.4	
2676~3450	17	19	23	參照 B.3.4	
3451~4350	18	20	24	參照 B.3.4	
4351~5450	19	21	25	參照 B.3.4	
5451~6800	20	23	26	參照 B.3.4	
6801~8500	21	25	27	參照 B.3.4	
8501~10700	22	27	28	參照 B.3.4	
> 10,700	按照上述進展	按照上述進展	按照上述進展	參照 B.3.4	

B.3.4 稽核時間調整因素

稽核時間表不應單獨使用。時間分配也應考慮到下列與 ISMS 複雜度相關因素，且需稽核 ISMS 的成果：

- a) ISMS 複雜度 (例如資訊的重要性, ISMS 的風險情況等)；
- b) ISMS 範圍內所執行的業務類型；
- c) 先前所展現的 ISMS 績效；
- d) 實做 ISMS 項目時採用技術之範圍和多樣性 (例如不同的 IT 平台數, 區隔的網路數)；
- e) ISMS 範圍內, 外包的範圍和第三方協議；
- f) 資訊系統發展程度；
- g) 場區數和災難復原(DR)之場區數；
- h) 針對追查或重新驗證稽核；有關 ISMS 變動量和程度依據 ISO/IEC 17021-1, 第 8.5.3. 條款規定

附件 C 提供如何將這些不同因素列入考量, 以計算稽核時間的範例。

下列例外因素, 需要額外的稽核時間：

- 涉及 ISMS 範圍內一棟以上建築物或場所的複雜後勤作業；
- 工作人員說一種以上語言(需要口頭翻譯或有礙個別稽核員獨立作業), 或以一種以上語文提供文件；
- 需要訪查臨時場區活動以確認被驗證管理系統的永久場區活動 (請參照下段列表)；
- ISMS 適用大量的標準和法規。

允許縮減稽核時間之因素有以下範例：

- 無或低風險的產品或流程；
- 流程涉及單一的一般性活動(例如只有服務)；
- 在組織控制下有高比例工作人員執行相同工作；
- 對該組織先前的瞭解 (例如, 組織已經由相同驗證機構以另一標準驗證) ；
- 客戶對驗證做好充分準備(例如, 已由其他第三方的方案驗證或認可)；
- 管理系統已具高成熟度。

在驗證客戶或被驗證組織在臨時場區提供其產品或服務情況下, 將這些廠區的評估納入驗證稽核和追查計畫內極為重要。

應考量以上因素, 並針對這些因素調節增減稽核時間, 以達到有效稽核。增加時間的因素可以被縮減時間的因素所抵銷。依稽核時間表而有所調整之案件, 均應保存充分證據和記錄以證明其變動之正當性。

B.3.5 稽核時間差異限制

為了確保執行有效稽核及確保可靠與可比較結果，稽核時間表上所提供的稽核時間不應減少超過 30%。

時間差異之正當理由應做成書面紀錄。

B.3.6 現場稽核時間

雖然規劃與報告撰寫可以計入稽核時間，但不能因此排擠現場稽核時間以致低於依 B.3.3h 與 B.3.4 所計算出來之時間的 70%。如果需要額外的時間規劃及/或撰寫報告，這不應成為減少現場稽核時間的理由。稽核員的差旅時間不包含在此計算之內，而是外加於稽核時間表 B.1 的時間。

註：70 % 是根據 ISMS 稽核經驗之因素。

B.4 追查稽核之稽核時間

初次驗證稽核週期中，對某組織的追查時間須與其初次稽核所需時間成比例，每年追查所需全部時間約為初次稽核所需時間的 1/3。所規劃的追查稽核時間須隨時審查以因應影響稽核時間的變動。為了稽核 ISMS 的變動(諸如稽核新增或變更控制項)應允許增加追查稽核時間。

B.5 重新驗證稽核之稽核時間

執行重新驗證稽核所需總時間應依第 9.4.3 條款及 ISO/IEC 17021-1 第 9.6.3 條款定義之任何先前稽核結果而定。重新驗證稽核所需時間量應與同一組織初次驗證稽核所用時間成比例，且至少須為同一組織初次驗證稽核所需時間的 2/3。

B.6 多場區的稽核時間

按照 B.3.3 中規定的程序計算出驗證範圍的現場稽核總人天數，應根據各場區與管理系統的關聯性及已鑑別出的風險，將人天數分配到不同場區。驗證機構應記錄分配人天數的理由。

初次稽核與追查稽核所花費的總時間是每一場區加上總部所需的時間總和，並且，時間總和不得低於以相同營運規模與複雜度的單一場區所計算出來的時間。

附件 C (參考性)

稽核時間計算方法

C.1 一般性

本附件提供有關推導稽核時間計算公式的進一步指導綱要。C.2 係將不同因素加以分類，以為稽核時間計算基礎，而 C.3 則提供稽核時間計算案例。

C.2 計算稽核時間因素之分類

表 C.1 提供有關 B.3.4 第 a)至 h)項所列稽核時間計算所用主要因素分類範例，。驗證機構可以按照第 9.1.4.1 條款利用這項分類推導出稽核時間計算方式：

表 C.1 — 計算稽核時間因素分類

因素 (參照 B.3.4)	工作量之影響		
	減少工作量	正常工作量	增加工作量
a) ISMS 的複雜度： • 資訊安全要求 [機密性、完整性和可用性 (CIA)] • 重要資產數量 • 流程和服務數量	<ul style="list-style-type: none"> 僅少數敏感或機密資訊，低可用性需求 少數重要資產(根據 CIA) 僅一項關鍵業務流程，涉及少數介面和少數業務單位 	<ul style="list-style-type: none"> 較高可用性要求或有些敏感/機密資訊 有些重要資產 2-3 項 簡單業務流程，涉及少數介面和少數業務單位 	<ul style="list-style-type: none"> 較多量的敏感或機密資訊 (例如，健康、個人資料、保險、銀行業務) 或高度可用性要求 許多重要資產 兩項以上複雜流程，涉及許多介面和業務單位
b) ISMS 範圍內所執行的業務類型	<ul style="list-style-type: none"> 無法規要求之低風險業務 	<ul style="list-style-type: none"> 高度法規要求 	<ul style="list-style-type: none"> 高度風險業務及(僅)有限的法規要求
c) 先前所展現的 ISMS 績效	<ul style="list-style-type: none"> 最近已驗證 未經驗證，惟 ISMS 實做已歷經多次稽核和改善週期，包括書面記載的內部稽核，管理審查以及有效持續改善系統。 	<ul style="list-style-type: none"> 最近經追查稽核 尚未驗證但已部份實施 ISMS：有些管理系統工具可用並已實施，有些持續改善流程雖就緒，但僅有部分書面資料。 	<ul style="list-style-type: none"> 沒有驗證且沒有較近的稽核 ISMS 是新的且尚未完整建置(例如缺乏管理系統具體控制機制，不成熟的持續改善流程，執行特殊流程)
d) 實做 ISMS 項目時所採用技術之範圍和多樣性 (例如不同的 IT 平台數量，區隔的網路數量)	<ul style="list-style-type: none"> 多樣性低且高度標準化環境(少量 IT-平台、伺服器、作業系統、資料庫、網路等) 	<ul style="list-style-type: none"> 標準化但係不同的 IT 平台、伺服器、作業系統、資料庫、網路 	<ul style="list-style-type: none"> 高度多樣性或複雜性的 IT (例如許多不同的網路區隔、伺服器或資料庫類型、關鍵應用數量)
e) ISMS 範圍內，外包的範圍和第三方協議	<ul style="list-style-type: none"> 無外包僅少數依賴供應商，或 完善定義、管理和監控的外包協議 外包商 ISMS 業經驗證 具相關獨立性保證報告 	<ul style="list-style-type: none"> 若干部分管理外包協議 	<ul style="list-style-type: none"> 高度依賴外包或供應商對重要業務活動影響很大，或者 外包數量或程度不明，或者 若干未管理的外包協定

因素 (參照 B.3.4)	工作量之影響		
	減少工作量	正常工作量	增加工作量
f) 資訊系統發展程度	<ul style="list-style-type: none"> 無內部系統開發 使用標準化軟體平台 	<ul style="list-style-type: none"> 使用標準化軟體平台，具有複雜的組態/參數 (高度) 客製化軟體 有些開發活動(內部或外包) 	<ul style="list-style-type: none"> 重要業務用途的專案正在進行大量的內部軟體開發活動
g) 場區數和災難復原(DR)場區數	<ul style="list-style-type: none"> 可用性要求低且沒有或只有一個替代性災難復原場區 	<ul style="list-style-type: none"> 中度或高度可用性要求，且沒有或只有一個替代災難復原場區 	<ul style="list-style-type: none"> 高度可用性要求例如 24/7 全天候服務 若干替代災難復原場區 若干資料中心
h) 針對追查或重新驗證稽核:有關 ISMS 的變動量和程度依據 ISO/IEC 17021-1, 第 8.5.3 條款	<ul style="list-style-type: none"> 自從上次重新驗證稽核後沒有變動 	<ul style="list-style-type: none"> ISMS 的範圍或 SoA 輕微變動，例如有些政策、文件等 上述因素變動不多 	<ul style="list-style-type: none"> ISMS 的範圍或 SoA 重大變動，例如，新流程、新業務單位，領域，風險評鑑管理方法，政策，書面記錄文件，風險處理 上述因素重大變動

C.3 稽核時間計算範例

C.3.1 概述

以下範例說明驗證機構如何運用 B.3 中所述因素以計算稽核時間。以下範例的稽核時間計算方式作業如下：

步驟 1：確定與業務和組織有關的因素(IT 除外)：鑑別 C.2 表中所列各類因素等級並總計結果。

步驟 2：確定與 IT 環境有關因素：鑑別 C.3 表中所列各類因素適用等級並總計結果。

步驟 3：根據上述步驟 1 和步驟 2 的結果，選擇表 C.4 中適當項目以鑑別影響稽核時間的因素。

步驟 4：最後計算：運用稽核時間表(表 B.1)所定之天數乘以步驟 3 產生的係數。若使用多場區抽樣，則根據執行多場區抽樣計畫所需工作量加總已計算的稽核天數。這項結果即是最定案的稽核天數。

表 C.2 — 與業務和組織有關的因素 (IT 除外)

項目	等級
業務型式和法規要求	<ol style="list-style-type: none"> 組織經營非重要業務別及非管制業務別^a 組織擁有重要業務別的顧客 組織經營重要業務別^a

項目	等級
流程與作業	<ol style="list-style-type: none"> 標準及重複性作業的標準流程；在組織控制下工作的大量人員從事相同的工作；少數產品或服務 標準但非重複性流程，及大量產品或服務 複雜流程，大量產品和服務，許多業務單位包含在驗證範圍內(ISMS 涵蓋高度複雜的流程或相當大量或獨特的活動)
管理系統的建置水準	<ol style="list-style-type: none"> ISMS 已經完善建置及/或其他管理系統也已存在 其他管理系統的部分項目已實施，部分則尚未實施 全然尚未實施其他管理系統， ISMS 是新的且尚未建立
^a 重要業務別係指可能影響到健康、安全、經濟、形象和政府運作能力的公共服務，可能對國家有非常負面衝擊的產業。	

表 C.3 — 與 IT 環境有關的因素

項目	等級
IT 基礎結構複雜性	<ol style="list-style-type: none"> 少數或高度標準化 IT 平台，伺服器，作業系統，資料庫，網路等 若干不同的 IT 平台、伺服器、作業系統、資料庫、網路 許多不同的 IT 平台、伺服器、作業系統、資料庫、網路
仰賴外包和供應商，包括雲端服務	<ol style="list-style-type: none"> 很少或不仰賴外包或供應商 有些仰賴外包或供應商，部分有關但非全是重要的業務活動 高度仰賴外包或供應商，對重要業務活動衝擊大
資訊系統的開發	<ol style="list-style-type: none"> 完全沒有或非常有限的內部系統/應用開發 有些重要業務用途有些內部或外包系統/應用開發 重要業務用途具大量的內部或外包系統/應用開發

表 C.4 — 影響稽核時間的因素

		IT 複雜性		
		低度(3 至 4)	中度(5 至 6)	高度 (7 至 9)
業務複雜度	高度 (7 至 9)	+5 % to +20 %	+10 % to +50 %	+20 % to +100 %
	中度 (5 至 6)	-5 % to -10 %	0 %	+10 % to +50 %
	低度 (3 至 4)	-10 % to -30 %	-5 % to -10 %	+5 % to +20 %

範例 1：欲稽核之組織擁有 700 名員工，因此根據表 B.1，初次稽核需要 17.5 日。組織並非從事重要業務別，擁有高度標準化及重複作業並正好已建立 ISMS。根據表 C.2，得知與業務和組織有關的因素為 1+1+3=5。組織雖擁有非常少的 IT 平台和資料庫但廣泛使用外包。組織沒有內部或外包開發。根據表 C.3，得知與 IT 環境有關的因素為 1+3+1=5。利用表 C.4，得知無需調整稽核時間。

範例 2：同上範例的組織，除了若干管理系統已經建立且 ISMS 也完善建置。依據表 C.2 的計算變成 1+1+1=3。依據表 C.4，得知可縮減稽核時間 5%至 10%，亦即，稽核時間會減少 1 至 1.5 日，總計為 16 至 16.5 日。

附件 D (參考性)

實施 ISO/IEC 27001:2013 附件 A 控制項的審查指引

D.1 目的

客戶為 ISMS 所選定必要控制項(按照適用性聲明項目)之實施情形，應於初次稽核第 2 階段期間，以及追查或重新驗證活動期間加以審查（參照第 9.3.1.2.2 條款 g 項）。

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，例如，可在客戶的程序及政策中說明。

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，該上鎖門已上鎖，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，管理階層(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)。證據可藉由面談在組織控管下工作的人員/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 一般性

表 D.1 提供 ISO/IEC 27001:2013, 附件 A 中所列控制項實施的審查指引，以及蒐集初次稽核和後續稽核期間有關其績效的稽核證據。本表無意提供 ISO/IEC 27001:2003 附件 A 規定外控制項之審查指引。

D.2.2 “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，所以在兩欄中都有標記。

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.2.3 “系統測試”欄

“系統測試”是指直接的資訊系統審查(例如系統設定或組態的審查)。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有使用電腦工具時，可用它來支援稽核工作；或對客戶(或其分包商)的績效評估結果加以審查。

本表格包含兩種技術控制項的審查：

- 「可能」：系統測試可能被用來評估控制項的執行，但在 ISMS 稽核中可能不需要；
- 「建議」：在 ISMS 稽核中系統測試通常是必要的。

備註 在本附件內除非另有規定，否則“系統”一詞意指“資訊系統”

D.2.4 “「目視檢驗」”欄

“目視檢驗”是指這些控制項通常需要現場的目視檢驗，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.2.5 “「稽核審查指引」”欄

“稽核審查指引”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 27001:2013 附件 A 的控制項	組織控制	技術控制	系統測試	目視檢驗	稽核審查指引
A.5 資訊安全政策					
A.5.1 資訊安全之指導方針					
A.5.1.1 資訊安全政策	X				
A.5.1.2 資訊安全政策之審查	X				
A.6 資訊安全組織					
A.6.1 內部組織					
A.6.1.1 資訊安全角色和責任	X				
A.6.1.2 職務區隔	X				
A.6.1.3 與權責機關之聯繫	X				
A.6.1.4 與特殊關注方之聯繫	X				
A.6.1.5 專案管理之資訊安全	X				
A.6.2 行動裝置與遠距工作					
A.6.2.1 行動裝置政策	X	X	可能		若適當，也檢查政策的實施
A.6.2.2 遠距工作	X	X	可能		若適當，也檢查政策的實施
A.7 人力資源安全					
A.7.1 聘用前					
A.7.1.1 篩選	X				
A.7.1.2 聘用條款與條件	X				
A.7.2 聘用期間					
A.7.2.1 管理階層責任	X				
A.7.2.2 資訊 安全認知、教育和訓練	X				詢問員工他們是否注意到他們應該注意的事情
A.7.2.3 懲處過程	X				
A.7.3 聘用之終止及變更					
A.7.3.1 聘用責任之終止及變更	X				
A.8 資產管理					
A.8.1 資產責任					
A.8.1.1 資產清冊	X				鑑別資產
A.8.1.2 資產擁有權	X				
A.8.1.3 資產之可被接受使用	X				
A.8.1.4 資產之歸還	X				
A.8.2 資訊分級					
A.8.2.1 資訊之分級	X				若適用，也檢查政策的實施
A.8.2.2 資訊標示	X				命名：目錄、檔案、列印報告、記錄媒體（例如卡帶、磁碟、光碟）、電子信息和文檔傳輸

ISO/IEC 27001:2013 附件 A 的控制項	組織控制	技術控制	系統測試	目視檢驗	稽核審查指引
A.8.2.3 資產之處置	X				
A.8.3 媒體處置					
A.8.3.1 可移除式媒體之管理	X	X	可能		
A.8.3.2 媒體之汰除	X			X	處置流程
A.8.3.3 實體媒體傳送	X				實體保護
A.9 存取控制					
A.9.1 存取控制之營運要求事項					
A.9.1.1 存取控制政策	X				若適當,也檢查政策的實施
A.9.1.2 對網路及網路服務之存取	X				若適當,也檢查政策的實施
A.9.2 使用者存取管理					
A.9.2.1 使用者註冊及註銷	X				
A.9.2.2 使用者存取權限之配置	X	X	可能		在組織控制下工作人員/承包商授權所有存取所有系統權利樣本
A.9.2.3 具特殊存取權限之管理	X	X	可能		職員內部傳輸
A.9.2.4 使用者之秘密鑑別資訊的管理	X				
A.9.2.5 使用者存取權限之審查	X				
A.9.2.6 存取權限之移除或調整	X				
A.9.3 使用者責任					
A.9.3.1 秘密鑑別資訊之使用	X				查證是否備有使用者指導綱要/政策
A.9.4 系統及應用存取控制					
A.9.4.1 資訊存取限制	X	X	已建議		
A.9.4.2 安全登入程序	X	X	已建議		
A.9.4.3 通行碼管理系統	X	X	已建議		
A.9.4.4 具特殊權限公用程式之使用	X	X	已建議		
A.9.4.5 對程式原始碼之存取控制	X	X	已建議		
A.10 密碼學					
A.10.1 密碼學式控制措施					
A.10.1.1 使用密碼學式控制措施之政策	X				若適當,也檢查政策的實施
A.10.1.2 金鑰管理	X	X	已建議		若適當,也檢查政策的實施
A.11 實體及環境安全					
A.11.1 安全區域					
A.11.1.1 實體安全周界	X				
A.11.1.2 實體進入控制措施	X	X	可能	X	存檔存取記錄
A.11.1.3 安全的辦公室、房間及設施	X			X	
A.11.1.4 防範外部及環境威脅	X			X	
A.11.1.5 於安全區域內工作	X			X	
A.11.1.6 交付及裝卸區	X			X	
A.11.2 設備					
A.11.2.1 設備安置與保護	X			X	
A.11.2.2 支援之公用服務事業	X	X	可能	X	
A.11.2.3 佈纜安全	X			X	
A.11.2.4 設備維護	X				
A.11.2.5 資產之攜出	X				資產記錄攜出場外
A.11.2.6 場所外設備與資產之安全	X	X	可能		可攜式裝置加密
A.11.2.7 設備汰除或再使用之安全	X	X	可能	X	磁碟消除,磁碟加密
A.11.2.8 無人看管之使用者設備	X				查證是否備妥使用者指導綱要/政策
A.11.2.9 桌面淨空及螢幕淨空政策	X			X	若適當,也檢查政策的實施
A.12 作業安全性					
A.12.1 作業程序與責任					
A.12.1.1 書面化作業程序	X				
A.12.1.2 變更管理	X	X	已建議		
A.12.1.3 容量管理	X	X	可能		
A.12.1.4 開發、測試和作業環境之區隔	X	X	可能		
A.12.2 惡意軟體之防護					

ISO/IEC 27001:2013 附件 A 的控制項	組織控制	技術控制	系統測試	目視檢驗	稽核審查指引
A.12.2.1 防範惡意軟體之控制措施	X	X	已建議		惡意控制軟體覆蓋配置和完整性。
A.12.3 備份					
A.12.3.1 資訊備份	X	X	已建議		審查政策，恢復測試
A.12.4 存錄及監控					
A.12.4.1 事件存錄	X	X	可能		以風險為基礎之事件記錄篩選
A.12.4.2 日誌資訊之保護	X	X	可能		
A.12.4.3 管理者及操作者日誌	X	X	可能		
A.12.4.4 鐘訊同步		X	可能		
A.12.5 運作中軟體之控制					
A.12.5.1 對運作中系統軟體之安裝	X	X	可能		
A.12.6 技術弱點管理					
A.12.6.1 技術弱點管理	X	X	已建議		風險為主修正程式管理和強化作業系統、資料庫和應用程式
A.12.6.2 軟體安裝的限制	X	X	可能		
A.12.7 資訊系統稽核考量					
A.12.7.1 資訊系統稽核控制措施	X				
A.13 通訊安全性					
A.13.1 網路安全管理					
A.13.1.1 網路控制措施	X	X	可能		網路管理
A.13.1.2 網路服務之安全	X	X	已建議		SLAs, 網路服務資訊安全規定 (例如 VPN, 網路路由和連接控制, 網路裝置的配置)
A.13.1.3 網路之區隔	X	X	可能		網路圖, 網路段 (例如 DMZ) 與隔離 (e.g. VLAN)
A.13.2 資訊傳送					
A.13.2.1 資訊傳送政策及程序	X				若適當, 也檢查政策的實施
A.13.2.2 資訊傳送協議	X				
A.13.2.3 電子傳訊	X	X	可能		確認樣本信息符合政策/程序
A.13.2.4 機密性或保密協定	X				合約審查
A.14 系統獲取、開發及維護					
A.14.1 資訊系統之安全要求事項					
A.14.1.1 資訊安全要求事項分析及規格	X				
A.14.1.2 保全公共網路之應用服務	X	X	已建議		以風險為基礎之應用服務設計
A.14.1.3 保護應用服務交易	X	X	已建議		保密、完整性、不得否認性
A.14.2 開發及支援過程中之安全					
A.14.2.1 安全的開發政策	X				若適當, 也檢查政策的實施
A.14.2.2 系統變更控制程序	X	X	已建議		
A.14.2.3 作業平台變更後之應用技術審查	X				
A.14.2.4 套裝軟體變更之限制	X				
A.14.2.5 安全的系統工程原則	X				
A.14.2.6 安全的開發環境	X	X	可能		
A.14.2.7 委外開發	X				
A.14.2.8 系統安全測試	X				
A.14.2.9 系統驗收測試	X	X	可能		
A.14.3 測試資料					
A.14.3.1 測試資料的保護	X	X	可能	X	
A.15 供應者關係					
A.15.1 供應者關係中之資訊安全					
A.15.1.1 供應者關係之資訊安全政策	X				若適當, 也檢查政策的實施
A.15.1.2 於供應者協議中闡明安全性	X				測試部份合約條件
A.15.1.3 資訊及通訊技術供應鏈	X				測試部份合約條件

ISO/IEC 27001:2013 附件 A 的控制項	組織控制	技術控制	系統測試	目視檢驗	稽核審查指引
A.15.2 供應者服務交付管理					
A.15.2.1 供應者服務之監督與審查	X				
A.15.2.2 管理供應者服務之變更	X				
A.16 資訊安全事故管理					
A.16.1 資訊安全事故及改善之管理					
A.16.1.1 責任與程序	X				
A.16.1.2 通報資訊安全事件	X				
A.16.1.3 通報資訊安全弱點	X				
A.16.1.4 資訊安全事件之評鑑與決策	X				
A.16.1.5 資訊安全事故之因應	X				
A.16.1.6 從資訊安全事故中學習	X				
A.16.1.7 證據之收集	X				
A.17 營運持續管理之資訊安全層面					
A.17.1 資訊安全持續					管理審查會議記錄
A.17.1.1 規劃資訊安全持續	X				
A.17.1.2 實作資訊安全持續	X				
A.17.1.3 查證、審查並評估資訊安全持續	X				
A.17.2 多重備援					
A.17.2.1 資訊處理設施之可用性	X	X	可能		
A.18 遵循性					
A.18.1 對法律及契約要求事項之遵循					
A.18.1.1 適用的法律及契約要求事項之識別	X		已建議		
A.18.1.2 智慧財產權	X				
A.18.1.3 紀錄的保護	X	X	已建議		
A.18.1.4 個人可識別資訊之隱私及保護	X				若適當，也檢查政策的實施
A.18.1.5 密碼學式控制措施之規定	X				
A.18.2 資訊安全審查					
A.18.2.1 資訊安全之獨立審查	X				審閱與報告
A.18.2.2 安全政策及標準之遵循性	X				
A.18.2.3 技術遵循性審查	X	X			

參考文獻

- [1] ISO 19011, 稽核管理系統指導綱要
- [2] ISO/IEC 27007, 資訊技術—安全技術—資訊安全管理系統稽核指導綱要
- [3] ISO 9001, 品質管理系統—要求

財團法人全國認證基金會

財團法人全國認證基金會

地 址：新北市淡水區中正東路二段 27 號 23 樓

電 話：(02) 2809-0828

傳 真：(02) 2809-0979

E-mail：taf@taftw.org.tw

Web Site：http://www.taftw.org.tw