數字政策辦公室

資訊保安

資訊科技保安風險管理
實務指引

第 1.1 版

2024 年 7 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	將「政府資訊科技總監辦公室」修改為「數字政策辦公室」		1.1	2024 年 7 月

目錄

1. 簡介

資訊科技保安風險管理是幫助組織主動識別和評估可能影響其目標的潛在資訊科技保安風險並確定風險優先權的重要流程。本文件提供參考模型，以使資訊科技保安風險管理實務和方法保持一致。通過參考該模型，管理使用者、資訊科技經理、系統管理員以及其他技術和操作人員能更好地了解資訊科技保安風險管理流程，亦能了解必要的準備事項、關鍵考慮因素和可實現結果。本文件旨在為決策局／部門提供全面框架，以開展符合其特定需求和背景的有效定制資訊科技保安風險管理實務。

1.1 目的

本文件描述了資訊科技保安風險管理的總體框架，且應與其他保安文件結合使用，如《基準資訊科技保安政策》[S17]、《資訊科技保安指引》[G3]以及相關程序（如適用）。

本實務指引適用於所有參與資訊科技保安風險管理的員工，以及為政府資訊科技保安風險管理流程提供支援的資訊科技保安顧問或審計師。

1.2 參考標準

以下的參考文件為應用本文件時必不可少的參考。

- 《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]，香港特別行政區政府
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO 31000:2018 Risk management — Guidelines
- NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM)
- NISTIR 8286A Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management
- NISTIR 8286B Prioritizing Cybersecurity Risk for Enterprise Risk Management
- NISTIR 8286C Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight
- GB/T 31722-2015 資訊科技-保安技術-資訊保安風險管理

- GB/T 20984-2022 資訊保安技術-資訊保安風險評估方法
- GB/T 24353-2022 風險管理-指引
- GB/T 22080-2016 資訊科技-保安技術-資訊保安管理體系-要求
- 資訊科技保安威脅管理實務指引
- 保安風險評估及審計實務指引

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	
資訊科技保安	資訊科技保安是保護網絡、裝置和資料免遭未獲授權接達或非法使用的技術，是確保資訊機密性、完整性和可用性的實踐。
風險管理	指導和控制組織風險的協調活動。
資訊科技保安風險管理	持續對與人為和/或操作問題相關的潛在資訊科技保安風險進行識別、確定其優先權並採取風險緩解和控制措施以使其達到可接受且可管理水平的過程。
利益相關者	可能受決策或活動影響或認為自己會受決策或活動影響的個人或組織。

1.4 聯絡方法

本文件由數字政策辦公室編制及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

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

CMMP 電郵： IT Security Team/DPO

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
- 態勢認知和資訊共用。

<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／部門亦須制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，以識別與安全性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安全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、應急和復原」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；
- 應急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資料保安風險，決策局／部門須啟動其常規保安事故管理計劃，以即時識別、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急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，並制定相關程序，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，並採取資訊保安的行業最佳實踐。

態勢認知和資訊共用

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佈的現時安全性漏洞訊息、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／部門可以利用威脅情報網絡平台接收和分享保安事務、安全性漏洞和網絡威脅情報的訊息。

人員亦可通過參加保安演習和參加研討會、展示會或瀏覽載有保安情報資訊和一般保安資訊（例如網絡保安資訊站、資訊保安網）的專題網頁來提高保安意識。

3. 資訊科技保安風險管理

3.1 資訊科技保安風險管理簡介及其重要性

資訊科技保安風險與資訊、資料或資訊（或控制）系統的機密性、完整性或可用性的喪失有關。該風險反映了對組織營運（即使命、職能、形象或聲譽）、資產、個人、其他組織和社會的潛在不利影響。

有效的資訊科技保安風險管理是一個重要的過程，涉及識別、評估和緩解組織的資訊系統、資料和技術基礎設施的風險，以及識別可能危及數位資產機密性、完整性和可用性的漏洞和威脅。組織有必要通過實施穩健的策略將資訊科技保安風險緩解到其制定的可接受水平。

在數位化時代，資訊科技保安風險管理對於保護敏感資料、關鍵基礎設施和業務連續性至關重要。由於對技術的依賴日益增加，與資訊科技威脅相關的潛在風險和漏洞越發普遍。通過實施穩健的風險管理實務，決策局／部門可主動識別和解決潛在安全性漏洞，並實現以下目標：

- 保護敏感資料、知識產權、客戶資訊和關鍵系統等重要資產。
- 提高潛在資訊科技保安風險的可見性，從而更好地分配資源和作出決策。
- 向管理層提供對現有資訊科技保安風險狀況和相應保安保障措施全面且系統的意見。
- 降低資訊科技保安事故發生的可能性和影響，保持業務連續性。
- 確保組織遵行相關的資訊科技保安法例和監管要求，避免潛在法律處罰和聲譽受損。

風險管理不達標可能會給各決策局／部門帶來嚴重後果。例如，資料泄露可能導致未獲授權披露敏感資料，從而造成法律和監管影響。此外，關鍵資料的丟失或損害可能會擾亂政府的必要服務、破壞公眾的信任和信心。

3.2 資訊科技保安風險管理框架

為確保資訊科技保安風險管理的一致性與有效性，決策局／部門須制定全面的資訊科技保安風險管理框架，概述如何識別、評估、緩解和監控決策局／部門及其系統相關風險。穩健的框架能夠提供管理資訊科技保安風險的結構化方法，有助於組織全面了解潛在威脅和漏洞。按框架行事，決策局／部門可加強其資訊科技保安態勢並有效管理資訊科技保安風險。

資訊科技風險管理框架通過一系列的風險管理活動和職能來提供結構化的風險管理方法。資訊科技保安風險管理的有效性取決於其在決策局／部門治理（包括決策）方面的融合程度，需要利益相關者，尤其是高層管理人員的支持。資訊科技保安風險管理框架的關鍵組成部分如下圖。

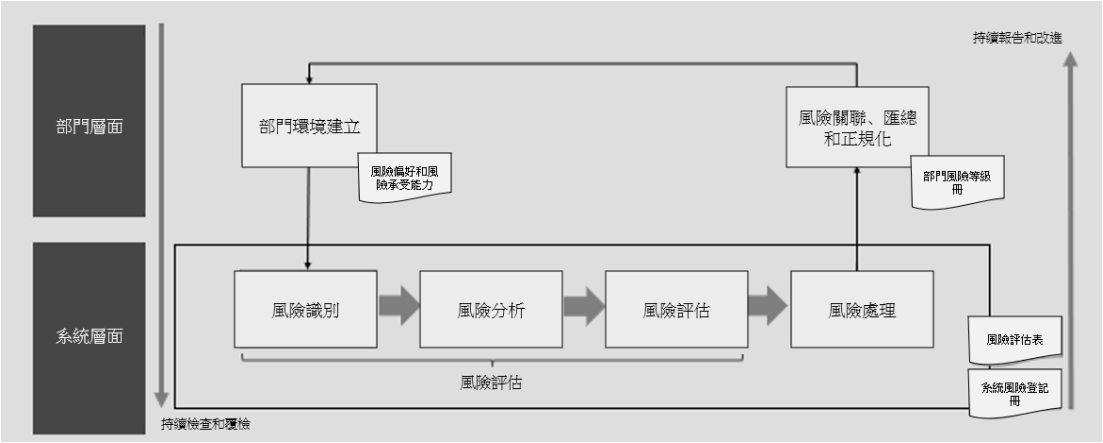

圖 3.1：資訊科技保安風險管理框架

i) 部門背景建立（第 3 節）
了解和制定可能影響決策局／部門資訊科技保安風險整體管理的內部和外部背景。

ii) 風險識別（第 4 節）
識別和記錄可能影響決策局／部門資訊系統和資料的潛在資訊科技保安威脅和漏洞。

iii) 風險分析（第 4 節）
進一步分析識別到的風險，了解其潛在影響和可能性。這有助於全面了解各項風險對決策局／部門營運和目標的潛在影響。

iv) 風險評估（第 4 節）
將經過分析的風險與決策局／部門風險標準進行比較，確定風險優先權。這有助於確定各項風險的重要性以及需要處理的風險。

v) 風險處理（第 4 節）
在風險評估後，建立適當的處理方案來管理風險。決策局／部門可通過採取控制措施來避免、轉移、緩解或接受風險，具體取決於決策局／部門風險偏好。

vi) 風險關聯、匯總和正規化（第 5 節）
審查風險之間的相互關係，總結和評估風險的總體影響，將風險計量正規化。這有助於全面了解決策局／部門風險環境並幫助其制定戰略決策。

迭代法可在每次迭代時增加評估深度和細節，平衡識別控制所花費時間和精力，並確保風險得到適當評估。

3.3 資訊科技保安風險管理政策

資訊科技保安風險管理政策為正式的資訊科技保安管理框架文件，應概述決策局／部門業務目標、需防範的威脅以及任何適用的法律和監管要求。資訊科技保安風險管理政策還應自上而下說明需保護的資產，並且決策局／部門將不會容忍任何違規行為。在建立資訊科技保安風險管理政策時，決策局／部門應參考本實務指引並根據其戰略和目標確定風險管理方法，如風險評估方法、風險評級機制及關鍵績效指標。資訊科技保安風險管理政策就決策局／部門應如何保護其資訊資產、系統和網絡免受潛在威脅和漏洞提出要求並提供指引。政策的具體內容可能因決策局／部門規模、複雜程度、行業和監管要求而異，但通常包含以下要素：

- 目的和範圍
- 職務和職責
- 在決策局／部門內部制定和執行保安風險管理框架
- 遵行和執行
- 培訓和意識
- 政策的覆檢和批准

決策局／部門應根據需要建基於此補充相應的標準和指引。

4. 部門背景建立

部門背景建立可制定風險管理流程，使決策局／部門能夠有效評估並適當處理風險。

4.1 風險管理範圍制定

制定各決策局／部門資訊科技保安風險管理活動範圍至關重要。

明確的範圍可幫助決策局／部門針對性地開展有效的風險管理工作。風險管理範圍制定包括建立全面的風險評估所涉資訊系統及其組成部分清單。相關資訊應記錄在資訊系統清單中。風險管理範圍應包括網絡圖或系統架構圖，直觀呈現系統 的連接、決策局／部門對系統的控制範圍及各系統所依賴的外部系統或服務。

制定風險管理範圍至關重要，關係到決策局／部門了解自身對其他政府實體或外部利益相關者的依賴關係，有助於促成合作和協調，以應對不同領域的資訊科技保安風險。

明確制定範圍至關重要，同時需要考慮以下各方面要素：

- 待制定的目標和決策。
- 流程步驟的預期結果。
- 時間、地點、包含及不包含的具體內容。
- 合適的風險評估工具和技術。
- 所需資源、職責和記錄方式。
- 與其他項目、流程和活動的關係。

通過建立明確制定的範圍， 決策局／部門可以根據行業最佳實踐加強其資訊科技保安風險管理實務， 有效應對潛在風險。

4.2 了解風險背景

決策局／部門在其目標、資產、威脅、漏洞和法律/監管要求形成的獨特風險背景下運作。全面評估和了解這一特定風險背景對決策局／部門至關重要。考慮這些因素能夠深入了解潛在風險，從而制定合適的風險管理策略。決策局／部門應收集、考慮並了解內部和外部背景因素。

外部背景因素包括但不限於以下例子：

- 國際、國內、區域或本地的社會、文化、政治、法律、監管、金融、技術、經濟和環境因素。
- 影響決策局／部門目標的關鍵驅動因素和趨勢。

- 外部利益相關者的關係、看法、價值觀、需求和期望。
- 合同關係和承諾。
- 網絡複雜性和依賴關係。

內部背景因素包括但不限於以下例子：

- 願景、使命和價值觀。
- 治理、結構、職務和問責。
- 戰略、目標和政策。
- 文化。
- 決策局／部門採用的標準、指引和模型。
- 根據資源和知識（如資本、時間、人員、智慧財產權、流程、系統和技術）理解的能力。
- 資料、資訊系統和資訊流。
- 與內部利益相關者的關係，對其看法和價值觀的考慮程度。
- 合同關係和承諾。
- 相互依存和相互聯繫。

4.3 風險偏好聲明及風險承受能力標準制定

風險偏好聲明和風險承受能力標準對決策局／部門資訊科技保安風險管理框架內的決策至關重要。其有助於建立可接受的風險水平並指導確定風險緩解工作的優先權。確保風險偏好和風險承受能力與風險管理框架相符，並根據活動的具體目的和範圍進行調整。其還應反映決策局／部門的價值觀、目標和資源，並與資訊科技保安風險管理政策和指引相符。

風險偏好代表決策局／部門在實現目標時願意接受的風險水平。而風險承受能力為一個閾值，超過該閾值的風險屬於不可接受的風險。決策局／部門應在資訊科技保安風險管理政策中注明其風險偏好及風險承受能力，據此建立風險管理戰略方法。儘早建立風險偏好及風險承受能力並定期覆檢，以確保其符合決策局／部門不斷變化的目標和風險環境。

制定風險偏好聲明及風險承受能力標準時應考慮決策局／部門的責任和利益相關者的意見。風險偏好聲明及風險承受能力標準應在風險評估流程開始時建立，必要時應定期覆檢和修訂。

制定風險偏好聲明及風險承受能力標準時應考慮以下因素：

- 可能影響結果和（有形和無形）目標的不確定因素的性質和類型。
- （正面和負面）影響和及其可能性的定義和衡量方法。
- 時間相關因素。
- 計量方法的一致性。
- 風險水平的確認方法。
- 對多種風險組合和順序的考量。

- 決策局／部門的能力。

4.3.1 風險偏好

風險偏好反映決策局／部門根據其目標、戰略目標、優先權和風險文化承擔風險的意願。高風險偏好意味著決策局／部門願意承擔較多風險以實現目標，低風險偏好意味著決策局／部門願意承擔的風險較少。風險偏好可以是定性的，也可以是量化的。決策局／部門應根據既定風險偏好調整其資訊科技保安性原則，為各部門保安意識和風險意識樹立基調，從而使決策局／部門平衡創新與風險緩解措施，確保將風險控制在可接受範圍。通過明確風險偏好，決策局／部門能夠建立風險評估及應對框架，指導決策過程並與總體目標保持一致。定性或定量風險偏好在制定風險承擔範圍方面均會考慮潛在利益和負面影響。確定風險偏好有助於在部門層面採取一致且明確的風險管理方法。

風險偏好示例：

- 對重要系統的停機時間，組織的風險偏好為 0.2%的黃色閾值。
- 對特定國家辦事處負面媒體報導，組織的風險偏好為 2 個及以上的紅色閾值。
- 對國內供應鏈風險，組織的風險偏好較高。
- 對投資於可能實現顯著營運改進和創新的領域，組織風險偏好較高。
- 對聲譽風險或潛在利益衝突，組織風險偏好較低。

在確定風險偏好時，決策局／部門應考慮多種因素以確保採取全面和明確的方法。這些因素在確定風險偏好和指導決策過程中發揮著關鍵作用：

- 戰略目標：風險偏好應與決策局／部門戰略目標和使命／願景相一致。決策局／部門應評估為實現這些目標願意承擔的風險，並認真評估其對組織長期目標的潛在影響。
- 風險文化：組織風險文化應考慮在內，包括對風險承擔的態度以及接受創新舉措或採取較保守方法的意願。
- 利益相關者期望：應考慮政府、監管機構、客戶和公眾等利益相關者的期望和偏好。了解利益相關者對風險的看法對於形成風險偏好至關重要，有助於保持組織的信任度和滿足社會期望。
- 法律和監管要求：遵守適用的法律法規和行業標準至關重要。決策局／部門應考慮與風險管理相關的法律和監管義務，並確保風險偏好設定符合相關要求。
- 行業和市場條件：決策局／部門的風險偏好受行業和市場條件影響。決策局／部門應評估競爭格局、市場波動、新興風險和行業良好實踐模式，以確定適當的風險偏好。
- 財務能力：應仔細評估決策局／部門承擔和管理風險的財務能力。決策局／部門應考慮組織的財務資源、對財務影響的風險承受能力以及對股東和投資者等利益相關者的潛在影響。

- 組織復原能力：應考慮決策局／部門承受不利事故並從中恢復的能力。決策局／部門應評估組織復原能力，並確定在不影響有效應對和恢復能力的情況下合理承擔的風險。

4.3.2 風險承受能力

風險承受能力指實現目標時可接受的績效變動水平，通常在計劃、目標或組成部分層面建立。決策局／部門應解釋其風險偏好，建立具體的資訊科技保安風險承受水平，同時確保這些水平符合總體目標和法律法規要求。

制定風險承受能力至關重要，因為其劃定風險承擔範圍，並指導控制和緩解措施的實施。決策局／部門可通過建立明確的風險承受閾值，在預設限值範圍內有效地管理資訊科技保安風險。如此可確保資源優先用於重要領域，並使決策局／部門恰當分配風險處理工作。明確風險承受能力、強化決策，提升資訊科技保安風險管理的資源配置效率。

風險承受能力示例：
在任何情況下，決策局／部門不接受任何在緩解措施實施後「高風險」事故引起的風險。同時，決策局／部門不接受任何在緩解措施實施後「中等風險」事故引起的風險（經部門資訊科技保安主任批准的除外）。

為管理資訊科技保安風險而建立明確的風險承受能力閾值時，決策局／部門應考慮以下因素：

- 主要目標：決策局／部門應確定主要目標。這通常涉及需防範資訊科技保安風險的資訊系統。
- 利益相關者諮詢：利益相關者包括高層管理人員、法務合規團隊、資訊科技部門和外部專家，須向其諮詢以收集意見並確保風險承受能力閾值的全面性和實用性。
- 監管要求和行業最佳實踐：決策局／部門應隨時了解與資訊科技保安風險管理相關的監管要求和行業最佳實踐，為設置風險承受能力閾值獲取指引。
- 定期監察和覆檢：應定期監察和覆檢風險承受能力閾值，確保其持續的相關性和有效性。隨著資訊科技威脅形勢的變化，決策局／部門應相應調整其風險承受能力閾值，並對其風險管理策略實施必要的調整。

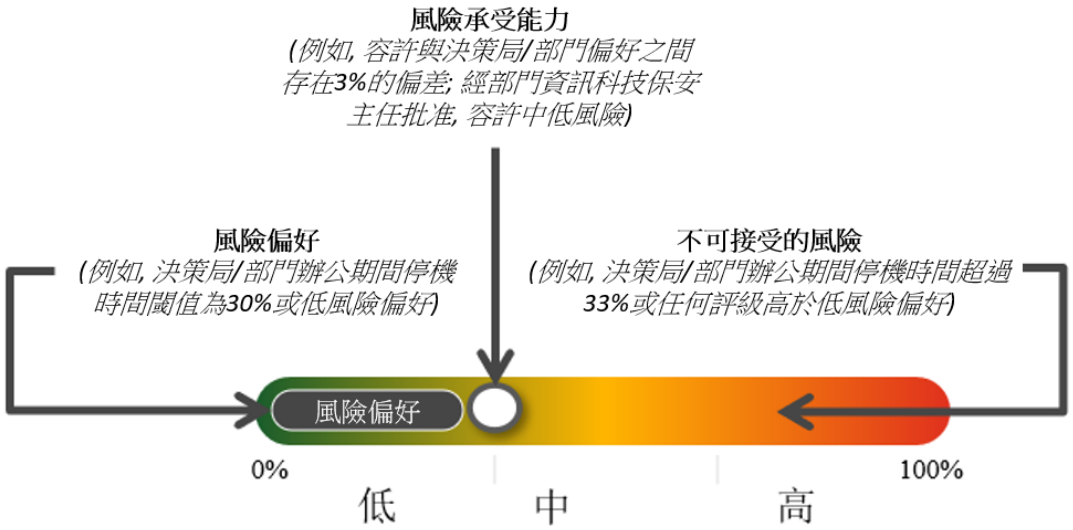

圖 4.1：風險偏好、風險承受能力和不可接受風險說明

4.4 資訊科技保安風險協調、整合及上報

協調並整合決策局／部門資訊科技保安風險管理工作對於採取全面的風險緩解方法至關重要。決策局／部門應建立協調和整合流程，確保風險管理活動與總體目標一致，如促進相關團隊、單位和利益相關者之間的合作，以分享資訊、行業最佳實踐和經驗教訓。此外，還應建立健全上報機制，保證資訊科技保安風險透明、可問責，確保相關資訊溝通及時。定期上報風險狀況和風險緩解進展有助於決策局／部門各級作出明確決策。

資訊科技保安風險協調、整合及上報是決策局／部門整體風險管理框架和流程的一部分。應在風險管理規劃早期建立該流程，並隨目標、風險和決策局／部門要求的變化而持續覆檢及更新。

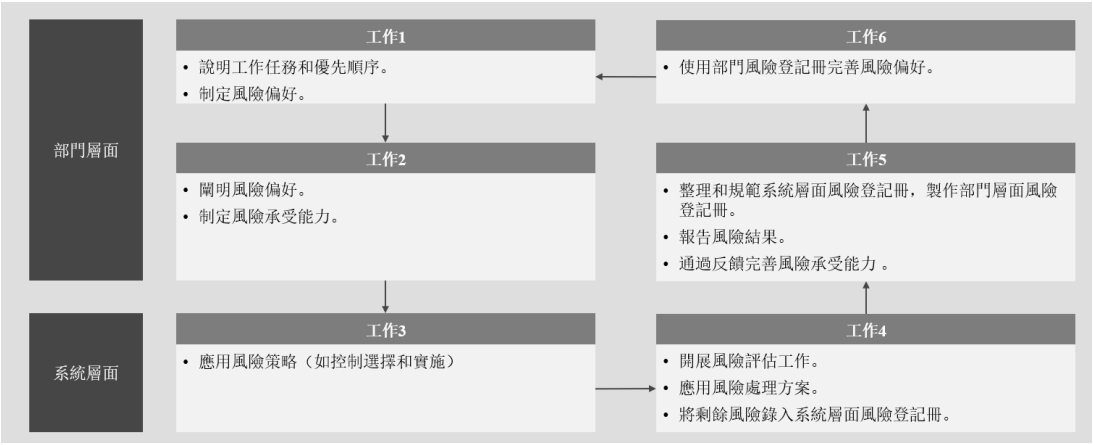

圖 4.2：風險協調、整合及上報說明

4.5 職務和職責

決策局／部門應識別資訊科技保安風險管理所涉及的主要職務，並制定其職責、上報關係及問責。決策局／部門應根據人員對所涉系統和流程的了解、經驗和理解分配職務。資訊科技保安職務和職責應在風險管理框架的計劃或實施階段制定。儘早確立職務和職責並定期覆檢和更新至關重要，確保其符合不斷變化的業務目標和風險環境。

職務和職責應涵蓋各級員工，從制定風險偏好和風險承受能力的高層管理人員到執行風險處理措施的操作人員。

決策局／部門層面職務包括戰略決策者和監督整體風險管理框架的人員。擔任該層面職務的人員應全面了解和掌握決策局／部門的業務目標、風險偏好和風險承受能力，應負責制定決策局／部門資訊科技保安風險框架，並確保其與決策局／部門使命和願景保持一致。

系統層面職務可能包括管理具體資訊系統並執行風險緩解措施的風險擁有者。擔任該層面職務的人員應詳細了解特定系統和已識別的風險。

4.5.1 風險擁有者

風險擁有者是獲授權負責管理風險的個人或職能部門。風險擁有者可能擔任流程負責人、職能負責人、項目經理或資產所有者或為高層管理人員或保安委員會成員。決策局／部門在確定風險擁有者時，應使用風險評估流程或建立相應標準。詳情請參閱《保安風險評估及審計實務指引》。在確定風險擁有者時應考慮以下因素：

- 風險水平和存在風險的資產。
- 管理風險所需責任及授權。
- 了解問題和作出充分決策的能力（如確定如何緩解風險）。

風險擁有者職責參考示例如下。

- 識別和評估潛在資訊科技保安風險。
- 建立和實施適當的戰略和保障措施來緩解風險。
- 監控已識別的資訊科技保安風險狀態和風險緩解計劃的有效性。
- 向職責範圍內的利益相關者傳達與風險相關的資訊、政策和程序。
- 向高層管理人員和部門資訊科技保安主任上報資訊科技保安風險。

5. 資訊科技保安風險評估與處理

資訊科技保安風險評估過程應包括識別、分析和評估內部和外部風險。內部風險指決策局／部門的漏洞和威脅，如技術缺陷、操作漏洞和人為相關因素（包括人為錯誤或內部威脅）。另一方面，外部風險指來自決策局／部門外部的威脅，如資訊科技保安攻擊、黑客攻擊和新興威脅媒介。

識別和評估內部風險至關重要，因其有助於發現決策局／部門系統、流程和人員的潛在弱點和漏洞。具體內容包括評估現有保安措施的有效性、評估技術控制的穩健性以及識別惡意行為者可能利用的任何操作漏洞。此外，了解人為相關因素（如員工意識、培訓和保安規約的遵行）對於緩解決策局／部門風險至關重要。

識別和評估外部風險也同等重要。具體內容包括分析威脅形勢及隨時了解新資訊科技威脅和攻擊途徑。通過了解威脅者使用的戰術、技術和程序，決策局／部門可主動採取適當的應對措施和預防措施。定期監察外部威脅和漏洞有助於識別潛在弱點，並迅速採取應對措施。更多詳情請參閱《資訊科技保安威脅管理實務指引》。

在風險評估過程中考慮技術、操作和人為相關因素，決策局／部門可全面了解其面臨的資訊科技保安風險。這對於建立針對性風險緩解策略和分配資源以有效應對已識別漏洞非常重要，同時有助於根據已識別風險的嚴重性和潛在影響確定風險處理工作的優先權。

如識別到資訊科技保安風險，應進行分析並確定其優先權，決策局／部門應選擇適當的風險處理方案，包括**風險接受、降低、避免**和**轉移**。

為全面有效實施資訊科技保安風險評估和處理流程，決策局／部門應參考**《保安風險評估及審計實務指引》**。該指引為識別、分析和評估政府機構資訊系統中的資訊科技保安風險提供了寶貴的指導意見和最佳實踐。

在資訊科技保安風險評估與處理過程結束時，將對收集和分析的資訊進行編譯和記錄。該過程的結果是詳細的風險評估表和風險登記冊，風險登記冊是追蹤所有已識別風險的列表，提供存在什么風險以及如何解決這些風險的清晰記錄。

6. 風險關聯、匯總和正規化

6.1 建立風險登記冊

建立和維護風險登記冊對決策局／部門開展有效資訊科技保安風險管理至關重要。風險登記冊是記錄已識別風險、風險可能性、影響和相關處理方案的中央存儲庫。風險登記冊應於識別和記錄風險時開始建立，記錄的風險包括威脅決策局／部門資訊系統和營運的內部和外部因素。

一旦風險被識別和評估，則應記錄於風險登記冊，並提供相關詳情，如風險描述、指定的風險擁有者、當前風險水平和風險處理計劃。定期更新風險登記冊以反映風險環境的變化和風險處理活動的進展至關重要。通過全面維護風險登記冊，決策局／部門可全面了解風險狀況，有助於其作出明確的決策和資源配置。

決策局／部門應先建立單個的系統風險登記冊，將其匯總為統一且全面的部門風險登記冊。整合涉及風險關聯、匯總和正規化流程。匯總風險登記冊全面概述決策局／部門的所有資訊科技保安風險，提供決策局／部門資訊科技保安風險環境的全面觀點。維護部門風險登記冊的目的是為決策局／部門高層管理人員提供清晰、有序、全面的資訊，使其了解決策局／部門需管理和定期覆檢的已識別資訊科技保安風險，有助於規劃、資源配置和風險處理。關於將多個系統級風險登記冊匯總為部門風險登記冊。更多說明和示例，參見第 6.2 節。

應持續更新部門風險登記冊，以反映風險環境的變化、控制措施的有效性或決策局／部門風險戰略的變化。同時確保部門風險登記冊對資訊科技保安風險和主動風險管理的知情決策保持關聯和實用性。

有關資訊科技保安風險登記冊範本的資訊，請參閱**附件 A**。

6.2 執行風險關聯、匯總和正規化

6.2.1 風險關聯

風險關聯指兩種或以上風險值波動或變化的關聯程度，用於衡量不同風險之間的統計資料關係或依賴關係，並揭示在風險環境中，這些不同風險因素如何相互作用或表現。決策局／部門應考慮並了解各系統風險之間的潛在聯繫和依賴關係。通過識別關聯風險，決策局／部門可評估關聯風險的整體影響，有效分配資源，並實施具有針對性的風險緩解措施。

值得注意的是，風險關聯可以通過關聯係數等統計指標進行定量評估，也可以根據專家判斷和歷史觀察進行定性評估。風險建模和模擬技術可以分析風險之間的關聯，並模擬它們對整體風險狀況的潛在影響。例如，一個系統中的風險

可能會對其他領域的風險產生依賴或影響。了解這些關聯有助於風險擁有者建立更加完善的風險管理方法。

風險關聯示例：

假設某決策局／部門有兩個獨立的系統：一個用於客戶資料管理，另一個用於交易處理。如果兩個系統中都存在未獲授權接達的漏洞，並且這兩個系統都可以從同一網絡接達，則這些風險具有關聯。攻擊者如果利用一個系統的漏洞獲得接達權限，就有可能利用另一個系統的相同漏洞，從而導致更大規模的資料泄露。在這種情況下，風險擁有者應進行充分溝通與合作，以建立一個全面的方法來管理相關風險。

6.2.2 風險匯總

各決策局／部門應對各系統中相似類別的風險進行分組，以簡化風險環境，使其更易於理解和管理。進行風險匯總的目的可包括但不限於以下方面：

- 匯總風險資訊，以全面了解資訊科技保安風險。
- 調整風險方向（如風險處理方案），優化決策局／部門的資源配置。
- 確保在各個層級進行監察和報告，以保持對風險環境變化的態勢感知。

風險匯總是指將類似或相關的風險整合為一個匯總風險。通過這種方式，決策局／部門能夠從一個更宏觀的視角看待風險，並評估其累積影響。匯總風險可使決策局／部門更清楚地了解所面臨的總體風險，並能更有效地確定緩解工作的緩急次序。風險匯總將系統資訊科技保安風險登記冊與其他登記冊結合進行風險匯總。每個登記冊中的資訊科技保安風險的類別（如接達控制、資料保安）都可能是有限且一致的，因此登記表中的該列對初步分類工作極其關鍵。整合系統層面的所有類似類別的風險後，匯總便是直接的活動，但也可能需要做一些手動調整。不同的風險擁有者可能會對同一情景的風險描述不同。因此，應記錄風險項的來源，以便於在原始登記冊中追溯該風險。

有關風險匯總類別示例，請參閱**附件 B**。

風險匯總示例：

假設系統 A 和系統 B 是決策局／部門的兩個系統；兩個系統風險登記冊將匯總為一個部門風險登記冊。

系統 A 風險登記冊												
編號	優先權	風險描述	風險類別	可能性	影響	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
1	高	外部攻擊者部署遠程接達工具外泄決策局／部門的預算計劃，導致敏感性資料泄露。	接達控制	2	3	3	高	降低風險	對所有敏感系統的遠端接達實施增強式驗證機制，例如多	員工 A	2024 年 12 月 31 日	進行中

									重身份驗證。			
2	高	識別系統中存在的未獲授權接達的漏洞。	威脅管理	2	3	3	高	降低風險	應用系統供應商或開發人員提供的安全修補程式和更新，解決發現的安全性漏洞。	員工 A	2024 年 12 月 31 日	進行中
3	中	系統使用不當，導致系統故障	人員保安	1	3	3	中	降低風險	為員工提供正確使用系統的保安意識培訓。	員工 A	2024 年 12 月 31 日	進行中

系統 B 風險登記冊												
編號	優先權	風險描述	風險類別	可能性	影響	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
1	低	洪水湧入一樓數據中心，導致多台資料庫伺服器進水受損，相關業務服務中斷。	物理保安	1	2	2	低	接受風險	不適用。	員工 B	不適用	已完成
2	中	識別系統中存在的未獲授權接達的漏洞。	威脅管理	2	3	2	中	降低風險	應用系統供應商或開發人員提供的保安修補程式和更新，解決發現的漏洞。	員工 B	2024 年 12 月 31 日	進行中
3	低	沒有為系統制訂事故應變和復原計劃，導致在發生事故時服務中斷。	事故應變計劃和復原計劃	2	3	2	中	降低風險	建立事故應變計劃和復原計劃	員工 B	2024 年 12 月 31 日	進行中

部門風險登記冊												
編號	優先權	風險描述	風險類別	可能性	影響	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
系統 A 編號#1	高	外部攻擊者部署遠程接達工具外泄決策局／部門的預算計劃，導致敏感資料泄露。	接達控制	2	3	3	高	降低風險	對所有敏感系統的遠端接達實施增強式驗證機制，例如多重身份驗證。	員工 A	2024 年 12 月 31 日	進行中
系統 A 編號#2， 系統 B 編號#2 （注 1）	中（注 2）	識別系統中存在的未獲授權接達的漏洞。	威脅管理	2	3	3，2	中（注 2）	降低風險	應用系統供應商或開發人員提供的保安修補程式和更新，解決發現的漏洞。	員工 A，員工 B	2024 年 12 月 31 日	進行中
系統 A 編號#3	中	系統使用不當，導致系統故障	人員保安	1	3	3	中	降低風險	為員工提供正確使用系統的保安意識培訓。	員工 A	2024 年 12 月 31 日	進行中

系統 B 編號#1	低	洪水湧入一樓數據中心，導致多台資料庫伺服器進水受損，相關業務服務中斷。	物理保安	1	2	2	低	接受風險	不適用。	員工 B	不適用	已完成
系統 B 編號#3	低	沒有為系統制訂事故應變計劃和復原計劃致在發生事故時服務中斷。	事故應變計劃和復原計劃	2	3	2	中	降低風險	建立事故應變計劃和復原計劃。	員工 B	2024 年 12 月 31 日	進行中

注 1：將不同系統風險登記冊中的類似風險項整合為一個匯總風險項。
注 2：根據決策局／部門的風險偏好、風險承受能力和資源，調整風險優先權和風險等級的差異。

6.2.3 風險正規化

在匯總系統風險登記冊時，決策局／部門應確保風險資訊的正規化。為方便進行有意義的比較和決策，決策局／部門內部風險資訊的正規化亦至關重要。正規化涉及建立一個共同的方法或標準，用於評估和比較不同系統的風險。這可確保決策局／部門在評估和溝通風險時保持一致。至少，較高級別（如部門風險登記冊）的風險正規化流程應使用相同的等級標準，以便進行比較和追蹤。這通常包括衡量影響和可能性的定義，以便對評估結果進行比較。風險標準還可能描述在確定風險嚴重程度時應如何考慮時間因素，如風險速度。決策局／部門在正規化風險時應考慮以下活動：

- 去除重複並匯總相同或相似的風險：若識別出與內部威脅相關的類似風險，將它們匯總為單個風險項目。此步驟可以全面評估並實施適當的控制措施。例如，決策局／部門內發現兩個類似的風險，第一個風險是「員工未獲授權接達財務系統的資料」，而第二個風險是「員工對人力資源系統的惡意行為」。由於這兩種風險都涉及員工未獲授權接達不同的資訊系統，因此可以將它們匯總為一個「接達控制」風險項：員工未獲授權接達資訊系統（財務系統和人力資源系統）。
- 根據決策局／部門的風險偏好、風險承受能力和敏感度調整風險：由於已在系統和部門層面建立了風險等級，因此有必要審查其累積影響和可能性，並建議更高或更低的風險評級調整。例如，決策局／部門高度重視突破界限和樂意採納技術進步。然而，它對與第三方供應商管理相關的風險的風險承受能力較低。因此，與特定關鍵第三方供應商相關的多重風險進行了調整，以反映決策局／部門的更高關注。
- 處理資訊科技保安風險登記冊中的差異：例如，如果對相同或相似風險有不同的風險等級和風險處理方案，風險擁有者應相互溝通並決定：(1) 在匯總風險項中同時顯示風險等級和風險處理方案；或 (2) 如果可以一起處理和追蹤這些風險，則考慮調整具有相同風險等級和相同風險處理方案的風險。
- 裁定關鍵風險：例如，負責的管理層強調並覆檢與支援決策局／部門業務連續性的關鍵系統相關的高風險，而這些風險需要在部門資訊科技保安風險登記冊進行追蹤和進一步溝通。

通過正規化風險，從各種系統資訊科技保安風險登記冊得出的結果，可以保證風險處理和溝通的一致性。此外，決策局／部門應識別並處理各系統風險登記冊中風險處理的差異，特別是當風險擁有者對相似情景採取不同的描述導致的差異。雖然不同的背景和情況可能導致差異，但了解根本原因並承認差異很重要。決策局／部門通過開展合作討論，邀請相關風險擁有者參與，並力求在風險處理方案上保持一致，從而使其資訊科技保安風險管理實務保持一致性和合理性。

風險正規化示例：

系統 C 風險登記冊												
編號	優先權	風險描述	風險類別	可能性	影響	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
1	低	員工使用共用帳戶接達系統。	接達控制	2	2	2	低	接受風險	不適用。	員工 C	不適用	已完成

系統 D 風險登記冊												
編號	優先權	風險描述	風險類別	可能性	影響	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
1	中	員工使用共用帳戶接達系統。	接達控制	3	2	2	中	降低風險	為目標員工提供保安培訓。	員工 D	2024 年 12 月 31 日	進行中

正規化風險後：

部門風險登記冊												
編號	優先權	風險描述	風險類別	可能性	影響	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
系統 C 編號 #1， 系統 D 編號#1	中	員工使用共用帳戶接達系統。	接達控制	3	2	2	中	降低風險	為目標員工提供保安培訓。	員工 C，員工 D	2024 年 12 月 31 日	進行中

7. 風險監察與報告

7.1 監察已識別的風險和風險處理活動

風險監察的目的包括但不限於以下方面：

- 確保風險處理方案的有效性、效率和成本效益。
- 收集資訊以加強未來的風險評估。
- 分析事故、變化、趨勢、成功和失敗並從中汲取教訓。
- 發現內部和外部環境（如風險標準和新興風險）的變化，從而調整風險處理方案和優先權。

監察已識別的風險和風險處理活動，是進行有效資訊科技保安風險管理的關鍵。一旦識別風險並將其記錄在風險登記冊中，定期評估其狀態並監察風險處理活動的進展至關重要。通過這種方式，可確保已實施的措施能夠有效緩解已識別的風險並降低其潛在影響。

維護全面的風險登記冊允許對不同程度的風險活動進行持續監察。風險擁有者應定期評估每項已識別的風險以確定其狀態、可能性和潛在影響。評估可以通過專家判斷、資料分析和歷史資訊。同時，定期更新風險登記冊，有助於決策局／部門記錄並適應不斷變化的威脅和風險環境。

此外，決策局／部門應定期監察和評估計劃實施或已實施的風險緩解措施是否達到預期結果並保持關聯。這可能涉及收集利益相關者的反饋意見，利用績效指標，或重新評估風險的影響和可能性。應記錄任何與計劃有關的變化或偏差並進行適當地溝通。根據監察結果對風險處理方案進行必要的調整，有助於確保採用積極的和適當的方法來緩解風險。決策局／部門通過定期監察和評估，可以主動管理其資訊科技保安風險，並確保其風險處理工作的有效性。

7.2 監察風險環境

決策局／部門應積極監察其風險環境，以了解風險環境的變化。風險環境包括可能影響決策局／部門營運和目標的所有潛在威脅和安全性漏洞。威脅管理是更宏觀的風險管理所組成的部分，其重點在於發現、評估和應對決策局／部門所面臨的威脅。

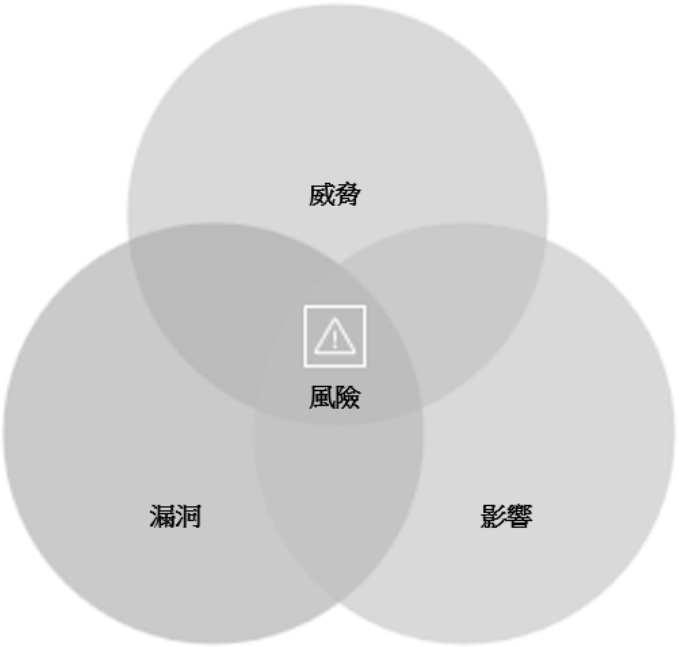

圖 7.1：風險與威脅之間的關係

通過監察風險環境，決策局／部門可以洞察新興威脅和趨勢，從而能夠積極主動地強化其資訊科技復原措施，以應對潛在風險。

為有效監察風險環境，決策局／部門可採用以下行動：

- 定期進行漏洞掃描和滲透測試，發現和確定保安漏洞數量。
- 利用威脅情報，隨時了解最新的網絡保安威脅和漏洞。
- 通過資產管理流程追蹤新的和現有的資產。
- 定期審查用戶接達權限，確保其符合當前的角色和職責。
- 定期審查和更新決策局／部門的風險偏好聲明。

持續監察至關重要，因為風險情景、資產價值、威脅、漏洞、可能性和影響可能在沒有任何跡象的情況下突然發生變化。通過持續監察這些因素，決策局／部門可檢測風險環境的變化，例如：

- 新的風險來源，包括新報告的安全性漏洞。
- 納入風險管理範圍的新資產。
- 資產價值的必要變動（例如，由於業務需求變化）。
- 確定已識別的漏洞，以便找出暴露於新威脅或重新出現的威脅之漏洞。
- 現有技術或新技術使用模式的變化，為攻擊提供可乘之機。
- 法律法規的變化。
- 風險偏好以及對可接受和不再可接受風險的認知發生變化。
- 決策局／部門內部和外部的資訊科技保安事故。

新的風險來源或可能性或影響的變化可能使之前評估的風險增加。因此，應定期重複風險監察活動，並定期檢視所選的風險處理方案。

為監察風險環境的趨勢，決策局／部門可以觀察關鍵風險指標，並設法確定各方面的情況，例如：

- 已識別風險的可能性是否在增加。
- 後果的嚴重程度是否在上升。
- 是否出現新的風險。
- 控制措施是否失效。

有關用於監察內部風險環境的風險指標示例，請參閱**附件 C**。

如果風險環境發生重大變化，決策局／部門可以採取以下行動：

調整風險處理方案：

- 如果這一變化屬於新型風險，如零日攻擊，應考慮任命一名風險擁有者，負責了解風險、建立風險緩解策略並持續監察風險。
- 根據環境變化，覆檢和更新風險處理方案。調整風險處理方案，通過對特定風險場景採取特定行動，以消除不一致性或實現不同結果。
- 這可能涉及加強風險處理措施，以減輕總體風險，或在接受一定程度的風險增加的情況下，放寬限制以獲得好處。可逐步實施這些變化，確保決策局／部門各個層級的全面風險管理。

利益相關者溝通與參與：

- 就風險環境的變化以及緩解潛在影響的步驟與利益相關者進行溝通。
- 如有必要，考慮尋求外部專家建議和／或協助，以了解這些變化帶來的影響，並幫助建立緩解潛在影響的策略。

改變策略方向：

- 根據共同商量的結果（提高或放寬風險限制），更新風險偏好聲明，調整策略方向。這可能涉及調整具體的量化目標，並修改對風險承受能力的理解，以利用機會或最小化不利風險的可能性和影響。

監察和指標：

- 當決策局／部門變更其風險方向或方法時，修改關鍵績效指標或關鍵風險指標以提高辨識度。風險擁有者可能會更改所監察的關鍵績效指標和關鍵風險指標。若當前的關鍵績效指標和關鍵風險指標無法充分體現影響和／或可能性的變化，則可合理引入不同的或額外的指標。若風險的影響和／或可能性的變化超過現有的監察頻率，則需要提高監察頻率。

風險相關方可能會發現，在監察過程中建立一份要採取的各項行動的清單很有幫助。例如，在確定某一風險領域發生重大變化時，可採取的行動包括：

- 成立工作組，討論並確定下一步行動。
- 將類似的風險項分配給專門的風險擁有者，以減少差異並確保問責。
- 確定其他保安控制措施，以提高對那些可能發生且具有影響力的風險的防禦、檢測和應對能力。這些過程可能包括添加額外的工具（如日誌記錄和事件編排）、進行應變培訓（如事故應變處理演習）或覆檢保險範圍。

7.3 定期風險報告

決策局／部門應建立系統化的風險報告流程，以便風險擁有者向高層管理人員、部門資訊科技保安主任和其他相關方溝通風險狀態和風險處理活動。應通過適當的機制記錄和報告風險管理過程及其成果，旨在：

- 在決策局／部門內傳達風險管理活動和成果。
- 為決策提供資訊。
- 改進風險管理活動。
- 促進與利益相關者的互動，包括負責風險管理活動的人員。

定期報告風險對決策局／部門內部進行有效溝通和決策至關重要。這是資訊科技保安風險管理管治架構的重要組成部分。通過報告風險提高與利益相關者的對話品質，並為高層管理人員和監督機構履行其職責提供支持。報告應考慮的因素可能包括但不限於以下內容：

- 不同的利益相關者及其特定的資訊需求和要求。
- 報告的成本、頻率和時間表。
- 報告的方法。
- 報告中的資訊與決策局／部門的目標和決策的相關性。

風險報告應包括已識別的風險、其當前狀態以及相關風險處理活動進展的全面資訊。應提供風險等級、可能性、潛在影響和關鍵風險指標等關鍵指標，以便利益相關者做出知情的決策。此外，報告還應強調需要立即關注或採取行動的任何新興風險或風險環境的變化。應定期和在發生重大變化時編制並分發這些報告。

為提高決策效率和及時應對新興風險，報告清晰簡明至關重要。風險報告中提供的資訊應通俗易懂，避免使用專業術語或不必要的複雜表達。通過這種方式，利益相關者能迅速掌握關鍵資訊，並就決策局／部門的資源配置、風險緩解策略和整體資訊科技保安狀況作出知情的決策。

8. 持續改進

8.1 反饋和經驗教訓

為培養持續改進的文化，決策局／部門應建立反饋機制，從以往事故、幾乎發生的事故或保安漏洞中汲取經驗教訓。這些機制可包括事故報告系統、事故後覆檢或與利益相關者開展定期回饋會議。決策局／部門通過積極尋求回饋，可以發現待改進領域，並鞏固其資訊科技保安實務。基於這些經驗，培養持續學習和改進的文化至關重要，可確保決策局／部門更加成熟且有效地應對新興資訊科技威脅。

為收集回饋意見，以及總結風險管理活動中的經驗教訓，決策局／部門可採取以下步驟：

(a) 收集：建立一種機制，從參與風險管理活動的利益相關者（如項目經理、風險擁有者和團隊成員）收集對風險管理框架的回饋意見。這可通過調查、訪談、工作坊或定期風險審查會議等方式進行。
(b) 文件記錄：記錄從風險管理活動中獲得的回饋和經驗教訓，包括具體實例、建議和改進措施。將這些資訊傳達給利益相關者，並將其納入未來的風險管理實務中。
(c) 知識分享：鼓勵決策局／部門的風險管理工作者分享知識。建立規約，在各項目和部門之間分享經驗、行業最佳實踐和汲取的教訓。這有助於營造持續學習和改進風險管理的文化。
(d) 覆檢和更新：根據回饋和經驗教訓，定期審查和更新風險管理流程、程序和準則。將改進措施納入資訊科技保安風險管理框架，以便在未來加強風險管理工作。

8.2 績效衡量

為評估決策局／部門內資訊科技保安風險管理的有效性，確定績效衡量指標尤為重要。決策局／部門應建立符合其目標的指標，為風險管理績效提供可量化的標準。定期進行績效衡量和報告，有助於追蹤進展、確定待改進領域和驗證控制措施的有效性。決策局／部門通過分析績效指標，可以了解趨勢，以行業標準為基準，並作出知情的決策，以強化其資訊科技保安體系。

風險管理中的績效衡量包括評估風險處理活動的有效性和效率，以及評估風險緩解成效。這有助於決策局／部門了解他們的風險管理成效，以及所實施的策略和控制措施是否達到預期效果。可根據與資訊科技保安風險管理目標的吻合度來制定關鍵績效指標，如已識別的風險、風險緩解效果、回應時間、緩解成本，以及事故或違規行為。

有關評估風險處理活動有效性的績效指標示例，請參閱**附件 C**。

決策局／部門應定期覆檢和分析績效資料，了解趨勢、差距和待改進領域。在完善策略，強化風險緩解工作並鞏固風險管理框架時應考慮這些資訊。

8.3 管理層覆檢及調整

有必要定期對資訊科技保安風險管理行為進行管理覆檢，以評估該行為的有效性並進行必要調整。高層管理人員應定期覆檢決策局／部門的風險管理流程，以確保其持續的適用性、充分性和有效性。這些覆檢應涉及高層管理人員和主要利益相關者，以確保與決策局／部門的目標和優先次序保持一致。在覆檢過程中，高層管理人員應評估現有的風險管理策略、政策和程序的執行情況。此外，高層管理人員還應處理識別出的差距或待改進的領域，並作出調整，以提高計畫的整體有效性。高層管理人員的參與和支持對推動必要變革以及將資訊科技保安風險管理活動納入治理框架至關重要。

管理層覆檢及調整旨在確保和提高資訊科技保安風險管理活動的品質和有效性，並應貫穿整個風險管理流程。

以下是在決策局／部門實施管理層覆檢及調整過程的示例：

工作	**資訊科技保安風險管理層覆檢及調整示例（由決策局／部門填寫）**	**狀態（若已完成，請勾選）**
定期管理層覆檢	對資訊科技保安風險管理框架進行年度覆檢。	
評估有效性	評估當前風險評估流程的有效性。	
必要調整	計劃採用一種新的且更全面的風險評估方法。	
確保持續的適用性、充分性和有效性	覆檢風險管理流程，識別可以更全面的風險評估流程。	
高層管理人員和主要利益相關方的參與	決策局／部門的高層管理人員、部門資訊科技保安主任、資訊科技保安管理組、系統擁有人和風險擁有者參與覆檢過程。	
與決策局／部門的目標和優先次序保持一致	決定採用符合決策局／部門提升資訊科技保安目標的風險評估新方法。	

工作	資訊科技保安風險管理層覆檢及調整示例（由決策局／部門填寫）	狀態（若已完成，請勾選）
推動必要的變革，將資訊科技保安風險管理納入治理框架	讓高層管理人員參與推動風險管理框架的變革。	
確保和提高資訊科技保安風險管理活動的品質和有效性	監察在下次覆檢中調整後的結果，以確保品質和有效性得到提高。	

完

附件 A：資訊科技保安風險登記冊模板示例

編號	優先權	風險描述	風險類別	影響	可能性	系統等級	風險等級	風險處理方案	風險處理描述	風險擁有者	預計完成日期	狀態
1												
2												
3												

- 編號（風險識別號）：風險登記冊中某一風險的連續數位識別碼。
- 優先權：風險登記冊中表示該條目重要性的相對指標，可以用序號值（例如，1、2、3）或參考給定等級（例如，高、中、低）表示。
- 風險描述：對（可能）會影響系統或決策局／部門的資訊科技保安風險的情景作簡要描述。風險描述通常以因果關係的格式編寫，例如「如果發生X，則發生Y」。
- 風險類別：風險類別分組，例如按保安和私隱控制系列進行分類（例如，存取控制、供應鏈風險管理，如 NIST SP 800-53 中記錄的風險類別）。類別可以是任何有助於匯總風險資訊並集成資訊科技保安風險登記冊以提供決策支援的分類法。
- 影響：分析如果沒有提供另外應對措施的情景的潛在好處或後果。這也可以被視為風險週期第一次迭代的初步評估。
- 可能性：在任何風險應對之前，對發生這種情景的概率的估計。這也可以被視為風險週期第一次迭代的初步評估。
- 系統等級：系統關鍵性的級別。
- 風險等級：基於影響、可能性和其他因素（例如系統關鍵性）的組合而確定的計算結果。
- 風險處理方案：用於處理已識別風險的風險處理選項。
- 風險處理描述： 風險處理的簡要描述。例如，「實施軟件管理應用程式 XYZ 以確保對軟件平台和應用程式進行盤點」或「制定並實施流程以確保及時收到來自[特定資訊共用論壇和來源的名稱]的威脅情報」。
- 風險擁有者：指定的個人或業務單元，負責確保按照相關要求維護風險。
- 預計完成日期：風險處理的目標完成日期。
- 狀態：用於追蹤當前的風險狀況和任何後續活動。狀態可以是一個簡單的指標（例如進行中、已完成、待定、放棄、轉移），也可以提供更詳細的描述（如「風險已接受，待 1 月 24 日季度風險委員會會議審查」）。風險狀態應該是一套連貫的指標，有助於匯總風險資訊並整合資訊科技保安風險登記冊，從而為決策提供支持。

附件 **B**：風險匯總的風險類別示例

- 資產管理
- 業務環境
- 治理
- 法規（遵行）
- 威脅管理
- 風險管理
- 安全系統開發
- 供應鏈風險管理
- 人員保安
- 實體保安
- 接達控制
- 數據保安
- 密碼學
- 防護技術
- 資訊科技基準維護
- 資訊科技事件管理
- 檢測技術
- 持續監察
- 檢測過程
- 事故應變計劃與復原計劃
- 事故溝通
- 事故分析
- 事故緩解
- 事故改進

附件 C：相關風險偏好、風險承受能力、控制措施、關鍵績效指標和關鍵風險指標示例

以下是相關風險偏好、風險承受能力、控制措施、關鍵績效指標和關鍵風險指標示例：

	示例 1	示例 2	示例 3
風險偏好	必須保護關鍵資訊系統免受已知網絡保安漏洞的影響。	為了確保受保護的健康資訊的安全性，我們必須首先確保只有獲授權方能接達我們的電腦系統。	我們的客戶將可靠性與公司的業績掛鉤，因此必須儘量避免面向客戶的網站出現服務中斷問題。
風險承受能力	對於被指定為關鍵的資訊系統，必須在發現其存在重大軟件漏洞（嚴重程度為 10 分）後的 14 天內，應用修補程式。	我們將發放獨一無二的使用者帳戶，並且電腦系統將審查成功和失敗的登錄事件。	區域經理可允許不超過 5%的客戶遭遇持續 2 小時的網站中斷。
控制措施	定期漏洞評估 部署修補程式的能力	獨一無二的用戶帳戶 驗證方法 審計日誌 審計日誌警報／評估	發電機 空調機組 上游網絡提供商 網絡負載等化器 網絡伺服器
關鍵績效指標	漏洞修補百分比	1 小時內登錄失敗的次數	服務中斷時長（小時）
關鍵風險指標	在 10 天內未修復的重大漏洞（通用漏洞評分系統評分為 10）的電腦數量	單個用戶 5 次登錄失敗 所有用戶 30 次登錄失敗	當前的網站服務中斷時長超過 2 小時並影響了超過 5%的客戶的故障