香港社福界資訊科技保安實務指南

版本 1.0

2021年5月

分發

副本編號	持有人
1	香港生產力促進局 (HKPC)
2	香港社會服務聯會 (HKCSS) 資訊科技資源中心 (ITRC)

版本記錄

版本	更新日期	說明	文檔名稱
1.0	20201 年 5 月	正式版本	香港社福界資訊科技保安實務指引 版本 1.0 (20210517)

擬備： 顧問團隊 核准：

香港生產力促進局

日期： 2021 年 5 月 日期：

目錄

參考表格

圖參考

前言

資訊科技和互聯網的快速發展徹底改變了我們的生活和工作方式。電腦科技在現代社會中除了帶來許多好處之外，但同時亦帶來了漏洞，因此電腦世界資訊安全問題亦應為所有電腦使用人士所關注。

非政府組織(Non-Government Organisation, NGO)，服務主要致力於特定社群，日常營運基金部分來源自外界資助及私人捐款，營運成本控制亦很重要， 組織機構負責人、管理層和員工都努力朝著這些目標方向前進。

非政府組織的運作和策略性應用都依靠資訊科技(Information Technology, IT)，很多大、中、小型非政府組織和商業企業在這方面分別不大，在許多社福界非政府組織中都有機會需要處理敏感資訊以及個人識別資訊（Personally Identifiable Information, PII）。對於非政府組織而言需要確保自身、員工數據和系統免受網絡攻擊的威脅，確保所持有機密資訊內容遭受不當存取或洩漏（機密性）、刪改（完整性）或失去（可用性）免受網路安全威脅實在非常重要。

非政府組織通常專注於利用資訊科技來支援其運作和服務。它們只會在發生大規模或嚴重的保安事故後，才會關注保安風險的問題。大多數香港企業在處理資訊科技保安方面較為成熟，但非政府組織在實現同等的安全級別方面仍然遠遠落後。其實社福界非政府組織可藉執行一些相應項目，以達到合理安全可控水平。

非政府組織中常見的資訊科技保安弱點有：

- 缺乏資訊科技和資訊保安的專業知識
- 資訊科技資源和優先次序
- 缺乏資訊科技合規和監管要求
- 資訊保安意識

1. 簡介

對積極主動的資訊保安管理方法的認可，維護穩定運作和資訊完整性的保護對非政府組織及相關人士之利益十分重要性，本「資訊科技保安實踐指引」制定了一種以風險為基礎的組織自我提升資訊保安方法 — 包括根據行業標準以及最佳作法，幫助香港社福界提供資訊科技保安的建議。

本指引目的是提供非政府組織使用具有成本效益的保安控制和風險管理技術，使其能自行根據本身需要制定和量化機構資訊保安規劃的能力。對於小型的非政府組織而言，本指引有助於他們了解如何為電腦系統和網絡提供基本保安功能、提高機構內部的保安意識以及如何保護社福界服務機構內的敏感訊息。對於大型的非政府組織而言，本指引提供了具成本效益的方式，可以根據機構的業務需要保護電腦系統，而無需對其業務執行額外的保安控制監管要求。

本指引中的主要論點包括：

- 具備有力領導的管治框架對於增強機構的資訊科技保安乃屬必需。董事會和高級管理層的參與對於在非政府組織的資訊科技保安控制以及為其賦予明確的權責層級等乃關鍵要素。

- 具有良好保安意識的員工可以作為抵禦網絡攻擊的第一道防線。有效的培訓可避免人員無意間成為網絡攻擊媒介（例如，因為無意中下載了惡意軟件），有助於降低攻擊成功的可能性。

- 個別非政府組織所採用的保安技術控制的複雜程度在很大程度上取決於其情況。雖然較小的非政府組織可能無法完全實施當中所需的控制，但是這些安全策略也可提供關鍵性的檢測指標從而以了解相關漏洞對應行業標準。

- 非政府組織經常使用第三方供應商提供資訊科技服務，例如雲運算服務和應用程式開發/支援服務等，就此供應商會有機會存取相關方面的敏感和機密訊息，例如服務用戶、員工或其他有關方面的個人資料，或者遠程訪問其系統。非政府組織應透過進行嚴格的盡職調查並制定清晰的操作和驗證政策來管理由這些連繫所引起的相關網絡保安風險。

本操作指引屬一般指引性質，其內容未必適用於所有情況。本指引旨在作為一份動態文件，會隨著業界在實施中反映的意見而不斷更新和完善。在向非政府組織分發本文件的早期階段中，我們所汲取的建議將被整合到將來的版本中。這將確保該文件在不斷變化的威脅和不斷創新的解決方案下持續滿足非政府組織的需求。

非政府組織在參考此指引時，需根據自身機構的目前情況、現有程序、資源、資訊及系統環境等因素作出合理判斷。若機構在採用此指引期間產生任何問題或未能滿足指引中的保安要求，香港社會服務聯會 (Hong Kong Council of Social Service, HKCSS)並不會負上任何責任。

本指引內容一覽

第1章	簡介本指引的建立源由及主旨。
第2章	概述了資訊科技保安對非政府組織的日常運作的重要性，以及本指引可如何助其發展成為具備資訊科技適應力的機構。
第3章	閱讀本指引的目標讀者群。
第4章	將不同的利益相關者引導到第 7 章的相應部分，以便了解 17 個資訊科技保安領域中的最佳行事方式。
第5章	為讀者提供了解資訊科技保安實踐框架的基本參考資訊。
第6章	介紹了保安設定的概念，並展示如何利用資訊科技評估範本進行資產風險評估。
第7章	展示每個資訊保安領域的最佳行事方式，以及各項保安操作所對應的恰當安全級別。
第8章	推薦的資訊模板及範本。
第9章	推薦給資訊科技團隊的網絡保安風險評估工具。

2. 非政府組織資訊科技保安概述

過去非政府組織對於網絡保安和數據私隱的重視程度一般相對較低。但是隨著時代變遷，非政府組織所面對的風險越來越高。系統入侵、資料外洩和網絡攻擊都是機構所面對的威脅，會擾亂非政府組織的日常運作和服務，使其承擔不必要的責任並破壞其努力建立起來的聲譽。

因此，非政府組織現在也開始重視資訊科技保安。然而，許多機構仍不了解應如何應對網絡風險。面對當今不斷變化的網絡環境，它們通常不知道如何制定能應付當前需要應對網絡保安及數據保護政策的挑戰。即使制定了政策，執行起來也常常不一致。非政府組織通常缺乏能有效實施網絡保安和隱私保護所需的預算、人力資源或管理時間，這使得它們的工作比商業或公共部門機構的工作困難得多。

為了能最大程度地減少這種風險，非政府組織應制定政策，以納入災難事故復原能力的概念，亦即可抵禦天然、人為和網絡威脅的能力。具體來說，他們應該努力確保資訊科技系統的保安和資料保密能力，以減少使其受益人、員工或資金捐助者遭受網絡攻擊的機會。機構首先需要自問兩個基本問題：

1. 機構自身是否有能力保護其員工和受益人免受惡意網絡攻擊？
2. 機構是否已準備好滿足日益嚴格的個人私隱保護要求，並了解到就一旦私隱保護出現不合規時各國施加的嚴厲罰則和捐贈者會繼續支持？

網絡保安並不艱難，只是較為繁瑣。網絡保安所面臨的挑戰是要以完整而全面的方式完成此等要求及其他相關工作，同時確保基本業務運作順暢。

網絡保安不僅是資訊問題，也是整個企業的問題，需要跨範疇並全面執行治理承諾，以確保業務的各個方面保持一致以支持有效實踐網絡保安。

在最理想的情況下，非政府組織應該定期評估其資訊科技保安，作為對所有業務系統進行更大範圍審查的工作一部分。這樣做的目的是確保其科技部件和流程與其業務策略保持同步。

本指引旨在幫助非政府組織應對網絡保安的各種挑戰，並幫助他們發展成為在資訊科技方面具備彈性的機構。它指出非政府組織所面臨的主要網絡保安和數據保護的困難，並引領非政府組織踏出第一步，加強網絡保安和數據保護。

3. 目標讀者群

本指引為機構高層管理人員、資訊保安專業人員，以及資訊和通信技術管理者提供準則，以制定和實施機構的最佳資訊科技保安實踐和指引。

非政府組織資訊科技人員可以通過閱讀指引所載的保安調控機制而得益的包括：

- 擁有存取系統權限的人員，包括一般用戶；
- 承擔資訊系統、網絡保安及風險管理及負責各監督職責的人員（例如首席資訊科技總監，高級資訊保安人員，資訊系統經理，及資訊保安經理）；
- 負責資訊系統開發的人員（例如項目經理，系統設計人員和開發人員，資訊保安工程師，系統整合服務商）；
- 負責資訊保安措施實施和運作人士（例如任務／業務擁有者，資訊系統擁有者，資訊擁有者／管理員，系統管理員，資訊系統保安人員）；和
- 負責資訊保安評估和監控人士（例如審計人員，系統評估人員，評核人員，獨立驗證人員／確認人員，分析員，資訊系統所有者）。

4. 保安領域和利益相關者

儘管機構中的每個人都在發揮自己抵禦網絡攻擊方面的作用，但是在每個保安領域裡都應有其相對應的網絡保安主要的利益相關者。本指引提供了有關十七個保安的良好實踐。下表列出每個保安領域的建議和利益相關者，亦推薦利益相關者深入研究相關的保安領域，或指派相關員工遵循對應的好做法，以管理好所有網絡保安領域的風險。

#	資訊科技保安領域	利益相關者	
		管理層	資訊科技/保安
7.1	資訊科技保安管治		
	7.1.1 資訊科技保安政策及程序	✓	
	7.1.2 資產管理和維護	✓	
	7.1.3 資訊分類	✓	
	7.1.4 資訊處理	✓	
	7.1.5 資產配置管理	✓	✓
	7.1.6 支援和技術勝任	✓	✓
7.2	密碼控制和驗證		
	7.2.1 傳統密碼控制	✓	✓
	7.2.2 NIST 推薦的新密碼控制方式	✓	✓
	7.2.3 驗證		✓
7.3	網站和網上應用程式		✓
7.4	數據管理		
	7.4.1 數據保安		✓
	7.4.2 數據庫保安		✓
	7.4.3 保護敏感的個人數據	✓	✓
7.5	電腦網絡保安		✓
7.6	電郵保安	✓	✓
7.7	雲端運算保安		
	7.7.1 雲端運算和數據保安	✓	✓
	7.7.2 避免雲端供應商鎖定	✓	✓
7.8	實體安全	✓	✓
7.9	流動保安		
	7.9.1 流動設備保安	✓	✓
	7.9.2 便攜式存儲保安	✓	✓
7.10	遠端訪問／在家工作	✓	✓
7.11	保安風險評估與審計	✓	✓
7.12	內部威脅	✓	✓
7.13	供應商管理	✓	
7.14	保安意識和培訓	✓	✓
7.15	保安事故回應管理	✓	✓
7.16	業務持續性運作管理	✓	✓
7.17	日誌管理與監控	✓	✓

表 1: 資訊科技保安領域

5. 資訊科技保安實踐框架

本指南旨在為非政府組織提供實用建議，以讓其做好更佳準備，從而保護機構免受網絡保安威脅。

讀者應注意，本指引無意成為有關資訊科技保安和數據保護的全面指引，當中所記載之常見做法和建議不一定可代表或適用於所有個案。

每個非政府組織都需要詳細檢查其運作情況，並選定最可行和最適合本身的保安措施。非政府組織可在必要時尋求有關資訊科技保安的專業建議和服務。

構成以下文件，原則和最佳行事方式的基礎參考基準如下：

- ISO 27001[1]標準提供了一組保安控制的最佳行事方式， 各機構可按本身所面臨風險有系統實施，以達致(經外部審核及核證所認定之) 合規性。
- 美國國家標準暨技術研究院National Institute of Standards and Technology (NIST) 網絡保安框架[2] Cyber Security Framework （CSF）提供了一種全面程序化的方式，可適用於任何機構的需求。該標準還可以通過與許多其他標準和框架集成擴展，包括 NIST 網絡保安框架 和 NIST 風險管理框架[3] Risk Management Framework (RMF)。
- 該NISTIR使用提升關鍵基礎設施資通訊保安之框架 （CSF）作為機構網絡保安風險管理流程和程序的範本，亦為 NIST 小型企業資訊保安基礎知識[4] NISTIR 7621r1。
- 《個人資料（私隱）條例》（Personal Data (Privacy）Amendment Ordinance 2012, PDPO）適用於私營部門和公共部門。它是技術中立且建基於原則上的。數據保護原則（Data Protection Principles, DPPs 或 DPP）概述了數據用戶應如何收集，處理，保全和使用個人數據，並輔以其他規定以達到進一步合規性要求的條款[5]。

96

[1] ISO/IEC 27001:2013 Information Security Management System (ISMS) https://www.iso.org/standard/54534.html

[2] National Institute of Standards and Technology (Cybersecurity Framework), NIST (CSF) version 1.1 https://www.nist.gov/cyberframework

[3] NIST Cyber Security Risk Management Framework version 1.1 https://www.nist.gov/cyberframework/risk-management-framework

[4] NIST Small Business Information Security: The Fundamentals (NISTIR 7621) https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

[5] Security and Privacy Controls for Code of Practice, Hong Kong – PDPO Cap 486., PCPD https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

6. 資訊科技資產估值

6.1. 保安狀況 [初級，中級，高級][6]

為了了解系統保安，我們必須首先知道系統有機會面對到的風險。本指引的目的是由管理和技術角度出發，為非政府組織提供有關常見資訊科技保安注意事項和最佳行事方式。

各機構可以考慮利用以下標準來評估其資訊資產（例如：伺服器，系統，應用程式，資料等）。

六種正式資訊評估模型			
基本措施 集中關注於改進方面 資訊管理形式		財務措施 集中關注於改進方面 資訊的經濟利益	
內在價值	該資產／資料的正確性，完整性和獨特性如何？ *例如具備重要樣本數量，及能帶來見解的高質量的研究數據。*	成本價值	如遺失此等資產／資料，會損失多少金錢／資源？ *例如系統恢復和重新輸入數據的時間和人力成本。* *系統故障或數據洩露時的補救措施和法律責任成本。*
商業價值	該資產／數據對於特定目的切身程度及有多大關聯？ *例如捐贈者用於經常性捐贈的銀行賬戶訊息。*	市場價值	出售該項資產／資料有什麼好處？
績效價值	該資產／數據如何影響推動關鍵業務？ *例如用於正在進行服務開發的服務統計*	經濟價值	該資產／數據如何為我們的利潤做出貢獻？

表 2: 六種正式資訊評估模型

96

[6] 8.1 資訊科技資產評估清單範本

我們建議每個非政府組織先選擇一項安全級別—**初級，中級**或**高級**。我們假設**初級**水平是一般非政府組織的默認慣常保安做法，非政府組織應遵守相關安全級別所屬要求。

初級水平是一般非政府組織所應對其系統實施的最基本的保安要求，而若非政府組織認為他們的系統需要額外的保護，則可以採用**中級水平**措施。至於**高級水平**則應對性質既敏感且關鍵，一旦遭入侵則可導致嚴重後果的系統實施。

具備**初級水平**的非政府組織亦可以選擇對某些關鍵系統採用更高的保安措施（**中級**或**高級**）。但是，它不會改變機構的整體安全級別。而非政府組織甚至可以將更高級別的**安全級別**訂為目標，並制定改進計劃以提高其安全級別。

有時非政府組織會希望提升其安全級別到**中級**甚至**高級**水平，但如何得知目前系統的安全級別是一個問題。

非政府組織對於它們的系統是否需要達到**中級**甚至**高級**安全級別存有疑問。資訊科技資產評估模板是一種方便簡易的方式以評估目前系統所需的安全級別。請在第6.2節資訊科技資產估值中找到有關資訊科技資產評估模板的詳細信息。

資訊科技資產評估範本會要求機構輸入六個系統屬性：「資產價值」、「資料分類」、「保安風險評估」、「系統更新」、「復原力」和「存取人士」以推算出系統的安全級別要求。

資訊科技資產評估範本是非政府組織用來評估系統安全級別要求的工具。系統可以是一個設備（如伺服器或數據庫），也可以是系統中的一組設備（例如：伺服器組合或雲端平台）。

6.2. 資訊科技資產評估範本

了解公司資產的價值是網絡保安風險管理的基礎，必須先了解其真實估值才可應用適當保安措施。

本指引將使用資訊科技資產評估範本[7]來確定資訊資產的價值，該範本特別為非政府組織而設計，用於評估資訊資產的風險水平和保護要求。

本資訊科技資產評估範本可自行解讀，用戶可以在這些欄位上以自由格式輸入資訊資產的資料，例如資產編號，資產資訊，描述，參考，位置。

用戶將資訊科技資產的屬性輸入到 F 欄到 K 欄，然後資訊科技資產評估範本將根據用戶輸入的資料，量度資產的威脅、影響和可能性，如表3：資訊科技資產屬性和風險組成部分。

資訊科技資產評估範本之後將評估出「初級」，「中級」和「高級」安全級別的保護要求。

資訊科技資產評估範本內容 (以風險為基礎)				
#	欄目名	說明	輸入數值	分類
A	資產編號	資訊資產編號。	自由格式	
B	資產資料	基本的資產資訊，例如資產標籤，內部 / 外部 IP 地址等。	自由格式	
C	資產描述	描述資產的詳情。資訊資產可以具有許多不同的形式、例如伺服器、數據、紙質文件等。	自由格式	資產說明
D	參考	資訊資產參考資料，例如序列號或許可證號，有效期。	自由格式	
E	位置	資訊資產運作或存儲的位置。	自由格式	
F	*資產價值	資產價值可以通過定性或定量的方式進行度量。	低，中， 高，極高	
G	*資產分類 (保密性)	資訊資產的分類/保密水平。	公開，內部，受限制，機密	屬性評級
H	*保安風險評估	系統執行的資訊保安風險評估的頻率	定期，	

96

[7] 8.1 資訊科技資產評估清單範本

資訊科技資產評估範本內容 (以風險為基礎)				
			3年以上，一次，無計劃	
I	*系統更新 (資料完整性)	系統更新修補程式或操作系統升級的頻率/資訊資產的完整性水平	定期，具計劃，過時，不確定	
J	*復原能力 (可用性)	資訊資產的系統彈性/可用性水平（例如：備份，演習測試，高可用性等）	高可用性，經過演習測試，擁有備份， 不可使用	
K	*存取人士	哪些實體和機構可以存取	內部，公開，內部與合作夥伴， 內部和公眾	
L	後果嚴重性 (影響程度)	資訊資產的評估威脅水平。（“保安風險評估”和“系統修補程式”得分的總和）	極高 高，中至 低，極低	
M	脆弱性 (威脅程度)	如保安漏洞被利用時可能導致的整體傷害或損失的後果/影響水平。（“資產價值”和“資訊分類”得分的總和）	極高 高，中至 低，極低	
N	出現風險 (可能性)	有關威脅會利用資訊資產的脆弱性的概率/可能性。（“可存取性”和“彈性”得分的總和）	極高 高，中至 低，極低	
O	保安評分	資訊科技資產基於其屬性的整體風險水平之總和。	3 ~ 15	保安評分
P	初級 (3 - 7)	非政府組織應對這些系統實施初級水平的技術和/或行政保安控制。	3 ~ 7	安全級別
Q	中級 (8 - 11)	非政府組織應對這些系統實施中級水平的技術和/或行政保安控制。	8 ~ 11	
R	高級 (12 - 15)	非政府組織應對這些系統實施高級水平的技術和/或行政保安控制。	12 ~ 15	
*資訊資產屬性				

表 3: 資訊科技資產評估範本內容

		影響級別（Impact）			
資產價值	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8
		1	2	3	4
		資料分類			

表 4: 影響級別程度 = 資產價值和資產分類（機密性）

		威脅級別 （Threat）			
系統更新	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8
		1	2	3	4
		保安風險評估			

表 5: 威脅級別程度 = 保安風險評估和系統更新（完整性）

		概率級別（Likelihood）			
復原能力	1	2	3	4	5
	2	3	4	5	6
	3	4	5	6	7
	4	5	6	7	8
		1	2	3	4
		存取人士			

表 6: 概率級別程度 = 可存取性和彈性（可用性）

欄目名	資訊科技資產屬性(1 ~ 4 級)	風險部份
F	*資產價值	影響程度 = 資產價值和資料分類
G	*資產分類（保密性）	
H	*保安風險評估（SRA）	威脅程度 = 保安風險評估和系統更新
I	*系統更新（資料完整性）	
J	*復原能力（可用性）	可能性 = 復原能力及存取人士
K	*存取人士	

表 7: 資訊科技資產屬性及風險部份

釐定足夠安全級別			
安全級別	影響，威脅，可能性	定義	顏色代碼
初級	保安評分 3 ~ 7分	大多數非政府組織應採用這些做法作為資訊保安要求中的最低控制手段。此保安級別充分利用有限的資源，尤其是對於小型非政府組織而言最有幫助。 例如，對於小型機構而來說，它們可能經常缺乏某種特定資訊科技支援，而其技術距離可能不止於保安以及其他，在這種情況下，建議遵循初級的良好做法。	✓
中級	保安評分 8 ~ 11分	機構中的所有資訊科技術資產和數據無須以相同的方式保護。 採用中等級別可以幫助非政府組織優先為其風險排序，並以足夠的資源提高資訊安全級別。	✓
高級	保安評分 12 ~ 15分	非政府組織所使用的技術越先進，並不意味著它們越安全。當非政府組織推出更多的資訊科技產品/服務時，它可能會受到更多的保安威脅。 此外，組織內部威脅是網絡保安中的大問題之一，這內部威脅引至了很大部份的攻擊來自內部而導至財務和聲譽的損失。 在這種情況下，非政府組織需更全面地考慮網絡保安，建議非政府組織採用高級別的保安良好做法。	✓

表 8: 資訊科技資產保護安全級別

下表列出三種不同場景

		非政府組織和公共網絡服務			跨非政府組織網絡服務			非政府組織內部網絡服務	
屬性	水平	比重	#		比重	#		比重	#
*資產值	1 ~ 4	高	4		高	4		高	4
*資產分類	1 ~ 4	內部	2		限閱	3		機密	4
*保安風險評估	1 ~ 4	一次	3		一次	3		一次	3
*系統更新	1 ~ 4	過時	3		過時	3		過時	3
*復原能力	1 ~ 4	備份	3		備份	3		備份	3
*存取人士	1 ~ 4	內部和公眾	4		內部與合作夥伴	3		內部	1
後果 (影響)	1 ~ 5	高	4		極高	5		極高	5
脆弱性 (威脅度)	1 ~ 5	高	4		高	4		高	4
機會率 (可能性)	1 ~ 5	極高	5		高	4		低	2
基準評分		高級	13		高級	13		中級	11

表 9: 基準評分範例

7. 非政府組織的資訊科技保安實踐

7.1. 資訊科技保安管治

資訊科技保安管治對任何業務都至關重要，因為資訊科技保安管治不但為預算，服務能力和新技術所必須，還有助於為一旦出現事故時做好準備。資訊科技保安管治領域的疏忽可能會導致董事會成員、董事或合作夥伴需要對違規行為、聲譽受損、甚至財務損失負責。資訊科技保安管治框架有助於概述非政府組織所要實現的目標、服務標準或框架。

為了減輕網絡攻擊的風險，非政府組織必須有效地執行工作流程和具有良好的網絡保安管治方針。例如，透過定期覆核審計日誌，可以發現在非正常時間內對特定文件的異常頻繁搜尋，從而警醒非政府組織保安人員進一步調查情況。

資訊科技保安管治涵蓋了整個機構及作出指導，管控和追究責任的流程。它包括機構中人員在系統行使的權限、問責、領導、指引和控制。只要在整個機構中執行良好的資訊科技保安管治原則和做法，就可排除萬難，這就是管治是至關重要的原因。

資訊科技管治包括以下領域：

- 資訊科技保安政策和程序
- 資產管理與維護
- 資訊分類
- 資訊處理
- 資產配置管理
- 支援與技術勝任

7.1.1 資訊科技保安政策和程序

資訊科技保安政策（Information Technology Security Policies, ITSP）是一組由機構制定的規則，以確保機構內的所有人士都須遵守按其權限範圍內對電子資訊的保安規定。

ITSP是管治如何保護資訊，這是機構所需要保護的眾多資產之一。機構需盡力協調各方期望，並對條款達成共識。

正確的資訊保安文件會包括五個主要部分：

（1）貫徹管理層意願的政策

（2）確立控制目標以滿足應有條件

（3）確立標準以列明所需達到的量化要求

（4）制定如何執行任務的程序

（5）建議但非強制性的指引

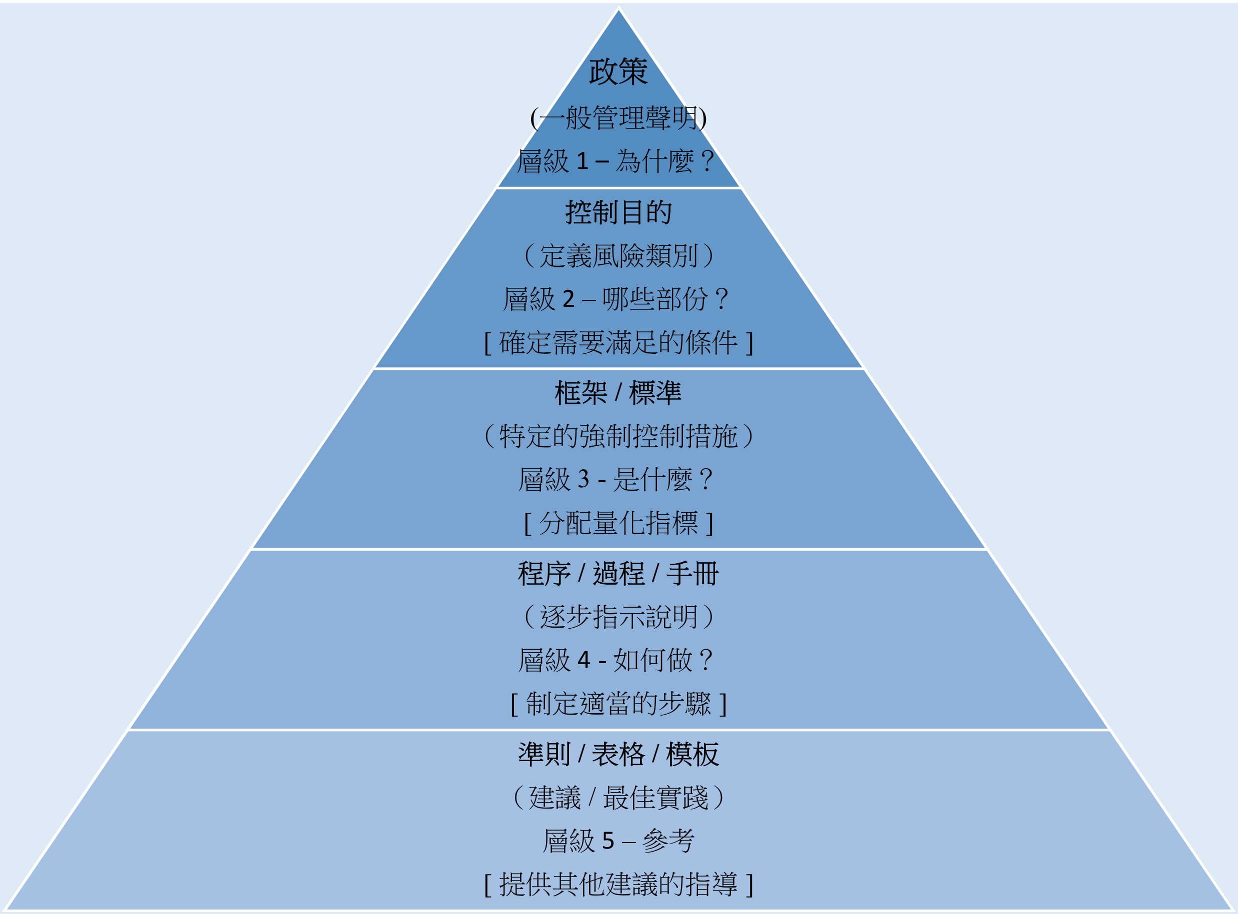


圖 1: 政策，標準，程序和準則之分層結構

機構的資訊科技保安政策、標準和程序應適用於所有員工、承包商、分包商以及與機構有任何處理、傳輸、存儲或刪除數據的簽約關係的第三方機構。

保安政策和程序	利益相關者：管理層			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	建立並執行資訊科技保安政策和相關程序。	✓	✓	✓
2	資訊科技保安政策應包括以下方面的要求： • 機構經營策略 • 機構治理和保安職能的分工責任 • 為機構提供服務的機構及相關第三方的保安和隱私的覆蓋範圍 • 機構管理層有責任去建立保安和業務持續性的文化 • 業務部門要負責評估和保護其系統保安和隱私的影響並採取相關措施應對 • 員工疏忽大意時或濫用的紀律處分 • 訂立法律、法規和合同規條及其實施細則 • 當前和預計環境的資訊保安威脅	✓	✓	✓
3	資訊保安政策應包含以下有關內容的陳述： • 訂立資訊保安目的和原則提供指引與所有資訊保安有關的活動 • 將資訊保安管理的一般和特定職責分配給已清楚訂明職能的單位 • 訂立一旦出現偏差和異常情況時作出處理的流程	✓	✓	✓
4	政策宜簡明扼要，主旨傳達了指導機構內部活動的原則。	✓	✓	✓
5	資訊科技保安政策必須簡潔，易讀，可操作，可執行和靈活等。	✓	✓	✓
6	修訂後的政策經管理層批准後應盡快發放給所有成員。	✓	✓	✓

7	資訊保安政策應由特定項目所支援，例如： a) 存取控制 b) 資訊分類和處理 c) 實體安全和環境保安 d) 與最終用戶相關的主題，例如： • 資產合理使用政策 • 清空桌面和屏幕政策 • 資料傳輸 • 流動設備和遠程辦公 • 對軟件安裝和使用的限制 e) 備份 f) 資料傳輸 g) 防範惡意軟件 h) 技術漏洞的管理 i) 加密控制 j) 通訊保安 k) 隱私和個人身份資訊的保護 l) 供應商關係 m) 遵從法規	✓	✓	✓
8	所有員工都應可取得保安政策和有關程序內容。	✓	✓	✓
9	各級員工均應知曉並接受保安政策內容，清楚理解應如何以機構的最大利益行事。	✓	✓	✓
10	非政府組織應遵守法律和法規要求，包括：數據保護，知識產權和版權，並確保滿足這些要求。	✓	✓	✓
11	非政府組織應定期審查和更新各類政策和程序。		✓	✓
12	定義管理層的職責，以確保所有員工在其工作期間都受到工作安全保護。		✓	✓
13	機構私隱政策中的適用資訊應納入至保安培訓活動中。		✓	✓
14	訂立正式違反保安政策的員工紀律處分程序。		✓	✓
15	評估並履行合規性和監管義務。這意味著機構理解和會執行直接適用於非政府組織的網絡保安相關的合規性和監管職責。		✓	✓

表 10: 保安政策和程序

7.1.2 資產管理與維護

非政府織中的資訊科技基建通常由各種硬件和軟件組成，例如應用程式，網絡設備和伺服器等。資訊科技資產清單可確保資產實施了有效保障並能知悉哪些資產遺失。

資訊科技資產包括硬件、軟件、數據和服務。它們必需被妥善管理，以防止出現如機密性受侵犯、喪失完整性、不能使用和不合規等後果。機構應定期審查庫存項目，以確保資產妥為擁有，保管和維護。制定資產清單是為了了解現正保存那些分類資訊以及誰應對此負責（即誰是資產擁有者）。

資產管理與維護		利益相關者: 管理層		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	制定準確的資訊科技資產清單並保持更新。機構應識別所有資產並記錄這些資產的重要性。	✓	✓	✓
2	所有硬件和軟件必須保有記錄（操作系統、中介軟件、應用程式等）。	✓	✓	✓
3	定期更新操作系統、固件、中介軟件和應用程式。	✓	✓	✓
4	按資訊科技產品供應商建議，確保系統及應用程式的重要性分類適時安裝相稱的保安修補。	✓	✓	✓
5	確保系統硬件和軟件的維護及升級安排由勝任技術人員執行，而且在進行維護或修理操作時，受影響的保安監控措施仍須正常運作。	✓	✓	✓
6	記錄資訊系統連接至互聯網及所有合作夥伴（供應商、銷售合作夥伴等）的網絡連接設定。		✓	✓
7	每年將已經登記了的資產清單與實際情況進行盤點審核以確保資產數量正確。		✓	✓
8	識別所需要保護的資產，以及它們會面對的威脅和風險。		✓	✓
9	資產清單內容應資產類型、格式、位置、備份資訊、授權許可資訊和商業務價值，以便災難復原時能夠提供必要所需的資訊。		✓	✓
10	非政府組織要有資產標籤系統為每項資產分配其唯一的資產標籤，確保可以在資產的生命週期內以此標籤加以識別。		✓	✓
11	建立特權帳戶記錄的詳細清單並確保定時更新。		✓	✓

12	利用自動化機制如監控程式來檢測資訊科技系統中是否有用戶安裝未經授權的軟件，並通知負責的管理人員。			✓

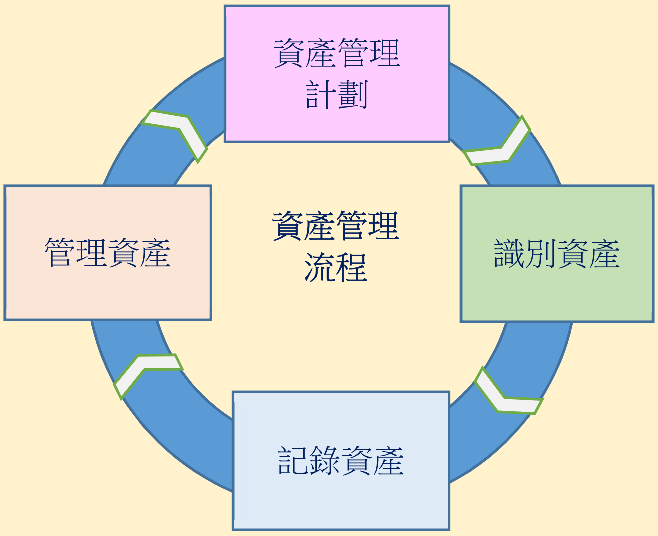


圖 2: 資產管理工作流程

表 11: 資產管理與維護

<u>相關工具：</u>
8.1 資訊科技資產評估清單範本
9.1 WINAUDIT 電腦軟硬體檢測工具

7.1.3 資訊分類

資訊保安標準指引如 ISO 27001建議應根據資訊的敏感程度對資訊進行保安等級分類和標記。資產擁有者應為每個資訊資產類別指定保安分類，並根據機構定義的分類反映資產的敏感程度。

要求非政府組織在整個機構中實施統一的資訊保安分類系統一開始可能會有一定困難，但依然建議機構對有關的機密文件，文件夾，檔案，電子郵件等進行相應的分類標記。

以下是資訊分類處理流程做法：

1. 在資產清單中輸入資產及詳細資訊
2. 定義資訊保安等級分類
3. 定義資訊保安等級分類標籤
4. 資訊處理方法

資訊分類	利益相關者: 管理層			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	該方案中的保護級別分類應通過分析資訊的機密性，完整性和可用性以及任何其他要求來進行評估。 機密資訊有不同的形式和類型的媒體分類，例如： a) 電子文件 b) 資訊系統/數據庫 c) 紙質文件 d) 儲存媒介（例如磁盤，USB可攜儲存裝置等） e) 口頭或通過電子郵件發送的資訊	✓	✓	✓
2	機構在進行資訊分類時，建議可按下表中的分類級別歸類為 4 個層級或以內。（見表 12）	✓	✓	✓
3	資訊分類方案應與存取控制策略保持一致。	✓	✓	✓
4	資訊分類方案應包括約定的分類和規範准則以作為評核標準。	✓	✓	✓

4 級	3 級	2 級
公眾	公眾	公眾
內部	內部	機密
限閱	機密	機密
機密	機密	機密

表 12: 建議的資訊分類對照表

<table>
<tr>
<td>5</td>
<td>定義資訊分類方案級別的建議（以下例子可供參考）：

機密（最高機密級別）
限閱（中等保密級別）
公眾（所有人都可以看到該資訊）
內部（一般級別的保密性）

<table>
<tr><th colspan="3">資訊分類標準例子</th></tr>
<tr><td>1</td><td>公眾</td><td>此類別包括沒有任何保密性要求或向公眾傳播的資訊資產。

例子：該組織對外公開的年度財務報告和在該組織的公開網站上所顯示的資訊</td></tr>
<tr><td>2</td><td>內部</td><td>此類別包括可以在組織，業務合作夥伴或承包商內部存取的資訊資產。

例子：辦公室命令和內部通函，部門間備忘錄，內部政策和程序</td></tr>
<tr><td>3</td><td>限閱</td><td>此類別包括特定部門、分部、單位、項目團隊或業務流程所需數據的資訊資產。此等資訊資產應僅可由相關單位、項目或業務流程的成員存取。

例子：客戶的個人和敏感資料檔案</td></tr>
<tr><td>4</td><td>機密</td><td>此類別包括具有高機密性的資訊資產。只有一組有限數目的授權用戶才能取用這些資訊資產。

例子：個人醫療檔案及工傷檔案</td></tr>
</table>
表 13: 資訊分類定義</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>資訊分類等級應根據資產其在生命週期中的價值、敏感性和重要性變化而更新。</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</table>

表 14: 資訊分類

7.1.4 資訊處理

非政府組織，團體和員工應有系統地妥善保管資訊，並確保職責能正確地分配及執行。

資訊處理	利益相關者: 管理層			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	確保提供培訓、指導和支援給負責保安處理資訊的人員。	✓	✓	✓
2	確保資訊擁有者和負責處理資訊的人員對保安要求，期望和局限性有同樣的理解。	✓	✓	✓
3	確保持續管理資訊數據，直到其被銷毀或責任轉移到另一個機構為止。	✓	✓	✓
4	一旦機構定義了資訊保安分類，就需要根據其保安分類級別分配適當的保安分類標籤。 通常分配資訊保安標籤是由資產擁有者的負責。	✓	✓	✓
5	應為每個分類級別制定處理程序，包括保安處理流程、儲存、傳輸、解密和銷毀。 當中應包括制定日誌記錄和任何與保安事故相關的證物保管規範。 （見下表 15）		✓	✓
6	當與其他機構進行資訊共享時，應在合約中列出資訊分類及資訊標籤的程序。		✓	✓
7	監控和維護 — 定期審查和完善資訊分類和處理程序，並在必要時進行更改。		✓	✓

	公眾	內部	限閱	機密
機構文件	✓	✓		
電子文件	✓	✓		
資訊系統		✓	✓	
儲存媒介		✓	✓	
口頭說話資訊		✓	✓	
電子郵件		✓	✓	✓

表 15: 資產總類處理範例

表 16: 資訊處理

7.1.5 資產配置管理

資產配置管理是指系統化地處理組織變更的方法，以有效地應對改變和運用可能產生的機會。它包括適應變更，控制變更並面對新變更的影響。

資產配置管理		利益相關者: 管理層, 資訊科技人員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	制定資產配置管理計劃（包括 配置任務，時間表，職責，權限，預算，資源，所需資訊等）	✓	✓	✓
2	制定變更管理流程，其中包括變更範圍，目標，影響，理由，回復方案，風險評估和批准授權。所有變更請求和報告應記錄在案。	✓	✓	✓
3	讓計劃相關人士適度參與配置變更過程。	✓	✓	✓
4	制定溝通計劃，其中顧及機構中可能需要知會的相關人士（客戶，外部服務提供者，其他相關人員等）。	✓	✓	✓
5	實施變更 — 與相關方的活動進行變更協調，以達到變更管理目標。	✓	✓	✓
6	衡量或確定變更的有效性。	✓	✓	✓
7	記錄最終變更結果（成功，失敗，回復，取消等）以進行審核。		✓	✓
8	從失敗和成功中學到教訓。獲得和分享沒有書面記載的知識和經驗。以改進流程、產品和服務的成果。		✓	✓
9	培訓人員 — 確定從事相關工作的人員具備所需的才能，透過這些管控能改進質量管理體系的績效和有效性。		✓	✓
10	透過跨職能團隊審查變更實施計劃，以提供和計劃相關風險的意見反映。			✓

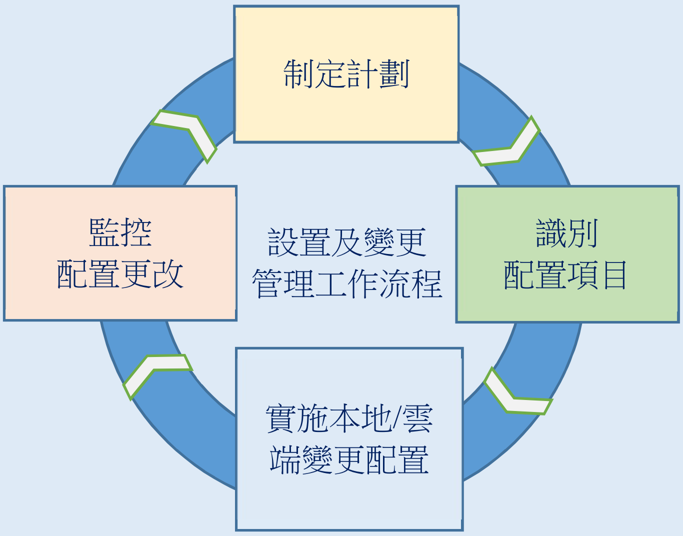


圖 3: 配置及變更管理工作流程

表 17: 資產配置管理

<u>相關工具：</u>
8.3　　供應商風險評估清單
錯誤! 找不到參照來源。　　網絡保安的七大習慣

7.1.6 支援與技術勝任

沒有組織能夠避免於網絡犯罪，這意味著所有人都需要將保安放在第一位。 成功的資訊保安專業人員所需的不僅是技術能力。他們若要在該領域繼續發展，應同時兼為戰略家，溝通者及終身學習者。

支援和技術勝任	利益相關者:管理層，資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	提供足夠資源給資訊保安管理活動。	✓	✓	✓
2	非政府組織應確定並提供建立、實施、維護和持續改進資訊保安管理系統所需的資源。	✓	✓	✓
3	確定所須要的工作人員必要的技術能力，因這些能力會影響在其控制下的資訊保安工作性能。	✓	✓	✓
4	確保有關技術勝任人員擁有合適的教育程度，培訓和經驗。	✓	✓	✓
5	各級管理人員應給予明確支持和投入。	✓	✓	✓
6	向所有管理人員、員工和其他相關方面分發有關資訊保安政策和機構標準的指引。	✓	✓	✓
7	向所有管理人員、員工和其他相關方有效地推廣資訊保安，以提高其保安意識。		✓	✓
8	提供適當的保安意識、培訓和教育。		✓	✓
9	保留適當的書面紀錄資訊作為才能證明。		✓	✓

表 18: 支援與技術勝任

7.2. 密碼控制和驗證

身份驗證，授權和密碼指引適用於其電腦系統上的任何電腦帳戶，任何使用電腦系統的用戶，以及系統管理員或程式開發人員都需要以密碼進行身份驗證和系統授權的。

7.2.1 傳統密碼控制

傳統密碼控制	利益相關者:管理層，資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	確保透過所有資訊科技來管理授權存取，並確保為所有層面級別設定存取監控機制以提高資訊保安性，這包括管控通過外部網絡連接到資訊科技系統的遙距用戶遠程登入。	✓	✓	✓
2	告知用戶不應把密碼以紙張記下（不論書寫或其他方法）以及張貼密碼至電腦或其他設備上，或與其他用戶分享密碼。	✓	✓	✓
3	基於一旦數據洩露所造成的損害風險，選用合適的身份驗證方法（無論是單因素驗證還是多重驗證）。	✓	✓	✓
4	確保用戶使用高強度密碼，例如長度至少為八（8）個或更多字符，最好包含至少一個字母字符，一個數字字符以及小寫和大寫字母。 另外，鼓勵用戶不要使用容易推論出來的密碼，例如他們的生日或姓名。	✓	✓	✓
5	確保用戶儘早將默認密碼或系統所產生的密碼更改為高強度密碼。	✓	✓	✓
6	限制用戶登入驗證其身份的最大嘗試次數。 當達到最大嘗試次數時，實施帳戶鎖定，以防止字典式或暴力式攻擊。	✓	✓	✓
7	確保要求用戶定期更改其密碼。 其上限次數亦要基於一旦數據洩露所造成損害的風險而定。	✓	✓	✓
8	不鼓勵用戶在不同的系統或應用程序之間使用相同的密碼，也禁止用戶使用最近三次密碼。	✓	✓	✓
9	為各個用戶分配獨特且清楚區分的用戶身份（User IDs）。	✓	✓	✓
10	確保用於身份驗證的密碼輸入時，該密碼應被隱藏在佔位符下，如星號 * 或圓點 •。	✓	✓	✓
11	確保用於身份驗證的密碼在傳輸過程中要有加密保護，並在儲存時加密或使之亂碼化（Hashed）。	✓	✓	✓
12	確保使用的密碼可包含特殊字符功能，例如“！”，“&”等。		✓	✓

13	定期檢查加密方法（如算法和密鑰長度），以確保該方法被業界確認為相關且安全。		✓	✓

表 19: 傳統密碼控制

7.2.2 NIST 推薦的新密碼控制方法

當要求用戶創建複雜的密碼時，用戶的密碼管理方式往往有欠安全（例如：在電腦顯示器上貼上密碼便條），並傾向使用較容易被推測出來的較弱密碼（例如：Password1-!）來滿足密碼要求。

為應對這種行為，SP800-63B 數碼身份準則（NIST SP800-63）[8] 建議使用一個長而簡單的密碼。該密碼只應在被入侵時才須要更改。 本密碼指引的重點是使密碼易於記住和難以猜測，不再要求密碼強制逾期失效，並允許在密碼輸入欄位中可使用複製和粘貼功能。

<table>
<tr><th colspan="2">NIST推薦的新密碼控制方法</th><th colspan="3">利益相關者: 管理層，資訊科技管理人員</th></tr>
<tr><td colspan="2">安全級別: E = 初級, I = 中級, A = 高級</td><td>E</td><td>I</td><td>A</td></tr>
<tr><td>1</td><td>較長的密碼通常比隨機的短密碼好，只要密碼長度至少有8到16個字符。實際上，只包含有小寫字母的長密碼比僅拼湊成一組字母或一堆數字亂碼更安全。
1. 人手設定時密碼最少要有八（8）個字符。
2. 由系統／服務設置時，密碼應最少要有六（6）個字符。
3. 密碼系統最大密碼長度至少可以支持六十四（64）個字符。
4. 應支持所有ASCII字符（包括空格）。
5. 密碼系統處理輸入的密碼不得刪截密碼長度。
6. 使用已知的密碼的字典來覆查用戶所選的密碼。
7. 鎖定用戶登入錯誤前至少要容許十（10）次登入錯誤。
8. 不須要有密碼複雜度要求。
9. 不須要有密碼有效期要求。
10. 不須要有登入密碼提示。
11. 不要有基於知識的身份驗證。（例如誰是用戶在高中時最好的朋友？）
12. 不要用短信息服務（SMS）的雙重驗証（2FA）短訊。（使用一次性密碼令牌（Token）或利用Google或Microsoft Authenticator等應用程式）</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>2</td><td>令密碼易於用戶使用：密碼應該讓用戶易於記憶及使用，密碼系統安全的責任在任何情下都應由密碼系統負責。</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>3</td><td>不要在密碼上強加其他組成密碼規則（例如不同字符類型的組合），應鼓勵用戶使用較長且當中有字母及數字的密碼短語 (passphrase)代替密碼。</td><td></td><td>✓</td><td>✓</td></tr>
</table>

96

[8] Authentication & Lifecycle Management, Digital Identity Guidelines SP 800-63B NIST https://pages.nist.gov/800-63-3/sp800-63b.html

4	除非有用戶要求或其密碼已有密碼被洩露的證據，否則不應隨意要求（例如定期）更改用戶所儲存的密碼。		✓	✓
5	使用常見的通用密碼或已洩露的密碼清單，以作為建立新密碼的篩選檢查要求。 需對新密碼作出檢查：NIST 建議用戶避免使用眾所周知的密碼或通用密碼，例如“Password-1”，“1q2w3e4r5t6y”等。			✓

表 20: NIST 所建議的密碼控制方式

7.2.3 驗證

用戶驗證是大部分資訊科技系統皆存在的功能。

以下為最常見的驗證方式：

- 挑戰與應答： 用戶名（User ID）及密碼（你所熟知的事物）
- 一次性密碼（One-time Password, OTP）：OTP 技術是基於儲存在身份驗證設備和身份驗證後台設備（您擁有的東西）上的共享機密。
- 生物特徵驗證：將人的特徵數據與該人的生物特徵範本作出比較，以確定兩者相似之處（即您的身份）。

驗證		利益相關者: 資訊科技管理人員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	就挑戰與應答系統而言： • 在啟動前應更改系統／供應商所設的默認憑證。 • 切勿在工作系統上使用弱密碼。 • 系統除非已配置了強力保護機制，否則切勿以純文本形式儲存密碼。 • 密碼請勿直接使用辭典中的單詞。	✓	✓	✓
2	用戶操作權限應剛好滿足運作要求。	✓	✓	✓
3	不應共享特權帳戶。	✓	✓	✓
4	用群組訪問控制權限作為配置用戶訪問控制和權限。	✓	✓	✓
5	切勿將特權帳戶用於日常操作。		✓	✓
6	使用 X.509 證書或公共密鑰身份驗證系統。		✓	✓
7	對於高風險或敏感應用程式，請使用多重驗證身份方式。		✓	✓
8	無密碼身份驗證：可考慮使用第三方身份驗證如 – Google／Facebook／Twitter 的 OpenID Connect[9] 或 OAuth2[10]。			✓

表 21: 驗證

96

[9] OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 family of specifications https://openid.net/

[10] OAuth 2.0 is the industry-standard protocol for authorization https://oauth.net/2/

7.3. 網站及網上應用程式

網站和網上應用程式通常用於對外溝通或提供服務。 由於網站和網上應用程式最終會連接到數據庫，而數據庫可能存有個人和機密數據，因此必須採取預防措施來防範網站和網上應用程式中常見的惡意活動。 非政府組織網站受到攻擊可能導致拒絕服務（Denial-of-Service, DoS）和數據洩漏。

網站及網上應用程式	利益相關者:資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	不應容許通過網站介面進行暴力破解，網站應限制連續多次登錄失敗嘗試。	✓	✓	✓
2	不應允許用戶繞過身份驗證來存取個人數據或機密數據。	✓	✓	✓
3	正確設定網絡伺服器以禁止瀏覽文件目錄（禁用目錄列表功能）。	✓	✓	✓
4	確保用戶無法通過網上應用程式或網絡伺服器存取個人資料數據或包含有機密數據的文件。即使使用未曾對外發佈的隱藏網絡鏈接，直接連向鏈接文件仍有機會可讀取這些文件。	✓	✓	✓
5	驗證所有用戶的輸入，所有用戶輸入資料在傳輸到後端數據庫之前均應經過驗證和過濾，並必須在伺服器端驗證輸入字段的長度格式和內容。		✓	✓
6	執行 cookie 數據驗證和超連結驗證，以確認使用中相對應的會話驗證令牌。		✓	✓
7	將用戶閒置逾時設置值盡可能設至最低，避免使用太長閒置時間。如果用戶關閉瀏覽器，其登入時段應即時失效。		✓	✓
8	用戶登出系統應用程式時，應立即刪除所有 cookie 及使會話驗證令牌失效。		✓	✓
9	將 Cookie 標記為 HttpOnly 並設置保安警示（Secure Flag），以強制所有網絡流量都應只通過用戶瀏覽器上的加密通道（SSL/TLS）。		✓	✓
10	應設置網站同源原則，以限制從某一網上來源載入的文檔或腳本與來自另一來源的資源互動。此舉有助於隔離潛在的惡意文檔，並減少可能的攻擊載體。		✓	✓
11	禁止使用網站框架（framing) 功能（X-frameOption：DENY）以防止點擊騎劫攻擊（ClickJacking）。		✓	✓
12	實施內容保安原則（Content Security Policy, CSP）以檢測並防範跨網站指令碼（Cross Site Scripting XSS）及數據注入攻擊（Injection）。		✓	✓

13	若情況許可，重新導向或強制使用 HTTPS （敏感資訊可經由未經保護的連結渠道外洩-HTTP）。		✓	✓
14	確保伺服器只使用網上安全性協議如 TLS 1.2 或最新保安加密演算法。		✓	✓
15	按照業界最佳行事方式是關閉不安全的網絡伺服器加密法如 MD5，RC4，SHA，DES， 3DES 等。		✓	✓
16	防止經由故障訊息洩漏資訊。為用戶網站錯誤回應設置專用的頁面。		✓	✓
17	使用跨站偽造請求（CSRF） 防護（例如使用一次性CSRF令牌，可按每次請求進行認證）。利用內置或現有實施中的CSRF防護作為CSRF 防護框架。		✓	✓
18	網上賬戶最低權限設定： 遵照應用程式及網絡保安最佳實踐，限制僅容許有需要者存取。		✓	✓
19	對網絡應用程式進行掃描以及進行源碼分析，以在發佈應用程式前查出漏洞。最好每兩年進行一次網絡應用程式漏洞掃描。			✓
20	使用網絡應用防火牆（Web Application Firewall, WAF）如 ModSecurity[11]保障網絡應用程式免受如注入 SQL 指令，跨網站指令碼及其他常見的網絡攻擊。			✓

表 22: 網站及網絡應用

96

[11] ModSecurity, TrustWave – Open Source Web-Application Firewall, supports Apache, Microsoft IIS, & Nginx https://www.modsecurity.org/

7.4. 數據管理

非政府組織應檢視其在文件/數據庫中所儲存的數據內容，以及員工和客戶如何存取此等數據（若客戶擁有存取權限）。

若個人資料有儲存在文件/數據庫中，非政府組織則應考慮所要儲存的個人資料內容，以及在一旦出現入侵事件導致個人資料被侵入時，對相關人士所會造成之傷害或不利影響的風險。

7.4.1 數據保安

數據保安	利益相關者:資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	在實施任何類型的數據安全策略之前，組織應評估其最敏感信息的存儲位置。 保護靜態數據，除了網站要受到防火牆保護外，還須對靜態數據進行加密以提供多一重保障。	✓	✓	✓
2	非政府組織在傳輸數據時，需確保其訊息及通訊系統可保證所傳輸數據的機密性和完整性，例如通過已加密的通訊管道進行數據傳送。	✓	✓	✓
3	根據數據備份程序製作常規數據備份。應安排進行備份數據還原演練以確認和驗證訊息的完整性和存儲媒體的可靠性。	✓	✓	✓
4	在數據或包含數據的電子媒體被銷毀之前，請將其存放在具備保安措施的儲存設備中，例如有鎖的櫃子或受監控的媒體儲存庫以保護電子媒體。	✓	✓	✓
5	啟動存儲媒體加密備份選項，使用加密機制來防止對在儲存中的數據進行未經授權的讀取和修改。敏感文件以及整套設備都應該進行加密。		✓	✓
6	使用有相當強度和完備的數據銷毀技術，該銷毀技術之水平應可符合銷毀存留在媒體上的資訊類型和機密性相稱要求，並確保從媒體中刪除的訊息無法被讀取或重組。		✓	✓
7	使用軟件機制來檢測和記錄對儲存中數據進行未經授權的更改，並在發生此類事件時觸發事故警報。		✓	✓
8	如按法律慣例打算將電子數據儲存外判或計劃將電子數據儲存至雲端，則必須對服務供應商進行盡職調查，並且應該議定外判書面協議，其中包括各項職責如就違反數據保護和保密責任的承擔責任和賠償。			✓

表 23: 數據保安

7.4.2 數據庫保安

數據庫用於儲存資訊以便於存取，管理和更新。數據庫軟件和管理系統可能具有不同的保安功能。

網絡攻擊是對數據庫安全性的長久挑戰。非政府組織必須確保其數據庫安全措施充足，方可以抵禦如數據庫注入 SQL 指令等攻擊。

數據庫保安可分為三層面：

- 在數據庫層面，對應數據庫本身（保護在一直使用中數據，包括數據屏蔽和加密）；
- 在存取級別保安層面，集中於控制誰可存取某些數據或包含該數據的系統，包括存取控制列表和權限；
- 對於外圍層面，決定誰可以通過網絡包括防火牆和VPN存取數據庫。

數據庫保安		利益相關者:資訊科技管理人員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	對數據庫的存取必須受身份驗證和授權機制控制。不應在互聯網上暴露數據庫的管理介面。	✓	✓	✓
2	無論機構數據庫伺服器是在本地還是在雲端運作，它都必須處於安全，有氣溫和濕度控制的環境中 。	✓	✓	✓
3	需保持監管誰在存取數據庫，在何時以及如何使用數據。數據監視解決方案可以在數據活動出現異常或風險時提醒系統管理員。		✓	✓
4	數據庫的所有備份，副本或鏡像都必須接受與數據庫本身保安程度相同（或同樣嚴格要求）的安全控制。		✓	✓
5	貫徹使用最新版本的數據庫管理軟件，並在最新修補程式可用時立即更新。			✓
6	保護靜態數據：為儲存在數據庫中的個人和敏感數據進行加密(特別是一旦受到威脅時可以對相關人士造成重大傷害或可能對相關人士造成不利影響的數據)。 • 加密儲存（即：BitLocker，透明加密數據庫（TDE）等） • 加密的密碼和其他配置設置 保護傳輸中的數據：在數據通訊中啟用加密： • 啟用網絡級加密協議 • 虛擬私人網絡（SSL / IPSec）			✓
7	記錄所有未經授權或異常的數據庫活動，以便可以跟踪和分析這些活動。可利用由伺服器所產生的警報訊息以監控數據庫操作。			✓

表 24: 數據庫保安

7.4.3 保護敏感的個人數據

在處理載有內部專用訊息，受監管訊息（例如個人資料 / 可辨識個人身份訊息（Personally Identifiable Information. PII）或詳細財務訊息）的文件時，員工之間如何協作非常重要。以下列出敏感訊息和可辨識個人身份訊息處理的最佳行事方式文件供非政府組織參考。

個人資料是指與一名在世人士有關及可確定個人身份的資料，亦必須以可供查閱及處理的方式記錄下來。

資料當事人是指屬於相關個人資料的當事人的個人。

資料使用者是指控制個人資料的收集、持有、處理或使用的人，不論是獨自還是聯同其他人共同控制。

資料處理者是指非為本身目的而是代另一人（資料使用者）處理個人資料的人。

保護敏感的個人數據	利益相關者:管理層，資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	訂立可辨識個人身份訊息的處理程序以保護隱私數據或敏感數據： • 定義資訊分類 • 實施資訊分類標籤 • 只允許員工存取與工作有關職務的敏感訊息 • 只可披露可辨識個人身份訊息給有授權人士以進行公務	✓	✓	✓
2	向所有員工和合作夥伴宣講有關保護可辨識個人身份訊息重要性的訊息 • 對員工個人身份訊息採取適當的保護措施 • 不要保留敏感訊息至超逾所需的時間 • 在處理可辨識個人身份訊息和敏感訊息時需考慮隱私問題 • 將可辨識個人身份訊息重要性視若財務訊息對待	✓	✓	✓
3	用戶不僅要限制所要收集的個人數據的類型和數量，還應考慮採用最佳行事方式，如不收集任何可辨識個人身份訊息，或者僅收集最低限度的可辨識個人身份訊息。	✓	✓	✓

4	進行加密可保障機構業務避免網絡犯罪分子存取敏感數據，或員工意外刪改數據。 機構通常會加密以下資料： • 組織的知識產權或專有數據 • 組織財務報告 • 可辨識個人身份訊息（Personally Identifiable Information, PII） • 研究開發數據 • 敏感的顧客/客戶數據 • 即將發布的產品/服務訊息	✓	✓	✓
5	非政府組織應採取一切切實可行的方法，以確保其手上的個人數據免遭未經授權或意外存取，處理，刪除，遺失或使用，其中包括： • 如果發生任何此類事件時，那些種類的數據會受到影響以及可能造成的損害； • 數據儲存的實際實體位置； • 在儲存數據的設備中實施了那些保安措施（無論是通過自動化還是其他方式）； • 為確保數據人員存取操作敏感數據時的操守，謹慎和能力勝任採取了那些措施；和 • 為確保數據的安全在通訊傳輸上採取了那些措施。	✓	✓	✓
6	通過互聯網（網站）收集和使用個人數據： • 把網上表格分為兩部分，將必須填寫與可選擇填寫的欄目清楚分開，而不是把兩者混合，使表格過於複雜。這做法可令資料使用者再行考慮是否應該避免收集那些可選擇提供的資料。	✓	✓	✓
7	兒童是容易受影響的組群，故此，在網上活動方面需要特別給予私隱保障。 兒童傾向毫不猶疑地依從指示、私隱意識偏低，以及在網上溝通時未必會小心謹慎。即使網上平台有作出警告，但兒童往往因未能完全了解過度披露或過度分享其個人資料所衍生的後果，而最終亦往往會忽視這些警告。 • 網上表格應避免使用開放式問題，因為可能會使兒童傾向提供過量資料予資料使用者； • 網上表格可採用「即時」提示或警告訊息，在兒童填寫每項欄目時，即時提醒他們提供最少量的資料；及 • 當收集第三者（例如家人或朋友）資料時，應明確地提醒兒童要先取得有關人士的同意才可提供他們的個人資料。			
8	如果資料使用者想要更改資料用途，則必須在最高管理層同意下尋求受影響的資料當事人明確的意願和同意。	✓	✓	✓

9	清楚訂明個人資料相關事故訊息呈報步驟 • 當呈報個人資料相關隱私事故時，可能需要提供詳細訊息，以了解所為何事故發生，何時發生以及哪些資訊被洩露。 • 任何已涉及違規的書面文件，網頁連結或系統相關資訊都應予呈報。 • 機構將採取適當的措施來減輕事件的影響，並報告事故原因和跟進結果予個人資料私隱專員公署(PCPD)。	✓	✓	✓
10	存儲，處理和傳輸個人資料的安全措施[12]： • 個人資料的存取權限應根據需要賦予僅限於需要知道的程度。 • 確保實施嚴格的密碼原則（即密碼長度，複雜度等） • 帶有敏感訊息／個人資料的文件必須附有適當的安全分類標籤。 • 提醒用戶應將其敏感訊息/ 個人資料保存在安全地方，或者如果以電子方式存儲，則應使用密碼進行保護。 • 要記錄用戶存取進程/敏感資料之使用情況，定期由資訊保安人員或負責人審閱。 • 如敏感訊息／個人資料必須共享，於網絡分享則應加密或通過安全通道進行。 • 當敏感訊息／個人資料儲存在機櫃或伺服器中時，應實施高強度的存取控制保護。 • 應該實施諸如防火牆之類的網絡隔離存取控制，以將內部網絡與外部網絡分開。 • 一旦不再需要的個人資料，應在釐定的時間內將其移除/銷毀。	✓	✓	✓

表 25: 保護敏感的個人數據

96

[12] Privacy Management Programme: A Best Practice Guide - PCPD 2018
https://www.pcpd.org.hk/english/publications/files/PMP_guide_e.pdf

7.5. 電腦網絡安全

無線局域網（一般稱為 WiFi 網絡）被公認為更易受到網絡攻擊，因為網絡攻擊者無需為了取得存取權而需要連接到相關的實體設備電腦網絡上。

可以用來提高電腦網絡安全性的防禦措施包括：

- 防火牆；以及網絡代理，防毒軟件和反惡意及反間諜軟件。
- 入侵防禦系統（Intrusion Prevention Systems, IPS） – 監視網絡或系統活動並阻止網絡惡意活動或違反保安政策的 設備或軟件應用程式；
- 入侵檢測系統（ Intrusion Detection Systems, IDS） – 監視網絡和系統活動中是否存在惡意活動的網絡保安設備，可在檢測到異常活動時發出警報；
- 資料洩露防護（Data Leakage Prevention, DLP） - 防止在未經授權下將數據從電腦網絡傳輸出去的保安設備。

電腦網絡安全		利益相關者：資訊科技管理人員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	除非絕對必要，否則禁止遠程管理網絡。	✓	✓	✓
2	限制員工存取已知的惡意網站。	✓	✓	✓
3	除非絕對必要，否則不應向資訊科技承包商和第三方供應商授予對資訊網絡或其他資訊科技基礎架構的管理員級別訪問權限。	✓	✓	✓
4	為網絡系統配備網絡防禦設備或軟件。		✓	✓
5	設計和分隔配置多重網域的內部網絡，並根據功能，實體位置，存取類型等將內部網絡隔離，並針對外部網絡架構設立網絡保護界線。		✓	✓
6	實施無線網絡存取指引，設立使用限制，配置要求，連接要求等。		✓	✓
7	通過利用安全連接技術或協議如 TLS 來保護電子數據傳輸，並確保網絡客戶端和網絡伺服器之間的通訊屬真確可靠。		✓	✓
8	禁止在沒有邊界保護設備（例如路由器和防火牆）的情況下，從內部專用網絡直接連接到外部網絡（例如互聯網）。		✓	✓
9	禁用交換機中並未使用的網絡端口。			✓
10	組織可以安裝流動設備管理（Mobile Devices Management MDM）解決方案，以幫助保護機構的流動設備安全。 適用於 Android 設備的免費的 MDM：			✓

	ManageEngine Mobile Device Manager[13], Miradore[14], Relution[15], Flyve MDM[16], Headwind[17] etc.			

表 26: 電腦網絡安全

相關工具：

錯誤! 找不到參照來源。 網絡保安的七大習慣

9.2 NMap/Zenmap 網絡保安掃描器

96

[13] ManageEngine Mobile Device Manager
https://www.manageengine.com/mobile-device-management/free-mobile-device-management-software.html

[14] Miradore
https://www.miradore.com/

[15] Relution
https://relution.io/en/

[16] Flyve-MDM
https://www.flyve-mdm.com/

[17] Headwind
https://h-mdm.com/

7.6. 電郵保安

非政府組織如其他行業一樣，需依靠大量電郵來進行日常營運。電郵容易受到一系列的威脅及網絡攻擊所影響，部份此類型攻擊包括商業電郵入侵（Business Email Compromise, BEC），釣魚及其他形式的惡意程式攻擊。

電郵保安		利益相關者：管理層，資訊科技管理人員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	安裝反惡意軟件應用程式在電子郵件伺服器和用戶工作站上，以防止將垃圾郵件發送給終端電腦用戶，或者減少發送的垃圾郵件的數量。保持防病毒軟件識別碼定時更新並定期執行電腦掃描。	✓	✓	✓
2	如果電郵看似有可疑，請通過帶外方式（Out-of-Band）驗證發件人的身份和電郵內容的正當性，如：（i）致電進行驗證；或（ii）檢查發件人的實際電郵地址或電郵回郵地址。 不要僅僅依靠所顯示的電郵顯示的名稱。如果用戶有任何疑問，請立即致電資訊科技部門幫助，不應嘗試點擊，打開或執行可疑附件。	✓	✓	✓
3	不要點擊無法識別的鏈接。鏈接縱使表面上看似為認可的，但當用戶將鼠標停留在電郵正文中所嵌入的鏈接上時，便可以進一步驗證實際鏈接所在。如果顯示的鏈接地址和實際鏈接地址不同，請不要點擊該鏈接。	✓	✓	✓
4	對包含個人資料的附件需要進行加密或以密碼保護，如果洩露了這些附件將會對相關人士有發生很大影響。加密密碼應不要用電郵傳達給相關人士。請確保使用強密碼用於保護敏感資料。 示例：使用 Microsoft O365 郵件加密進行加密時，請在電子郵件中，選擇「選項」，再選擇「加密」，然後選擇附帶機構所指定需要強制執行的限制方式的加密，例如「僅加密」和「不轉發」。		✓	✓
5	使用雙重驗證（2FA）使其他人難以只用帳戶和密碼便可登錄 Microsoft O365 的戶口以保護用戶。 使用 Microsoft 帳戶（O365 帳戶）進行兩步驗證[18]，O365 E1 用戶支持免費的 2FA，有關 E3 免費的 2FA[19]請與微軟聯絡。		✓	✓

96

[18] Setup two-step verification with Microsoft account
https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4

[19] Features and licenses for Azure AD Multi-Factor Authentication
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

6	實施發件人策略框架（ SPF[20],[21]），域密鑰標識的郵件（DKIM[22],[23]） 電子郵件身份驗證方法和協議。）以及基於域的消息身份驗證，報告和一致性（DMARC[24],[25]） 電子郵件身份驗證方法和協議。			✓

表 27: 電郵保安

SPF，DKIM 和 DMARC 是目前的最佳行事方式安全框架，用於保護傳輸中的電子郵件並維護機構網域的聲譽。

DKIM —網域密鑰標記郵件：另一種公共密鑰（PKI）應用，DKIM 是一種控件，讓系統管理員通過使用控件在傳輸過程中驗證雜湊編碼 Hash 以檢出被篡改內容的郵件。

SPF —發件人策略框架：SPF 是一種控件，可以做到僅允許某些網 域使用機構域名發送郵件。與 DKIM 相似的是，SPF 還依賴 DNS 記錄作為其實施基礎。

DMARC —網域訊息身份驗證，報告和適應性：同時以作為 TXT DNS 記錄的方式實施，允許電郵伺服器通過 SPF 和 DKIM 當中的一件或兩件工具來處理郵件身份驗證配置守則，並包括有關轉發，丟棄和隔離郵件規範的設置。基本上，DMARC = DKIM + SPF + 額外報告和策略設立／執行功能。

96

[20] How Microsoft 365 uses Sender Policy Framework (SPF) to prevent spoofing - Microsoft https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing

[21] Help prevent email spoofing with SPF records – Google Workspace (former G-Suite) https://support.google.com/a/answer/33786

[22] Use DKIM to validate outbound email sent from your custom domain - Microsoft https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email

[23] Set up DKIM to prevent email spoofing – Google Workspace (former G-Suite) https://support.google.com/a/answer/174124?hl=en&ref_topic=7564555

[24] Use DMARC to validate email - Microsoft https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email

[25] Manage suspicious emails with DMARC – Google Workspace (former G-Suite) https://support.google.com/a/answer/2466563?hl=en&ref_topic=7562942

7.7. 雲端運算保安

雲端運算允許用戶通過互聯網從任何方位存都可存取應用程式和資訊科技資源。雲端保安包括整個基於在網上的基礎架構、應用程式和操作平台上並保能持資料私密和安全。

大多數雲端運算保安風險都與雲數據保安有關。無論是缺乏對數據的可見性、或不勝任管控數據，還是雲中數據被盜，大多數問題都會回到客戶放在雲中的數據上。

在每個雲端運算服務中——例如 Microsoft Office 365 般的軟件即服務（SaaS）；Google Apps、DropBox，到像 Amazon Web Services（AWS）、Google Compute Engine、阿里雲等等的基礎架構即服務（IaaS）；以及 Windows Azure、Wasabi、Soho Creator 等平台即服務（PaaS）——雲端運算客戶自己始終須負責保護其數據，免受保安威脅和控制對數據的存取。雲端運算供應商（CSP）將雲端的保安性問題和風險視為與客戶的共同責任。

下表顯示了 AWS 和 Azure 雲端服務提供者（CSP）與其客戶之間的共同保安責任模型：

<table>
<tr><td rowspan="4">客戶負責
雲端內及數據
的保安</td><td colspan="12">客戶 / 用戶數據</td></tr>
<tr><td colspan="12">平臺、應用程式、身份和存取管理</td></tr>
<tr><td colspan="12">操作系統、網路和防火牆的配置</td></tr>
<tr><td colspan="4">客戶端數據
加密與數據
完整性及認證</td><td colspan="4">伺服器端數據加密
（文件系統和數據）</td><td colspan="4">網絡流量保護
（加密 / 完整性 /身份
認證）</td></tr>
<tr><td rowspan="5">AWS 負責雲端
平台的保安</td><td colspan="12">軟件</td></tr>
<tr><td colspan="3">運算</td><td colspan="3">儲存</td><td colspan="3">資料庫</td><td colspan="3">網絡</td></tr>
<tr><td colspan="12">硬體 / AWS 全球基礎設施</td></tr>
<tr><td colspan="4" rowspan="2">全球基礎設施</td><td colspan="4">地域</td><td colspan="4" rowspan="2">外界連接位置</td></tr>
<tr><td colspan="4">架構可用區</td></tr>
</table>

表 28: AWS 共享雲平台保安責任模型

雲端成分	SaaS	PaaS	IaaS	On-prem	責任
資訊和數據					始終由客戶承擔責任
裝置（流動和個人電腦）					
帳戶和身份					
身份和目錄基礎結構					責任因服務類型而異
應用程式					
網路控制					
操作系統					
實體主機					責任轉移到雲服務提供商
實體網路					
實體數據中心					
	Microsoft		Customer		

表 29: Azure 共享雲平台保安責任模型

7.7.1 雲端運算和數據安全

採用雲端服務的非政府組織應認識到雲端服務所面臨的特有安全性和合規性問題。非政府組織應該評估雲端服務供應商所提供的安全保護級別是否可滿足儲存在雲端上的個人資料和機密數據的需求。

雲端運算與數據安全	利益相關者：管理層，資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	注意雲端運算的保安風險： • 失去可見度 • 違反合規性 • 缺乏雲端安全策略和架構性 • 內部威脅 • 違約 • 應用程式介面（API）的鎖定 • 雲端服務設定錯誤 • 雲端供應商鎖定	✓	✓	✓
2	注意哪些法律適用於在雲端儲存的個人數據，以及該數據儲存所在地的司法管轄權。相關法例如： • 《個人資料（私隱）條例[26]》PDPO（第486章）（《條例》）－ PCPD 通用數據保護條例（EU）（GDPR）[27]	✓	✓	✓
3	離線備份機構的雲端數據，無論是否存在於雲端。 • 至少需備有三個最近期的副本（稱為3-2-1規則），其中一個副本需真正離線。 • 如果機構本身已有線上備份控制台，請盡可能使用2FA保護，例如在微軟的Azure Cloud[28]、Google Cloud[29]。 • 利用已存取之電腦備份資料來還原網站應是最佳方式。 • 定期測試備份還原是否正確無誤。	✓	✓	✓
4	安全地管理機構數據。將數據存儲在雲端時，請確保數據得到正確保護，雲端的環境應可支援數據加密傳輸（如虛擬專用網絡 VPN），以容許數據遷入和遷出雲端。	✓	✓	✓

96

[26] 個人資料（私隱）條例 - 個人資料私隱專員公署
https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html
[27] The General Data Protection Regulation (EU) 2016/679 (GDPR)
https://gdpr-info.eu/
[28] Features and licenses for Azure AD Multi-Factor Authentication
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing
[29] Google 2-Step Verification
https://www.google.com/landing/2step/index.html

5	機構需制定雲端數據刪除政策， 當機構最終準備遷離目前使用的雲端服務供應商時（即：遷移到新的雲端服務供應商或切換回內部架構），確保機構能完全地從雲端系統中刪除敏感資訊/數據之餘同時保持合規性。	✓	✓	✓
6	對終端設備如筆記本電腦，桌面電腦和流動設備實施電腦終端保安。機構需要保護其網絡和用於存取其雲端帳戶的設備。	✓	✓	✓
7	制定存取控制和安全移除政策，以管理具存取權限的雲端用戶。機構應為不同的用戶設定特定的權限和存取規則，以確保每個員工只能查看或使用其工作所需的應用程式或數據。	✓	✓	✓
8	向員工提供有關雲端安全實踐的培訓。有時，對機構雲端技術的最大安全威脅是來自本身的機構及其員工（內部人員）。機構應花時間來培訓將會使用雲端環境的員工有關使用雲端服務的最佳保安實踐。	✓	✓	✓
9	當員工離職時，請確保他們不再能夠存取您的雲端存儲，系統，數據，客戶信息和知識財產。	✓	✓	✓
10	加密是保護雲端系統的最佳方法之一： • 通信加密 • 敏感數據加密 • 保護靜態數據，並對上傳到雲端中的所有數據進行端到端加密。		✓	✓
11	雲端加密的最佳方式包括以下步驟： • 制定雲端加密政策 • 界定哪些數據需要加密，何時加密 • 確定數據所儲存的位置 • 實施加密解決方案和密鑰管理		✓	✓

12	使用相關工具以保護及保障雲端數據
	• AWS[30] EC2 (Linux/Windows) / Azure[31] (Linux/Windows) / Google Cloud[32]
	  - 硬碟加密
	  - 檔案/資料夾加密
	• AWS RDS / Azure MSSQL
	  - 支援透明資料加密 （TDE）
	• Google Cloud SQL
			✓	✓

96

[30] Amazon AWS Cloud Services
https://aws.amazon.com/
[31] Microsoft Azure Cloud Services
https://azure.microsoft.com/en-us/
[32] Google Cloud
https://cloud.google.com/

	- Google Cloud 已在存儲級別被加密 • AWS S3 - S3儲存桶(Bucket)的預設伺服器端加密			
13	確保雲端服務供應商已按需要取得相關 ISO 標準認證。 相關標準可以包括ISO / IEC 27001：2013[33]，ISO / IEC 27017：2015[34]，ISO / IEC 27018：2019[35]或其他公認的國際標準。情況許可，向雲端服務供應商索取證書副本供機構備存。		✓	✓
14	通過雙重身份驗證來保護所有非政府機構雲端用戶的雲端存取權限，以確保只有授權人員才能登入雲端應用並存取敏感數據。		✓	✓
15	為了清楚知悉雲端情況，啟用實時監控和分析用戶活動功能，以偵測雲端上的可疑活動，監控任何未經授權的存取活動和其他問題。。		✓	✓
16	定期執行例行滲透測試，可讓機構雲端管理人員檢測雲端系統中是否存在任何風險隱患。		✓	✓
18	深度防禦對保護雲端環境特別重要，因為它可以確保即使一個控件出事，其他保安功能也可以確保其他應用，網絡和數據的安全。			✓
19	若情況許可，機構應與雲端服務供應商量安排執行第三方審核，並要求供應商向機構提供有關這些審核的報告。			✓

表 30: 雲端運算和數據安全

96

[33] ISO/IEC 27001:2013 specifies the requirements for establishing, maintaining and continually improving an information security management system within the context of an organisation.
https://www.iso.org/standard/54534.html

[34] ISO/IEC 27017:2015 provides guidelines for information security controls applicable to the provision and use of cloud services.
https://www.iso.org/standard/43757.html

[35] ISO/IEC 27018:2019 relates to the protection of personally identifiable information and provides guidance on ensuring that cloud service providers offer suitable information security controls to protect the privacy of client data.
https://www.iso.org/standard/76559.html

7.7.2 避免雲端供應商鎖定

將系統遷移至雲端可以為機構帶來一系列好處，例如運作更迅速，更具彈性及更節省成本。儘管有上述好處，但不少有意遷移至雲端的機構仍有所顧慮，其中原因之一正是缺乏標準化導致被鎖定於單一家雲端供應商。

供應商鎖定的問題是，一旦出現情況時會很難轉移到其他雲端服務供應商。使用單一雲端供應商通常會遇到四種主要的鎖定風險。當中包括：

- 數據轉移風險
- 應用轉移風險
- 基礎設施轉移風險
- 人力資源知識風險

<table>
<tr><th colspan="2">避免雲端供應商鎖定</th><th colspan="3">利益相關者：管理層，資訊科技管理人員</th></tr>
<tr><td colspan="2">安全級別: E = 初級, I = 中級, A = 高級</td><td>E</td><td>I</td><td>A</td></tr>
<tr><td>1</td><td>盡職調查：
• 仔細評估雲端服務
• 確定機構遷移到雲端的目的
• 評估機構當前的狀況以及基礎架構，成本和資源水平
• 選擇所需的雲端環境類型 - 公眾，私有還是混合雲
• 確定必要的特定雲端組件</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>2</td><td>儘量提高數據可遷移性：
• 資料備份
• 確保數據可以容易遷移</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>3</td><td>將組織應用系統設計至可容許鬆散耦合：
• 將應用系統在設計或可遷移性上做到盡可能靈活和應用之間可鬆散耦合。
• 業務邏輯組合不僅應與應用邏輯組合分開，而且應明確定義和用文本記錄下來。</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>4</td><td>多雲端服務或混合雲端策略：
• 多雲端服務方式整合了多個雲端供應商，從而減少了對任單一供應商的依賴。
• 在混合雲端中，某些數據將保持由機構直接控制(無論是在私有雲端中還是在本地儲存中)。</td><td></td><td></td><td>✓</td></tr>
</table>

5	應用DevOps工具和流程： • 像Kamatera[36]這樣的DevOps[37]工具已越來越多地被應用以儘量提高代碼的可移植性。 • 通過諸如Docker[38]及CoreOS[39] 的容器技術構建應用程式協助將軟件與其環境隔離開來，並讓其避免過度依賴雲端服務供應商。			✓
6	使用配置管理工具（如Chef[40], Puppet[41], 及 Juju[42]）可幫助雲端管理員自動配置其機構應用運行的基礎結構。			✓

表 31: 避免雲端供應商鎖定

96

[36] Kamatera Express
https://www.kamatera.com/express/compute/
[37] Jenkins CDF, X, Tekton, Spinnaker
https://www.jenkins.io/
[38] Docker
https://www.docker.com/
[39] CoreOS
https://coreos.com/
[40] ChefDK
https://download.chef.io/product/chefdk
[41] Puppet
https://puppet.com/try-puppet/open-source-puppet/
[42] Juju
https://juju.is/docs/clouds

7.8. 實體安全

實體安全是保護機構工作場所所需要的技術和系統。實體安全主要涉及保障機密資料，重要數據，資產，網絡，設備，場地設施等。

一旦實體安全未獲適當執行，倘若有入侵者可通過實體安全進入場地，所有安全措施都會失效。因有更多小型裝置出現(如 USB 儲存設備，筆記本電腦，流動裝置等)，現時實體安全變得更具挑戰性。

實體安全		利益相關者:管理層，資訊科技管理人員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	培養保安意識以確保所有工作人員皆重視資訊保安。實體安全應顧及機構人員，數據，知識產權與實體資產。	✓	✓	✓
2	確保電腦室僅供授權及指定人員進入場所。工作場所內的每台電腦和設備都應貼上庫存編號標籤。	✓	✓	✓
3	訪客管理系統和人員進出控制是構成有效實體安全的主要部份。	✓	✓	✓
4	利用閉路電視監控電腦室/數據中心，並在入口處設立警告字句提示其他人士他們已被錄影，不應嘗試進行違法行為。	✓	✓	✓
5	伺服器及存有敏感資料的儲存設備應要放置在上鎖的專用電腦機櫃並具備監控的電腦室中。	✓	✓	✓
6	確保將儲存媒介和敏感文件鎖於上鎖櫃或安全房間中。	✓	✓	✓
7	應在機構的數據儲存設備上啟用存取控制保護功能，例如密碼保護。	✓	✓	✓
8	啟用流動設備存取控制保護，以防止未經授權的人員存取設備內容。	✓	✓	✓
9	定期備份機構的電話內部數據如以防止丟失。	✓	✓	✓
10	在手機上安裝防病毒軟件或反惡意軟件程式。	✓	✓	✓
11	在所有公共場所的用戶筆記本電腦要以筆記本防盜纜接駁，以防止設備被盜。		✓	✓
12	媒介上的敏感資料應儲存在安全地方以防止意外事故（如火災）和蓄意事故（如盜竊或故意破壞）。建議將備份與伺服器分開儲存。		✓	✓
13	在伺服器室內安裝入侵檢測器，活動探測器和警鐘。			✓

表 32: 實體安全

7.9. 流動保安

日趨成熟的流動設備可以執行許多個人電腦功能。此類設備包括筆記本電腦，流動電話，平板電腦，USB 儲存設備及便攜式硬碟等。這些設備除具備移動性這種額外好處外，還可以廣泛使用在各類應用程式之上。

以下為與流動設備有關的五大顧慮：

- 設備丟失和被盜
- 被別人取用
- 最終用戶設備擁有者問題
- 需長時間運行而增加數據用量
- 保安意識不足

引入流動設備往往是擴大當前風險而不是導致新風險，它或有可能使某些風險更為嚴重。

7.9.1 流動設備保安

流動裝置保安可以提防各種會侵犯您的隱私並獲取手機上所儲存的任何其他訊息的威脅。這些攻擊手段若用在您的流動設備上，可導致您的私人資料如銀行訊息，登錄訊息和機構數據被人奪取。

流動設備保安	利益相關者:管理層，資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	設定靈活但可實施的政策，以確保其可有效規限機構所面臨的風險： • 流動設備的一般保安要求 • 驗證（密碼/ PIN）要求 • 儲存/傳輸加密要求 • 多次嘗試登錄後要求自動刪除設備的要求 • 流動設備的使用限制 • 公司機構責任 • 監控，管理和刪除的權限 • 機構指定支援的型號 • 在旅途上使用流動數據的最佳行事方式 • 合理使用政策（若與一般合理使用政策不同）	✓	✓	✓
2	為非政府組織所控制的流動設備（例如公司擁有但由個人啟動（COPE）設備）建立使用限制，配置要求，連接要求和實施指引。	✓	✓	✓
3	評估設備使用情況並參考最佳行事方式以減低各種不同風險。	✓	✓	✓

4	執行行業標準規定的安全政策：加密整個設備，使用 PIN 碼，限制登錄失敗後再嘗試登錄的次數及遠程刪除等。	✓	✓	✓
5	設置安全基準以使用企業認證的硬件/操作系統。	✓	✓	✓
6	保障設備和應用程式安全，使用反惡意軟件流動應用程式來保護非政府組織擁有的或自行購置的流動設備。 *請參閱第 7.5 節“電腦網絡安全表＃26”中的解決方案。	✓	✓	✓
7	僅安裝經授權的應用程式。	✓	✓	✓
8	定期檢查，監視和修訂各種政策。	✓	✓	✓
9	將流動設備風險納入機構的保安意識培訓活動中。		✓	✓
10	設立設備程式修補流程，以鼓勵用戶更新其流動設備。		✓	✓
11	如為自行購置設備，請盡可能把員工個人數據與業務環境和數據區分開來 (公認的保安原則是應把一個網絡劃分為在不同範圍之間具有嚴格的存取限制的邏輯操作區域)。		✓	✓
12	設立相關機構流動設備小組並儘早讓各利益相人士參與討論流動設備保安要求。		✓	✓
13	測試並驗證流動設備保安措施的有效性。		✓	✓
14	設立並實施適當的自行購置設備支援和使用政策。 *請參閱第 7.5 **錯誤! 找不到參照來源。**節“電腦網絡安全表＃26”中的解決方案。		✓	✓
15	為關鍵業務引入更嚴格的身份驗證和存取權限應用程式。			✓
16	投入流動設備管理（MDM）解決方案，以實施保安政策並若可能監控使用情況和存取情況。 *請參閱第 7.5 **錯誤! 找不到參照來源。**節“電腦網絡安全表＃26”中的解決方案。			✓
17	改善現有技術支援流程以包括設備的保安配置和取消配置（刪除）功能，並提高自助水平。 *請參閱第 7.5 **錯誤! 找不到參照來源。**節“電腦網絡安全表＃26”中的解決方案。			✓

表 33: 流動設備保安

7.9.2 便攜式存儲保安

應對存有敏感和機密數據的便攜式儲存裝置（如 USB 儲存設備，快閃記憶體設備和便攜式硬碟）採取合理的保安措施來保護數據機密。便攜式設備可能在機構以外使用，亦可能會連接到其他電腦，並且容易丟失和被盜。

<table>
<tr><th colspan="2">便攜式儲存保安</th><th colspan="3">利益相關者:管理層，資訊科技管理人員</th></tr>
<tr><td colspan="2">安全級別: E = 初級, I = 中級, A = 高級</td><td>E</td><td>I</td><td>A</td></tr>
<tr><td>1</td><td>對於越來越多的數據洩露威脅，便攜式存儲設備現在一般已有內置保安配置（即加密的 USB 儲存設備/加密的便攜式硬盤等）。在要加密便攜式存儲設備上儲存的文件，要用一個長密碼來作為保護。</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>2</td><td>若要對不具備加密保護功能的 USB 儲存設備和便攜式硬盤驅動器上的資訊進行加密，微軟 BitLocker-To-Go 是其中一個解決方案。

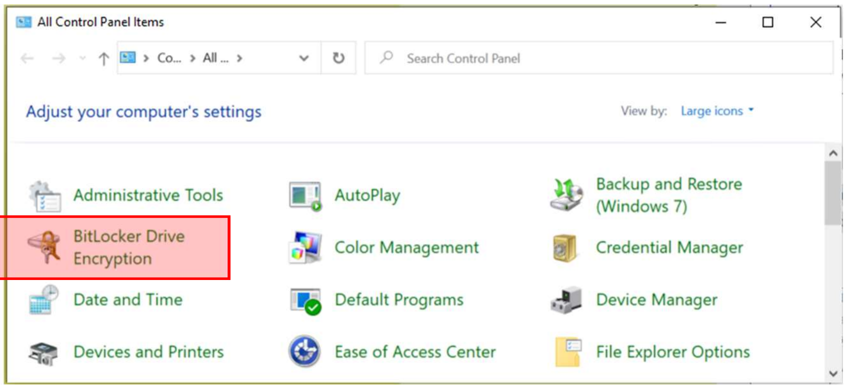
啟動 BitLocker-To-Go 加密文件的步驟如下：
1. 將可移動儲存設備或 USB 儲存設備接駁到電腦。
2. 到控制面板然後選擇 BitLocker 硬碟加密。
3. 選擇要加密的可移動儲存硬碟，然後點擊啟用 BitLocker。


圖 4:硬碟加密控制面板
4. 選擇您要如何加密硬碟
5. 選擇加密模式
6. 按照步驟完成便攜式硬碟加密

備註的鏈接[43]是關於啟用 BitLocker 設備加密以加密儲存在便攜式硬碟上的數據的詳細資訊。</td><td></td><td>✓</td><td>✓</td></tr>
</table>

96

[43] 在可移動數據驅動器上執行驅動器加密類型 https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings#enforce-drive-encryption-type-on-removable-data-drives

4	可使用第三方工具保護USB儲存設備和便攜式硬碟上的靜態數據： • 加密便攜式硬碟上的整套儲存設備 - VeraCrypt[44]是一種多平台，免費的開源工具，旨在為用戶提供實時加密功能，其中包括創建虛擬加密硬碟並將其掛載的功能。 • 加密個別文件 - 7-zip[45] 是一個免費的開源多平台文件歸檔實用程式，用於將文件（或文件組）壓縮到稱為檔案的容納檔中。		✓	✓

表 34: 便攜式存儲保安

96

[44] VeraCrypt 開源磁碟加密軟體
https://www.veracrypt.fr/en/Home.html
7 Zip 壓縮程式
[45] https://www.7-zip.org/

7.10. 遠端訪問/在家工作

如今越來越多機構要求其員工在家工作。對於日常運作通常以辦公室為基礎的企業來說，這帶來了多種不同的網絡保安挑戰和風險。

此外，由於員工在不同的環境中工作，他們的網絡風險狀況會有所不同，有些人會一併使用多種的個人設備。

機構需要管理一些常見風險，包括網絡釣魚攻擊，設備丟失，使用個人設備和/或在公共場所工作等。

遠端訪問/在家工作	利益相關者:管理層，資訊科技管理人員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	用戶應以密碼保護其家用電腦和流動設備的存取權限，而密碼應為強密碼（如用戶密碼必須至少 8 個字符）。	✓	✓	✓
2	在工作上盡可能使用機構提供的電郵、訊息傳遞、會議以及其他服務工具。	✓	✓	✓
3	建議用戶在工作後清除其網絡瀏覽器歷史記錄，以避免其他用戶取得敏感資訊。	✓	✓	✓
4	建議用戶在其瀏覽器上禁用自動填充設置。	✓	✓	✓
5	使用個人工作站在線上查看敏感訊息時，可選擇網絡瀏覽器的私隱瀏覽模式（私隱瀏覽例如 Firefox / 無痕模式，Chrome / 無痕模式，Edge / InPrivate）等等。	✓	✓	✓
6	啟用系統和應用程序自動更新配置，保持遠程操作系統和應用程式更新。	✓	✓	✓
7	建議在家工作用戶為其個人設備的防病毒應用程式更新為最新的病毒識別碼，並更新機構軟件和操作系統。	✓	✓	✓
8	建議在家工作用戶保護其文件，包括在外部硬碟上離線備份（或在雲端備份）其重要文件。確保他們安全地保存其紙質文件。		✓	✓
9	為在家工作用戶提供多重身份驗證，以存取機構辦公室網絡的敏感信息。		✓	✓
10	確保在家工作用戶可以通過加密的虛擬私人網絡管道存取機構遠程辦公室雲端基礎架構。此外，若無法使用虛擬私人網絡，會同時提供使用加密和強密碼保護家庭 Wi-Fi 的指引。		✓	✓
11	確保在家工作用戶在機構的雲端硬碟或加密 USB 儲存裝置上離線備份其日常工作。		✓	✓

表 35: 遠端訪問/在家工作

7.11. 保安風險評估與審計

風險評估計劃可確保持續識別和解決對機構的最大風險。保安風險評估可助非政府組織發現其保安狀況況中最關鍵的漏洞，從而使非政府組織能夠能優先考慮其保安資源投放優次。每個機構都有自己獨特的風險情況。非政府組織通過識別個別保安漏洞和最有可能的威脅，進一步創建網路保安路線圖，從策略上降低風險。

保安風險評估與審計	利益相關者：管理層、資訊科技管理員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	評估機構的風險，考慮機構的整體業務策略和目的。籍着風險評估幫助，可以識別哪些對資產的威脅，系統的脆弱性及發生的可能性，估計潛在風險影響。	✓	✓	✓
2	非政府組織進行保安風險評估的要考慮的問題包括： • 合理的預算 • 對機構運作的影響 • 高級管理層的支持 • 相關人士的溝通	✓	✓	✓
3	保安風險評估要求： • 項目範圍和目標 • 約束條件 • 利益相關者的角色和責任 • 保安風險評估方法 • 項目規模和日程 • 資訊和工具	✓	✓	✓
4	行風險分析時需考慮以下項目： • 資產識別和估值 • 威脅分析 • 漏洞分析 • 資產 / 威脅 / 漏洞關聯 • 影響和可能性評估 • 風險結果分析 • 編製保安風險評估報告和後續計劃	✓	✓	✓
5	資產的價值和風險可能會在其開始至完結週期內發生變化（例如：在正式發布後，未經授權的披露或非政府組織財務帳戶的盜竊行為所帶來的影響會降低），但是資訊保安在各個階段都仍然具有重要意義。	✓	✓	✓

6	明確的職責分工，確保同一人員不會執行相互衝突的職能，例如管理保安訪問控制以及執行審核職能。		✓	✓
7	確保審計資訊受到保護，避免未經授權的存取、修改和刪除，並保留資訊用於行政、審計或其他運營目的，直到不再需要這些記錄為止。		✓	✓
8	定期審查和分析資訊科技系統和服務審核的記錄和日誌。若發現不適當或異常活動，報告調查結果給負責管理此類事件的有關人仕。			✓
9	進行風險評估，包括未經授權訪問、使用、披露、中斷、修改或破壞資訊科技系統，以及存儲、處理和傳輸的資訊，而造成損害的可能性和其嚴重程度。			✓
10	定期對資訊科技系統進行漏洞掃描，以檢測過時的系統、缺少修補的應用程式和存在保安漏洞的資訊科技系統和軟體應用程式。			✓
11	定期進行保安審計（建議每兩年一次），並由最高級別的人員對該審計計劃的執行情況進行監測。			✓

表 36: 保安風險評估與審計

<u>相關工具：</u>

8.6　保安風險評估指引
9.3　Nessus Essentials
9.4　OWASP Zed 攻擊代理(ZAP)
9.5　Kali Linux

7.12. 內部威脅

內部人員是受信託保護機構機密和智慧財產權的個別人士。隨著敏感數據的快速增長、對數據的過度存取，以及員工保安意識的缺乏，內部人員所構成的威脅日益嚴重。內部威脅包括：欺詐、知識產權盜竊、間諜活動和 IT 基礎設施破壞。

內部威脅可根據內部人員威脅的意向和目的定義為四種類型：

1. 粗心大意的員工會錯誤處理數據，違反使用政策並安裝未經授權的應用程式
   - 微軟資料庫因員工疏忽而導致洩露數據[46]

2. 內部人員替外部人士竊取資訊
   - Twitter 內部員工替黑客拿到了內部系統管理工具實施行騙[47]

3. 前員工／心懷不滿的員工試圖傷害機構
   - 前思科員工故意損壞其雲端基礎架構[48]

4. 利用現有特權竊取資訊以謀取私利的惡意內部人員
   - 通用電氣員工竊取商業機密以獲取業務優勢[49]

96

[46] Microsoft Security Shocker As 250 Million Customer Records Exposed Online
https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=498a691f4d1b

[47] 2020 Twitter bitcoin scam
https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam

[48] Ex-Cisco Engineer Pleads Guilty in Insider Threat Case
https://www.bankinfosecurity.com/ex-cisco-engineer-pleads-guilty-in-insider-threat-case-a-14917

[49] Investigation Into Theft of Intellectual Property from GE Leads to Two Guilty Pleas
https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920

由於內部威脅是「人事問題」，而不是資訊科技問題，因此應利用威懾、檢測和緩解威脅的行動為主。

內部威脅		利益相關者：管理層、資訊科技管理員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	建立資訊保安原則與程序： • 制定一套清晰的資訊保安政策和程序。保安策略應包含內部威脅計劃，該計劃應具有可操作性、可持續性，並尋求可衡量的結果。 • 發展出一套具有既定政策和程序的保安文化，以阻止、檢測和緩解相關威脅，將保安事件的頻率和影響降至最低。 • 建立諸如工作時間表和數據傳輸之類的活動的基準線，釐定超出規範的範圍，然後藉此找出偏離既定界線的人員。 • 將內部威脅意識納入機構的強制性培訓中以教育員工。 • 員工應接受培訓，以了解內部威脅，有能力識別上述風險指標並適當報告觀察到的行為。	✓	✓	✓
2	建立事件檢測平台 • 實施用戶監視和資料外洩防護系統，這可以提醒保安團隊注意未經授權的數據存取。 • 保安資訊和事件管理（Security Information Event Management, SIEM）有助於檢測異常情況和在保安事故後分析發生的情況。	✓	✓	✓
3	針對內部威脅的威懾方法 • 所有機構都應實施適用於實體和網絡保安的最小權限原則。 • 建立保安策略和數據加密，還應包括存取控制。 • 除非有必要執行其工作職能，否則個人或第三方不應存取網絡、數據或與業務無關的內部場所。 • 越少人獲得存取權限，潛在惡意行為或疏忽大意的員工未經授權訪問和入侵帳戶的機會將更少。	✓	✓	✓
4	授權的保安人員和正式員工應注意其他員工的行為； 識別高風險指標是防止內部威脅問題的關鍵組成部分。		✓	✓
5	保安人員可以與資訊科技部門一同實施技術限制，包括禁止使用 USB、外部驅動器或其他設備插件、阻止從未經授權的互聯網下載以及限制對某些下載的訪問。		✓	✓
6	注意心懷不滿的員工或會尋求報復，或者有資歷的員工為了在新僱主中尋求競爭優勢，他們可能會嘗試在終止合約之前或終止時獲取機構的數據。		✓	✓

7	為了防止未經授權的數據刪除，人力資源部 / 資訊科技部應在員工離職時限制離職員工公司內部和資訊設施的存取權限，歸還員工證並護送個人離開機構。		✓	✓
8	人力資源部與資訊科技部門協調，機構應在員工離職之前留意網絡數據流，並在員工離職後將該個人電郵從電子郵件分發列表中刪除。		✓	✓

表 37: 內部威脅

7.13. 供應商管理

機構選擇承包商或服務供應商需要有正式的甄選過程。確保機構選擇的供應商所提供的服務或產品是合適的，以下幾點可幫助機構選擇適合其業務的供應商。

供應商管理		利益相關者：管理層		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	機構應明確訂立供應商可以訪問哪些信息，並在資訊保安策略中明確定義授權存取控制。	✓	✓	✓
2	建立所有相關的資訊保安要求，並與供應商達成一致保安協議，協商那些訊息可以存取、處理、存儲、傳送、或機資訊科技基礎架構。	✓	✓	✓
3	在訂立了業務需求後，在選出合資格的供應商名單中提出投標請求（RFP）或報價請求（RFQ）。 RFP 或 RFQ 應包含以下部分： • 提交投標內容 • 簡介和執行摘要 • 業務概述和背景 • 詳細規格 • 投標假設與約束 • 條款和條件 • 選擇條件要求	✓	✓	✓
4	提案評估和供應商選擇階段的主要目標是最大程度地減少個人情感和政治立場的影響，以便做出符合公司最大利益的決定。 在選擇供應商時應考慮以下因素： • 價格 • 產品或服務的質素 • 產品用戶一覽表 • 客戶服務 • 清晰的溝通 • 供應商的道德和誠信 • 專業員工 • 其他人的推薦	✓	✓	✓

5	非政府組織應該訂立供應商需要滿足的供應商選擇標準列表，以便滿足非政府組織所需要求。 供應商選擇標準列表可包括以下項目： • 從收到訂單到交貨所需時間 • 服務水平協議 • 維護和支援詳細資訊 • 歷史銷售記錄和參考 • 供應商績效 • 質量保證流程 • 付款條款和條件 • 可聯繫的客戶參考	✓	✓	✓
6	供應商管理要留意產品與服務的總擁有成本，而不僅僅是初始成本。	✓	✓	✓
7	非政府組織應定義不同類型的供應商可獲得的資訊類型，並監控其存取控制。	✓	✓	✓
8	非政府組織應定出適用於供應商的保護機構資訊的責任。	✓	✓	✓
9	非政府組織應要求在雙方簽署的協議中，訂立資訊保安要求和控制條件。	✓	✓	✓
10	非政府組織應監察供應商是否有遵守機構保安要求的義務。	✓	✓	✓
11	除供應商所提供的一般資訊保安要求外，非政府組織還應確立適用於採購信息通訊技術產品或服務的保安要求。	✓	✓	✓
12	非政府組織應要求供應商在整個供應鏈中包括產品及其元件推行適當的信息通訊技術保安實踐。		✓	✓
13	非政府組織應實施一個可接受的監測方法和手續，來驗證供應商所提供的資訊和通信技術產品與服務是否遵守規定的保安要求。		✓	✓
14	非政府組織和相關的供應商協議與合同中應包含對相關供應商進行審計的權利。		✓	✓

表 38: 供應商管理

相關工具：

8.3 供應商風險評估清單（模板）

7.14. 保安意識和培訓

每個機構必需提供員工保安意識培訓，這是一種教育員工瞭解到網路釣魚或其他線上詐騙危險的方法。保安意識培訓的目的是協助機構減少保安事故的發生。

機構應向所有員工提供合適的保安意識，教育和培訓，以及正確使用資訊處理設施的方法，以降低機構的保安風險。

保安意識培訓有以下好處，可幫助保護非政府組織免受黑客、偷竊和其他不良行為的侵害。

- 培訓可減少人員錯誤。
- 培訓可增強安全級別。
- 受過良好教育的員工可以提高合規性。
- 培訓可以有效保護非政府組織的聲譽。

保安意識和培訓		利益相關者：管理層、資訊科技管理員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	高級管理層有責任培養保安和業務可持續的意識和文化。	✓	✓	✓
2	非政府組織的所有僱員均應接受與其工作職能相關的保安意識培訓，並定期更新機構政策和程序。	✓	✓	✓
3	提醒所有用戶，他們是機構防禦的最後一道防線。為機構用戶建立正式的保安事件報告程序，以通過適當的管理渠道盡快報告保安／威脅事故。	✓	✓	✓
4	為新員工提供初始保安意識培訓，並定期開展培訓課程，讓員工瞭解最新的網路保安威脅和保安措施。	✓	✓	✓
5	應灌輸基本網路保安知識給員工，包括：反網路釣魚策略、密碼保安、實體安全和社交工程攻擊等。		✓	✓
6	為機構提供與網絡保安相關的服務供應商需清楚了解並遵循機構的隱私政策。			✓

表 39: 保安意識和培訓

7.15. 保安事故回應管理

要確保與資訊系統相關的資訊保安事故和弱點的溝通管道暢通，並能夠及時採取糾正措施，應制定正式的事故回應報告和上報程序流程。

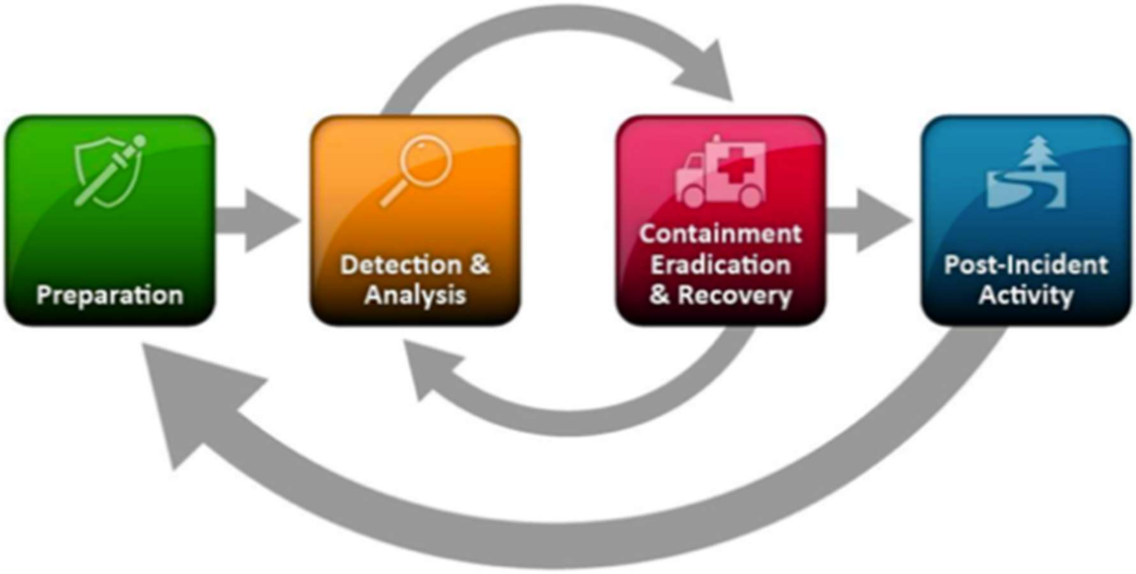


圖 5: NIST SP800-61r2 事故回應週期[50]

所有員工應盡快將任何發現的資訊保安事故和弱點，報告給指定的有關人員。

事故回應程序流程

- 準備 — 使用適當的防護措施保護資產。
- 檢測 — 檢測入侵、違規和未經授權的存取。
- 消除遏制 — 應對潛在的網絡保安事件。
- 恢復 — 透過復原的日常操作和服務，從網絡保安事件中恢復。
- 事故後檢討 — 對所發生的情況和機構對事故回應計劃的進行最終審查，以解決及改善系統、政策或程序中任何有漏洞的步驟。

96

[50] Computer Security Incident Handling Guide - NIST 800-61 revision 2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

保安事故回應管理	利益相關者：管理層、資訊科技管理員			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	定義四級的事故回應級別，根據預計的業務延誤/中斷影響做好準備，範圍從最嚴重到最不嚴重： • 等級 A: 影響整體運作/危及人員生命； • 等級 B: 影響關鍵性業務； • 等級 C: 影響日常運作； 及 • 等級 D: 影響輕微	✓	✓	✓
2	建立和每年審查事件回應策略、程序和計劃。 每年檢查事故回應程序和計劃。在發生數據保安事故時，實施已訂立的回應模式。	✓	✓	✓
3	準備 • 在發生保安事故的地方實施組織擬定的回應模式。 • 評估事故發生時的影響並確定風險的優先級。 • 對獨特，新的和敏感情況的事件使用人工回應。 • 在可能的情況下實現事故回應自動化，建立以計劃性分流機制對應常見的情況。	✓	✓	✓
5	開發事故報告模板以方便日後進行事故處理和報告。	✓	✓	✓
6	制定與外部各方就保安事故進行溝通的準則與指引。	✓	✓	✓
7	選擇保安事故回應團隊的結構和人員配備组合。	✓	✓	✓
8	確定事故回應團隊所提供的服務。	✓	✓	✓
9	事故回應團隊與內部（例如：資訊科技部門）和外部（例如：執法機構）的其他小組之間應建立關係和溝通渠道。		✓	✓
10	配備適當人員和培訓事故回應團隊，持續學習並改善機構事故回應流程。		✓	✓
11	定期對網路保安事故回應能力進行演練測試，以測試能力和整體成效，並找出潛在的弱點或缺陷。		✓	✓
12	如果可以將保安異常歸因於錯誤的配置，或許可以通過使用正確的配置重新部署資源來消彌差異以資捕救。			✓
13	跟蹤、記錄和報告 資訊科技保安事故。 通過把日誌、快照和其他證據複製到集中式保安雲端帳戶來保留這些證據，並使用標籤、原有數據和機制來實行強制保留策略。			✓

14	查看事故的根本原因，以改進檢測和保護流程。事故管理流程可能需要修訂。			✓

表 40: 保安事件回應管理

<u>相關工具：</u>
8.2.1　資訊保安事故回應報告表格
8.2.2　資訊保安事故回應記錄

7.16. 業務持續運作管理

運作管理（BCM）是一個全盤管理系統，以識別對機構潛在威脅的影響，並提供賴以構建有效的應變框架及計劃以維持業務持續運作能力，維護其主要利益相關者的利益、聲譽、品牌和價值創造活動。

建立和維護業務持續運作管理流程可從三個步驟開始：

1. 決定業務持續性管理；
2. 確定和定義可行的業務持續運作管理框架的關鍵組成部分
3. 將業務持續運作管理放在機構風險管理的環境中

業務持續性規劃（BCP）指機構建立必要的功能，以保護其資產，並在出現自然或人為事件導致意外的業務中斷等災難後，繼續保障關鍵業務運作的流程。

業務持續性管理是有效公司管治的關鍵因素。它通常位屬風險管理範疇，(機制)並允許利益相關者提出及檢索相關問題，例如:

- 公司的業務和運營模式
- 創造出(機構)關鍵價值的產品和服務
- 關鍵依存關係－關鍵的資產和工作流程
- 公司將如何應對這些損失或威脅
- 當前和即將到來的主要威脅是什麼
- 業務持續性計劃實行時會起作用的證據

業務持續運作管理	利益相關者：管理層			
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	識別非政府組織策略，目標及文化以制定業務持續運作規劃政策： 1. 與最高管理層團隊面談 2. 進行業務影響分析 3. 審查機構業務持續運作規劃相關的文件 • 業務計劃，戰略計劃 • 年度報告，市場報告 • 當前的管理訊息報告，當中描述了工作流程概要，數量，目標以及活動的量化值		✓	✓
2	進行業務影響分析（BIA） • 在戰略層面確定業務運作優次要求並定出產品和服務的排定次序。 • 確定非政府組織哪些產品和服務的優先流程。 • 確定並排定最緊急產品和服務活動的優次，並確定繼續進行這些活動所需的資源。		✓	✓

3	在進行網絡風險偏好的決策時，可考慮以下的問題： • 支持我們實現機構目標的關鍵資產和業務流程是什麼？ • 該機構的總體風險承受能力如何， 那種損傷會是災難性的？ • 有甚麼東西是此機構可以暫且缺乏，而可維持多久？ • 哪些資訊絕對不應落入外人手中或被公諸於世？ • 什麼會對員工，客戶，合作夥伴，訪客造成人身傷害？		✓	✓
4	建立業務持續運作計劃。業務持續運作策略確定了業務持續運作計劃的界限和要求，並說明實施該計劃的原因。它界定了機構遵循的指導原則並衡量其績效。		✓	✓
5	業務持續運作管理能力和技能： • 項目管理技能和理解持續改進的重要性。 • 了解機構文化以及如何影響機構文化。 • 了解業務持續能力和所需技能，以及培訓和意識提高的能力。 • 與業務影響分析相關的分析技能，包括分析資訊，發現問題和制定可行的解決方案的能力。 • 了解風險評估和緩解措施		✓	✓
6	業務持續運作計劃設計和實施： • 持續運作和恢復策略和技巧，包括冗餘，多樣化和手動解決方法 • 緩解威脅以應對不可接受的風險 • 事件回應架構		✓	✓
7	審查和測試對業務持續運作而言非常重要： • 對計劃進行高層次核查，確保仍然達到所有目標—需每年 一次 • 審查風險評估，業務影響分析和回復計劃—需每兩年一次 • 有規劃地進行計劃演練—需每兩年一次 • 全面審查—需每兩年一次 • 回復模擬測試—需每兩年或三年一次		✓	✓
8	在檢查並測試了業務持續運作計劃後，將結果用於： • 更新業務回復計劃 • 制定明年的測試時間表 • 向高級管理層/董事會提交檢測報告			✓

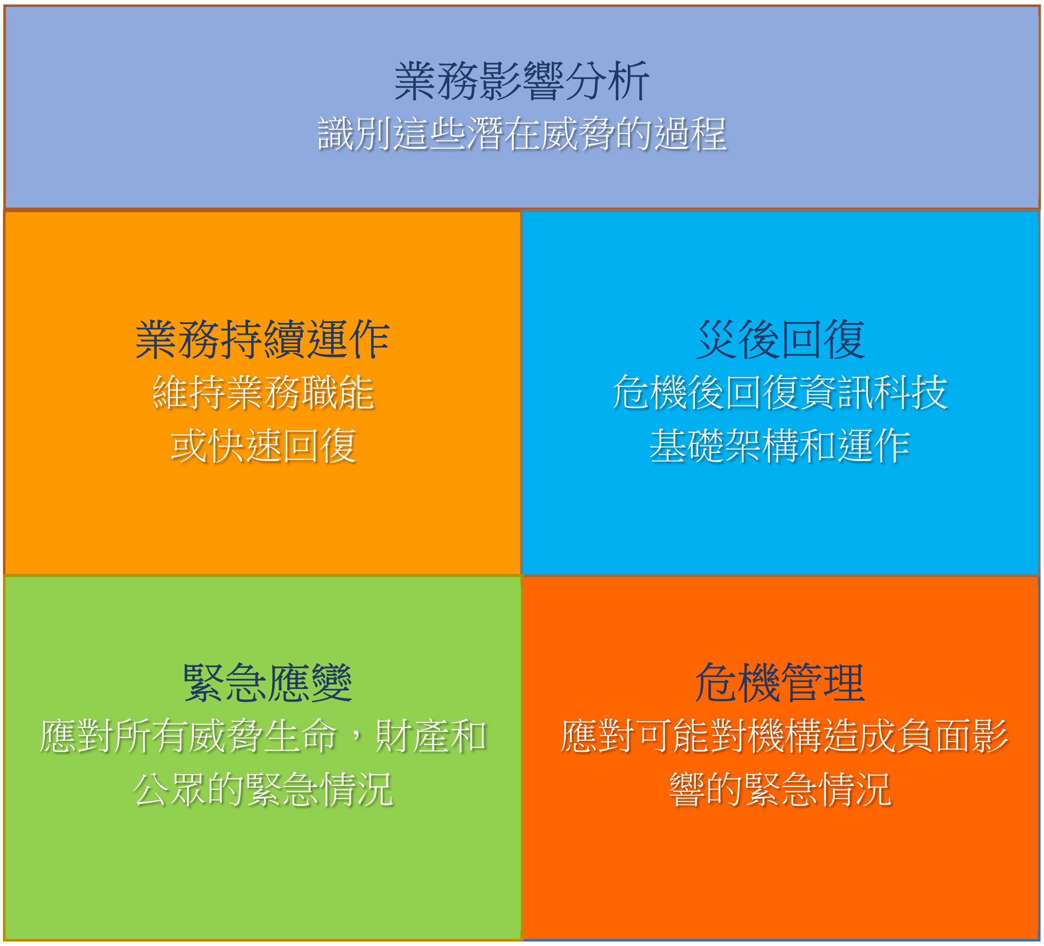


圖 6: 業務持續性管理項目

表 41: 業務持續性管理

7.17. 日誌管理與監控

日誌記錄和監視密切相關，因為日誌數據是機構可用於執行應用程式/存取控制監視的關鍵數據源之一。雖然日誌並不是機構賴以監視具有價值的應用程式的工作指標的唯一來源，但自應用程式、伺服器、網路基礎設施和更多方面等所創建的日誌，提供了可詳細觀察網路及應用程式運行情況的窗口。

日誌管理和監控的目的是檢測未經授權的網絡及系統資訊處理活動，有效的日誌管理對於保安性和合規性都至關重要。

如果沒有正確管理環境中有用的應用程式監控工具所獲取數據，可能會導致機構缺乏監控所需的關鍵數據來源。如果監控沒有成效，系統管理員／保安人員將無法理解日誌內容，以瞭解機構的應用程式的運作性能；系統管理員/保安人員也無法排除問題並防止問題再次發生。

日誌管理／保安資訊和事件管理（Security Information Event Management, SIEM）的解決方案可能很多，機構也可以採用各式各樣的開源解決方案，但是通常需要有豐富經驗的技術知識和充足的時間來設置及操作。另一種選擇是實施 NCSC[51] 的 Logging Made Easy[52]（LME）工具，以收集 Windows 客戶端中基本的日誌記錄，用作檢測攻擊之用。

日誌管理與監控		利益相關者：管理層、資訊科技管理員		
安全級別: E = 初級, I = 中級, A = 高級		E	I	A
1	網絡及系統應該保持監察系統，並記錄資訊保安事故。		✓	✓
2	日誌應從以下來源收集：反惡意程式，關鍵應用程式、用戶身份驗證、防火牆、IDS / IPS，NAS、網絡設備，操作系統、遠程訪問軟件（例如 ：VPN、RDP）、網絡代理和網絡伺服器等等。		✓	✓
3	應定期記錄和審查操作人員日誌和系統故障日誌，以及早發現資訊系統問題。		✓	✓
4	應制定審計日誌記錄用戶操作活動，異常和資訊保安事件，並在既定的期限內保存，以幫助將來進行調查和存取控制監控。		✓	✓
5	日誌管理系統必須設定以解析對機構而言至為重要的事件和數據，以讓報表具有業務和技術價值。		✓	✓

[51] National Cyber Security Centre, UK (NCSC)
https://www.ncsc.gov.uk
[52] Logging Made Easy, NCSC, UK
https://github.com/ukncsc/lme

6	定期查看警報控制台，系統管理員/保安人員從而不會遺漏重要的保安事故。		✓	✓
7	除了維持日誌管理操作之外，還應該定期審查日誌條目。		✓	✓
8	系統伺服器時間應和時間伺服器同步以使日誌記錄的時間戳同步相對應。這可以通過設置時間伺服器來完成。		✓	✓
9	應按需要保留的日誌記錄天數和容量進行日誌伺服器磁碟空間容量估算規劃。		✓	✓
10	定時透過網絡日誌可找出系統或網絡上過去發生了什麼事或剛觸發了什麼事件。			✓
11	可外判日誌管理或要設置日誌管理系統 / SIEM以進行保安事故監察。			✓

行動
（主要由人手操作）
-回應，補救和恢復
-升級
-調查
-事故管理
-報告
-變更管理

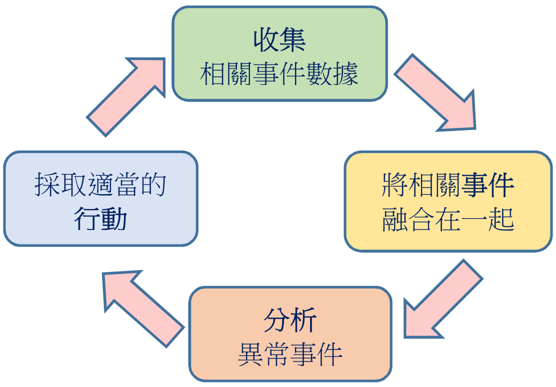


圖 7: 網絡安全監控關鍵組件

收集
（主要經機器操作）
-日誌識別
-規範化
-保留
-過濾

分析
（主要由人手操作）
-預先擬定規則
-分流
-工作流程
-趨勢/模式/風險分析
-威脅情報

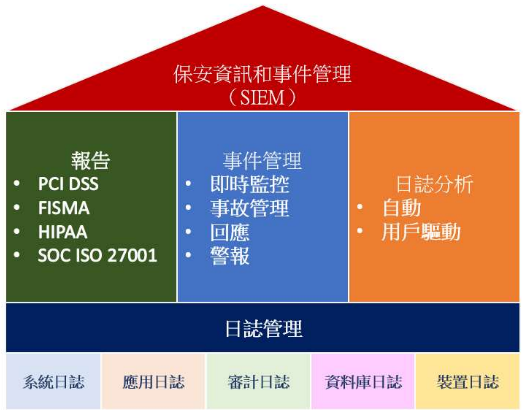


圖 8: SIEM 傘視圖

融合
（主要經由機器操作）
-自動化
-SIEM 規則
-防火牆規則
-IDS / IPS 識別碼
-損害指標 IOC

表 42: 日誌管理與監控

相關工具：
9.6　Logging Made Easy (LME)

8. 清單及範本

8.1. 資訊科技資產評估清單範本

資訊科技資產評估清單是用作悉知機構所擁有、管理或以其他方式使用中的資訊科技設備清單。這些設備包括：電腦（如：桌面機、筆記本電腦、伺服器）、網絡設備（如：交換機，路由器等）、打印機、其他裝置設備（如：網絡連接存儲，具有網絡功能的相機等），以及非政府組織的數據資產。

資訊科技資產評估清單重要而有用的原因有許多，包括：

- 提供資產價值記錄，以進行會計/追踪
- 協助指出有潛在保安隱憂 (如：筆記本電腦有否儲存私隱敏感的資料應指涉及個案資料、伺服器保養服務是否過期等等)
- 業務發展規劃所需要的重要資料
- 當需要技術支援，或發生如盜竊遺失時提供有用的資料

	A	B	E	F	G	H	I	J	K	L	M	N	O
1	資產編號	資產資料	位置	資產價值	資料分類 (保密性)	保安風險管理	系統更新 (資料完整性)	復原力 (可用性)	存取人士	後果嚴重性 (影響程度)	脆弱性 (威脅程度)	出現風險 (可能性)	保安評分
2	WAS-001	網上應用程式, 接通互聯網, 跨機構	NGO DC-001	很高	限閱	只有一次	過時的	定期備份	機構內部	非常高	高	低	11
3	WAS-002	網上應用程式管理系統 (保密)	NGO DC-002	低	內部	只有一次	經常	定期備份	機構內部	非常低	低	低	5
4	WAS-003	公用網站	Public Cloud (Azure)	高	公共	只有一次	過時的	沒有計劃	內部及公眾	低	高	非常高	11
5	SYS-001	網上應用程式(供非政府機構及公眾	Public Cloud (Azure)	高	內部	只有一次	有計劃	定期備份	公眾	中	中	中	9
6	SYS-002	網上應用程式(內部使用)	On-premises	中	內部	定期評估	有計劃	定期備份	機構內部	低	非常低	低	5
7	SYS-003	網上應用程式(內部敏感資料)	On-premises	中	限閱	只有一次	有計劃	定期備份	機構內部	中	中	低	8
8	Mobile-001	內部使用流動應用程式	Out Door	中	內部	只有一次	有計劃	沒有計劃	機構內部	低	中	中	8
9	NGO-Data	非政府機構擁有者資料	NGO	中	限閱	只有一次	有計劃	定期備份	機構內部	中	中	低	8
10	NGOs-Data	非政府機構共用資訊	G-Suite-Google	中	限閱	只有一次	過時的	高可用性	機構內部	中	高	非常低	8
11	WEB-001	非政府機構網站	Cloud	中	內部	只有一次	過時的	定期備份	機構內部	低	高	低	8
12	WEB-002	非政府機構內聯網	On-premises	中	內部	沒有計劃	過時的	沒有計劃	機構內部	低	非常高	中	10
13	HRS-1002	227.12.27.5	HRM-Azure-Cloud	中	內部	3年或以上	過時的	定期備份	機構內部	低	中	低	7
14	FIN-1001	226.50.1.10	IMS-Azure-Cloud	中	限閱	3年或以上	過時的	進行過演練	公眾	中	中	低	8
15	NGO-APP-001-P	非政府機構公用程式	HQ-DC-01-P	中	內部	只有一次	過時的	定期備份	公眾	低	高	中	9
16	IFS-HQ-DC-OA-01	10.10.20.100	HQ-DC-01	中	內部	沒有計劃	過時的	定期備份	機構內部	低	非常高	低	9
17	IFS-HQ-DC-CASE-01	10.10.20.101	HQ-DC-01	中	限閱	沒有計劃	有計劃	定期備份	機構內部	中	高	低	9
18	WEB-HQ-DC-01	10.10.1.10/225.128.1.2	Cloud AWS	中	內部	3年或以上	過時的	定期備份	內部及協作夥伴	低	中	高	9
19	IDB-HQ-DC-01	10.10.5.5	HQ-DC-01	高	限閱	只有一次	過時的	高可用性	機構內部	高	高	非常低	9
20	IDB-HQ-DC-02	10.10.5.6	HQ-DC-01	高	機密	沒有計劃	不清楚	沒有計劃	機構內部	非常高	非常高	中	13

圖 9: 資訊科技資產評估清單

資訊科技（IT）資產評估（模板）（

8.2. 資訊保安事故回應報告表格及記錄（範本）

8.2.1 資訊保安事故回應報告表格

此資訊保安回應表格提供了一個範本，方便當資訊保安事故發生時，能詳細記錄事故的始末並向機構報告相關情況。

資訊保安事故回應報告表格

事故發現資訊	
通報日期及時間:	
事故發現者資料:	
姓名:	發現日期及時間:
職位:	地點:
電話/聯絡資訊:	系統/應用程式:
事故摘要	
事故類別: ☐ 拒絕服務 ☐ 惡意程式碼 ☐ 非法使用 ☐ 非法進入 ☐ 突然停機 ☐ 其他	
事故描述: 嚴重程度: 補救措施:	
其他人士姓名及聯絡資料:	
事故通報 – 其他	
☐ 資訊保安管理者 ☐ 系統/程式擁有人 ☐ 系統/程式供應商 ☐ 資訊保安事故應對小組 ☐ 公共事務 ☐ 法律顧問 ☐ 行政 ☐ 人力資源 ☐ 其他	
動作	
偵測方法 (核實及評估事故, 其他偵測評估方法):	

圖 10: 資訊保安事故回應報告表格（範本）

資訊保安事故回應報告表格及記錄（範

8.2.2 資訊保安事故回應記錄（模板）

此表格提供範本以方便非政府組織報告及記錄資訊保安事故。

資訊安全事故回應報告表	
匯報季度 / 年份	請選擇
部門	
組別	
聯絡人	
電郵地址	
電話號碼	
日期	
指示	請按下列指示填寫本表格 1. 填寫本頁各項 2. 按“詳細匯報”頁面填寫各必要項目 3. 入侵指標為必須填寫項目。然而，當需要填寫的入侵指標眾多時，請前往"IOC" 頁面輸入事故參考編號、選擇類別及輸入入侵指標資料 4. 完成填寫「封面」、「詳細報告」、及「入侵指標」各頁面後，請將此檔案傳送至機構的資訊安全應變小組 - 電郵地址: ITSec_XXXX@XXXX.org.hk - 主旨: <部門名稱> - Q<編號> - <年份> - 季度資訊安全事故報告
更多資訊	請參考非政府機構資訊科技安全事故匯報指引

圖 11: 保安事故回應報告記錄（模板）

資訊保安事故回應記錄（模板）.xlsx

8.3. 供應商風險評估清單（模板）

非政府組織較常因資源問題需要尋找第三方供應商以供應設備及服務。

由於管理供應商風險是網絡保安的基礎，確保運作順暢及保持合規性，對供應商的風險管理是重要的。穩健的供應商風險管理計劃可協助機構控制本身的風險，以減輕由第三方及第四方供應商之間所帶來的風險，而非依靠事故發生後的應對。

設計供應商風險評估調查問卷旨在協助機構識別第三方供應商和合作伙伴中可能導致數據外露、數據洩漏或其他類型的網絡攻擊的潛在的問題。

供應商風險評估範本

#	供應商號碼	供應商名稱	聯絡人	目的	是否需要存取客戶資料	是否需要存取財政資料	重要性分數
1							
2							
3							
4							
5							
6							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							

圖 12: 供應商風險管理記錄（模板）

供應商風險管理記錄（模板）（中文

8.4. 保安審計清單（範本）

在進行資訊科技保安審計時，審計人員會審視機構所制定的風險管理和保安策略，以確定機構的合規工作的投入力度。未能通過合規審查表明機構內存在保安缺陷，若不採取補救行動的話後果可能非常嚴重，最終包括可危及機構的業務運作。

	機構名稱:			日期:	
	審核清單				
	主題		狀況	客戶回應	備註
1	保安計劃	問題			
1.1	角色及責任	機構是否已經委任職員統籌保安事件？			
		a) 如有，此職位由何人出任，以及在機構內擔當什麽的職位？			
		b) 有否清楚紀錄有關職責？（如職位描述，資訊保安政策）			
1.2	外間組織	機構是否需要與存取資料的外間機構合作（如：互聯網供應商）			
		a) 機構與外間機構有否簽訂合作協議？			
		b) 如否，機構使用什麽措施監察及評估外間機構（如：透過虛擬私人網絡登入）			
2	保安政策				
2.1	資訊保安政策及程序	機構是否已訂立保安政策及程序？			
		a) 是否已制定資料分類程序？ 請加以描述 (如重要、基本、普通)			
		b) 是否已爲資產訂立可接受使用守則？(資產包括資料、電腦設施、通訊設備等)			
		c) 是否有既定程序維護保安政策？			
3	培訓及意識				
3.1	在職培訓及教育	a) 僱員是否已接受正規資訊安全訓練？			
		b) 有關政策是否已知會各僱員？有否定期覆修課程？（如：迎新課程、周年培訓、公用地方宣傳品、電郵提示等）			

圖 13: 資訊科技審計清單（範本）

資訊科技（IT）審計清單（模板）（

8.5. 網絡保安的七大習慣

香港生產力促進局（生產力局）轄下 香港電腦保安事故協調中心 (HKCERT) 編寫了《網絡保安七大攻略》指引，涵括以下七個層面：

- 資訊保安政策和資訊保安管理
- 終端保安
- 網絡保安
- 系統保安
- 保安監察
- 保安事故處理
- 用戶保安意識

這「七大習慣」指引的內容包括如何建立良好作業模式，以及簡單的保安風險自我評估清單，有助中小企及非政府組織運用有限的資源，以應付日趨複雜的網絡保安威脅。

安全層面	控制理念	最佳實踐	自我評估（✓所適用的）
1. 安全政策和安全管理	安全政策是企業裡的重要文檔。 它闡明了管理層在網絡安全風險管理方面的安全要求和態度。管理層應建立一種機制，定期維護和宣傳安全政策對員工的要求。	✓ 員工應有機會閱讀安全政策，了解公司的安全要求，並在入職時確認他們會遵從要求。 ✓ 安政策應放在員工可以輕易參閱的地方。 ✓ 安全政策應定期更新，也應讓員工定期重新確認政策。	☐ 我的機構沒有安全政策 ☐ 我的機構有安全政策，員工可以輕易參閱安全策略 ☐ 員工入職時需要確認安全政策 ☐ 員工需要定期重新確認安全政策

圖 14: 網絡保安的七大習慣

非政府組織網絡保安的七大習慣.docx

8.6. 保安風險評估指引

風險評估並不是一次性就能為決策者提供永久和明確的資訊、以指導和為資訊保安風險的應對提供資訊的工作。相反，機構在整個系統開發週期內及運作期間，應跨越所有不同風險管理層級，持續進行風險評估，而風險評估的頻率和評估期間使用的資源，須與評估時明確界定的目的和範圍相稱。

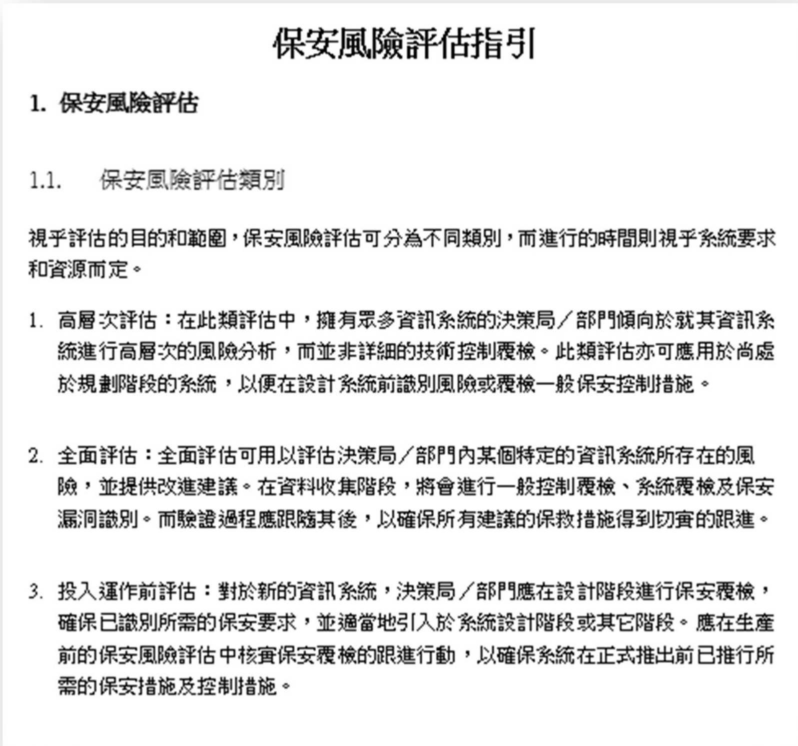
此保安風險評估指引側重於風險管理的風險評估部分，為機構在以下方面提供了每一步驟的過程：

(一)如何準備風險評估；

(二)如何進行風險評估；

(三)如何將風險評估結果向機構主要人仕溝通；以及

(四)如何持續進行風險評估。



保安風險評估指引

1. 保安風險評估

1.1. 保安風險評估類別

視乎評估的目的和範圍，保安風險評估可分為不同類別，而進行的時間則視乎系統要求和資源而定。

1. 高層次評估：在此類評估中，擁有眾多資訊系統的決策局／部門傾向於就其資訊系統進行高層次的風險分析，而並非詳細的技術控制覆檢。此類評估亦可應用於尚處於規劃階段的系統，以便在設計系統前識別風險或覆檢一般保安控制措施。

2. 全面評估：全面評估可用以評估決策局／部門內某個特定的資訊系統所存在的風險，並提供改進建議。在資料收集階段，將會進行一般控制覆檢、系統覆檢及保安漏洞識別。而驗證過程應跟隨其後，以確保所有建議的保救措施得到切實的跟進。

3. 投入運作前評估：對於新的資訊系統，決策局／部門應在設計階段進行保安覆檢，確保已識別所需的保安要求，並適當地引入於系統設計階段或其它階段。應在生產前的保安風險評估中核實保安覆檢的跟進行動，以確保系統在正式推出前已推行所需的保安措施及控制措施。

圖 15: 保安風險評估準則指引

保安風險評估準則指引（中文）.docx

9. 保安風險評估工具

9.1. WinAudit

免費資產管理工具 (適用於微軟視窗作業系統)

WinAudit 是一套為微軟視窗作業系統而設的資產管理工具，它可依據相關電腦配置、硬件和軟件建立綜合報告清單，它是一套免費應用軟件，任何人皆可分發及使用。

WinAudit 可對電腦內的微軟視窗作業系統、使用許可證、保安配置、硬件、網絡設置等執行審計及建立清單。

WinAudit 特點：

- 簡單易用
- 免安裝
- 可匯出結果至 csv / html / pdf / xml 格式報告
- 可匯出結果至數據庫
- 可以在命令行執行
- 詳細的操作文件

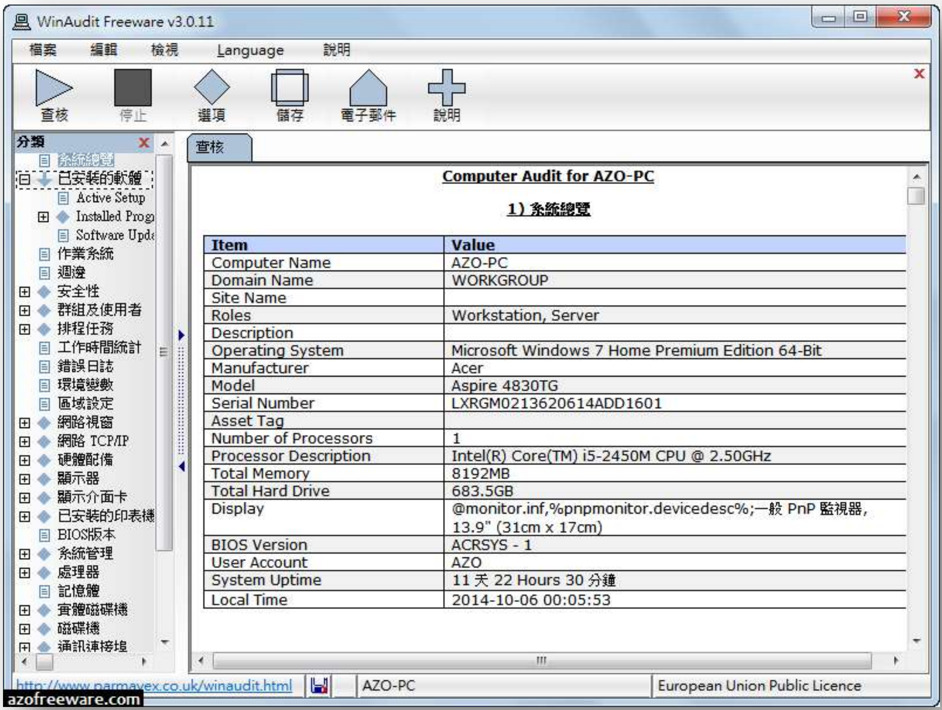


圖 16: WinAudit 資產審計工具

WinAudit 電腦庫存工具	http://www.parmavex.co.uk/winaudit.html
WinAudit 示範	https://briian.com/7359/

9.2. NMap/Zenmap 網絡保安掃描器

網絡保安掃描器 (適用於 Windows, Linux, Mac OS X)

Nmap ("Network Mapper") 是一套為網絡保安審計而設的開放源碼工具。許多系統和網絡管理員認同它對於建立網絡清單，管理服務升級計劃，以及監測主機或服務正常運行時間等工作非常有用。

該工具可用於查找網絡上正在活動中的主機，執行連接端口掃描、ping 掃描、操作系統版本檢測等。

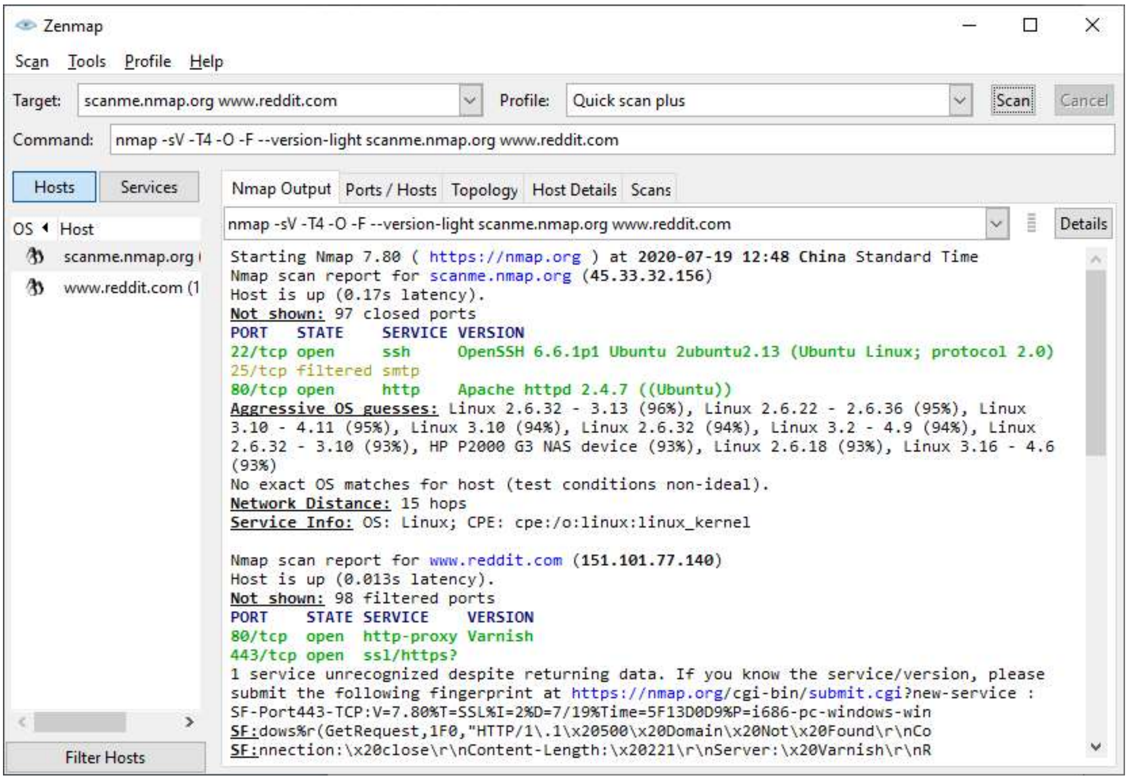


圖 17: Nmap 網絡保安掃描器

Nmap 網絡保安掃描器 GUI https://nmap.org/download.html

如何使用 Zenmap 掃描網絡 https://linuxhint.com/zenmap_scan_network/

9.3. Nessus Essentials

網絡及主機保安漏洞掃描工具 (適用於 Windows, Linux, Mac OS X)

Nessus 是現時在漏洞評估和滲透測試（包括惡意攻擊）界中最多人使用的漏洞掃描工具之一。

Nessus 可用於執行各種掃描任務，包括：漏洞檢測掃描、配置審計掃描和修補程式狀態掃描。掃描後可以產生出詳細報告，方便進一步分析系統問題和如何進行修復工作。

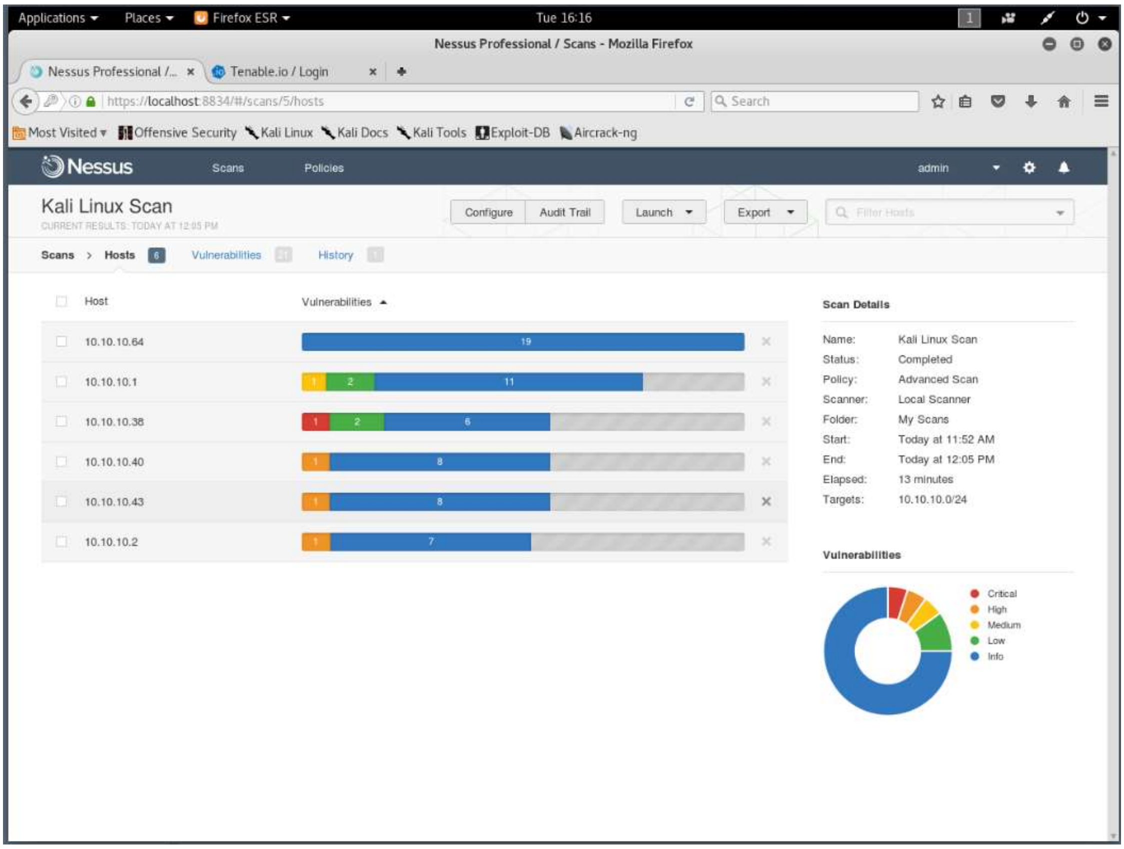


圖 18: Nessus 保安漏洞掃描工具

Nessus 保安漏洞掃描工具 https://www.tenable.com/products/nessus

啟動並運行您的 Nessus 漏洞評估工具
https://zh-tw.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus

9.4. OWASP Zed 攻擊代理 (ZAP)

網上應用程式掃描軟件（適用於 Windows, Linux, Mac OS X）

Zed Attack Proxy （ZAP）是由開放網路應用程式保安計劃 （Open Web Application Security Project - OWASP） 旗下的一套免費開放源碼的網上應用系統滲透測試工具，它是專為測試網上應用程式而設計，且既靈活又具擴展性。

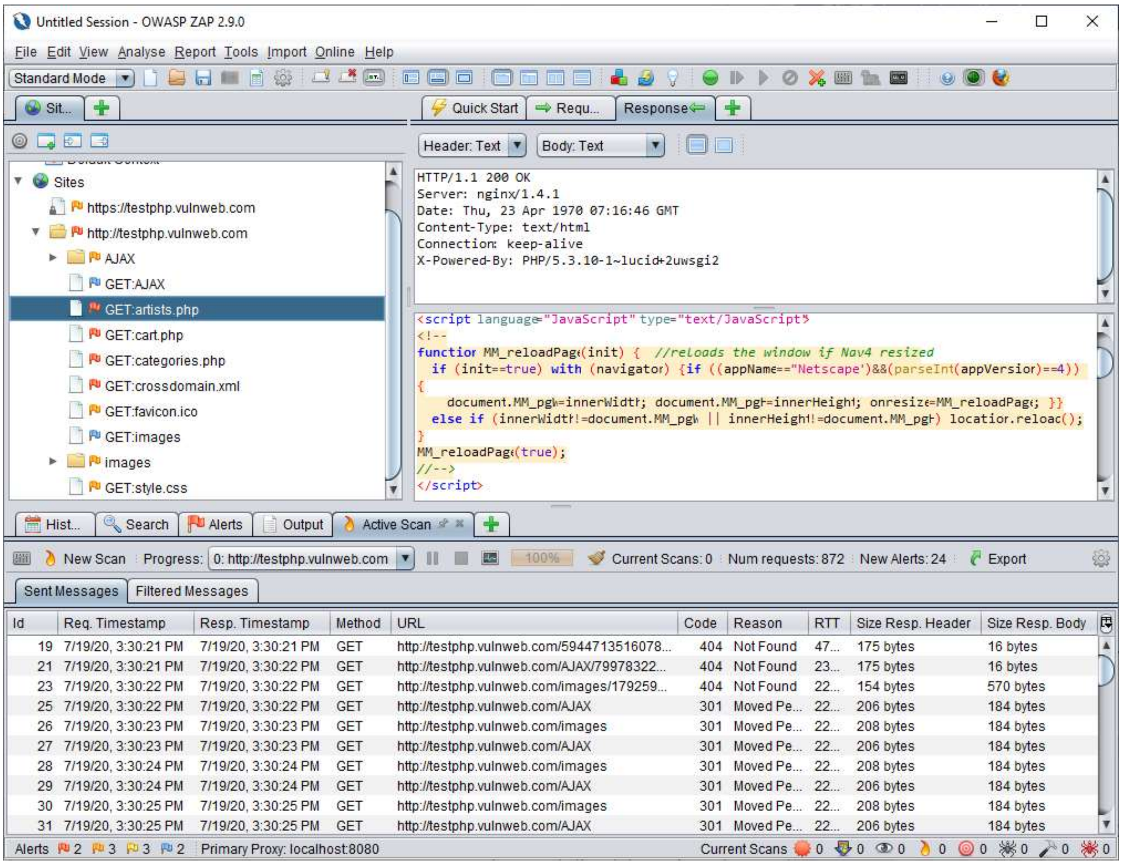


圖 19: Zed 攻擊代理 OWASP

The OWASP Zed 攻擊代理 https://www.zaproxy.org/

Zaproxy 教學影片 https://github.com/zaproxy/zaproxy/wiki/VideoTutorials

9.5. Kali Linux

專業滲透測試的 Linux 發行版本 (Linux 系統)

Kali Linux 系統建基於 Debian Linux 的發行版本，目的是旨在建立一套可進行高級滲透測試和保安審計的電腦網絡系統的環境。

Kali Linux 已預先安裝了 600 多套可進行各種不同滲透測試方法的套件，內容包括： nmap（網路連接端點掃描工具），Wireshark（網絡封包分析工具），John the Ripper (密碼破解工具），Aircrack-ng（可進行無線局部區域網絡滲透測試的軟件組合），Burp suite 及 OWASP ZAP （兩者皆為網上應用系統掃描工具）。

除了直接用下載的 DVD 安裝在本機硬碟上運行，亦可從光碟或 USB 儲存裝置在電腦上實時運行，或以虛擬機器運作。

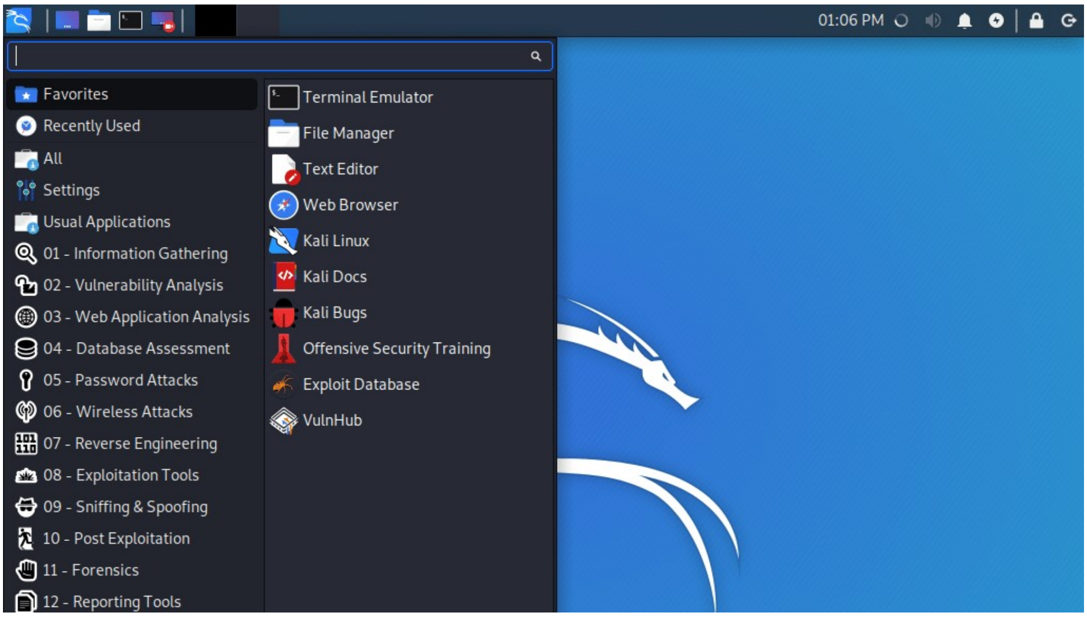


圖 20: Kali Linux

Kali Linux https://www.kali.org/

安全滲透教程 https://wizardforcel.gitbooks.io/daxueba-kali-linux-tutorial/content/

9.6. Logging Made Easy (LME)

Logging Made Easy (LME)

Logging Made Easy 是一套專為小型機構定製的保安日誌管理自助安裝教程，旨在為 Windows 用戶端提供基本級別的中央收集式保安日誌管理，並提供檢測攻擊的功能。 它是一個集合多種免費開放源碼軟件（當中一些軟件受 Apache V2 以外的使用許可涵蓋）的整合套裝，其中 LME 幫助用戶/系統管理者將電腦日誌記錄整合以產生點對點的日誌記錄功能。此軟件還提供了一些預製的配置文件和編程範本，或可以選擇由系統管理者自行配置執行。

非政府組織可考慮使用 Logging Made Easy (LME)，若：

- 機構內部沒有網絡保安監控中心（security operations center ,SOC）、保安資訊和事件管理（Security Information Event Management, SIEM）或任何監控架構
- 在機構缺乏預算、時間和保安日誌管理的認知，機構如何去安裝日誌管理系統收集日誌
- 認識到需要收集日誌以監察機構的資訊科技運作
- 了解到 LME 其局限性，不能與專業工具相比，但聊勝於無
- 非政府組織系統未能夠監控在小型分隔網絡內的電腦
-

Logging Made Easy (LME) 可以：

- 通知系統團隊該登記設備中的該設備軟件修補水平的信息
- 顯示該登記設備在那些地方執行過系統管理員指令
- 知悉誰人正在使用哪些電腦
- 結合威脅報告，可以藉由工具、技術和程序（TTP）的方式，可了解是否存在保安威脅

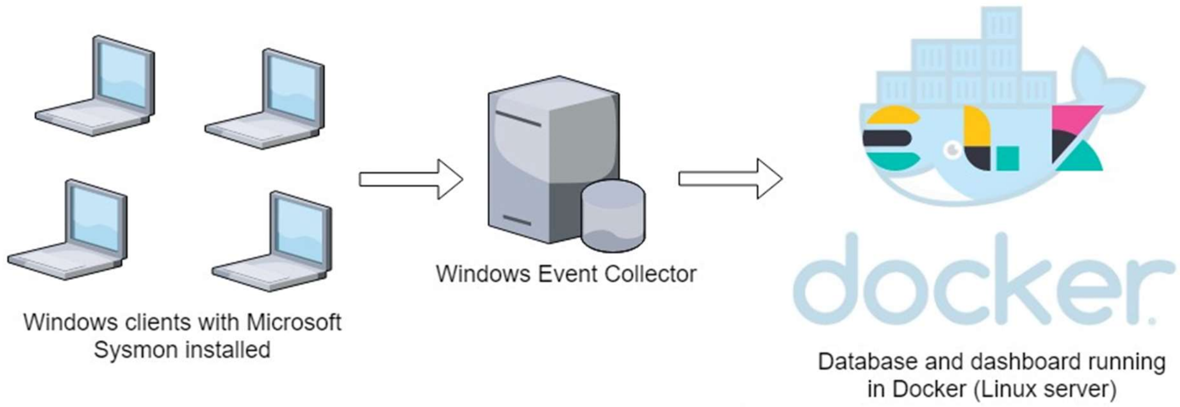


圖 21: Logging Made Easy

Logging Made Easy, NCSC, UK https://github.com/ukncsc/lme

9.7. VeraCrypt

VeraCrypt (Windows, Linux, Mac OS X)

VeraCrypt 是一套為 Windows, Mac OSX 及 Linux 而設的開放源碼磁碟加密軟件。

VeraCrypt 的 主要功能包括：

- 建立一個虛擬且加密的儲存器檔案，並將其作當為真實磁碟安裝
- 為整個硬碟分區或存儲設備，例如 USB 儲存器或硬碟加密
- 安裝 Windows 的分區或磁碟（在引導程序前預先啟動身份驗證）加密
- 其加密是自動、實時的（動態的）且對用戶透明。
- 藉由並行化和流水線處理技術，令設備可以像未經加密的磁碟一樣，快速地讀寫數據
- 在現代的處理器上可以硬件加速加密處理
- 以防萬一用戶被黑客手段強迫透露密碼時，通過隱寫術隱藏硬盤空間以隱藏操作系統 。

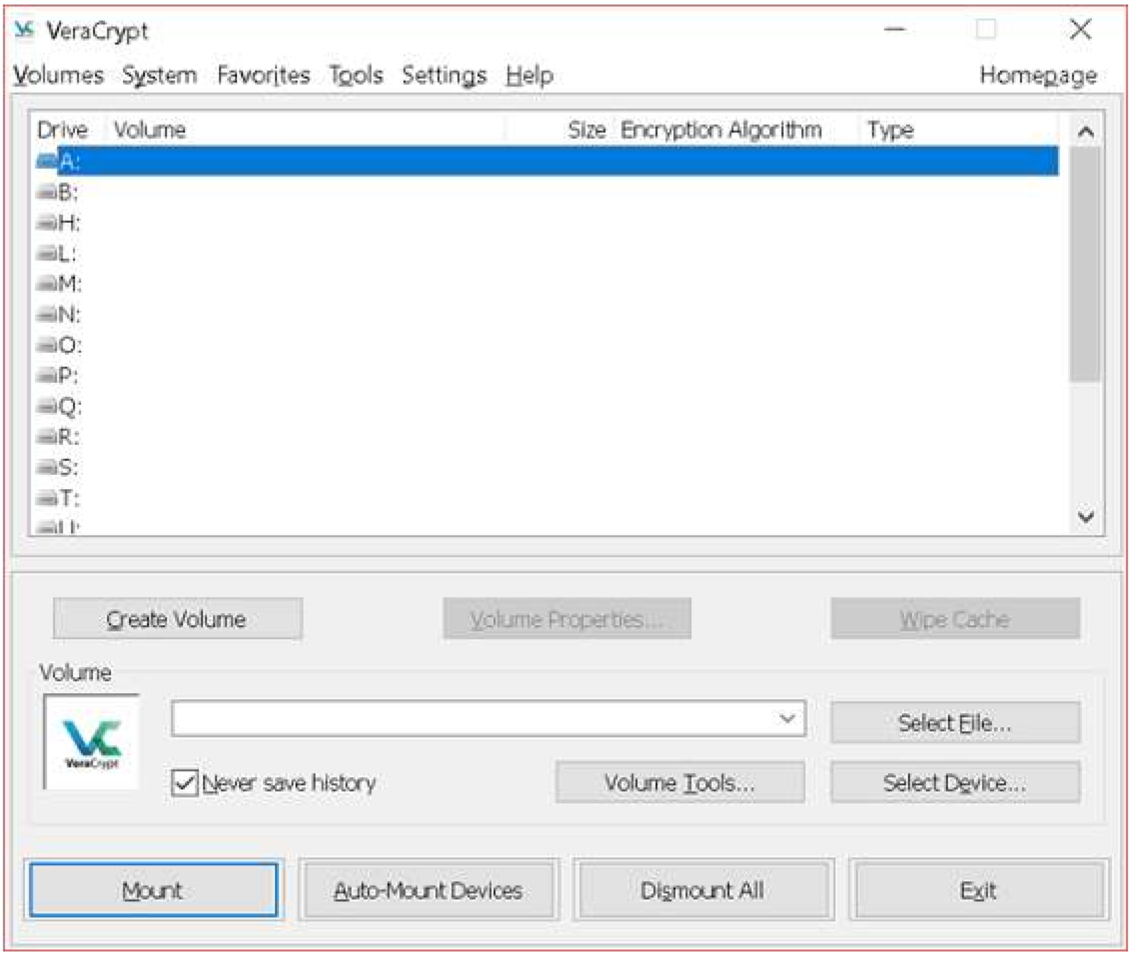


圖 22: VeraCrypt

VeraCrypt https://www.veracrypt.fr/code/VeraCrypt/

VeraCrypt 教程 https://izaka.tw/2015-3-8-226/

附錄 A-參考

法律，法規，標準， 政策和準則

本指引借鑒了各種網上資訊來源，包括來自國防、審計、財務、工業/流程控制和情報界的保安操作指引，以及由國家和國際標準機構所制定的控制機制。這些指引乃純粹從技術角度編製，旨在為非政府組織成員制定的一套完善且可被廣泛使用的資訊科技和電腦系統保安作為指引。

以下文件是由原理和最佳行事指引構成的參考資料：

A. ISO/IEC 27001:2013 資訊保安管理系統 (ISMS)
- ISO / IEC 27001：2013規定了在機構範圍內建立、實施、維護和持續改進資訊保安管理系統的要求。它還包括針對機構需求所制定的資訊保安風險評估和處理要求。 ISO / IEC 27001：2013中列出的要求為通用性質，旨在應用於所有不論類型，規模或性質的機構。
  https://www.iso.org/standard/54534.html

B. ISO/FDIS 9001:2015 質量管理體系 (QMS)
- ISO 9001：2015適用於任何規模或行業的機構。 ISO 9001按照計劃 （Plan） - 實施 （Do） - 檢查 （Check）- 和處理（Action）方法體系提供了一種以流程為導向的工作方式，用於記錄和審查賴以在機構中實現有效質量管理所需的結構，職責和程序。
  https://www.iso.org/standard/62085.html

C. 保安和隱私控制行為準則
- 涵蓋六項數據保護原則的國際保安控制標準（Data Protection Principles 1 - 6）。
  https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

D. 小型企業訊息保安：基礎知識 (NISTIR 7621)
- 概述了小型企業為保障其訊息，系統和網絡所必須採取的行動。
  https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

E. 聯邦訊息系統和機構的保安和隱私機制 (NIST SP 800-53.r4)
- 保安操作機制國際標準涵蓋17個領域，當中包括：存取控制、事故回應、業務持續性和災難回復性。
  http://dx.doi.org/10.6028/NIST.SP.800-53r4

附錄 B-詞彙表

通用術語和界定

縮略語	描述
進階持續性滲透攻擊(APT)	進階持續性滲透攻擊（APT）是一種長期且有針對性的網絡攻擊，入侵者取得對網絡的存取權限，並且在很長一段時間內都未被發現。啟動 APT 攻擊是為了竊取數據，而不是破壞目標機構的網絡。
資產	屬於企業或由企業擁有的具有一定價值的任何物品（包括各種形式的資訊和電腦系統）。
業務延續性管理	業務持續運作管理是整個管理系統的一部分，該系統實施，操作，監視，審查，維護和改善業務延續性。
業務延續性計劃	業務延續性計劃有記錄地收集流程和資訊，這些流程和資訊經過開發，編譯和經常覆核，可隨時於遇到某事故時派上用場，以使機構能夠繼續以預定可接受的水平提供其關鍵產品和服務。
商業電子郵件侵奪(BEC)	商業電子郵件侵奪(Business Email Compromise，BEC)是可招致最大經濟損失的網絡犯罪之一。在 BEC 騙局中，犯罪分子會透過已入侵的合法來源電子郵件發送正當指令以作出請求，例如批准付款或釋放客戶數據。電子郵件經常通過社交工程方式誘騙受害者將錢轉入欺詐者的銀行帳戶。
BitLocker	BitLocker 硬碟加密是一項集成於操作系統的數據保護功能，可以解決遺失，被盜或被不當停用的電腦對數據造成的盜竊或暴露威脅。
保安漏洞	保安漏洞是由於疏忽或故意攻擊而引起的安全隱患, 可能違反守則或法律，並且經常進一步被用來進行有害或刑事犯罪行為。
CSRF	跨站點請求偽造(CSRF)是一種攻擊方式，誘騙受害者發送惡意請求。它取得受害者的身份和特權，可以以受害者名義執行不當功能。
網際 (Cyber)	與用於存取互聯網並與其互動的電腦，軟件，通信系統和服務有關。
DKIM	網域密鑰標識郵件（DKIM）是一種電子郵件身份驗證技術，它使接收方可以驗證該網域的擁有者確實已發送並授權該電子郵件。
DMARC	基於網域的郵件身份驗證，報告和一致性（DMARC）是一種電子郵件驗證系統，旨在保護機構的電子郵件域免被用於電子郵件詐騙，網絡釣魚詐騙和其他網絡犯罪。 DMARC 利用現有的電子郵件身份驗證技術 SPF（發件人原則框架）DKIM（網域密鑰標識郵件）。

加密文件系統	微軟視窗上的加密文件系統（EFS），提供文件系統級別的加密。
加密	將訊息轉換為只有擁有必要（通常是唯一的）密鑰和特殊軟件的授權人員才能閱讀的代碼，以便他們可以逆轉該過程（例如解密）以使用該訊息。
防火牆	防火牆是裝置在網絡環境之間的一道保安屏障。它可以是專用設備，也可以是幾種組件和技術的組合。僅允許在本地保安守則下所授權流量通過。
GCHQ	政府通信總部，通常稱為 GCHQ，是一個情報和保安機構，負責向聯合國政府和武裝部隊提供信號情報（SIGINT）和資訊保障。
身份盜取	複製他人的個人身份訊息（例如其姓名和社會保險號碼），然後假冒該人進行欺詐或其他犯罪活動。
入侵指標	入侵指標（IOC）可在網絡或操作系統中觀察到的現象，而我們高度確信所述現象顯示電腦正遭入侵。
IDS/IPS	入侵檢測系統（IDS）分析網絡流量中與已知網絡攻擊相匹配的簽名，然後發出警報以警告操作員。 入侵防禦系統（IPS）還可以分析數據包，但也可以根據其檢測到的攻擊類型阻止數據包的傳遞，從而有助於阻止攻擊。
ITSPG	資訊科技保安實踐指南
惡意軟件	惡意軟件通過有意製造和分發手段以造成損害。惡意軟件最常見的實例是病毒。
OAuth2	OAuth 2.0 授權框架讓第三方應用程式能夠通過協調資源擁有者和 HTTP 服務之間的核准流程，或通過允許第三方應用程式代表資源擁有者來獲取對 HTTP 服務的有限存取權。
OpenID	OpenID 是一種分散式身份驗證協議。它允許用戶通過使用第三方服務的協作站點（稱為依賴方或 RP）進行身份驗證，從而無需網站管理員提供自己的臨時登錄系統，並允許用戶登錄多個不相關的網站而無需為每個帳戶分別設置身份和密碼。
修補程式	在不替換整個原始程式的情況下對所應用的任何形式的軟件進行的更新或修復。軟件開發人員提供了許多修補程式程式來解決已識別的保安漏洞。
滲透測試	滲透測試旨在識別特定的系統配置以及機構流程和實踐中的弱點，這些弱點可被利用來破壞安全。

釣魚郵件	一種特定類型的垃圾郵件並同時針對一個或多個特定人士，透過冒充合法郵件欺騙收件人。
風險	當威脅出現時會出現負面結果的機會。
保障措施	旨在應對特定威脅的保安流程、實體安全機制或技術工具。有時也稱為控件。
SIEM	保安資訊和事件管理（SIEM）是電腦保安領域的一個輔助環節，當中通過軟件產品和服務結合保安資訊管理（SIM）和保安事件管理（SEM）。它們提供對由應用程序和網絡硬件生成的保安警報的實時分析。
SOAR	SOAR（保安協調，自動化和回應）是指一組可讓機構在三個關鍵領域：威脅和漏洞管理、事件回應以及自動化保安操作上提升保安操作效率的軟件解決方案和工具。
SPF	發件人策略框架（SPF）是一種電子郵件身份驗證技術，用於防止垃圾郵件發送者代表機構全體發送郵件。一個機構可以借助 SPF 推出授權的郵件伺服器
SRA	SRA（安全風險評估）是指量化或定性描述資訊安全風險，並使機構能夠根據其嚴重性對風險進行優次排序的方式。它可確定資訊資產的價值，並確定所覆蓋（或可能覆蓋）的威脅和漏洞，以及確定現有控制措施及其對所識別風險的影響，再評定其潛在後果並為這些風險排序。
威脅	對業務安全構成危險的任何潛在事件或行為（有意或意外）。
保安漏洞掃描	保安漏洞掃描的目的是確定任何存在已知漏洞的系統所在
保安漏洞	軟件，硬件，實體安全性或人為操作方面所存在的弱點，可被利用進行進一步攻擊。
WAF	網上應用系統防火牆（WAF）監視和篩選進出機構網站的流量，阻止居心不良者，同時容許正常安全流量。

表 43: 詞彙表

附錄 C - 縮略語

常用的縮寫

Abbreviation	Description
ACL	Access Control List 訪問控制列表
AD	Active Directory 活動目錄
AES	Advanced Encryption Standard 進階持續性滲透攻擊
AP	Wireless Access point 無線接入點
APT	Advanced Persistent Threat 高級長期威脅
Audit	Security Audit 保安審計
BEC	Business Email Compromise 商務電子郵件詐騙
BIOS	Basic Input Output System 基本輸入輸出系統
BitLocker	BitLocker Drive Encryption 微軟磁碟加密技術
BYOD	Bring Your Own Device 自攜裝置
CASB	Cloud Access Security Brokers 雲端存取安全代理程式
CIO	Chief Information Officer 資訊總監
COPE	Company Owned/Personally Enabled 企業擁有、個人使用
CSO	Chief Security Officer 總保安主任
CSRF	Cross-Site Request Forgery 跨站請求偽造
DKIM	Domain Keys Identified Mail 域名金鑰辨識郵件
DMARC	Domain-based Message Authentication, Reporting and Conformance 基於域的消息認證，報告和一致性
DNS	Domain Name System 網域名稱系統
EFS	Microsoft Encrypting File System 微軟加密文件系統
G-Suite	Google Workspace (原稱為 G Suite)
Guide	IT Security Practice Guide 資訊科技保安實用指引
GCHQ	Government Communications Headquarters, UK 英國政府通信總部
HTTP	Hyper Text Transfer Protocol 超文本傳輸協定
IDS/IPS	Intrusion Detection system / Intrusion Prevention System 入侵檢測系統 / 入侵防預系統
IOC	Indicatorof Compromise 入侵指標
IP	Internet Address 互聯網通訊協定地址
ISP	Information Security Policies 資訊安全策略
IPSec	Internet Security Protocol 互聯網安全協定
IT	Information Technology 資訊科技
LAN	Local Area Network 區域網路
Malware	A Malicious Software - Viruses, Trojans, Spyware, and Ransomware etc. 惡意軟件 - 病毒，特洛伊木馬，間諜軟件和勒索軟件等等
MDM	Mobile Device Management 行動裝置管理
NAS	Network Attached Storage 網絡附加儲存
NCSC	National Cyber Security Centre, a UK Government department

	英國國家網絡安全中心
NDA	Non-Disclosure Agreement 保密協議
NGO	Non-Government Organisation 非政府組織
NIST	National Institute of Standards and Technology (USA) 美國國家標準技術協會
O365	Office 365 Cloud Services – Office mail, Cloud Drive etc. Office 365 雲服務 – Office 郵件，Cloud Drive 等
OAuth2	OAuth 2.0 Framework OAuth 2.0 認證框架
OpenID	OpenID Foundation (OIDF) 網上身份認證系統
Pen. Test	Penetration Testing 滲透測試服務
PKI	Public Key Infrastructure 公開金鑰基礎建設
Port Scan	Scan networking device/system for Open Ports 掃描網絡設備/系統的開放端口
RDP	Remote Desktop Protocol 遠端桌面協定
RSA	RSA (Rivest – Shamir – Adleman), an Asymmetric-Key Cryptosystem RSA 加密演算法是一種非對稱加密演算法，在公開金鑰加密和電子商業中被廣泛使用
PBKDF2	Password-based Key Derivation Function 2 基於密碼的密鑰派生功能 2
SIEM	Security Information and Event Management 保安資訊和事件管理
SLA	Service Level Agreement 服務水平協議
SOAR	Security Orchestration, Automation and Response 自動回應資安威脅
SPF	Email Sender Policy Framework 發件人策略框架
SRA	Security Risk Assessment 保安風險評估
SSL	Secure Sockets Layer 傳輸層安全性協定
SWD	Social Welfare Department 社會福利署
TLS	Transport Layer Security, a successor of SSL 傳輸層安全性協定, 前身安全通訊協定
UAC	User Account Control 使用者帳戶控制
USB	Universal Serial Bus 通用串列匯流排
User ID	User Identity 用戶身份
VLAN	Virtual Local Area Network 虛擬區域網路
VPN	Virtual Private Network 虛擬專用網路
Vuln. Scan	Vulnerability Scanning 弱點掃描
WAF	Web Application Firewall 網站應用程式防火牆
WAP	Wireless Application Protocol 無線應用通訊協定
WIFI	Wireless Fidelity 無線相容認證

表 44: 縮略語

* * * 資訊科技保安實務指引 * * *