政府資訊科技總監辦公室

資訊保安

保安風險評估及審計

實務指引

[ISPG-SM01]

第 1.2 版

2021 年 6 月

版權公告

修改記錄				
修改次數	修改詳情	經修改頁數	版本編號	日期
1	G51 保安風險評估及審計指引第 5.0 版已轉換成保安風險評估及審計實務指引。修改報告可於政府內聯網「資訊科技情報網」查閱：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	增加關於資訊科技保安管理的新章節、修定保安風險評估與保安審計的描述，及與其他實務指引保持參考上的一致。	整份文件	1.1	2017 年 11 月
3	根據最新版本的《基準資訊科技保安政策》[S17] 第 7.0 版和《資訊科技保安指引》[G3] 第 9.0 版的更改加入相關更新	整份文件	1.2	2021 年 6 月

目錄

1. 簡介

資訊科技保安風險評估和保安審計是資訊保安管理的重要組成部分。本文件提供了參考模式，以便獨立保安顧問或審計師所提供的服務，在範圍、方法及成品各方面互相配合。透過這模式，可提高管理層用戶、資訊科技管理人員、系統管理員及其他技術和操作人員對保安風險評估和審計的認識，讓他們了解進行保安審計所需的準備工作、應注意的各個方面及保安審計可能得出的結果。

1.1 目的

本文件闡述資訊科技保安風險評估和保安審計的一般架構。本文件應按需要與其他保安文件如《基準資訊科技保安政策》[S17]、《資訊科技保安指引》[G3]及相關程序等一同使用。

本實務指引旨為政府所有需要處理保安風險評估或保安審計的人員，以及為政府進行保安風險評估或保安審計的保安顧問或審計師而設。

1.2 參考標準

以下的參考文件為本文件在應用上的參考：

- 香港特別行政區政府《基準資訊科技保安政策》[S17]
- 香港特別行政區政府《資訊科技保安指引》[G3]
- Information technology - Security techniques - Information security management systems – Overview and vocabulary (fourth edition), ISO/IEC 27000:2016
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- Information technology - Security techniques - Information security risk management (second edition), ISO/IEC 27005:2011

1.3 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用，以及以下的定義及慣用詞。

縮寫及術語	
保安風險評估	是識別、分析和評估保安風險的過程，並決定緩解措施以降低風險至可接受水平。
保安審計	是以資訊科技保安政策或標準為基礎的遵行狀況審計，以確定現有保護的整體情況，並驗證現有的保護措施是否已經妥善地實行。

1.4 聯絡方法

本文件由政府資訊科技總監辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@ogcio.gov.hk

Lotus Notes 電郵： IT Security Team/OGCIO/HKSARG@OGCIO

CMMP 電郵： IT Security Team/OGCIO

2. 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資訊資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和應用這些原則的法則，來迅速有效地管理實體、財務、人力資源和資訊資源，以及確保資訊資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下的範疇：

- 保安管理框架與組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力建立；和
- 態勢認知和資訊共享。

<u>保安管理框架與組織</u>

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須界定資訊保安的組織架構，並為有關各方就保安責任提供清晰的定義和適當的分配。

<u>管治、風險管理和遵行要求</u>

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

決策局／部門須定期和在必要時對資訊系統和生產應用系統進行保安風險評估，以識別與保安漏洞相關的風險和後果，並為建立具成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應變和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應變措施是指在發生不良事件或事故時，採取協調行動來遏制損害；和
- 復原措施是將資訊系統的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並引致服務中斷的事件，故此保安事故仍可能會發生。若保安事件危及業務的連續性或引起數據保安風險，決策局／部門須啟動其常規保安事故管理計劃，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應變以消除不信任或不必要的猜測。當制定保安事故管理計劃時，決策局／部門應規劃和準備適當的資源，並制訂相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安是每個人的責任，所以決策局／部門應不斷提升機構內的資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢認知和資訊共享

因應網絡威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發布的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以利用網絡風險資訊共享平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

3. 保安風險評估與審計簡介

3.1 保安風險評估與審計

保安風險評估和審計是一個持續的資訊保安實踐過程，以發現和糾正保安事務。如圖 3.1 所示，它們涉及一系列活動。它們可以被描述為需要持續監察和控制的迭代過程的循環。 每個過程由不同的活動組成，以下為一些例子。

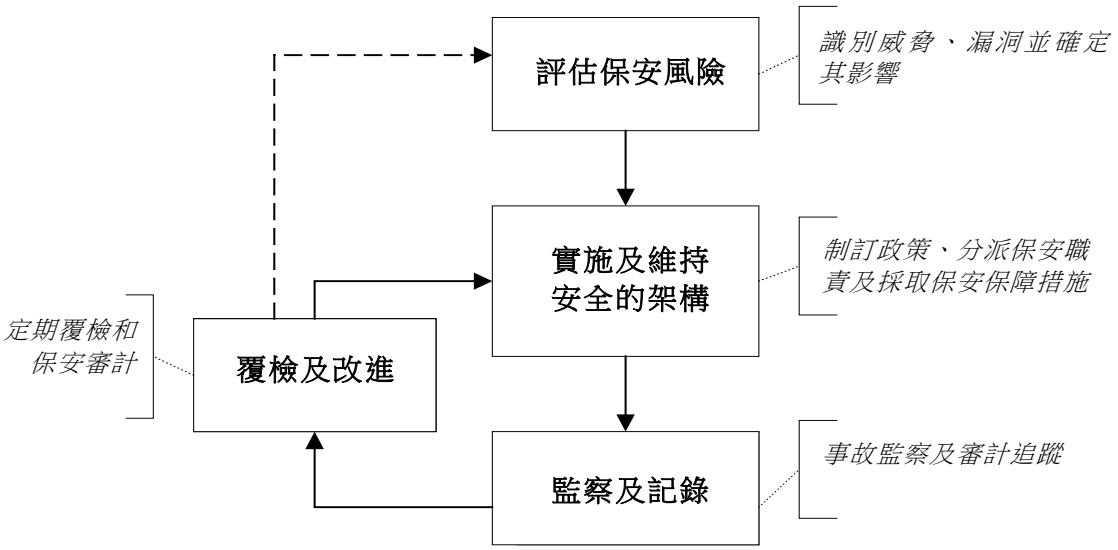

圖 3.1 保安風險評估與審計的循環程序

評估保安風險是評估和識別與保安漏洞相關風險及後果的第一步，同時可為管理層提供基礎，以制訂具成本效益的保安計劃。

根據評估結果，應採取適當的保安保護和保障措施，以維持安全的保護架構，其中包括制訂新的保安要求、修訂現時的保安政策和指引、分派保安職責和採取保安技術保護措施。

通過實施保安架構，還需要持續的監察及記錄，以便妥善安排處理保安事故。此外，日常操作如需使用資源或資訊以作用戶接達的嘗試和活動，應進行適當的監察、審核和記錄。

評估後要對措施的遵守情況，進行周期性覆檢和重新評估，以確保保安控制措施獲切實執行，達到用戶的保安要求，並緊貼急速發展的科技和不繼轉變的環境。此模型有賴持續反饋和監察。覆檢可透過定期保安審計進行，以找出需要改進之處。

3.2 保安風險評估與保安審計

保安風險評估和保安審計都是持續的過程，但在性質和功能方面是有所不同。

保安風險評估是識別、分析和評估保安風險的過程，並決定緩解措施以降低風險至可接受水平。保安風險評估是風險管理流程的一部分，旨在為資訊系統提供適當的保安級別。它有助識別保安漏洞所造成的風險和後果，並為建立具成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

對於新的資訊系統，保安風險評估通常在系統開發生命周期開始時進行。對於現有的系統，評估須在整個系統開發生命周期中定期進行，或在資訊科技環境有重大改變時進行。

資訊保安審計是以資訊科技保安政策或標準為基礎的遵行狀況審計，以確定現有保護的整體情況，並驗證現有的保護措施是否已經妥善地實行。保安審計是持續的過程，以確保現時的安全措施符合部門的資訊科技保安政策、標準和其他協議上或法律要求。

雖然保安風險評估與保安審計在某些功能上有相似之處，但兩者之間有以下主要分別。

保安風險評估	保安審計
識別威脅和漏洞、評估所涉及的風險水平、確定可接受的風險水平和相應的風險緩解策略	確定在部門資訊科技保安政策、標準和其他協議上或法律要求的保安措施有效地實行的過程
從風險角度出發，評估範圍不一定與保安政策和標準相關	從遵守規定角度出發，評估根據保安政策、標準或其他預定的準則
對於新的資訊系統，在系統開發生命周期的早期和系統投入生產之前進行 對於現有的資訊系統，至少每兩年一次或有重大變更時進行	定期審查，持續進行
可自行評估或由獨立第三方完成	必須由獨立第三方完成
主要成品：風險登記和風險緩解措施	主要成品：遵行要求清單

第 4 節和第 5 節會分別介紹實行保安風險評估和保安審計流程的細節。

4. 保安風險評估

保安風險評估是識別、分析和評估保安風險的過程，並決定緩解措施以降低風險至可接受水平。

系統評估程序包括識別和分析：

- 系統的所有資產和相關程序
- 可影響系統機密性、完整性或可用性的威脅
- 系統漏洞和相聯的威脅
- 威脅活動帶來的潛在影響和風險
- 減低風險所需的保護要求
- 適當保安措施的選擇和風險關係的分析

應就系統編製完整清單及保安要求，以作為識別和分析活動的資料，使分析的結果更為有用和準確。與管理員、電腦／網絡操作員或用戶等有關各方進行訪談，亦可提供更多分析資料。視乎評估的範圍、要求和方法，亦可利用自動化保安評估工具進行分析。評估所收集的資料後，呈報已發現的保安風險清單，並就各項風險而決定、推行及採用適當的保安措施。

負責分析所收集的資料及權衡保安措施工作的人員需具備深厚的專業知識和豐富的經驗，應委任合資格的保安專家進行保安風險評估。

4.1 保安風險評估的好處

- 可全面和有條理地向管理層反映現有的資訊科技保安風險和所需的保安保障措施
- 以合理客觀的方式制訂資訊科技保安開支和成本預算
- 為決策和政策考慮提供不同的解決方案，使資訊保安管理能夠從策略性的層面推行
- 為日後比較資訊科技保安措施的變化提供依據

4.2 保安風險評估頻率和類別

4.2.1 保安風險評估頻率

保安風險評估是一項持續進行的工作。對於一個新的資訊系統，評估工作應在系統開發生命周期之初進行，以便及早識別保安風險和選擇適當的保安控制。對於使用中的資訊系統，必須至少每兩年或於系統有重大改動時作評估，以了解資訊系統存在的風險。該兩年期的定義為獲得批准撥款後連續兩次評估工作的開始日期，或兩次評估報告的發布日期之間的期間。這兩年的間距不包括推行保安保障措施的時間。保安風險評估只能概括地揭露在某特定時間資訊系統所存在的風險。對於關鍵業務資訊系統或具高風險接達的系統，應更頻密地（最好每年一次）進行保安風險評估。

4.2.2 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。

- 高層次評估：此類評估注重以較具策略的角度和有系統的步驟，分析部門的保安狀況及系統的整體基礎結構或設計。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，以便在開發系統前識別風險或覆檢一般保安控制措施。

- 全面評估：一般會定期對決策局／部門的資訊系統進行此類評估，以確保系統的安全性。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。隨後應通過一個驗證過程，以確保所有建議的補救措施得到切實的跟進。

- 投入運作前評估：與「全面評估」所進行的工作類似，通常會在新的資訊系統推出前或原有系統出現重大功能變動後進行此類評估。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他階段。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。

4.3 保安風險評估步驟

保安風險評估包括圖 4.1 所示的幾項主要工作：規劃、資料收集、風險分析、保安保障措施識別及選擇，和監察及推行。

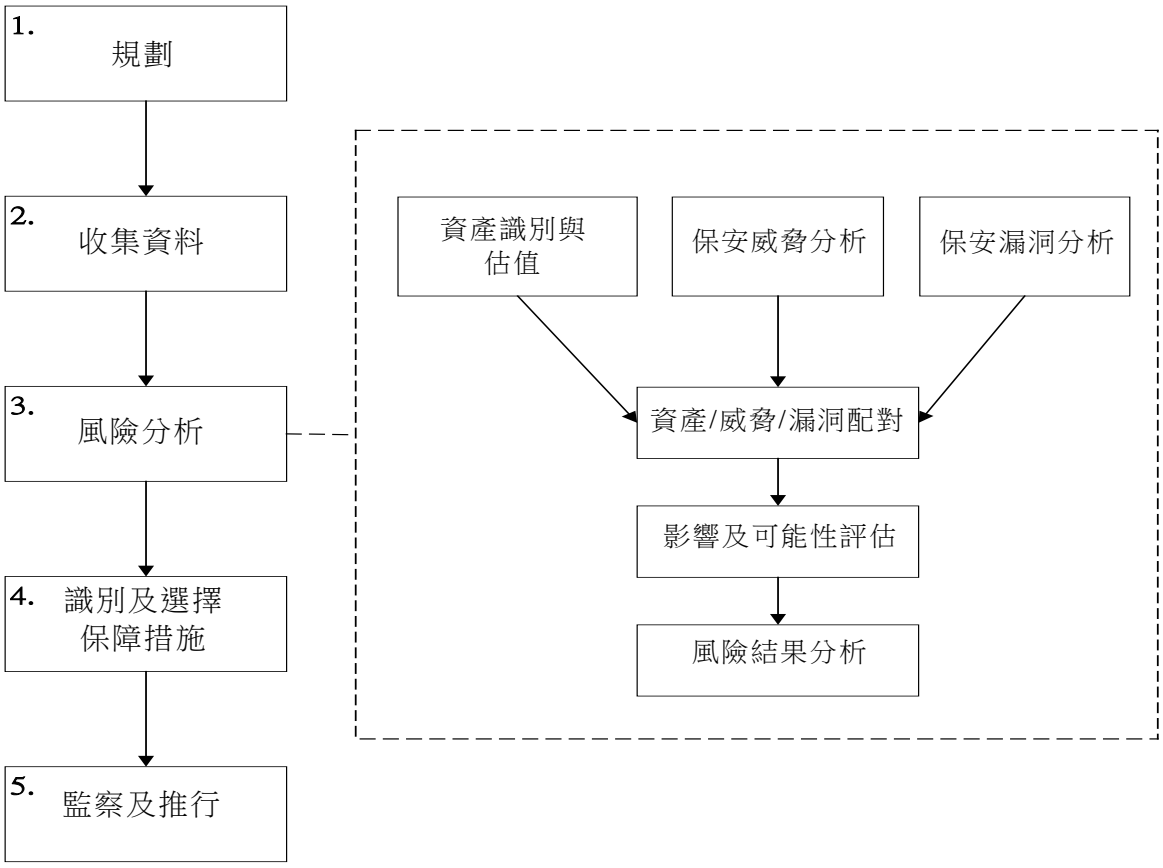

圖 4.1 一般保安風險評估步驟

4.3.1 規劃

在評估保安風險前，須就籌備、監察和控制等工作進行規劃。其中一個建議是假如風險評估活動牽涉滲透測試或漏洞掃描，應事前通知持份者如網絡小組、應用系統小組及保安事故處理小組，以避免產生過多錯誤警報，影響日常運作。下列為應事先界定的主要事項。

- 計劃範圍和目標
- 背景資料
- 限制
- 相關人士的職務和職責
- 方式和方法
- 計劃規模和時間表
- 保護數據和工具

4.3.1.1 計劃範圍和目標

計劃範圍和目標可影響分析方法和保安風險評估所得的成品種類。保安風險評估的範圍可涵蓋內部網絡與互聯網的連接、電腦中心的保安保護措施，以至整個部門的資訊科技保安狀況。因此，相應目標可能需要識別保安要求，如內部網絡與互聯網連接時的保護措施、識別電腦室內潛在風險的地方，或評估部門的整體資訊科技保安水平。保安要求應根據業務需要而制訂（一般由高級管理層決定），以識別決策局／部門所需採取的保安措施。

4.3.1.2 背景資料

背景資料是指可就評估供顧問作初步參考的有關資料，例如正受評估系統的過去和現況資料、有關聯的各方、上次評估的撮要資料，或即將發生並可能影響評估的改變。

4.3.1.3 限制

各種限制包括時間、財政預算、成本和科技等均應加以考慮。建議決策局／部門及早提交撥款申請，以確保保安風險評估與審計工作獲得所需款項。這些限制可能影響計劃的時間表和支援評估的可用資源。舉例來說，評估宜需在非繁忙辦公時間，甚至非辦公時間進行。

4.3.1.4 相關人士的職務和職責

應小心界定參與計劃各方的職務和職責。為使評估達到最佳效果，宜分派代表各個工作領域的團隊或小組，分別負責指定的工作。視乎工作安排和要求，部分或全部下列人士均可參與計劃：

- 系統或資料擁有人
- 資訊科技保安管理員或主任
- 電腦操作人員
- 系統或網絡管理員
- 應用程式或系統開發人員
- 數據庫管理員
- 用戶或高級用戶
- 高級管理層
- 外聘承辦商

4.3.1.5 方式和方法

評估方式和方法是指分析資產、威脅、漏洞和其他因素之間的關係。分析方法有許多，大致上可分為兩大類：定量和定性分析。

為發揮更大效用，為評估所選的方法應能夠就風險的影響和保安問題的後果作出定量報告，同時作出一些定性分析，以描述對風險減到最低的適當保安措施及其影響。下文將闡述這兩種分析方法的詳情。

4.3.1.6 計劃規模和時間表

編定計劃的時間表是評估的重要步驟之一。時間表須列明評估計劃中將要進行的所有重要工作。預計的計劃規模（例如計劃成本和參與計劃的人數）可直接影響計劃時間表。計劃時間表可用來控制進度和監察計劃。

4.3.1.7 保護數據和工具

在保安風險評估的各個階段，將收集大量數據和系統配置，而其中可能包含敏感資料。

因此，評估小組應確保安全地儲存所收集的所有數據。在規劃階段應準備檔案加密工具和鎖櫃／可上鎖的工作室，以防止未獲授權人士取閱敏感資料。

此外，應妥善存置、控制及監管評估工具以免遭濫用。只有評估小組內的有關專家方可運作有關工具，以防對系統造成損害。除非採取適當控制措施以防止未獲授權接達上述工具，否則亦應在使用後即時將該等工具和其產生的數據刪除。

完成評估程序後，將會編撰保安風險評估報告以記錄發現的所有風險。如遭未獲授權接達有關資料(尤其是在修正系統前)，可能會對有關決策局／部門構成直接威脅。因此，評估小組在編撰保安風險評估報告中及完成報告後，必須採取適當的措施保護有關報告。高級管理層亦應嚴格保密保安風險評估報告。最後，評估小組須將所有要求提供的資料和文件歸還有關決策局／部門。

4.3.2 資料收集

資料收集的目的在於了解現有系統和狀況，並透過分析所收集的資料／數據，以確認風險所在。

一般來說，不論相關資料以何種格式儲存，都應予以收集。下列是一般收集的資料：

- 保安要求和目標
- 系統或網絡的結構和基本設施，例如顯示資訊系統資產配置和互連情況的網絡圖
- 證據或證明文件，顯示電腦室的實體環境符合根據所存放數據的保密類別而訂定的實體保安要求，例如建築署發出的認證／通知或上次保安風險評估與審計報告的相關結果
- 向公眾公開或網頁上發布的資料
- 硬件設備等實體資產
- 操作系統、網絡管理系統及其他系統
- 數據庫、檔案等資訊內容
- 應用系統和伺服器資料
- 網絡支援的規約和提供的服務等資料
- 接達控制措施
- 業務流程、電腦操作程序、網絡操作程序、應用系統操作程序等程序
- 識別及認證機制
- 相關的法定，規管及合約要求以符合有關最低保安控制的要求
- 政策和指引

常見的資料收集方法一般有兩種：

- 一般控制覆檢
- 系統覆檢

4.3.2.1 一般控制覆檢

一般控制覆檢是透過人手，以訪談、實地走訪、文件覆檢、觀察等方法，以識別在現時環境推行中一般控制的潛在風險和威脅。這些控制和程序包括但不限於：

- 部門資訊科技保安組織，特別是人員的職務與職責
- 管理職責

- 資訊科技保安政策
- 人力資源保安，包括保安意識培訓
- 資產管理
- 接達控制，例如密碼政策、接達權限
- 加密方法
- 實體及環境保安
- 操作保安
- 通訊保安
- 系統購置、發展及維護
- 外判資訊系統的保安
- 保安事故管理
- 資訊科技保安方面的業務連續性管理
- 遵行要求

在收集資料時可採用以下方法：

- 實地走訪：應安排走訪數據中心、電腦室和辦公室，以找出實體保安風險。此外，保安小組應在實地觀察時記錄有關系統操作和終端用戶的行為（例如使用設置密碼的屏幕保護），以覆核有關保安政策是否被嚴格遵從。

- 小組討論：評估小組可舉辦小組討論或研討會，以蒐集有關決策局／部門或資訊系統現時保安情況(控制或風險)的資料。視乎所欲取得的目標資料，可以任何形式及話題進行討論。

- 與各級人員進行訪談：此外，與不同級別的重要人員或代表進行實地訪談也宜驗證之前收集到的資料，從而提高所收集資料的準確度和完整性。

- 問卷調查：問卷調查或清單是有效的簡單工具用來識別潛在風險。問卷調查可由保安顧問按環境的個別情況設計。

舉例來說，與各級人員進行訪談的對象可包括以下人員級別：

- 高級管理層：負責作出策略性決策（例如評估範圍和目標）

- 業務管理層：須了解受策略性保安更改影響的主要業務流程和程序

- 人事部人員：須識別就系統保安和使用權對人員招聘、終止僱用及轉調推行的具體控制措施

- 操作和技術人員：提供技術和操作資料

就高層次評估或設計階段的評估而言，採用實地走訪及問卷調查的方法未必適合或可行。因此，保安評估小組應着重透過小組討論和與各級人員進行訪談等活動收集資料。

附件 A 所載為保安風險評估的一般提問清單。

4.3.2.2 系統覆檢

系統覆檢是從內部接達點，識別網絡或系統的任何保安漏洞和薄弱環節。系統覆檢着重不同平台的操作系統、管理和保安監察工具。

系統覆檢的內容包括：

- 系統檔案或記錄
- 操作中的程序
- 接達控制檔案
- 用戶列表
- 配置設定
- 保安修補程式級別
- 加密或認證工具
- 網絡管理工具
- 記錄或入侵偵測工具

評估小組也應找出是否存在企圖入侵等異常活動。

為了更有效及全面地收集上述資料，可在目標主機上採用因應個別需求而設計的自動化腳本及／或工具，藉以取得有關系統的具體資料。這些資料將會用於稍後階段的風險分析。

在覆檢後，應適當地記錄和在設計階段或其他階段處理所識別的風險和建議。

當有需要時，應進行技術性漏洞測試如漏洞掃描、滲透測試和應用程式原始碼檢測，以識別網絡或系統的漏洞和弱點。在進行漏洞掃描及／或滲透測試前，評估小組應就範圍、可能的影響、及回退／復原程序得到決策局／部門的同意。如果涉及關鍵業務系統，則應以業務連續性計劃及運作復原計劃爲基礎。

在適當情況下，應進行網絡、主機及系統的漏洞掃描以覆蓋至少以下內容：

- 網絡層面試探／掃描和發現
- 主機漏洞測試和發現
- 系統／應用程式（包括網上系統／應用程式）掃描

評估小組應覆檢是否已對所有適用及已知的漏洞，包括但不限於由政府電腦保安事故協調中心所發出的所有相關保安警報，安裝修補程式或採用替補的措施。

對於面向互聯網並處理保密資料的網上應用系統、設有輸入欄位的網站或關鍵業務系統，亦應進行網頁滲透測試。

有關漏洞掃描及／或滲透測試的詳情，請參考第 4.3.3.3 節－保安漏洞分析。

投產前的保安風險評估應核實開發小組已完成應用程式原始碼檢測，以確保所需的保安措施和控制措施均已在系統內妥善推行。

對於高層次評估或設計階段的評估，實地走訪和問卷調查方法有時可能不適用或不可行。在這種情況下，保安評估小組應集中從各項活動（如小組討論和多層次訪談）收集資料作補充。

附件 A 列出一般保安風險評估的提問清單。

4.3.3 風險分析

風險分析有助釐定資產價值及其相關風險。應進行各方面的風險分析，包括但不限於以下範疇：

- 人力資源保安
- 資產管理
- 接達控制
- 加密方法
- 實體及環境保安
- 操作保安
- 通訊保安
- 系統購置、發展及維護
- 外判資訊系統的保安
- 資訊科技保安方面的業務連續性管理

風險分析程序一般可分為上文圖 4.1 所示的子程序：

- 資產識別與估值
- 保安威脅分析
- 保安漏洞分析
- 資產／威脅／漏洞配對
- 影響及可能性評估
- 風險結果分析

下文將概括闡述風險分析子程序。

此外，決策局／部門在分析與電子服務(包括政府與市民(G2C)和政府與僱員(G2E)應用系統)登記和認證程序有關的風險時可參考《電子認證風險評估參考架構》中的保證模式。

4.3.3.1 資產識別與估值

保安風險評估範圍內的所有資產必須予以識別，包括資料、服務、聲譽、硬件和軟件、通訊、界面、實體資產、支援設施、人員和接達控制措施等有形和無形資產。

數據分類是評估程序的關鍵步驟，而各項資產可歸入不同的類別，例如資產可歸類為程序、應用程式、實體資產、網絡或某類資料。歸類的目的是反映這些資產對評估對象系統或領域的重要性。

值得注意的是，資產估值法將會因應採納的分析方法不同而各不相同。風險分析法將在第 4.3.3.6 節－風險結果分析中闡述。

資產價值可以下列方式表達：

- 有形價值，例如資訊科技設施的重置成本、硬件、軟件、系統數據、媒體、供應器、檔案，以及支援系統的資訊科技人員
- 無形價值，例如商譽和服務品質的改善
- 資訊價值，例如機密性、完整性及可用性
- 資產所儲存、處理或傳輸資料的數據分類

資產識別與估值是製備資產清單的先決工序。資產清單以有形價值和無形價值反映資產的相應價值(如有)，或以機密性、完整性及可用性等顯示資產的資訊價值。清單所列的資產價值如越需精確，完成資產識別與估值工序所需的時間也越長。

資產清單包括但不限於：

- 資訊資產的名稱和種類
- 資產的實體位置
- 儲存媒體和銷毀儲存／處理資料前的保留期
- 儲存／處理資料的性質，例如是備份還是正本
- 顯示資產重要性／價值的指標，例如敏感程度、操作需要或關鍵性
- 傳入／發出的資訊流通，例如經互聯網、電郵、撥號調解器或其他電訊媒介連接的傳輸資訊模式
- 已安裝的操作系統和軟件
- 開發和維修費用
- 各項已識別的資產價值
- 資產所儲存、處理或傳遞資料的數據分類

4.3.3.2 保安威脅分析

保安威脅是指可能會為資訊資產、系統及網絡的機密性、完整性及可用性帶來負面影響的潛在事件或任何情況。保安威脅分析宜不時修訂，以反映資訊資產所面對的任何新潛在威脅。

保安威脅源自：

- 人為錯誤
- 心懷不滿的僱員
- 惡意或粗心大意的人員
- 濫用系統及電腦資源
- 電腦詐騙
- 盜竊
- 商業間諜
- 自然災害

保安威脅分析的目的是找出保安威脅，並釐定發生保安威脅的可能性及其破壞系統或資產的潛力。系統誤差或控制記錄可轉化為保安威脅資料和統計數字，所以是有用的資料來源。

保安威脅可分為三大類：

- ***社群威脅***：與人為因素直接相關的蓄意或無意保安威脅，例如人為錯誤、遺漏或疏忽造成的結果、盜竊、詐騙、濫用、損害、破壞、泄漏及竄改數據
- ***技術威脅***：因技術問題導致的保安威脅，例如程序錯誤、設計瑕疵、通訊線路（例如電纜）的破損
- ***環境威脅***：因環境災害導致的保安威脅，例如火災、水浸、停電、及地震

4.3.3.3 保安漏洞分析

保安漏洞是指於操作、技術和其他保安控制措施和程序中能夠令保安威脅有機可乘，以致資產因而受損的薄弱環節，例如第三方攔截傳輸中的數據，未獲授權接達資料等。

保安漏洞分析是指找出和分析系統及環境中的保安漏洞。保安漏洞分析強調系統化地衡量這些漏洞。

各個漏洞均可評定為不同級別或程度（例如高、中、低）以反映其重要性。而重要和關鍵資產必須先行確認。

識別保安漏洞是在自動化工具或程序的輔助下，採用以下一種方法找出網絡的保安漏洞：

(i) 保安漏洞掃描

評估小組可使用自動化保安漏洞掃描工具進行保安漏洞掃描，從而快速找出目標主機或網絡設備存在的保安漏洞。與抗惡意軟件方案相類似，掃描工具安裝在評估小組的電腦上，並需在使用前定期更新漏洞識別碼檔案。根據用戶要求，會對單個或一組主機／網絡進行已知保安漏洞掃描服務（例如系統容許匿名檔案傳送規約、電郵轉遞）掃描，以確定是否存在任何保安漏洞。

在保安漏洞掃描過程中，由於自動化漏洞掃描工具可產生大量系統要求，故接受掃描的各目標組群的系統和網絡的性能可能受到影響。評估小組應與系統和網絡管理員合作制訂計劃，以使保安漏洞掃描過程中發生服務中斷的可能性降至最低。

此外，值得注意的是，自動化掃描工具找出的保安漏洞，在該系統環境中未必是真的保安漏洞。舉例來說，由於可能已採取輔助控制措施，故自動化掃描軟件標記的某些「保安漏洞」實際上未必會成爲安全隱患。因此，此測試方法可能會發出虛假警報，故評估小組須作出專業判斷以確定所發現的保安漏洞是否對系統有所影響。

網絡保安漏洞掃描是在短時間內收集漏洞資料的有效方法。與滲透測試不同，網絡保安漏洞掃描並無滲透入網絡內部，亦無嘗試利用發現的保安漏洞測試網絡。因此，倘需要進行更為深入的保安分析，可採用滲透測試。

應用程式如網上應用程式或流動應用程式，在保安漏洞被利用前，應該先進行應用程式保安漏洞掃描，以找出保安漏洞。

(ii) 滲透測試

滲透測試可在內部或從外部進行。滲透測試以人手程序，並輔助以可安裝在便攜式電腦的自動化工具，來掃描網絡或系統，以得出連接工作站和伺服器的網絡圖，同時嘗試滲透被測試的網絡和系統，在網絡和系統內部或從外部找出保安漏洞。

滲透測試也可能包括與用戶進行訪談和運用不同的黑客入侵技巧測試系統或網絡。在進行入侵測試前，必須全面地計劃和商定具體的入侵程度和種類。入侵測試宜在接達某系統後，或在進一步深入分析被滲透的系統後停止。在決定進行入侵測試前，應尋求服務供應商或保安評估小組的建議。若要進行外來的道德黑客入侵，應事先解決法律上的問題。

滲透測試的目的包括但不限於：

- 測試系統抵禦蓄意攻擊的能力，以找出保安薄弱環節
- 測試及驗證保安防護及控制的效率
- 測試偵測及應對攻擊的防禦能力

有關描述滲透測試的一般步驟見下圖 4.2：

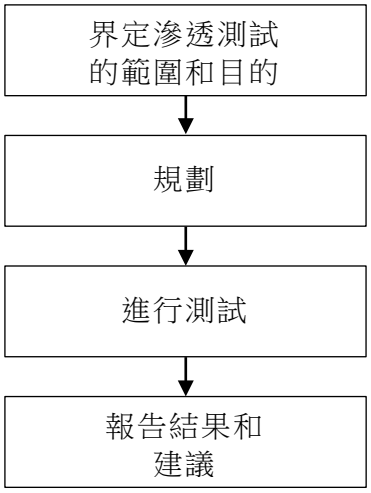

圖 4.2 滲透測試的一般步驟

決策局／部門在進行滲透測試時應特別小心，因為該測試可能會給系統造成與真實攻擊類似的影響，例如服務中斷、未獲授權接達或未獲授權修改數據等。因此，在進行滲透測試之前，決策局／部門應考慮以下保安問題：

- 必須清晰界定測試的範圍和目標；不得對界定範圍以外的機器／系統進行測試。
- 進行滲透測試的服務供應商應與系統擁有人討論及得到其准許，決定進行入侵攻擊、暴力攻擊及拒絕服務攻擊是否適當及其影響。
- 服務供應商須簽署不可向外披露資料協議，以保障系統內數據的保密或機密性。
- 只委聘信譽卓著而且紀錄良好的服務供應商，並考慮對服務供應商進行背景和資格審查，以確保有關供應商具備所需的經驗和專業知識。
- 由於滲透測試可能會影響目標系統中數據的完整性，所以必須為目標系統制作最新的完整系統備份。
- 清楚界定「達成任務」的條件，例如將檔案放入指定目錄、取得某些測試帳戶的密碼、接達到擁有妥當接達控制保護的指定網頁等。不得修改或刪除生產數據。
- 向服務供應商提供聯絡人名單（例如系統擁有人、資訊科技管理員），在突發事件發生時作聯絡之用。如在測試過程中出現任何突發事件，服務供應商應聯絡有關人員，匯報情況。
- 取得服務供應商的聯絡人名單，以在必要時即時停止所有測試。
- 在進行滲透測試之前，知會並警示保安監控供應商，除非測試旨在評估保安監控供應商監控的效能。
- 事先取得將進行測試的機器的源互聯網規約地址，以便透過檢查和比較入侵偵測／防禦系統記錄以判斷是否遭受真實攻擊。
- 考慮安排滲透測試在非繁忙工作時間進行。
- 確保服務供應商即使可成功接達用戶數據，亦不會修改任何數據。

滲透測試示例如下：

- 遠程互聯網防火牆滲透測試：互聯網規約地址試探、傳輸控制規約或用戶數據報規約試探、基於規約的拒絕服務攻擊，例如互聯網控制訊息規約癱瘓、域名稱服務偽冒，和基於服務的滲透測試，例如電郵伺服器的滲透測試、暴力密碼攻擊和電郵轟炸
- 實地防火牆滲透測試：小包嗅探、互聯網規約地址偽冒、源路由小包及劫持通訊對話
- 撥號網絡滲透測試：暴力密碼攻擊和撥號式掃描
- 應用系統滲透測試：包括但不限於配置及使用管理測試、認證測試、

身分管理測試、對話管理測試、錯誤處理等

須對這些自動化工具推行嚴格的接達控制，以限制任何未獲授權接達和使用。由於利用這些工具能夠對系統、網絡或網上應用程式發動拒絕服務攻擊等模擬攻擊，在使用自動化工具時，保安評估小組和系統管理員應密切監視這些工具。

有關滲透測試的詳情，請參閱《滲透測試實務指引》。

4.3.3.4 資產／威脅／漏洞配對

將威脅與資產和漏洞配對有助確認資產、威脅和漏洞可能形成的各種組合。各個威脅均能夠與一個特定漏洞，甚至多個漏洞配對。除非漏洞令威脅有機可乘，否則威脅並不能對資產構成風險。

在進行風險結果分析前，應減少各種可能形成的組合。部分組合可能毫無意義或根本不能形成。資產、威脅及漏洞三者之間的關係對分析保安風險至關重要。計劃範圍、財政預算和其他限制等因素，也可能影響配對的深度和廣度。

4.3.3.5 影響及可能性評估

為資產、威脅和漏洞配對後，便能夠確定影響和可能性。

(i) 影響評估

影響評估（或稱影響分析或後果評估）即估計可能發生的整體破壞或損失的程度。評估的影響包括收入、利潤、成本、服務水平和政府聲譽、對相關系統機密性、完整性及可用性的損害。此外還須考慮能夠承受的風險水平，以及哪些資產會如何和何時受到這些風險影響。保安威脅的影響越嚴重，風險也越高。

(ii) 可能性評估

可能性評估是對保安威脅發生頻率的估計，即發生的或然率。可能性評估須觀察影響風險發生可能性的環境。一般而言，一個系統的漏洞令某一威脅有機可乘的可能性可根據不同情況衡量，如系統可供接達的程度和獲授權用戶的人數。可接達系統的程度可能受實體接達控制、系統配置、網絡種類、網絡布局和網絡界面等多種因素影響。與互聯網連接的系統比內部系統的漏洞更容易令威脅有機可乘。前者的獲授權用戶（即公眾）人數亦可能遠多於後者，內部系統的用戶人數通常有限。與用戶人數成千上百的系統相比，只有一名用戶的系統受到威脅的機會顯然較

小。能夠接達系統的人數越多，確保個別用戶只進行獲准操作的難度便越大。正常來說，當獲授權用戶的人數愈多，漏洞被利用的可能性便愈高。

可能性的高低可視乎發生次數的多寡（例如每天一次、每月一次及每年一次）而定。保安威脅的可能性越高，風險也越高。舉例來說，如應用軟件有一個眾所周知的保安漏洞，乘此漏洞發生蓄意社群威脅的可能性就很高。如果受影響的系統為關鍵系統，則影響也很嚴重。由此得出的結果是該威脅具有高風險。

釐定已確認的各個風險的影響和可能性，便能夠估計整體的風險水平。在估計風險水平時應訂明假設。

4.3.3.6 風險結果分析

風險結果可利用不同的方式和方法分析：定性、定量和矩陣法。

(i) 定性和定量法

定性法是根據經驗和判斷，以描述性、文字等級或排序反映重要／嚴重程度的方法，例如過去的經驗、市場調查、行業實務及標準、調查、訪談和專業人士／專家的判斷。定性法須主觀地為風險評級，例如按高、中、低評級；由 1 至 5 按序排列；或從重要程度最低向最高排列等。定性法較為主觀。

舉例來說，資產的價值可以重要程度表達，例如不重要、重要和非常重要。

定量法是利用數字資料得出百分比或數值的方法，例如成本／效益分析。定量法所需的時間和資源均多於定性法，因為定量法需要考慮並為每個可能的因素（即資產、威脅或漏洞）評級。

舉例來說，資產的價值可以購入價或維修費用等金錢價值表達。保安威脅的頻率可以發生率表達，例如每月一次或每年一次。

定性法一般在初步篩選時使用，而定量法則用來對一些關鍵因素進行更詳盡和具體的分析，以及進一步對高風險領域進行分析。

(ii) 矩陣法

矩陣法以三種不同的嚴重程度（高、中、低），記錄和估計保安保護措施的三個關鍵要求：機密性、完整性及可用性。風險水平可根據各風險因

素的嚴重程度排列次序。風險詮釋應局限於最重要的風險，以節省整體人力物力和減低複雜程度。

表 4.1 所示為某個特定保安威脅對某功能或某資產的風險分級矩陣示例。影響和可能性欄內的數字顯示了風險級別（3——高、2——中、1——低）。由於風險水平是影響值乘可能性值的積，所以風險水平值可介乎 1 至 9 不等（9——高、4 及 6——中、1 至 3——低），不包括 5、7、8（因為影響值乘可能性值的積不可能等於 5、7、8）。利用風險分級矩陣便能夠將各個保安威脅歸入某個整體風險水平級別。

風險類別	影響 （高、中、低）	可能性 （高、中、低）	風險水平= 影響 X 可能性 （高、中、低）
機密性	3	2	***6***
完整性	3	1	***3***
可用性	2	1	***2***
整體	***3***	***2***	***6***

表 4.1 風險分級矩陣示例

表 4.1 備註：

- 影響（高）：　非常重要：可對機構造成重大損失和嚴重破壞；造成極大的、災難性或嚴重的長期破壞／干擾

  例如拒絕服務，未獲授權接達系統
- 影響（中）：　重要：對機構不利的中度損失；造成嚴重的短期破壞／干擾或有限的長期破壞／干擾

  例如入侵者可收集系統的關鍵資料，以便在未獲授權的情況下接達，或展開進一步攻擊
- 影響（低）：　不重要：對機構損害輕微，或不構成損害的輕微損失；造成有限的短期破壞／干擾

  例如入侵者可能取得非關鍵資料
- 可能性（高）：　在大部分情況下預期會發生
- 可能性（中）：　偶爾會發生
- 可能性（低）：　在某特定時間或在特殊的情況下發生
- 風險水平（高）：　對風險的承受能力低，即需要最高級別的保安保護措施
- 風險水平（中）：　對風險的承受能力一般

- 風險水平（低）： 對風險的承受能力較強
- 整體結果 在各級風險類別中，最高保安風險水平

將風險類別再細分為子類別，再附上更多風險水平的加權數值，便能夠進一步擴充上列矩陣。

確定風險水平後，便能夠為已確認的各項資產編製技術、操作和管理要求清單。由於不可能完全杜絕風險，有關清單(如表 4.2 所示)可成為承受、減低、避免或轉介風險決策的依據。

評估結果	可選方案	描述
• 後果輕微／可能性低 • 可用性或其他因素比保安因素重要	承受風險	承擔責任
• 不可承受的高風險	減低風險	減輕後果或減低可能性，或一併減低
• 風險過高，或費用過高，因而無法減低，也無法管理	避免風險	採用其他方法，或不再進行可能引發風險的工作
• 另一方願意承受風險 • 另一方控制風險的能力更強	轉介風險	將部分或全部風險責任轉移給另一方

表 4.2 風險方案表

對於選定的任何方案，必須向管理層提出如何實施所選方案的建議。此外，如果選擇減低風險，還須建議保障和保安措施。

然後按風險的重要性和潛在影響，為各個風險排列先後次序。一般而言，保安風險水平越高，排列先後次序時便有較大的優先權。換言之，有較大優先權的風險一般是無法承受，以及需要管理層高度關注的風險。

4.3.4 識別及選擇保安保障措施

在覆檢保安風險評估的結果後，便能夠識別及評估保安保障措施的效用。保安評估小組會建議採取可行的保安保障措施，將已找出的威脅和漏洞的可能性及其影響減至可接受的水平。

4.3.4.1 常見保安保障措施類別

保安保障措施可以是快速修復在現行系統配置所發現的問題程式，也可以是系統升級計劃。保安保障措施可以是技術性或程序性的控制措施。

保安保障措施一般可分為三個常見類別：

- 杜絕入侵途徑：完全杜絕未獲授權者接達關鍵資源
- 鞏固防禦能力：使未獲授權者難以接達關鍵資源
- 系統監察：協助即時、準確地偵測和應付攻擊

保安保障措施包括：

- 制訂／改善部門資訊科技保安政策、指引或程序，以確保達到保安成效
- 因應在保安風險評估所發現的薄弱環節重新配置操作系統、網絡構件和設備
- 運用密碼控制程序或認證機制，確保採用強化密碼
- 運用加密或認證技術保護數據傳輸
- 改進實體保安保護
- 制訂保安事故處理及報告程序
- 提高人員的保安意識，並為他們提供培訓，確保人員遵守保安要求

4.3.4.2 確定和選擇保安保障措施的主要步驟

選擇適當的保安保障措施，有賴負責選擇的人員精通系統知識和專業技術，所以並不簡單。管理風險的成本須與風險水平相稱，即為某特定資產減低風險的成本，不應超過有關資產的總值。

下列為確定和選擇保安保障措施的主要步驟：

- 為各目標漏洞選擇適當的保安保障措施
- 確定各保安保障措施的相關成本，例如開發、推行和維修成本
- 將保安保障措施／漏洞組合與所有保安威脅配對，即在保障措施與威脅之間建立關係
- 釐定及量化保安保障措施的影響，即採取選定的保安保障措施後得以減低的風險幅度

保安保障措施可能涉及實體、管理、程序、操作和技術保安保障措施等的不同組合。進行分析能夠為不同的情況選定最適當的組合。

一項保安保障措施可能減低多項威脅帶來的風險，但有時採取多項保安保障措施卻只能夠減低一項威脅帶來的風險。因此，將所有保安保障措施整合，能夠顯示減低全部風險的整體效益。

在採取保安保障措施前，應測試採用不同措施的影響，為此，選擇程序可能要進行數次才能掌握建議的更改對風險結果的影響。

除保安風險評估找出的因素外，選擇保安保障措施時還須考慮其他因素。

例如：

- 組織因素，例如部門的目標和目的
- 相關的法定、規管及合約要求
- 文化因素，例如社會習俗、信仰、工作風格
- 質量要求，例如安全程度、可靠程度、系統性能
- 時間限制
- 支援服務和功能
- 技術、程序和操作要求和控制措施
- 市面上現有的技術

4.3.5 監察與推行

應妥善地以文件記載風險評估結果。這些文件可供審計保安風險評估程序之用，並有助持續監察和覆檢。

必要時應重新進行評估。另一項重要工作是追蹤環境轉變和已發現風險及其影響之優先次序的變化。保安審計是覆檢保安措施推行情況的方法之一。

應明確界定、覆檢和分派操作員、系統開發人員、網絡管理員、資料擁有人、資訊科技保安主任和用戶等相關人士的職務和職責，以配合推行保安保障措施。管理層應撥出專用資源，並支持對推行保安保障措施的監察和控制。

4.4 常見的保安風險評估工作

下列是保安風險評估的部分常見工作，以供參考，實際工作將視乎評估範圍和用戶要求而定。

- 識別可能影響資訊科技和保安整體方向的業務需要及修訂要求。
- 就每個資訊系統的操作，定出及記錄所有適用的相關法定、規管及合約要求。
- 分析資產、威脅、漏洞、其影響和可能性。
- 評估電腦設備和其他網絡構件的實體保護措施。
- 對網絡結構、規約和構件進行技術和程序覆檢與分析。
- 覆檢及檢查遠程接達系統、伺服器、防火牆和外部網絡連接（包括客戶互聯網連接）的配置、實施和使用情況。
- 覆檢密碼和其他認證機制。
- 覆檢機構內部人員目前的保安意識和投入感。
- 覆檢有關供應商和承辦商所提供服務或產品的協議。
- 提出切實的技術建議，以處理所發現的漏洞，並減低保安風險的水平。
- 執行自動應用程式原始碼掃描，以加強各決策局／部門所開發應用程式的保安保障措施。

4.5 成品

保安風險評估在進行的各個階段，可能提交不同的評估成品。下表（表 4.3）所示為不同成品的清單。**附件 B** 載列了不同成品內容的示例，以供參考。

	工作	成品	簡介
1	確定保安要求	保安要求報告	就已確定的資產、威脅、漏洞及其影響和可能性，闡述用戶保安要求的報告
2	保安風險評估	保安風險評估報告	就已確定的資產、威脅、漏洞、其影響及改進建議或補救措施，闡述保安風險評估結果的報告
3	覆檢現行的保安政策、指引和程序	嶄新／經修訂的保安政策、指引和程序	一份或一套保安相關內容文件，以控制保安保護措施在評估領域的推行

表 4.3 成品列表

5. 保安審計

保安審計是以資訊科技保安政策或標準為基礎的遵行狀況審計，以確定現有保護的整體情況，並驗證現有的保護措施是否已經妥善地實行。它的目標是確定當前環境是否按照預定的保安政策要求受到適當的保護。保安審計應定期執行，以確定符合保安政策和有效地實行安全措施。

保安審計需要保安政策和標準、審核清單和物品清單，並可能涉及不同領域，如網上應用系統、網絡架構、無線通訊等。附件 C 列出不同的審計領域。附件 D 提供不同保安範疇的審計檢查清單樣本。附件 E 提供作為遵行證據的已記錄資料樣本清單。保安審計可能涉及使用不同的審計工具和不同的審查技術，以揭示保安不合規處和漏洞。在審計過程後會準備一份審計報告，用以指出當前的保護措施與保安政策和指引所規定的要求之間的符合情況和差距。

在揀選審計師和進行審計工作時，必須確保審計過程客觀而公正。作為一般原則，審計師不得審核本身有份參與的工作。保安審計師可以覆檢與系統相關的文件，以了解是否存在不足或不合規之處。

保安審計的主要目的在於：

- 檢查保安措施是否符合現行的保安政策、標準、指引和程序
- 識別不足之處，並檢驗現行政策、標準、指引和程序的成效
- 識別及覆檢相關法定、規管及合約要求
- 識別、分析並了解現存的漏洞
- 覆檢現行的操作、行政和管理事項的保安控制措施，並確保在操作、行政和管理等方面貫徹落實有效保安措施並符合最低保安標準
- 為改進提供建議和糾正措施

5.1 審計頻率及時機

5.1.1 審計頻率

保安審計是持續進行的活動，而非一次性的事件。保安審計應定期進行，以確保符合保安政策、指引和程序，並確定將風險減至可接受水平所需的最低要求控制措施。值得注意的是保安審計只能概括地揭露在某特定時間所發現的保安漏洞。

5.1.2 審計時機

保安審計應在不同情況下進行，而進行的確切時機則視乎系統要求和資源而定。

- 安裝／升級後審計：在啟用嶄新或經過重大升級的系統前，為確保符合現行政策、指引及配置標準的審計
- 定期審計：定期（例如每年一次）以人手或使用保安相關的工具自動進行審計，確保已採取最低限度的控制措施以偵測及處理保安漏洞
- 抽樣審計：隨機檢查，以反映實際作業情況
- 晚間或非辦公時間審計：在非辦公時間或晚間進行審計以減低相關風險

5.2 審計工具

審計工具中有不少自動化工具可幫助找出保安漏洞。選擇採用何種審計工具則視乎保安需要和監察工作負荷的影響而定。

舉例來說，有些保安掃描工具可透過掃描和發動模擬攻擊，查出網絡（基於網絡的掃描工具）或特定主機（基於主機的掃描工具）目前的存在保安漏洞。檢查結果會記錄在審計報告中以供進一步分析。

這些市面上供應的現成工具可與保安審計師自行開發的工具一併使用。保安審計師還可能使用在黑客圈子中最新的工具，以模擬層出不窮的攻擊活動。

社交工程攻擊和審計清單等人力覆檢技術也可用來對機構內部的整體保安意識水平進行非技術覆檢。

5.3 審計步驟

一般而言，保安審計可分為以下幾個步驟：

- 規劃
- 收集審計資料
- 進行審計測試
- 報告審計結果
- 保護審計資料和工具
- 改進與跟進

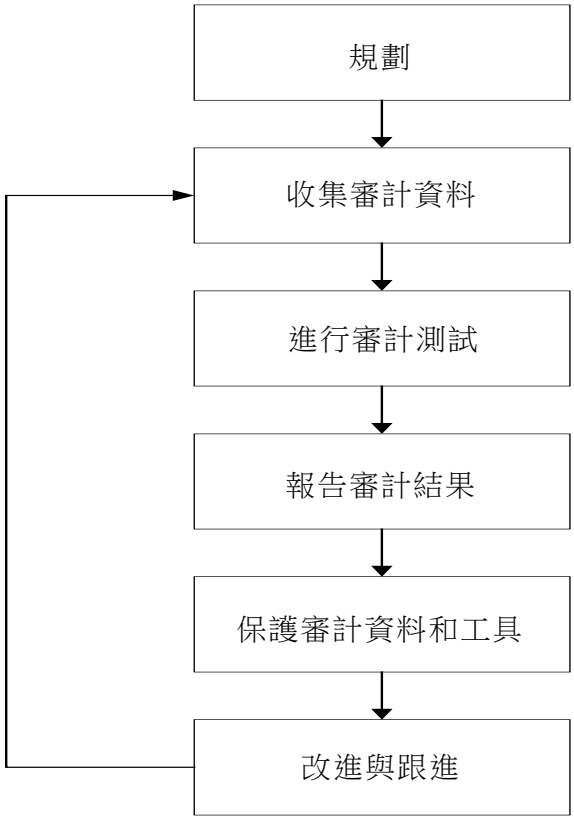

圖 5.1 一般審計步驟

5.3.1 規劃

規劃有助釐定和挑選有效益和有效率的方法，以進行審計和收集所需的所有資料。規劃所需的時間視乎審計的性質、範圍和複雜性而定。

5.3.1.1 計劃範圍和目標

審計應有清晰的範圍和明確的目標。在進行審計前，應與保安審計師確認和商定用戶要求。

保安審計的範圍包括：

- 互聯網保安
- 內部網絡的一般保安
- 關鍵任務系統
- 主機保安
- 網站伺服器、電郵伺服器等網絡伺服器的保安
- 防火牆、路由器等網絡構件和設備
- 電腦室的一般保安
- 目錄服務、郵件傳遞服務、遠程接達服務等網絡服務
- 系統文件和記錄

部分審計目標列舉如下，以供參考：

- 為遵守系統保安政策和程序提供證明
- 檢驗和分析系統的保安保障措施，以及操作環境
- 評估保安機制設計在技術和非技術方面的實施情況
- 證實所有保安功能的欠缺、恰當或不當整合和操作

5.3.1.2 限制

應為審計預留充裕時間，以確保能依時完成所有的測試。有些時候，當進行審計時，系統或網絡須離線或暫停運作，以致可能發生服務中斷的情況。在展開保安審計工作前，必須為目前的配置和資料進行備份及復原處理。

5.3.1.3 職務和職責

與進行保安風險評估類似，應小心及清楚界定各參與者的職務和職責。有關一般參與計劃的成員可參閱第 4.3.1.4 節－相關人士的職務和職責。

尤其是，保安審計師在獲委聘後，應計劃進行保安審計工作前的預備事項：

- 通過翻查文件、訪談、會議和人力覆檢確定和核實目前的環境
- 確定與審計相關的重要領域或操作事項
- 確定可能影響審計的一般控制措施
- 確定和估計審計所需的資源，例如審計工具和人力資源
- 確定審計所需的任何特殊或額外處理程序

保安審計必須在妥善的監控和授權下進行。決策局／部門與保安審計師之間必須建立溝通渠道。

另一方面，應先考慮以下兩方面事項：

- 保安審計師的獨立性

  應就保安審計的性質，考慮所委聘的保安審計師是否適當的人選。選擇獨立和可信賴的第三方作為保安審計師可確保審計觀點正確、公平和客觀。委聘內部或外部保安審計師的工作應慎重計劃，尤其是委聘處理保密資料的保安審計師。在審計過程中，揀選審計師必須客觀。審計師不得審核本身有份參與的工作。

  保安審計是持續發現和糾正保安問題的過程。應避免長期聘請同一保安審計師，以避免獨立性下降，以及避免由於使用相同方法重複進行審核而導致的保安覆檢盲點。

- 人手編排

  保安審計應由具備足夠技術和經驗的審計師，在系統管理員的陪同下進行。事先應清晰界定和分派參與審計各方的職務、職責和責任。

5.3.2 收集審計資料

對於需要收集多少資料、收集哪類資料，以及如何過濾、儲存、接達和覆檢審計資料和記錄，都必須明確釐定。

收集資料的數量取決於審計範圍、目標及數據可用性。

收集資料須慎重規劃。收集資料的安排必須符合政府法例和規例，而且必須避免挑起或引發其他潛在的保安威脅和漏洞。必須收集、妥善保存和保護所有需要的數據，以防止未經授權的接達。

審計資料可以多種不同的方式儲存，例如，

- 記錄檔案，例如系統啟動及關閉的資料、用戶的登入和退出、曾執行的指令、違反接達控制的事件、帳戶和密碼更改。
- 記錄，例如審計追蹤、日誌、摘要、所有事項的詳盡報告、統計報告或例外報告。
- 存儲媒體，例如光碟。

除收集電子數據外，部分實體事件或人為工作亦應妥為記錄，以供將來參考之用。

這方面的工作包括：

- 電腦設備維修保養工作，例如日期、時間、提供支援的供應商資料及工作情況
- 變更控制和管理事項，例如更改配置、安裝新軟件、數據轉換或更新修補程式
- 保安審計師或訪客等外部人士的親身實地走訪
- 政策和程序更改
- 操作記錄
- 保安事故記錄

一般來說，收集審計資料的步驟可能會遵從保安風險評估所採用的資料收集技術。但是，保安審計的目的並非評估操作環境所存在的風險，而是覆檢操作、行政和管理方面的現有保安控制，以及確保符合既定的保安標準。收集審計數據或證據旨在證實有否採納適當的保安控制並已妥善執行。有關數據收集技術的詳情，請參考第 4.3.2 節－ 資料收集。

5.3.3 進行審計測試

經過全面的規劃和數據收集後，保安審計師可進行：

- 根據既定的審計範圍，對現行的保安政策、標準或指引進行的一般覆檢
- 對保安配置的一般覆檢
- 利用不同的自動化工具進行診斷覆檢及／或滲透測試的技術性調查

視乎審計範圍，保安審計所涉及的系統或網絡也各有不同。

附件 C 所載為不同審計領域的目的和範圍。

5.3.4 報告審計結果

保安審計報告須在完成審計工作後提交。保安審計師應分析審計結果並提交反映目前保安狀態的報告。為了去除不適用的結果和誤報，應加以分析由掃描工具產生的報表。嚴重程度可能要因應決策局／部門的個別環境情況而作出調整。

有關審計報告須可讓資訊科技管理人員、行政管理人員、相關系統管理員和系統擁有人、及審計組和控制組人員等不同人士看懂。

有關保安審計報告建議內容，請參閱**附件 B**。

5.3.5 保護審計資料和工具

在整個保安審計的各階段中，妥善保障審計數據和工具是不可缺少的。

審計數據和所有與審計相關的文件須予以適當保密分類，並根據其保密級別受到保護。

審計工具應妥善備存、控制及監察以免被濫用。審計工具應只由保安審計師在受控制的環境下使用。除非已採取適當的控制措施保護審計工具以防未獲授權接達，否則在使用後應立即移除審計工具。

保安審計師在完成審計工作後，必須向有關各決策局／部門歸還所有審計資料。有關歸還資料的安排必須在委聘保安審計師前，與保安審計師達成協議。

5.3.6 改進與跟進

如果需要採取糾正措施，部門應分撥資源，以確保盡快作出改進。如有任何不合規之處，應通知系統管理層。有關跟進工作的詳情，請參閱較後章節。

6. 服務的先決條件和一般工作

6.1 假設和限制

在進行保安風險評估或審計時，應作若干假設：

- 時間和資源有限
- 目的在於盡可能減低及控制保安風險

6.2 用戶的責任

由外聘人士進行保安風險評估或審計時，決策局／部門應配合並負責下列各項工作：

- 對提供服務的供應商和保安審計師進行背景和資格審查，以確保有關供應商和保安顧問／審計師具備所需的經驗和專業知識
- 在展開任何評估或審計活動前，編製一份協議予提供服務的供應商簽署。協議內包括但不限於免責聲明、服務詳情及不可對外披露資料聲明。編製協議的工作對決定進行外部滲透測試（例如撥號式掃描或從互聯網模擬黑客入侵內部網絡）尤為重要
- 調派人手擔任與供應商聯絡的第一（及第二）聯絡人
- 向供應商提供聯絡人名單，以便有需要時在辦公及非辦公時間聯絡
- 保持合作開放的態度。如確實有保安需要，應認同評估結果，並制訂改善計劃
- 只開放進行評估所需的系統、網絡或電腦設備的實體和邏輯接達權，並保護可能受評估服務影響的所有資產
- 向供應商索取有關在測試時網絡、服務或系統所受影響或損害程度的正式通知，以便在測試前準備好復原計劃和適當的事故處理程序
- 在合理的時間內回覆保安顧問／審計師的查詢
- 提供足夠的辦公地方和辦公室設備，讓供應商能夠提供服務；宜向供應商提供限制出入的辦公地方
- 提供評估和審計特定領域需要的一切文件，包括日誌記錄政策或其審查程序，例如接達日誌記錄的檢查
- 與供應商定期舉行計劃控制和覆檢會議
- 當評估相關風險並準備好復原方案後，應盡早推行更改或採取改進措施，尤其是針對極高風險領域的措施

6.3 服務的先決條件

應符合的先決條件如下：

- 提供所需的所有正式或非正式已記錄資料，例如網絡圖、操作手冊、用戶接達控制清單、保安政策、標準、指引和程序。有關已記錄資料作為遵行證據示例清單，請參閱**附件 E**。
- 提供與評估領域相關的人員支援，例如互聯網使用、防火牆配置、網絡及系統管理、保安需要和要求等。
- 安排評估人員在陪同下參觀場地，以收集更多評估和審計資料。
- 選擇由獨立的第三方進行保安審計。

6.4 保安顧問／審計師的責任

為決策局／部門進行保安風險評估或審計的保安顧問／審計師應：

- 具備必要的技術和專業知識。
- 了解各個工具的影響，並估計它們對決策局／部門有怎樣的影響。
- 向互聯網服務供應商、警方或其他有關方面索取適當的書面授權，這一點在進行黑客入侵測試時尤其重要。
- 不論測試成功與否均予以記錄。
- 確保報告能反映決策局／部門的保安政策和運作需要。
- 運用良好的判斷力，向決策局／部門即時報告在審計過程中發現的任何重要保安風險和不合規之處。

6.5 一般工作示例

事項	工作清單	工作詳情
1	簡介會	商定服務範圍、目的和成品
2	計劃規劃	制訂一份雙方同意的提交成品時間表和服務期限
3	準備檢查清單	準備一份檢查清單，並得到決策局／部門的同意
4	準備技術性漏洞測試回退／復原程序 (例如漏洞掃描、滲透測試等)	在技術性漏洞測試及滲透測試前準備回退／復原程序
5	資產識別與估值	在協議的範圍內識別和評估資產
6	保安風險評估	
	一般控制覆檢	透過文件覆檢、實地走訪、與各級人員進行訪談、小組討論、調查等進行一般控制覆檢
	系統覆檢	進行系統覆檢以識別系統漏洞。按需要進行漏洞掃描、滲透測試和原始碼掃描
	風險和影響分析	識別資產、威脅、漏洞及其風險和影響
	保安保障措施分析	識別和挑選可供選擇的保安保障措施
	提交保安風險評估報告	編撰評估報告，列明評估結果和建議
	演示保安風險評估結果	向管理層演示評估結果和發現
7	保安審計	
	遵行要求檢查	透過文件覆檢、實地走訪、與各級人員進行訪談、小組討論、調查等，並根據 S17 及部門保安政策或在保安審計範圍內相關的政策進行遵行要求檢查
	提交保安審計報告	編撰保安審計報告
	演示保安審計結果	向管理層演示審計結果和發現
8	妥善保障資料和結果	完成保安風險評估和保安審計工作後，應妥善保障所有收集到的資料、測試結果和工具

事項	工作清單	工作詳情
9	跟進行動	
	制訂跟進計劃	制訂一個回應建議並有推行時間表的跟進計劃
	保障措施推行的覆檢	覆檢推行保障措施後的保安狀態
	提交驗證報告	編撰驗證報告，總結每項發現的最終結果
10	結束	
	提交驗證結果	將結果提交管理層以結束該項目

表 6.1 一般工作示例

7. 保安風險評估及審計跟進

7.1 跟進的重要性

保安風險評估和審計的好處不在於所提出的建議，而在於有效地落實建議。在建議提出後，基本上由管理層負責落實建議。如果管理層決定不落實建議，便須承擔相關的保安風險和不合規之處，並應為不落實建議的決策提出充分理由。

保安風險評估和審計所提建議主要涉及以下三方面：

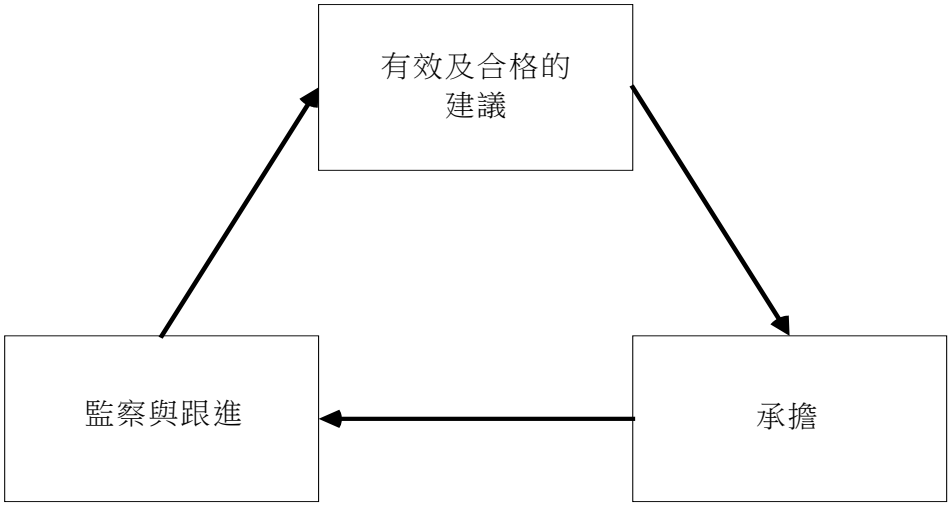

圖 7.1 就建議採取的跟進行動

7.2 有效及合格的建議

保安顧問／審計師必須提出有效及合格的建議，這些建議應符合以下條件：

- 明確清晰、容易理解和可識別
- 具說服力、證據充分
- 具重大意義
- 切實可行

此外，保安顧問／審計師的建議應針對問題的真正成因，並在足夠證據和充分理由的基礎上提出最佳的選擇方案。有關建議須全部提交管理層，而管理層則有權批准及落實建議。

7.3 承擔

個人和部門的承擔對落實建議至關重要。保安顧問／審計師、人員和管理層可能有不同的考慮和着眼點，和對落實建議的次序亦可能持不同意見。

7.3.1 保安顧問／審計師

保安顧問／審計師是首先提出改進建議的一方。他們應：

- 對自己的建議有信心，如果用戶遵從其建議，應能夠產生理想的改善效果；
- 了解決策局／部門在環境、時間、資源和文化等方面的限制；以及
- 通過適當及有效的溝通途徑提出建議。

7.3.2 人員

人員在這裡尤其是指直接或間接受建議影響的一方。人員可能須支援落實建議，也可能就是實際上須改變日常操作程序的用戶。人員應：

- 獲部門鼓勵以加強與保安顧問／審計師合作；
- 獲足夠時間和資源以作出改進；以及
- 獲保證他們能夠從建議中得益。

7.3.3 管理層

管理層在落實改進建議的工作中扮演重要角色。管理層應：

- 在保安事務上採取積極主動而不是消極被動的態度；
- 在整個評估或審計過程中給予充分的支持；
- 調撥充足的資源以作出改進；
- 認識到跟進責任的價值和重要性；
- 鼓勵在規劃、控制和溝通足夠的情況下立即採取改進行動；以及
- 提高人員的保安意識並加強培訓。

7.4 監察與跟進

監察與跟進包含三個主要步驟：

- 建立有效的監察與跟進機制
- 確認建議並制訂跟進計劃
- 主動監察及報告

7.4.1 建立監察與跟進機制

管理層應就建議訂立監察與跟進機制。除負責保安風險評估或審計的人員外，管理層可調派額外人手監督監察機制的整體成效。

管理層負責提供充分的支持、整體指引和方向。監察機制的範圍、目的和功能可由管理層制訂。此外，管理層還可制訂基本規則和指引，作為保安評估監察與跟進的一般參考。

7.4.2 識別建議並制訂跟進計劃

為有效並及時地採取改進措施，應進行以下各項工作：

- 識別主要、重大和關鍵建議，以便進行額外監察，並投放最多的人力物力。
- 為所有建議，制訂跟進計劃。跟進計劃包括落實方案、估計時間、行動清單、成果驗證程序和方法。
- 匯報並強調重點建議和跟進工作。
- 根據計劃，跟進所有建議。

7.4.3 主動監察及報告

在完成落實建議的工作前，必須主動監察及報告跟進行動的進度和進展情況，並就所有建議採取跟進行動。

7.4.3.1 跟進行動的進度和進展情況

跟進行動有不同的進度和進展情況：

- 尚未展開或採取的行動
- 已完成的行動
- 正採取行動而且已定下目標完成日期
- 不採取行動的理由
- 建議以外的其他行動

7.4.3.2 跟進行動

下列是一些建議採用的跟進行動：

- 覆檢落實方案、文件和行動時間表。
- 找出並記錄不採取行動的理由。
- 建立額外的步驟或工作項目，以解決技術、操作或管理方面的困難。
- 因應突發環境或要求轉變，找出並推行其他可行的建議。
- 在證實建議已落實及測試成功、或不再有效、或已採取跟進行動但仍未湊效時，決定「終止」建議的日期。
- 評估糾正行動的成效。
- 向管理層報告成果、進展情況和進度。
- 在適當情況下提請管理層跟進，特別是在關鍵建議落實不足、延誤、或不採用時。

完

附件 A：保安風險評估提問樣本清單

在識別保安風險之前，可能須視乎保安風險評估的範圍，評估很多不同的領域。在進行保安風險評估時，顧問可能會設計問卷調查，向決策局／部門內各級人員收集最新資料。以下為問卷可能提出涉及不同類別的問題示例。顧問會根據評估的範圍和環境改進檢查清單。

提問示例
規則和政策
• 是否已制訂適當的保安政策、指引和程序？ • 現行的保安政策／程序／指引是否已充分列明准許及禁止的行為？ • 人員及用戶在獲授接達權前，是否知悉有關的法律、保安政策和程序，以及須承擔的責任？ • 用戶可否輕易取閱保安政策／指引／程序？ • 有否定期監察和覆檢有關的保安文件？ • 系統所用的所有軟件是否都符合現行的知識產權和特許協議？ • 有關人員有否確實遵從和遵守所有規則和政策？ • 有否定期覆檢保安文件以應對新科技導致的威脅？
使用和支援系統服務
• 系統是否只用來履行公務上的職責，而在使用時可曾發生大規模的違反保安事件？ • 全體用戶是否已接受足夠的培訓，懂得使用獲提供的系統／服務？ • 是否已建立任何書面申請和授權程序，方便人員申請和管方授予服務或系統的使用權？ • 提供支援的供應商（例如互聯網服務供應商）有否提供可靠及符合成本效益的支援服務？ • 互聯網服務供應商代存的電郵是否已獲得適當保護？ • 有否適當地監察、控制及覆檢支援服務的供應商的表現？

提問示例
系統／網絡的完整性
• 有否禁止用戶自行連接或接達服務或系統（例如互聯網連接）？ • 有否配置所有主機和工作站，防止引入主動式內容或微應用程式？ • 系統記錄或誤差記錄會否保存一段適當時間？ • 是否已採取措施保護所有記錄，包括邏輯和實體控制記錄免被未獲授權接達及竄改？ • 系統或網絡內是否已採取保護措施防止外部接達？ • 是否有任何保密資料未經加密便在網絡上傳遞？ • 是否已採用數碼證書技術？若是，請說明哪些服務或應用系統已採用該技術？
入侵偵測及監察
• 是否已制訂任何保安事故應變／處理程序？ • 相關的全體人員是否均了解和遵從本程序（他們是否起碼了解和遵從應由他們負責或可能受影響的部分）？ • 保安事故應變／處理程序是否已列明一旦發生可疑活動應立即採取的行動？ • 如有任何可疑活動，是否會發出任何審計追蹤／記錄、報告或警報？ • 是否定期或有規律地覆檢本程序？ • 是否會作出周詳的報告，以便監察用戶的活動，例如用戶名稱、登入／退出、連接日期／時間、所用服務、發出／收到的資料類別、獲授予的接達權、使用電郵、互聯網、打印機和抽取式媒體的情況、用戶獲分配使用的電腦設備等？ • 是否定期編製和覆檢用戶活動監察報告？ • 過去可曾發生任何違反保安事件？ 最近／上一次違反保安事件是什麼？當時如何處理該事件？ • 是否有專人監察服務／網絡？ • 是否已制訂應變計劃？ 是否已測試及試運行這些計劃？ 是否定期覆檢及測試這些計劃，以順應系統／網絡的變化？ • 對不斷出現的威脅，如拒絕服務攻擊、分布式拒絕服務攻擊、高級持續性網絡攻擊，及勒索軟件等有否任何偵測及監視機制？ • 有否任何措施緩解當時網上威脅？

提問示例
實體保安
• 是否有任何證據或文件，顯示電腦室符合根據所存放數據的保密類別而訂定的實體保安要求？證據或證明文件的例子包括建築署發出的認證／通知或上次保安風險評估與審計報告的相關結果。 • 網絡的所有關鍵構件，例如防火牆、伺服器、路由器和交換器是否已放置在限制出入或安全的地方？ • 對放置網絡構件的地方是否已採取環境控制措施，以免構件受火災、停電或供電不穩定、水浸影響？ • 是否已適當地將所有備份保存在安全的地方？ • 對網絡構件有否推行任何接達控制，例如進出電腦室時必須在記錄簿簽字登記、對電腦室門匙的使用加以控制？
變更控制管理
• 是否已明確界定及指配系統管理員、用戶及操作員於接達系統／網絡的職務和職責？ • 在更改配置前，所有行動是否均已正式獲批准、經過徹底測試並已作文字記錄？ • 對配置文件是否已採取保護及接達控制措施，以防止未獲授權接達？ • 操作系統及軟件是否已採用所有最新的修補程式？ • 對管理工作（如有）是否已採取任何內部和遠程邏輯接達控制？ • 是否有專人負責每天的監察、管理和配置工作？ • 是否已向人員提供有關操作系統／網絡必要配置功能的培訓？ • 是否在內部及遠程均全面為所有配置備份？是否已妥善保存所有備份媒體？
保安風險評估及審計
• 是否曾進行任何保安風險評估和保安審計？ • 每次保安風險評估和保安審計的時間和內容是什麼？ • 曾找到什麼主要的保安風險？ • 是否已制訂任何跟進計劃以落實建議？ • 是否已妥善地解決所有保安風險？ 如果沒有，原因為何？ • 是否已將未解決的跟進計劃通知管理層？ • 是否已適當地保存及儲存評估和審計結果？

提問示例
防範惡意軟件
• 是否已採用標準的惡意軟件偵測及修復措施或工具？ 所有主機和伺服器是否均已安裝這些軟件或工具？ • 是否已就如何使用這些惡意軟件偵測及修復措施或工具，制訂標準或指引？ • 所有工作站和主機是否均已安裝最新版本的惡意軟件定義，及相應的偵測及修復引擎？ • 是否已確保使用最新的惡意軟件定義檔案？ 一般相隔多久會更新或向用戶派發定義檔案？ • 是否已定期通知用戶可供使用的最新版本惡意軟件定義？ • 這些工具是否能夠偵測任何電郵宏指令病毒、壓縮檔案、電郵附件、常駐記憶體資料等？ • 是否有任何支援人員負責處理惡意軟件攻擊事件？ • 如果偵測到惡意軟件，是否會進行調查及採取跟進行動？
教導及培訓
• 是否提供任何關於資訊科技保安的培訓或講座？ • 是否定期向用戶宣布或介紹資訊科技保安技術、政策的變動或相關的新聞？ • 提供支援的全體人員是否均獲得足夠的培訓，確保適當地配置、管理和監察網絡／系統？

附件 B：成品內容示例

B.1 保安要求報告

該報告載錄對評估領域的最低保安要求。這些保安要求可根據決策局／部門本身的需要劃分為高層次或低層次要求。一般而言，這些要求根據資產、威脅和漏洞及其影響劃分。

以下是供參考的保安要求示例清單：

- 提高保安意識及加強培訓
- 確保有足夠的接達控制
- 編製一套完整的資訊系統和操作文件
- 制訂保安事故處理及應變程序
- 制訂正式的書面應變計劃
- 定期進行保安審計
- 備存足夠和適當的記錄
- 制訂授權接達和控制程序
- 確保資料傳輸的安全，包括為保密資料加密

B.2 保安風險評估報告

該保安風險評估報告應包括但不限於下列各項：

- 引言／背景資料
- 摘要
- 評估範圍、目的、方法、時間表和假設，評估所包括及不包括的範圍
- 當前環境或系統的描述，並附上網絡圖（如有）
- 保安要求
- 風險評估小組
- 評估結果及建議的摘要
- 就已確認的資產、威脅、漏洞及其影響和可能性，提供風險分析結果，界定風險水平並提出適當的理由
- 建議保安保障措施，如果提出多個建議供選擇，便須附連成本／效益分析，例如安裝防禦機制或加強現行的保安政策和程序等
- 結論
- 附件包括已完成的一般控制檢查清單、漏洞掃描報告、滲透測試報告、資產識別與估值結果等。

B.3 保安政策、指引和程序

除報告外，保安顧問／審計師可協助決策局／部門制訂和提出某些政策和指引。

例如：

- 部門保安政策
- 變更管理控制程序
- 密碼管理指引
- 資訊保安事故應變及處理指引
- 一般主機保安指引
- 具體的資訊系統保安政策
- 目錄服務保安政策

B.4 保安審計報告

審計報告應包括但不限於下列資料：

- 引言／背景資料
- 撮要
- 審計範圍、目的、方法、時間表，以及假設和局限
- 當前環境的描述
- 保安要求
- 審計小組
- 保安審計師的獨立性聲明 1
- 審計結果摘要
- 測試及測試結果詳情
- 根據所發現的問題領域提出建議和糾正行動，例如違反保安政策、配置不當、已知的漏洞和潛在的漏洞、泄露資料、不使用的服務（特別是預設服務）和不使用的帳戶等。
- 結論
- 附件包括審計檢查清單、漏洞掃描報告、滲透測試報告等。

[1]倘若由於參與審計以外的事宜而可能有損審計師的獨立性，有關非審計職務的資料須予披露。

附件 C：各種審計領域

C.1 防火牆

這項審計領域的目的是確保適當配置防火牆及相關系統，以最少和最有效的保安保護措施推行保安政策。對防火牆的審計不限於配置，還涵蓋防火牆的實體接達控制。

這審計領域可包括下列各項：

- 對防火牆主機實體接達控制
- 防火牆操作系統的版本和修補程式
- 防火牆配置及對互聯網通訊的控制，例如規則庫和開啟埠
- 容許或禁止通過防火牆的服務
- 互聯網連接目前的結構，例如與路由器、代理伺服器、電郵伺服器及網絡伺服器的連接
- 為獲得額外服務與其他第三方產品的連接，例如惡意軟件偵測及修復措施
- 遠程連接支援和配置
- 管理和變更控制程序
- 接達控制清單（如有）

保安審計報告應概述對防火牆的評估，並就防火牆結構、配置、管理和操作提出建議。

C.2 內部網絡

這項審計領域的目的是找出可能被獲授權內部用戶利用的任何保安漏洞，並確定內部系統及網絡控制措施的強弱之處。另外還可覆檢內部網絡基礎設施的布局。

審計測試一般包括內部網絡掃描，從而在指定時間或預定時段內檢查任何保安漏洞。測試可包括對關鍵主機或工作站的掃描。

此審計領域可能包括：

- 對內部工作站、伺服器或網絡的掃描，以確認主機、服務和網絡配置
- 找出操作系統、內部防火牆、路由器、網絡構件和基礎設施的保安漏洞、規約和配置誤差
- 嘗試入侵內部網絡和系統
- 評估與接達控制及監察、管理及變更控制程序和作業模式相關的內部保安措施
- 就加強網絡保安提出建議

C.3 外部網絡

這項審計領域的目的是從外部（例如互聯網）找出系統和網絡的保安薄弱環節。外部網絡審計通過掃描，並在指定和預定時間及地點，從互聯網向內部網絡發起攻擊（即黑客入侵），預測可能引發違反保安事件的外來攻擊。

這項審計領域可包括：

- 掃描內部伺服器，以找出容易受攻擊的埠和服務
- 掃描外部網絡通訊閘，以確定可使用的埠、服務和網絡布局
- 嘗試從外部收集內部配置資料
- 從外部向內部系統發起入侵攻擊

審計師和用戶雙方必須制訂協議，明確地界定審計範圍和測試程度詳情，例如受攻擊的網絡部分／構件或可接受的攻擊嚴重程度。保安審計師必須承諾將干擾減到最低程度，並避免對系統和網絡造成破壞。

C.4 主機保安

這項審計領域的目的是評估不同電腦平台的操作系統層面保安。操作系統配置不當可產生不為系統管理員所知的保安漏洞。

在考慮操作系統保安時，帳戶及密碼管理、檔案系統、連網工作組、接達權限和審計／日誌記錄均為不可遺漏的常見組件。詳情列述如下：

帳戶及密碼管理

- 密碼控制政策，例如密碼的最短和最長的長度
- 用戶配置檔案和權限
- 預設用戶或管理帳戶
- 共用帳戶
- 帳戶政策，例如帳戶鎖定、帳戶有效期

檔案系統

- 系統檔案保護措施及接達權限
- 檔案接達控制清單
- 網絡檔案系統的使用

連網工作組

- 領域及信賴關係
- 工作組
- 共用的資料夾
- 複製的資料夾
- 遠程接達控制

接達權限

- 預設資料夾權限
- 共用工作站權限
- 共用打印機權限
- 登記權限
- 共用檔案權限

審計／日誌記錄

- 事件記錄／系統記錄／誤差記錄審計
- 檔案及資料夾審計
- 登錄審計
- 打印機／抽取式媒體記錄審計
- 警報
- 帳戶處理和審計追蹤保護措施

C.5 互聯網保安

這項審計領域的目的是找出系統和網絡中與互聯網應用相關的保安薄弱環節。此類審計內部網絡與外部網絡結合的審計領域，重點在於互聯網通訊閘。

審計領域包括但不限於下列各項：

- 防火牆和路由器配置。
- 網站伺服器、郵件伺服器、認證伺服器等主機伺服器的保安控制。
- 主機、系統和網絡保安管理，以及控制政策與程序。
- 互聯網通訊閘網絡構件及伺服器的實體保安。
- 互聯網通訊閘部分，以及與內部網絡連接界面的網絡保安。
- 從外部向內部互聯網通訊閘發起拒絕服務攻擊或分布式拒絕服務攻擊的防禦能力。
- 破解內部網絡構件。

C.6 遠程接達

這項審計領域的目的是解決與透過撥號連接和寬帶連接（例如虛擬私有網絡、傳輸層安全協議虛擬私有網絡）等通訊鏈路提供遠程接達服務的相關的保安漏洞。此類審計領域可包括下列各項工作：

- 利用自動撥號／連線軟件識別遠程接達用戶。
- 覆檢遠程接達伺服器的保安和配置，以及這些伺服器所在的網絡。
- 進行實地走訪，以覆檢調解器或遠程連接設備的實體控制和位置。
- 制訂遠程接達控制政策或程序。

沒有採取任何控制措施的遠程接達可能會成為外來入侵者的方便之門。問題在於如何建立安全的連接。

這項審計領域可能會識別和覆檢下列項目：

- 需要遠程接達的應用系統／服務及其保安要求。
- 有關遠程接達的現行政策和程序。
- 現有遠程接達連接，例如採用調解器、遠程接達伺服器、調解器群的連接或寬帶連接。
- 現行的遠程接達控制方法。
- 目前存在的問題和改善情況的建議。

C.7 無線通訊

這項審計領域的目的是解決與無線通訊相關的保安漏洞。此類審計領域應包括（但不限於）以下各項工作：

- 評估服務設定識別碼（SSID）命名和命名約定及其他保安配置。
- 評估現有無線網絡加密規約和加密密碼鑰和密碼算法的強度，例如 Wi-Fi 保護存取 3（WPA3），支持強大的加密。
- 評估採用虛擬私有網絡。
- 取得接駁點清單並了解其覆蓋範圍。
- 識別任何未獲授權或非法無線接駁點。
- 嘗試與無線通訊連接。
- 嘗試透過無線通訊收集內部系統資料。
- 評估有否進行實地調查及有關場地的無線通訊的覆蓋範圍。
- 評估客戶裝置上的密碼匙是否獲妥善保護。

C.8 電話線

這項審計領域的目的是找出將內部電腦直接與電話網絡連接的沒有記載或不受控制的調解器。此類審計有助杜絕任何未獲授權或不當的調解器連接和內部網絡及系統配置。

這項審計領域可包括：

- 評估已連接的各個調解器進入點
- 找出任何沒有記載的撥號進入點
- 嘗試與內部網絡連接
- 嘗試透過連接收集內部系統資料

C.9 網上／流動應用系統

這項審計領域的目的是解決與網上／流動應用系統相關的保安漏洞。這項審計領域應包括以下測試：

- 驗證保安要求是否已在早期界定。
- 驗證所推行的保安控制是否符合功能規格文件內訂明的保安要求。
- 驗證是否處理或過濾不正常的用戶輸入。
- 為網上應用系統評估因錯誤訊息及超文本傳輸規約標頭上的元數據所造成的資料泄漏。
- 重演系統驗收測試文件內編製的保安測試個案，以確保維持適當的保安控制。
- 評估網上／流動應用系統的網絡及應用系統結構。
- 評估有否採取適當的接達控制措施。
- 評估加密機制與規約。
- 評估網上／流動應用系統程式的權限。

有關網上應用程式保安的良好作業模式，請參閱《網頁及網上應用程式保安實務指引》。

C.10 保安政策、指引和程序

此章節的目的是覆檢現行的保安政策、指引及程序。覆檢的對象可以是高層次／整體／整個機構的保安政策，或是集中關注的特定系統、網絡或保安組件。

下列是一些集中關注的保安組件示例：

- 遠程接達控制
- 互聯網接達控制、使用和監察
- 互聯網電郵系統
- 操作系統管理
- 密碼控制政策
- 用戶帳戶管理
- 網絡、系統或通訊閘管理
- 變更管理作業模式
- 網絡保安作業模式

附件 D：審計檢查清單樣本

以下所列是從遵行及良好作業模式方面，保安審計可能檢查的部分事項舉例。本檢查清單僅供初步參考，不能涵蓋所有範圍。審計師會根據審計的範圍和環境來改進檢查清單，並可能要求決策局／部門提供相關記錄或文件。

審計事項
管理職責
□ 已界定部門資訊科技保安組織框架及相關的職務和責任。 □ 已推行足夠職務分工，避免單一個體執行資訊系統的所有保安功能。 □ 部門預算包括提供必需的保安防護及資源。
資訊科技保安政策
□ 保安政策以文字方式清楚載明，而且容易理解。 □ 保安政策便於有關各方取閱。 □ 定期覆檢及更新保安政策並獲批准，以反映最新情況。 □ 用戶均知悉並承擔推行保安政策的責任。 □ 保安政策所列的所有規則已落實推行。 □ 保安政策由決策局局長／部門主管及管理層核准、發布和執行。
人力資源保安
□ 所有人員在委任新職位及於整個僱用期間，都獲悉本身的資訊科技保安責任。 □ 明確界定所有職務和職責。 □ 向有關各方提供足夠的保安培訓。 □ 只限曾接受公務員事務局局長所規定適當操守審查的人員才可接達限閱類別以上的保密資料。 □ 已訂明終止或職位變動後的資訊保安責任及工作，並已與人員就此進行溝通。

審計事項
資產管理
□ 妥善管有、保存及維護資訊系統、硬件資產、軟件資產、有效保用證、服務協議書和法律／合約文件的清單。 □ 當人員被調職或不能為政府提供服務時，向政府歸還電腦資源及資料。 □ 資料獲妥善保密分類，其儲存媒體亦已按政府保安要求附上標籤及處理。 □ 已對存有保密資料的儲存媒體執行適當的保安措施，以防範非授權接達、濫用或實體損傷。 □ 所有保密資料都在棄置或重用儲存媒體前徹底清除或銷毀。
接達控制
□ 處理個人資料時已遵守《個人資料（私隱）條例》（第 486 章）。 □ 記錄和覆檢各類用戶在接達系統上所獲授的權限，並確保職務分工恰當。 □ 訂有明確的程序，可定期重新確認用戶在接達系統和應用系統上的權限。 □ 已清晰界定及定期覆檢用戶權限及數據接達權限（例如至少每年一次，最好每年兩次）。 □ 已備存接達權限審批及覆檢記錄。 □ 用戶名稱只代表一名用戶。 □ 所有用戶只獲得僅足以履行其職責的最小權限。 □ 用戶知悉其權限和接達權。 □ 依據所接達的資料類別，制訂適當和安全的程序以分派用戶帳戶和密碼。 □ 妥善備存用戶活動記錄，例如登入／退出時間、連接的時間、連接點、所進行的操作等。 □ 系統／網絡沒有不再使用的帳戶。 □ 向管理員另外提供用戶帳戶。 □ 管理員帳戶只用來進行管理工作。 □ 用戶分為不同的類別，各個類別的權限明確。 □ 具有為系統／網絡而編製完善的密碼政策文件。 □ 關鍵資訊系統採用嚴謹密碼政策。

審計事項
□ 嚴謹密碼政策： ■ 當密碼更新時，不可重複使用 8 個先前使用過的密碼。 ■ 密碼須設定失效期（3-6 個月）。 ■ 輸入錯誤密碼的次數以 5 次為限。 □ 不應選用可在字典內查到的詞彙、用戶名稱或容易猜出的短語作為密碼。 □ 用戶須定期更換密碼，或在收到新帳戶時立即更換密碼。 □ 用戶不得將密碼寫在標籤或容易被他人窺看的地方。 □ 訂有適當的政策與程序，闡明有關流動資訊處理及遠程接達的保安要求。 □ 訂有遠程接達電腦、應用系統和資料的控制措施。 □ 高風險接達採用雙重認證。 □ 在通過虛擬私有網絡連接遠程接達決策局／部門內部網絡，或經互聯網遠程接達決策局／部門內部電郵系統方面，實施雙重認證。 □ 通過虛擬私有網絡傳輸資料時，使用嚴格的加密功能及／或雙重認證（只適用於機密資料），並啟動閒置對話逾時登出功能。 □ 設有正式的使用政策和程序，並須採取適當的保安措施以防範物聯網裝置的風險。
加密方法
□ 密碼匙在整個生命周期，包括密碼匙的產生、儲存、存檔、收回、分發、退役及銷毀，都會得到妥善管理。
實體及環境保安
□ 備有證據或證明文件，顯示電腦室／伺服器室／電腦操作區的實體保安要求，符合部門資訊科技保安政策、政府保安要求和其他相關標準訂明的要求。例子包括上次保安風險評估與審計報告或建築署發出的認證／通知。 □ 所有電纜保持整潔，並適當地貼上標籤，以便維修和偵測故障。 □ 妥善清潔所有地板下的空間（如有）。 □ 定期清潔天花，以免積聚塵埃和污垢。 □ 水浸探測器（如有）裝入地板下空間，以自動探測水浸情況。 □ 將電纜妥善安裝在天花空隙。 □ 為有需要的設備安裝不間斷電源供應器。

審計事項
□ 不間斷電源供應器能夠在預定的一段時間內提供足夠的電力。
□ 定期測試不間斷電源供應器。
□ 不間斷電源供應器放置在安全的地方。
□ 已適當地教導電腦室操作員有關電源供應控制和應付停電情況的知識。
□ 電腦室內沒有存放任何易燃設備或物料。
□ 所有自動火警探測系統均處於正常的操作狀態，並定期進行測試和檢查。
□ 定期測試所有自動滅火系統，確保有關系統處於良好狀態。
□ 穿過電腦室或地板下的所有水管（如有）均處於良好狀態。
□ 電腦室溫度和濕度受到監控，並已調校至適合電腦設備在良好狀態運作的水平。
□ 妥善分發、保管及記錄電腦室的所有門匙。
□ 制訂明確清晰的鎖匙處理及分發程序。
□ 全體人員均已受訓並知悉如何使用滅火器和其他實體保護機件。
□ 電腦室內禁止吸煙、飲食。
□ 帶入電腦室內的便攜式電腦、流動裝置和其他電腦設備應受管制。
□ 指定專人負責安排清潔電腦室的工作。
□ 定期檢查設備及設施。
□ 所有訪客取得授權並確認身份後才能進入電腦室。
□ 在任何時間所有訪客都有授權人員陪同。
□ 所有訪客在進入電腦室時領取訪客標貼。
□ 記錄所有訪客的到訪。
□ 電腦室推行適當的出入管制。
□ 所有電腦室入口已上鎖，以管制出入。
□ 只准獲授權人員進入電腦室，而獲授權人員進出電腦室都必須簽字登記。
□ 所有手冊和文件不得隨意擺放，而應該經存檔處理後放上書架，並推行查閱管制。
□ 電腦室內的電腦文具足夠操作所需便可。避免存放過量的文具以防引起火災。
□ 妥善保存及管制所有電腦文具。
□ 制訂分發、授權及記錄電腦文具的程序。

審計事項
□ 為所有電腦設備備存及檢查適當的清單並加以檢查。 □ 抽樣實地核對電腦設備和清單記錄，確保清單記錄準確無誤。 □ 確保流動裝置或抽取式媒體於無人看管時有措施保護。 □ 被帶離場地的資訊科技設備得到適當管制。 □ 已使用及開啟所有電腦的自動重新認證功能。 □ 在物聯網裝置方面，須根據物聯網裝置儲存、處理和傳遞資料的保密類別來實施保安控制措施，以防裝置遺失、被盜和遭受破壞。
操作保安
□ 所有從互聯網下載的軟件及檔案都經抗惡意軟件篩選及驗證。 □ 具有為備份和復原工作而制訂和編寫的程序。 □ 為已進行的所有備份和復原工作備存記錄，包括日期／時間、所用備份媒體、負責人等。 □ 備份不少於兩份，其中一份存置於場外。 □ 備份媒體有明確的保留期及棄置程序。 □ 妥善地為所有備份媒體標籤並鎖入安全的地方。 □ 在任何時間均鎖好存放備份媒體的地方或儲物櫃。 □ 為場外存放的媒體採取適當的運送控制措施。 □ 妥善控制及記錄接達媒體的情況。 □ 為所有儲存媒體備存清單。 □ 妥善備存、覆檢和分析每日記錄，如系統記錄、誤差記錄或用戶活動記錄等。 □ 由政府資訊科技總監辦公室或決策局／部門中央提供的核准電郵系統和互聯網接達服務記錄須予記錄。 □ 只限獲授權人士接達操作系統設施。 □ 操作系統帳戶沒有執行不使用／可疑的服務。 □ 操作系統沒有保留不使用的用戶帳戶。 □ 每天或定期妥善編製及覆檢系統記錄。 □ 資訊系統的時鐘已與可信賴的時間源保持同步。 □ 對更改資訊系統採取控制措施。已備存更改記錄。 □ 定期安裝操作系統的修補程式，以修補操作系統內已知的保安漏洞。

審計事項
□ 建立和備存決策局／部門常用的硬件設備、套裝軟件（包括修補程式管理系統本身）和其版本號碼的詳細記錄。 □ 決策局／部門須評估使用有關已終止支援軟件的保安風險，以及採取適當保安措施保護資訊系統和相關數據。
通訊保安
□ 與互聯網連接的網絡受到防火牆保護。 □ 推行入侵偵測策略，在網絡關鍵節點安裝網絡入侵偵測系統或網絡入侵防禦系統，以偵測網絡異常活動。 □ 採用網絡分段／隔離，並以此作為所有新推行的系統或現有系統進行大規模升級和變更時須遵守的標準。 □ 接入內部網絡的所有遠程接達，均以認證和記錄作妥善控制。 □ 只限獲授權人員進行網絡構件的管理工作。 □ 對共用檔案、打印機等網絡資源的使用，採取控制措施，只准已獲授權及認證的用戶使用。 □ 只限獲授權人士更新網絡所安裝的軟件。 □ 制訂政策以控制網絡及其資源，使其得以適當使用。 □ 為容許經網絡傳輸和傳遞的資料採取保安保護措施，例如加密。 □ 指定專人負責監察網絡性能和每日操作情況。 □ 妥善保管所有網絡用戶配置檔案，以防止未獲授權接達。 □ 以文件記載網絡配置，並將文件存放在安全的地方。 □ 將所有網絡構件存放在安全的地方。 □ 已制訂並推行適當保安措施確保由另一決策局／部門或外聘機構控制的資訊系統與本部門資訊系統連接時，被連接的資訊系統的保安級別不會降級。 □ 決策局／部門與外聘機構已就各方之間安全傳遞保密資料達成協議，該協議亦已被記錄。 □ 定期覆檢 Wi-Fi 基礎設施，以評估在 Wi-Fi 通訊標準和規約所發現之保安漏洞的影響。 □ 政府互聯網網域的資源記錄須受現行的保安控制措施（即域名系統安全擴展）所保護。 □ 所有互聯網服務（包括資訊網站）推行加密傳遞，例如超文本傳輸安全規約。
系統購置、發展及維護

審計事項
□ 具有為變更控制程序而編撰完善的文件。 □ 對更改要求的影響作評估或估計。 □ 在更改前妥善核准、記錄及測試所有更改。 □ 在更改前後進行充分備份。 □ 在每次更改前訂明復原程序。 □ 採取控制措施，確保測試資料／程式不會殘留在生產環境內。 □ 在變更應用在生產環境後進行檢驗（例如人手覆檢），以確保所有變更均按要求和計劃推行。 □ 只向專責人員或管理員授予適當的接達權，以修正系統／網絡的配置。 □ 如有需要，修訂備份和復原程序以反映更改。 □ 為涵蓋整個系統發展周期的系統發展及整合工作，建立安全的發展環境。 □ 應建立版本控制機制，記錄程式源碼在應用系統發展過程中的變更。
外判資訊系統的保安
□ 已識別及評估使用外聘服務或設備的風險。 □ 妥善管理已簽署的機密及不可向外披露資料協議文件。 □ 在服務到期或終止時，或應政府要求，所有在外聘服務或設施的政府數據都會按政府保安要求被清除或銷毀。
保安事故管理
□ 已根據各系統的特定操作需要而建立事故監察及應變機制。 □ 已預先設定記錄的保留期限，以便在需要時追蹤保安事故。 □ 定期覆檢保安事故應變／處理程序並進行演習（至少每兩年一次，最好每年一次）。 □ 發生保安事故時，有關人員根據既定的通報渠道妥善處理及提請管理層跟進。 □ 向終端用戶提供最新版本的事故監察／應變程序。
資訊科技保安方面的業務連續性管理
□ 根據所定次數，覆檢和更新運作復原和緊急應變計劃並進行演習。 □ 詳細編寫及定期測試關鍵業務資訊系統的運作復原和緊急應變計劃，並將計劃與業務連續性計劃緊扣一起。 □ 有適當復原能力以符合資訊科技服務及設施的可用性要求。

審計事項
遵行要求
□ 保安政策應要求定期進行保安風險評估及審計。 □ 已跟進上一次保安風險評估及審計所作的建議。 □ 已就系統的操作，定出及記錄所有適用的相關法定、規管及合約要求。 □ 保存保安要求的遵行證明記錄及支持相關保安措施獲有效推行的審計記錄。 □ 揀選審計師和進行審計的工作客觀持平。 □ 限制及控制使用軟件和程式來進行保安風險評估或審計。 □ 對於涉及個人資料的資訊系統，在整個資料生命周期內推行適當的保安措施。

附件 E：作為遵行證據的已記錄資料樣本清單

編號	已記錄資料
1	資訊科技組織圖表（連人員姓名及照片）
2	資訊保安組織架構
3	資訊保安組織會議的會議記錄
4	對部門資訊科技保安政策、標準、指引及程序的近期覆檢或審批記錄
5	近期派發部門資訊科技保安政策連接收人士記錄
6	資訊科技服務及設備的許可使用政策
7	近期派發資訊科技服務及設備的許可使用政策記錄及接收人士記錄
8	保安意識培訓的出席名單
9	保安意識培訓教材
10	外聘服務供應商所簽署的不披露協議書
11	已通知外聘服務供應商其保安責任的證明
12	數據中心或伺服器室設備及通訊設施的檢查記錄
13	用作進入數據中心或伺服器室的接達鑰匙、咭、密碼的申請及分發程序
14	用作進入數據中心或伺服器室的接達鑰匙、咭、密碼的申請和分發審批記錄
15	獲授權接達數據中心或伺服器室人士的清單
16	獲授權接達數據中心或伺服器室人士清單的覆檢記錄
17	數據中心或伺服器室的訪客記錄
18	資訊系統（關鍵資訊系統須加上標記）、硬件資產（包括手提電腦、流動裝置和 USB 盤）、軟件資產（包括桌面應用程式、流動應用程式）、有效保用證、服務協議書和法律／合約文件的清單
19	清單檢查記錄
20	要求資訊科技設備的記錄
21	用戶帳戶維護程序
22	新增／修改用戶帳戶以接達內部網絡的審批記錄
23	部門資訊科技保安主任對新增共用用戶帳戶以接達內部網絡的審批記錄

編號	已記錄資料
24	由部門資訊科技保安主任批准的共用用戶帳戶清單
25	停用接達內部網絡的用戶帳戶的記錄
26	在員工辭職／終止僱用／調職時，電腦資源的移交及歸還記錄
27	接達內部網絡的非活躍用戶帳戶的覆檢記錄
28	用戶帳戶的數據接達權限覆檢記錄
29	密碼政策或標準
30	關於使用流動運算及遠程接達時保安要求的使用政策及程序
31	用戶對使用流動裝置及遠程接達時的自身保安責任的接受聲明
32	可作遠程接達的用戶帳戶清單
33	顯示遠端接達點的網絡圖
34	決策局／部門主管對經私人擁有電腦資源或物聯網裝置連接內部網絡的審批記錄（如有）
35	決策局／部門主管對使用私人擁有電腦或流動裝置處理機密／限閱資料的審批記錄（如有）
36	外聘服務供應商就棄置硬磁碟前消磁的證書
37	備份及復原政策或程序
38	備份活動的覆檢記錄
39	儲存媒體的復原測試記錄
40	備份媒體的運送記錄
41	關鍵操作記錄的覆檢記錄
42	資訊系統的強化指引和推行記錄
43	系統文件的覆檢記錄
44	部門資訊科技保安主任對外部連接 ／或系統界面的審批記錄（如有）
45	對使用獨立電腦作寬頻連接的審批記錄（如有）
46	保安修補程式的評核及測試記錄
47	不採用保安修補程式的諮詢記錄
48	安裝保安修補程式的要求及審批記錄

編號	已記錄資料
49	電腦設備及軟件安裝記錄
50	獲批准用戶安裝的軟件清單和其覆檢記錄
51	對端點用戶工作站或流動裝置內已安裝軟件的監察記錄
52	安裝不在獲批軟件清單上的軟件的要求及審批記錄
53	無線保安政策
54	無線網絡的網絡圖
55	資訊系統活動記錄政策
56	伺服器、網絡設備、打印機和抽取式媒體審計記錄的覆檢記錄
57	最新的保安風險評估報告及跟進行動計劃
58	記錄適用於資訊系統運作的有關法列、監管及合約規定的文件，例如合約、服務水平協議、運作水平協議等
59	保安審計報告及跟進行動計劃
60	於保安風險評估及／或保安審計中執行軟件及程式（例如掃描工具）的審批記錄
61	保安事故應變／處理程序
62	保安事故應變／處理演習報告
63	近期派發保安事處理／報告程序連接收人士記錄
64	最新的保安事故報告
65	雙重認證標準或政策