數字政策辦公室

資訊保安

設計層面保安實務指引

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

隨著數碼格局的快速發展，安全威脅日益突顯，對政府的資訊系統和資產構成重大風險。僅僅依靠事後處理或採取被動措施已無法充分解決保安問題。相反，決策局／部門應採取積極主動的方法，將保安因素納入核心業務要求，而非僅作為一項技術功能。本實務指引旨在為決策局／部門的系統發展計劃提供參考指引。

1.1 目的

本文件提供了設計層面保安的總體框架，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）。

本實務指引旨為決策局／部門內參與系統發展周期所有階段的各級員工而設。另外，本文件亦供為政府提供資訊科技服務的供應商、承辦商及顧問使用。

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
- 《保安風險評估及審計實務指引》[ISPG-SM01]，數字政策辦公室
- 《敏捷軟件開發執行指引》[G62]，數字政策辦公室
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2022
- Information technology - Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2022
- Security-by-Design Framework, Cyber Security Agency of Singapore
- "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default", Cybersecurity and Infrastructure Security Agency
- "What Is Shift Left Security?", Fortinet

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	
SDLC	系統發展周期
IRS	初始化請求聲明
SA&D	系統分析及設計
SBD	設計層面的保安
DMZ	非軍事區
RBAC	基於角色的接達控制

1.4 聯絡方法

本文件由數字政策辦公室編製及備存。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、推行和持續提升，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。

保安管理框架與組織

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。

管治, 風險管理與遵行要求

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推行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推行全面的保安措施，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。

保安事件與事故管理

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。

保安意識培訓與能力建立

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／部門可以利用威脅情報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。

人員亦可以通過參與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（例如網絡安全資訊站、資訊安全網）的專頁來提高保安意識。

3 設計層面的保安

必須掌握系統發展周期本身的基礎知識，才能真正理解設計層面保安的重要性及其與系統發展周期的協同作用。

3.1 系統發展周期

系統發展周期是一個結構化框架，涵蓋系統發展的各個階段，包括規劃、分析、設計、推行、測試、部署和維護。這一周期為管理系統建立到退役的整個生命周期提供了框架。《資訊科技保安指引》[G3]中所示的系統發展周期概括如下：

- ***計劃開展：***使用者應提交初步請求聲明以申請資訊科技解決方案。初步請求聲明將被評估，並決定計劃是否應進入下一階段。

- ***可行性研究：***評估資訊科技解決方案的可行性，並量化擬議解決方案的要求、範圍、成本、好處和其他影響。

- ***系統分析及設計：***調查現有系統，指定新系統，並執行系統分析和邏輯系統設計，詳細說明計劃推行要求。

- ***計劃推行：***推行實體系統設計、程式發展、各種測試、安裝和計劃評估覆檢，以推行系統分析及設計的發現。

- ***計劃推行後的覆檢：***評估已推行系統的成本效益，並評估系統是否已及時實現其商定目標以及預期好處。

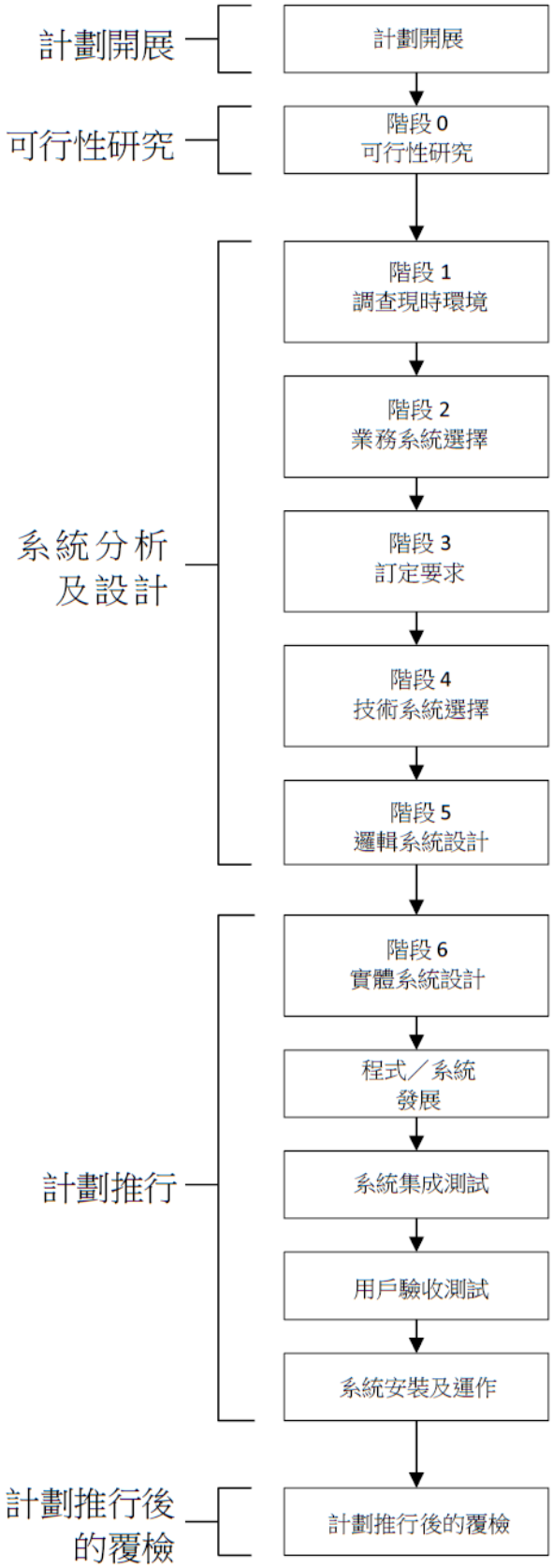

圖 3.1：系統發展周期各個階段

系統發展周期有不同模式，如瀑布式開發和敏捷式開發。瀑布式開發在各個階段遵循線性和順序進展，而敏捷式開發則以靈活性和適應性促進重複發展周期。根據計劃性質，決策局／部門宜應計劃需要，靈活採用多種軟件發展方法並應用多種實踐。

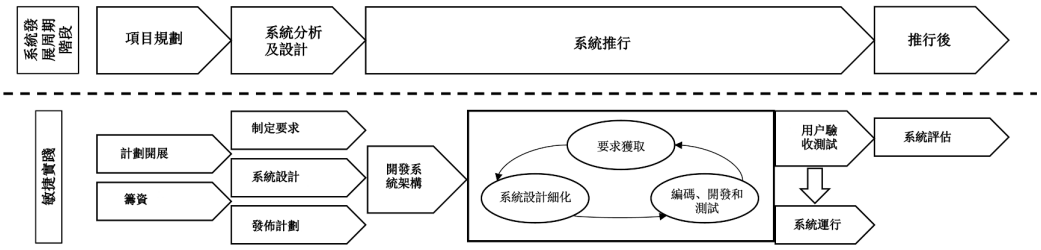

圖 3.2：敏捷軟件發展實務指引所述的敏捷式開發

有關敏捷軟件發展的更多詳細資訊，請參閱以下文件：

- **敏捷軟件開發執行指引**
  可於政府資訊科技情報網獲取。
  (https://itginfo.ccgo.hksarg/content/bpg/Agile/agile.html)

本文件中描述的設計層面的保安框架適用於瀑布式和敏捷式發展周期。

3.2 設計層面的保安簡介及其重要性

設計層面的保安屬於系統開發概念，在整個發展周期中優先考慮和整合保安措施。設計層面的保安旨在發展過程的早期主動識別和解決保安風險和漏洞，減少產生保安漏洞的可能性，並確保創建穩健且具復原能力的系統。通過從一開始就納入保安原則，決策局／部門可最大限度地降低發生代價高昂的保安事故的可能性，並保護其系統和資料的機密性、完整性和可用性。設計層面的保安框架包括指導保安系統設計和發展的原則。而框架之間各有差異，以下是多種設計層面的保安框架中常見的原則：

- ***核心政府要求：***將設計層面的保安視為一項政府基本要求，保持其與策略目標、運作需求和法規要求一致。將安全性視為競爭優勢，並將其與其他政府核心要求一同優先考慮，確保必要的關注、資源和執行支持。

- ***積極主動的方法：***在系統設計的早期階段即採取積極主動的思維方式來解決保安問題。保安不應是事後考量，而應是發展過程中不可或缺的部分。

- ***端對端保安：***考慮整個系統的保安，包括硬件、軟件、網絡和使用者介面。滿足每一層面的保安要求，並確保它們的協同運作以提供全面保護。

- ***風險管理：***開展全面風險評估，以識別潛在的威脅、保安漏洞和影響。制定風險緩解策略，並根據風險級別和潛在影響決定保安措施的優先順序。

- ***保安監管：***建立明確的職務、職責和流程，以在系統的整個生命周期內實施保安管理，包括制定問責制、決定權以及監察和執行保安要求的機制。

- ***保安架構：***設計安全且具復原能力的架構，其中包含各個層面的保安控制，包括網絡設計、資料流、接達控制和職責分離。遵循已建立的架構模式和最佳保安實踐。

- ***安全發展實踐：***採用將安全性放在首位的安全編碼實踐和發展方法，包括安全編碼指引、威脅建模、程式碼審查和保安漏洞測試。定期更新和修補軟件組件，以解決已知的保安問題。

- ***第三方保安：***評估第三方組件、服務和供應商的保安狀況。建立選擇可靠和安全的合作伙伴的標準。在整合外部系統時，制定合同協議並盡職執行保安。

- ***整合到系統發展周期中：***將保安活動和注意事項嵌入到每個系統發展周期階段，包括收集要求、設計、推行、測試、部署和維護。安全性在整個發展周期中應該是一個持續和重複的過程。

- ***保安測試與驗證：***在整個系統發展周期中，開展全面的保安測試和驗證活動，包括漏洞掃描、滲透測試、配置審查和源碼掃描，以識別和解決保安弱項和漏洞。

在所有系統發展周期階段都應考慮這些注意事項。但系統發展周期的某些階段亦有需要注意的特定範疇，該等範疇列載於下頁圖示右方欄內。

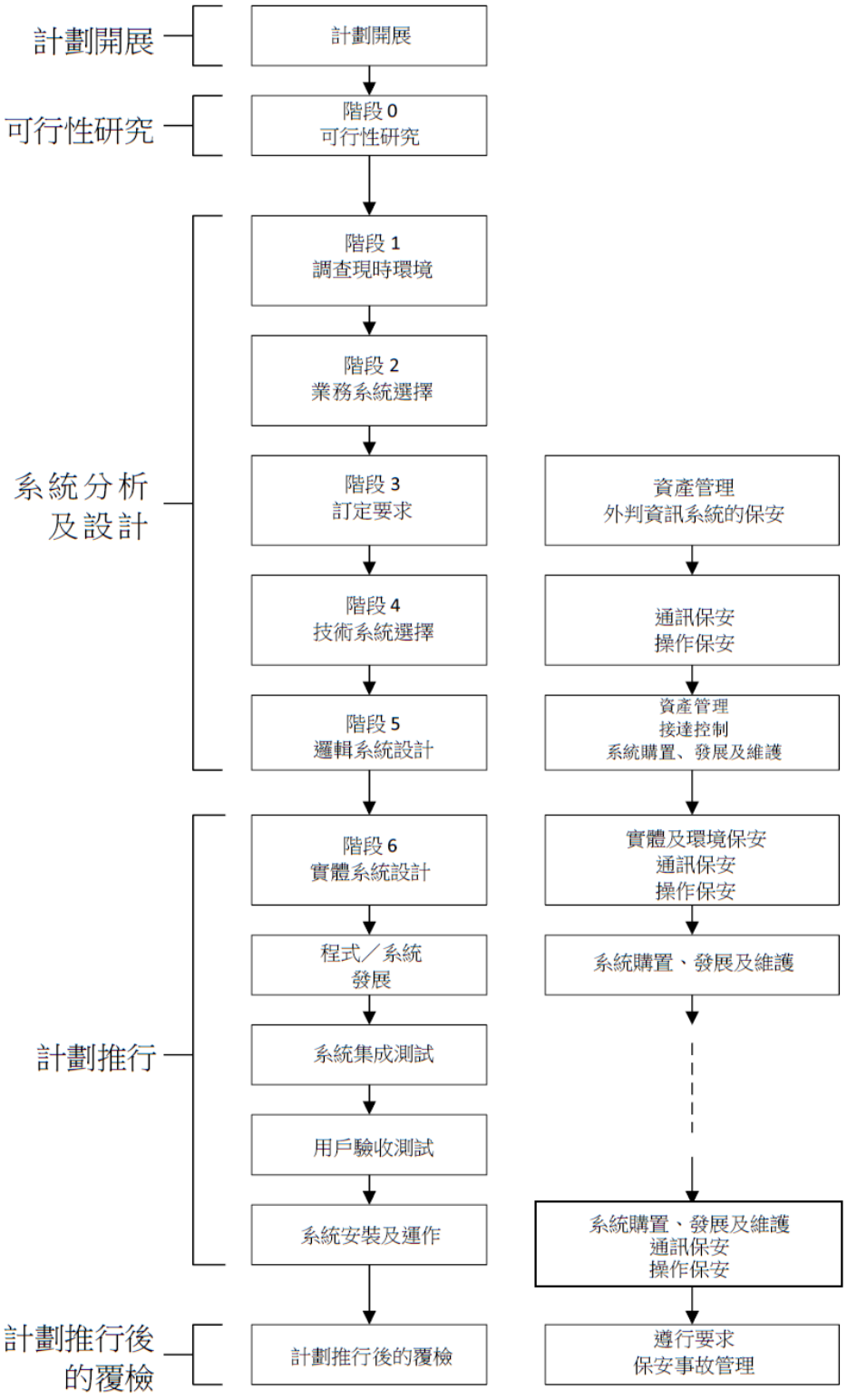

圖 3.3：系統發展周期不同階段涉及的保安考慮

保安左移這一概念與設計層面的保安密切相關，它涉及從計劃和評估階段中考慮安全性。

傳統上，安全性往往只在測試階段和軟件構建後才得到解決。這可能會減慢發展速度，並且在測試階段識別保安問題時通常需要重做。而保安左移則可以在測試之前執行保安控制活動，預測保安需求並減少發展後期的潛在問題。但有一點非常重要，設計層面的保安超越了系統發展周期和保安左移，涵蓋整個系統設計和架構。設計層面的保安強調將安全注意事項和實踐整合到系統設計、架構和推行中，而非將安全視為事後考量。

為確保在推行資訊系統及應用系統時存在適當的保安及資料保護措施，決策局／部門應將設計層面的保安概念納入系統發展周期。設計層面的保安強調從初步設計階段到系統發展周期的所有階段都採用保安實踐。借此，決策局／部門可以主動識別和降低保安風險和漏洞，最終降低網絡安全損害對其聲譽、資料完整性和運營造成的潛在代價。

下文重點介紹了將設計層面的保安納入系統發展周期的一些主要益處：

- ***緩解風險：***通過消除不必要和易受攻擊的組件來減少攻擊者可利用的潛在入口。

- ***節約成本：***最大限度地減少對發展流程後期階段發現的保安問題的修復需求，這可能既昂貴又耗時。

- ***增強系統復原能力：***加入安全更新、增強功能和新功能，提高資訊系統應對不斷變化的保安要求和威脅的可擴展性和適應性，從而更好地保護資訊系統免受未經授權的接達、資料洩露和其他保安事故的影響。

3.3 設計層面的保安周期和框架

3.3.1 設計層面的保安周期

在系統發展周期中，主要的關注點是有效開發系統，通常將保安作為事後考量。這種處理並修補保安漏洞的方式既不可靠，成本又高。從一開始就設計安全的系統是一種更有效的方法。

設計層面的保安周期通過將保安注意事項納入每個階段的流程中，與系統發展周期的各個階段保持一致。其貫穿於所有階段，因為需要在計劃階段及早識別保安風險，並在後續階段加以解決。保安風險可通過以下方式解決：

a) 調整規定或部署，以避免已識別的保安風險。

b) 推行替代或緩解控制，將風險降至最低。

c) 必要時通過適當的風險管理流程接受風險。

d) 採用重複流程來評估每個階段的安全性，並確定是否需要採取額外的保安措施來獲得滿意的結果。

下圖說明設計層面的保安周期如何與系統發展周期並行：

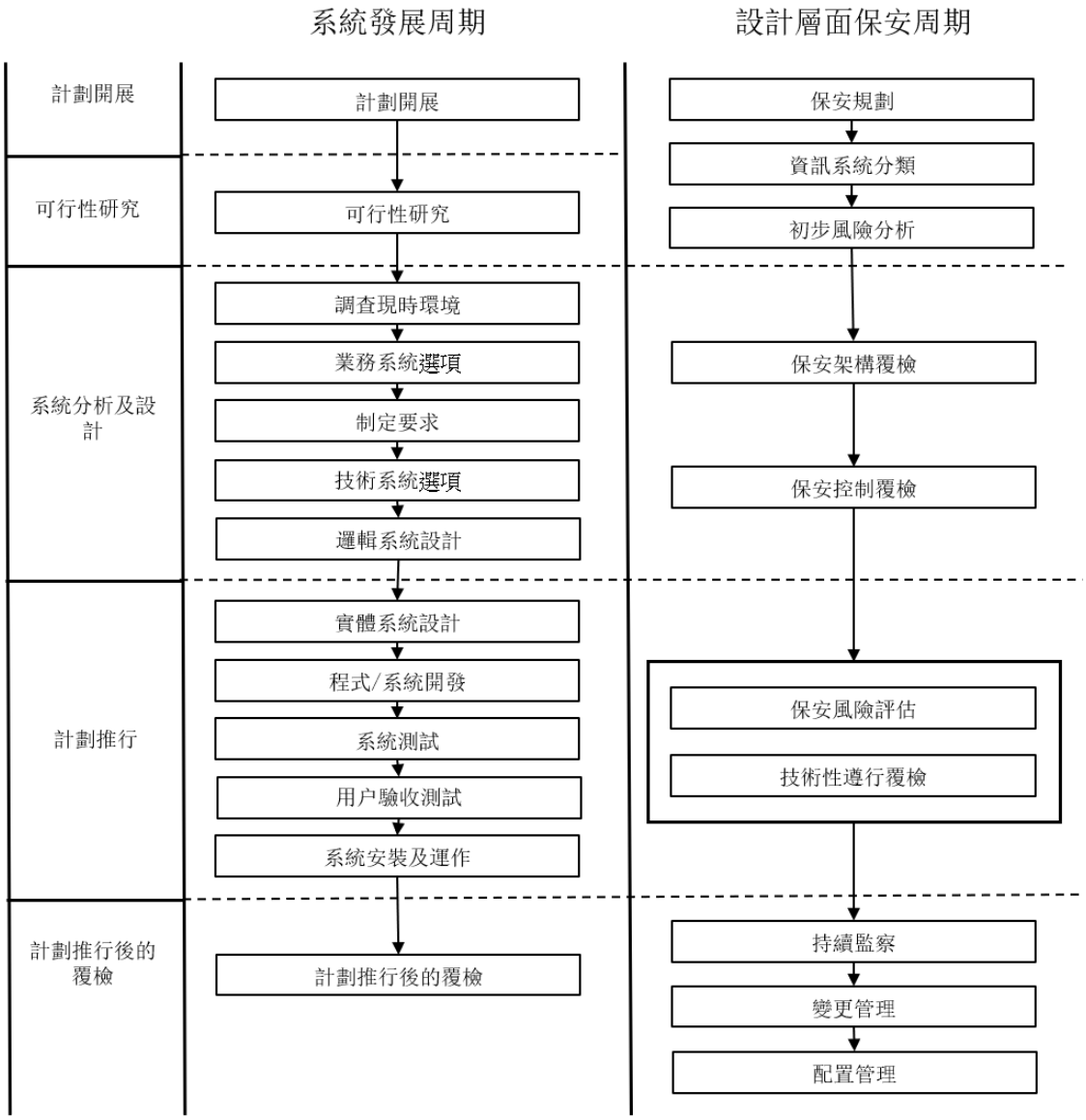

圖 3.4：系統發展周期／設計層面保安周期

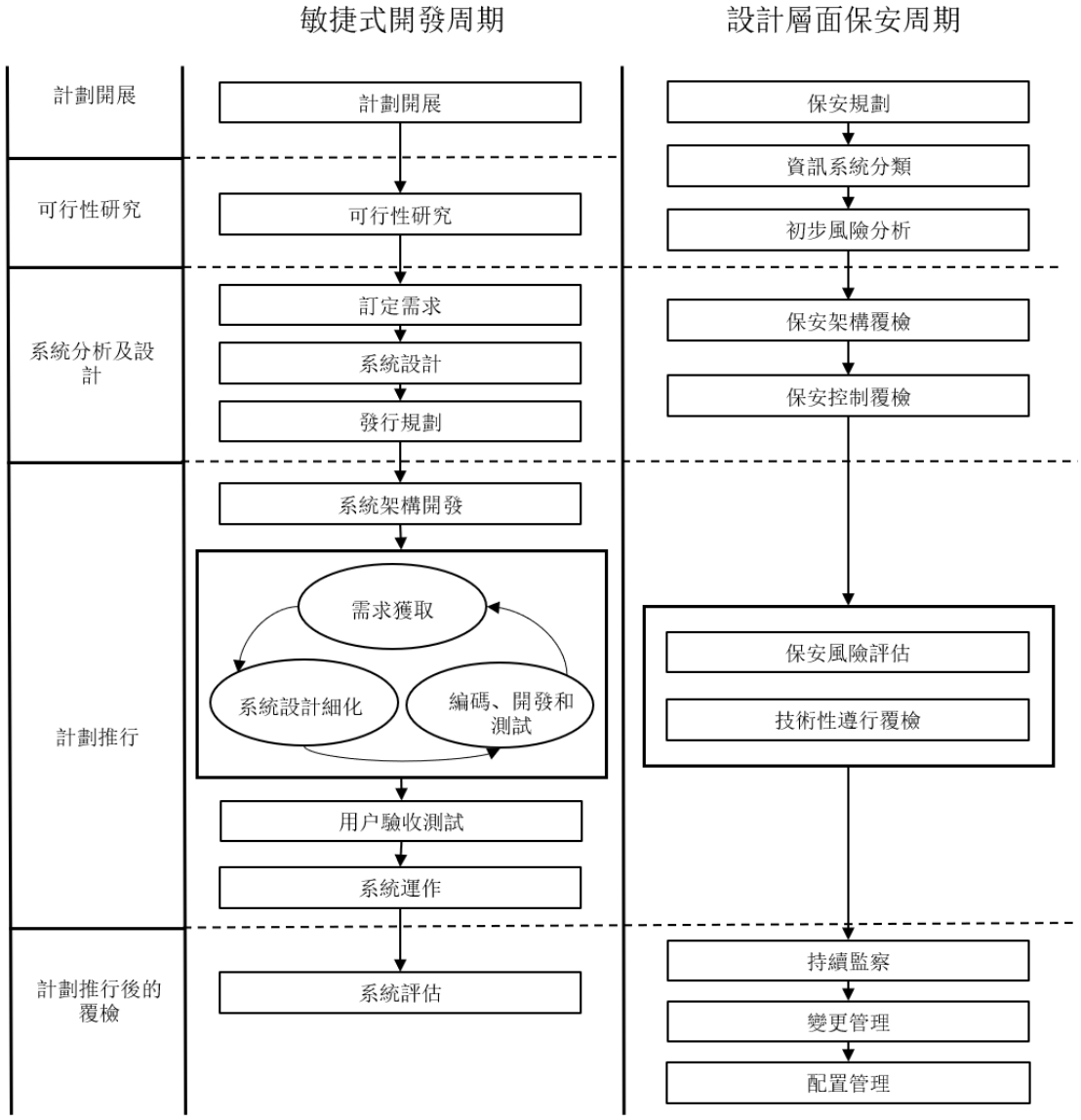

圖 3.5：敏捷式發展周期／設計層面保安周期

在系統發展周期每個階段引入安全性具有多種優勢，它確保高級管理層和關鍵人員能夠看到並充分了解保安風險，從而及時做出明智的決定，將風險降低到可接受的水平。通過在整個系統發展周期中納入保安考量，決策局／部門可以主動解決保安問題，並更有效地將潛在風險降至最低。

3.4 設計層面的保安方法

設計層面的保安方法由三個部分組成，即：

- 生命周期：將保安相關流程與系統發展周期相結合，以指導計劃實現設計層面的保安目標。

- 活動：支援保安周期流程的保安相關活動。

- 門控：從保安角度評估系統開發工作的時間點，以及管理層確定計劃是否應按原樣繼續推進、改變方向或終止的時間點。

設計層面的保安方法對於將保安考量納入保安周期流程各階段至關重要。該流程涉及將基本保安元素納入系統發展周期方法的活動。設計層面的保安流程始於系統發展周期階段的早期，在整個系統發展周期中對資訊系統的保安功能和發展態勢的形成發揮著關鍵作用。

如果未能在系統發展周期的各階段充分執行該等流程，可能會導致更高的推行成本。因此，在系統發展周期各階段確定保安流程的優先順序，並有效執行，對於建立穩健且具有成本節約效益的保安框架至關重要。

將設計層面的保安方法納入系統發展周期，對於開發穩健且安全的資訊系統至關重要。決策局／部門應盡可能採用設計層面的保安原則。在系統發展周期中推行設計層面的保安目標包括：

- ***建立設計層面的保安框架：***創建一個全面的設計層面保安框架，在強制要求採用設計層面的保安方法時，供持份者參考。框架應概述系統發展周期的關鍵原則、標準和指引。

- ***推行設計層面的保安流程：***制定和推行設計層面的保安流程，確保開始時就管理保安風險，並在整個系統發展周期中持續開展評估。流程應納入系統發展周期階段，並遵循周期方法。

- ***開展保安風險評估：***保安風險評估是設計層面的保安流程的一部分，實施保安風險評估，以識別和評估潛在的保安風險和漏洞。定期評估和更新系統的風險狀況，以確保採取適當的保安措施。

- ***推行保安活動：***將特定的保安活動納入系統發展周期中，以有效管理保安風險。保安活動宜包括威脅建模、安全編碼實踐、安全測試、漏洞掃描和程式碼審查。確保在適當的系統發展周期階段，開展保安活動。

- ***門控和決定點注意事項：***在系統發展周期各階段建立門控和決定點，以確保在未對相關保安風險進行全面評估的情況下，不會作出任何決定。這包括在進入下一階段之前，開展保安覆檢並獲得必要的批准。

4 設計層面的保安框架

4.1 框架概述

下圖描繪了一種結構化和紀律化的方法，用於整合政府系統發展的保安流程。

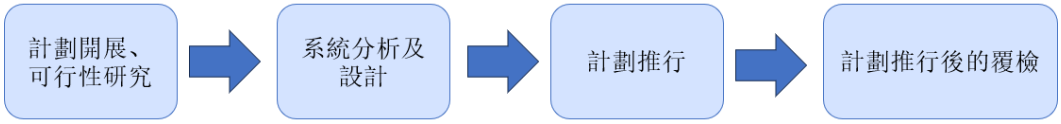

圖 4.1：系統發展周期

設計層面的保安框架由四個主要階段組成，強調持續風險管理，概述如下文。且每個階段的活動在相應的章節中都有更詳細的描述。為有效推行保安管理方法，決策局／部門應在所有保安流程中採用一致的風險管理方法，並應在系統發展周期的所有階段考慮資訊保安。

決策局／部門在系統發展中應採用設計層面的保安方法，確保資訊資產的機密性、完整性和可用性，並處理其他安全事宜，以應對不斷變化的威脅形勢和技術。通過推行直接措施，決策局／部門有效降低並控制與人為和運作問題相關的潛在資訊保安風險，將風險維持在可接受和可控的水平。決策局／部門亦應考慮採用適合其業務和運作環境的良好實踐。

保安措施和控制措施應具有回應性和適應性，以抵禦新出現的保安威脅並降低其風險。決策局／部門應充分了解系統發展中新出現的保安威脅及相關風險。

在設計層面的保安框架中，每個階段都伴隨著一組以安全為重點的活動，該等活動概述了需採取的關鍵行動。圖 4.2 說明了活動相互保持一致及開展的方式。每項活動都包含必要資訊，如對將要採取的行動的描述、關鍵人員的職務和職責以及預期輸出，目的都是為了加強系統安全性。

在每個階段完成後，決策局／部門應進行控制驗證，以在進入下一階段前，評估是否已充分解決安全考量、是否已推行足夠的保安控制，以及是否已徹底了解已識別的風險。

4.2 框架推行

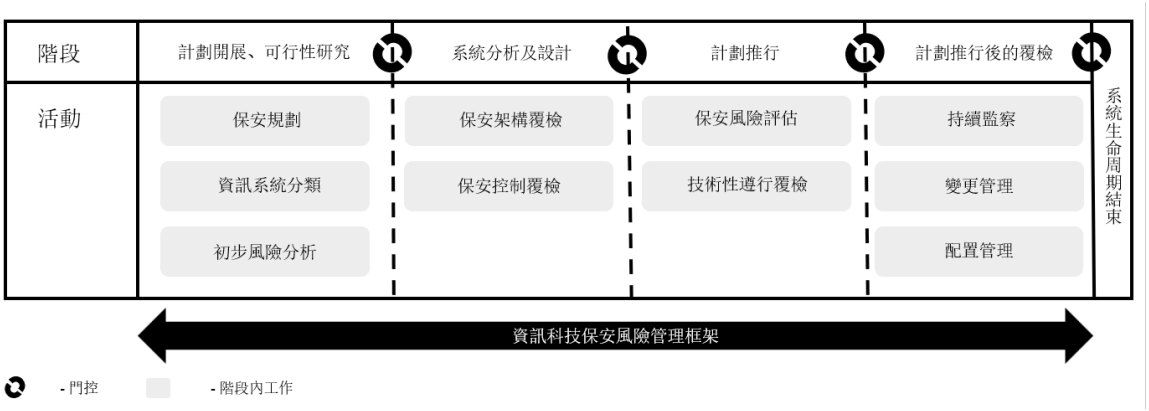

圖 4.2 - 設計層面的保安框架

A. 計劃開展、可行性研究（第 5 節）

適當的規劃可確保識別必要的保安控制、政策和程序。在這一階段，決策局／部門應清楚制定保安目標、範圍和系統要求。

這一階段涉及的主要活動包括：

- 保安規劃
- 資訊系統分類
- 初步風險分析

B. 系統分析及設計（第 6 節）

系統分析及設計是系統發展周期中的一個重要階段，系統或應用系統在這一階段根據制定的需求生成。其目的是評估保安架構，控制待開發的系統或應用系統。通過展開全面覆檢，在部署系統前，識別並處理潛在保安漏洞和缺陷，從而增強系統的整體安全性。此外，決策局／部門應確保符合政府規例、資訊科技保安政策和指引。

這一階段涉及的主要活動包括：

- 覆檢保安架構
- 覆檢保安控制

C. 計劃推行（第 7 節）

在這一階段，決策局／部門應關注徹底的測試以驗證功能，並準備部署系統。

這一階段涉及的主要活動包括：

- 保安風險評估
- 技術性遵行覆檢

D. 計劃推行後的覆檢（第 8 節）

系統部署後，決策局／部門應持續管理、監察和維護已部署的應用系統，以確保其在整個周期內保持安全、穩定和最佳表現。

這一階段涉及的主要活動包括：

- 持續監察
- 變更管理
- 配置管理

4.3 職務和職責

決策局／部門應清楚地制定、識別和授權所有設計系統發展周期涉及的員工職務和職責。系統發展周期涉及的員工可能包括：

4.3.1 高層管理人員（適用於大規模公眾面向的資訊科技系統）

- 提供戰略性計劃領導，並確保與決策局／部門的目標保持一致。

4.3.2 資訊科技保安管理組

- 對推行保安控制提供保安建議。

4.3.3 資料擁有人

- 制定資訊的敏感性、機密性、完整性和可用性要求。
- 對資訊進行分類，並將其保安要求傳達給項目經理。
- 最終批准推行與其擁有的資訊相關的保安控制。

4.3.4 項目經理

- 在商定的約束範圍內管理計劃，並協調所有活動。
- 協調保安風險管理活動，並確保符合相關的保安標準。
- 確保保安活動被整合到項目計劃中。
- 促進團隊溝通，以確保保安方法的一致性。
- 根據需要，上報保安風險和事項。

4.3.5 資訊科技保安管理員

- 執行特定的保安任務，如識別和緩解系統的保安漏洞。

4.3.6 局部區域網絡／系統管理員

- 管理系統的日常操作，確保保安機制按照設計進行維護。
- 在資訊科技保安管理員的指導下，推行配置更改和保安修補程式。

4.3.7 應用系統發展及維修小組

- 開發符合既定程序的系統，並從一開始就納入保安要求。
- 開展安全編碼實踐並修復保安漏洞。
- 通過與資料擁有人密切合作，確保整個軟件發展周期安全性的持續整合。

4.3.8 用戶

- 根據其知識和需求，提供早期階段輸入的有關保安要求的資料。
- 提供有關系統安全性的反饋，並在保安審計中根據需要提供資訊和幫助。
- 及時報告任何保安問題。

5 計劃開展、可行性研究

適當和超前的規劃可確保識別必要的保安控制、政策和程序。在這一階段，決策局／部門應制定系統的保安目標、範圍和要求。此外，初步風險分析有助於確定保安工作的優先順序，並確定最有效的風險減緩策略。

5.1 活動

規劃和評估涉及的主要活動如下：

- 保安規劃
- 資訊系統分類
- 初步風險分析

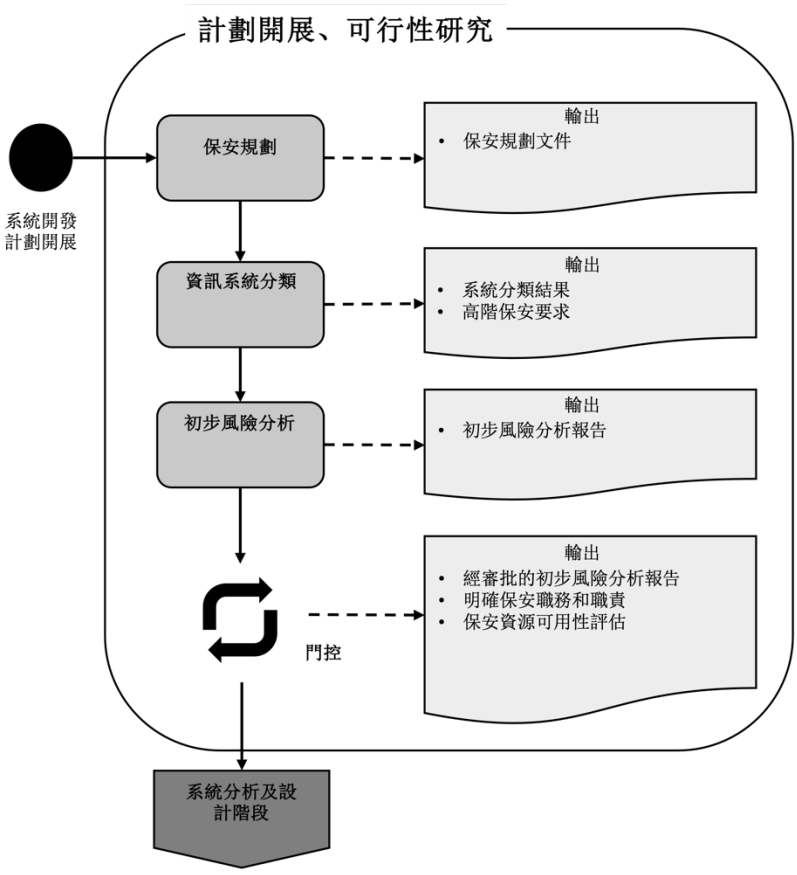

圖 5.1：計劃開展、可行性研究

5.1.1 保安規劃

決策局／部門應制定保安規劃，並至少涵蓋以下內容：

- 制定資訊系統保安目標、範圍和要求；
- 建立監管架構，明確在系統發展周期內納入安全的責任；
- 確定相關保安標準、規例和可指導安全計劃程序的良好實踐；以及
- 概述關鍵保安事故和活動。

5.1.2 資訊系統保安分級

決策局／部門須評估資訊系統的分級，確保系統受到與相應風險水平相匹配的保安控制措施的保護。有關系統分級的更多詳細資訊，請參閱以下文件：

- **資訊科技保安指引[G3]**
  可於政府資訊科技情報網獲取。
  (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap_tc.shtml)

5.1.3 初步風險分析

初步風險分析旨在識別資訊系統面臨的威脅和保安漏洞，明確資訊系統面對的風險水平，並推薦適當的保護級別。

該分析流程應包括：

- 識別並分析所有系統資產和相關流程。
- 評估可能影響系統機密性、完整性或可用性的威脅。
- 識別系統保安漏洞和相關威脅。
- 評估潛在影響和風險。
- 確立減低風險的保護要求。
- 選擇適當的保安措施，分析風險關係。

在購置情況下，決策局／部門應該明確制定具體的保安要求，例如資訊系統級別所需的更嚴格的保安要求，已確定的風險緩解措施或應包含在招標文件中選定的保安措施。

5.2 職務和職責

5.2.1 應用系統發展及維修小組

- 提供有關高階保安需求和系統開發風險的技術專業知識。
- 協助系統分級，並從開發角度進行風險分析。

5.2.2 項目經理

- 概述並將關鍵保安事故和活動寫入計劃中。
- 確保適當的系統和資訊分級，並且及時開展了全面的初步風險分析。
- 協調初步風險分析，識別和評估威脅、漏洞和風險，並確定適當的保護措施。

5.2.3 資料擁有人

- 根據資訊分類，傳達高階保安需求。
- 參與風險分析，給出對於特定業務威脅和風險的見解。

5.2.4 用戶

- 從用戶角度提供對於保安要求和操作風險的見解，增強風險分析的實用性。

5.3 預期輸出／交付

- 保安計劃文件，包含：
  - 資訊系統保安目標、範圍和要求的清晰定義。
  - 制定的監管架構，明確的具體責任以在系統發展周期內確保安全。
  - 已知可指導保安規劃流程的相關保安標準、規例和良好實踐。
  - 關鍵保安里程碑和活動的時間線。
- 系統分級結果和依據系統分級的高階保安需求。
- 初步風險分析報告，報告詳述可能影響操作的潛在威脅和風險，以及需推行以減低風險至可接受水平的保安控制。

5.4 門控

計劃開展和可行性研究是計劃成功進行的基礎，建議的控制驗證應包含：

控制驗證	驗證標準	門控操作
批准初步風險分析報告	• 確保初步風險分析報告內容全面且已獲得批准，並可用於制定詳盡的保安要求和控制。 • 驗證初步風險分析報告內容是否包括對潛在影響和風險的評估以及保護要求和建議的保安措施。	• 覆檢和批准風險初步分析報告。 • 確認初步風險分析報告將告知詳細保安要求和系統設計的後續發展。 • 加入高階保安需求。
加入高階保安需求	• 確認初步風險分析報告中囊括所有高階保安需求。 • 驗證高階保安需求是否被指定為需加入系統設計中的保安控制。	• 確保高階保安需求向詳細的系統保安控制過渡過程清晰可溯。
確認職務和職責	• 在項目組中建立並清晰記錄職務和職責，尤其是系統發展周期內保安監管有關職務和職責。	• 覆檢監管架構和職責文件。 • 從所有項目組成員處獲知其保安相關的具體職務和職責。
評估保安資源可用性	• 評估所需時間內用於支持計劃的保安資源（包括人員、技術和預算）是否可用和充足。	• 如有必要，展開資源差距分析，並制定資源配置計劃。 • 根據資源的可用性、計劃時間的可行性，決定計劃的進行／不進行狀態。

6 系統分析及設計

系統分析及設計是系統發展周期中的重要階段，系統或應用系統基於制定的需求開始成形，其目的是評估正在開發中的系統或應用系統的保安架構和控制。在部署系統前，通過全面覆檢識別並處理潛在保安漏洞和缺陷，從而增強系統的整體安全性。此外，涉及購置第三方或商業現成軟件時，決策局／部門應確保所購置的系統或服務符合政府規例、資訊科技保安政策及指引。

6.1 活動

這一階段，主要有兩項活動：

- 覆檢保安架構
- 覆檢保安控制

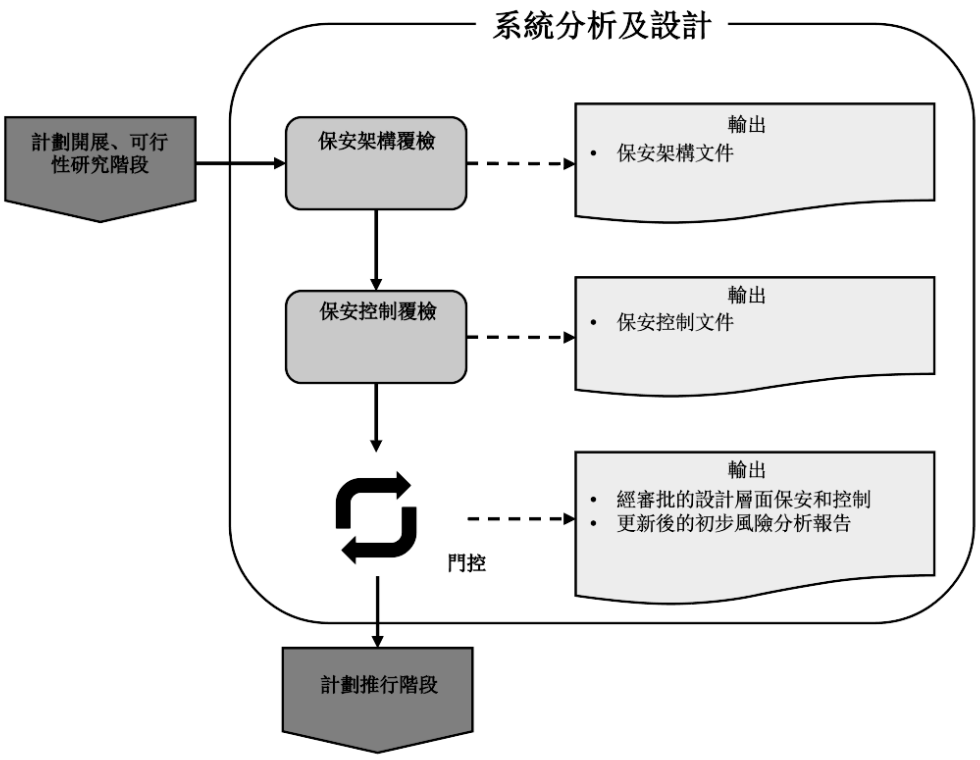

圖 6.1 系統分析及設計

6.1.1 覆檢保安架構

決策局／部門應全面覆檢系統或應用系統的保安架構，評估保安措施的設計和推行情況，識別任何潛在差距或保安漏洞。決策局／部門應重點覆檢確保保安架構與行業良好實踐，規管和政府保安要求一致，包括所需保安控制，遵行相關標準和規例，安全資料處理要求以及供應商的任何具體保安期望。

6.1.2 覆檢保安控制

決策局／部門應評估系統或應用系統內推行的保安控制的有效性，確保保安控制保護系統或應用系統能夠抵禦潛在威脅，緩解風險，並與制定的保安要求和標準保持一致。如購置，決策局／部門應評估潛在供應商的保安能力是否滿足制定的保安要求。

決策局／部門評估潛在供應商的保安能力時，宜評估以下方面：

- 保安管理實踐；
- 事故應變能力；以及
- 安全認證。

決策局／部門應根據評估結果製備一份報告，用作供應商選擇流程中的決定依據。

該報告應包括以下內容：

- 第三方風險評估
- 遵行和認證情況
- 評估標準和得分情況
- 建議及決定

該報告應為選擇合適供應商的綜合依據，確保系統性地解決了所有保安考量。

6.2 職務和職責

6.2.1 資訊科技保安管理組

- 在系統設計階段，提出必要的保安措施和控制的專業建議。

6.2.2 資料擁有人

- 根據資料分類制定資訊保安要求。
- 批准用於保護資料擁有人所擁有資訊的保安控制。

6.2.3 項目經理

- 確保保安措施無縫地融入系統設計。
- 協調對新系統進行的保安架構審查，確保符合相關標準。
- 確保所提出的保安架構和控制與決策局／部門的業務目標和保安要求一致。
- 確保各方就保安考量溝通一致。
- 確保制定的保安要求與投標要求一致，如購置，確保已提出保安評估建議並已納入投標評估。

6.2.4 資訊科技保安管理員

- 在系統設計階段執行保安相關具體工作，例如建議設計的保安漏洞評估。

6.2.5 局部區域網絡／系統管理員

- 提出對建議保安架構可管理性和可維護性的見解。
- 計劃未來將推行的保安配置和修補程式管理。

6.2.6 應用系統發展及維修小組

- 開發包含保安控制的系統設計。
- 計劃對設計潛在保安漏洞的補救。
- 負責在系統發展周期其餘階段持續整合保安。

6.2.7 用戶

- 為系統提供保安要求和期望。
- 對系統設計中保安措施相關的潛在可用性問題提供反饋。
- 承諾報告任何在建議設計中發現的保安缺陷。

6.3 預期輸出／交付

- 保安架構文件：
  全面概述了系統或應用系統中的保安架構，包括：

  - ***系統概況：***對系統、系統組件和系統用途的整體描述。
  - ***保安目標：***確立機密性、完整性和可用性的保安目標。
  - ***網絡架構：***網絡設置的架構圖和說明，包括分段、防火牆和非軍事區。
  - ***組件設計：***各系統組件的詳細安全資訊，包括伺服器、數據庫和應用系統。
  - ***數據流：***數據在系統內流動的視覺化呈現或描述，以識別數據可能有風險的地方。
  - ***接達控制：***認證機制和授權機制的描述，包括基於角色的接達控制矩陣。
  - ***加密方法：***靜止和傳輸中的資料加密標準詳情。
  - ***入侵偵測防禦：***概述偵測和預防未授權接達或異常的機制。
  - ***保安規約：***所有保安規約的清單，比如通訊安全的傳輸層安全協議。
  - ***遵行標準：***識別相關遵行標準和系統架構的遵行情況。
  - ***安全域：***網絡安全域的定義和其分隔及保護方法。
  - ***復原能力和容錯能力：***確保系統即使在組件故障或受到攻擊期間仍能安全運行的設計選擇。

- 保安控制文件：
  詳述了所推行的具體保安措施以及其對構建系統整體安全態勢的作用。
  - ***控制清單：***所有推行的保安控制清單，包括防火牆、殺毒軟件、入侵偵測系統等。
  - ***控制描述：***詳細描述在系統中每項控制的功能、配置和操作。
  - ***風險緩解：***分析每項控制如何具體緩解的已識別風險。
  - ***分層防禦：***說明保安控制如何協同工作，以創造分層（或縱深防禦）保安策略。
  - ***遵行對應：***保安控制與遵行要求的相互參照，顯示每個保安控制如何滿足特定要求。
  - ***控制擁有權：***每項控制的負責人資訊，包括控制擁有者或保管人的聯繫資訊。

6.4 門控

決策局／部門在開發系統前，應驗證並接受建議的保安設計和控制。初步風險評估的更新和變更應反映保安要求和設計變更。建議的控制驗證包括以下內容：

控制驗證	驗證標準	門控操作
驗證保安設計和控制	保安設計與控制與決策局／部門架構標準和政策一致。	覆檢並批准建議的保安設計和控制。
與決策局／部門架構一致	決策局／部門現有架構中整合的系統設計，包括保安組件。	確認決策局／部門架構中已加入系統設計並保持一致；尋求批准。
遵行保安要求	所有議定的保安要求已在系統設計階段履行。	驗證要求是否已履行；記錄持份者正式接受系統設計。
正式接受的系統設計	關鍵持份者同意建議的系統設計滿足項目目標和保安要求。	獲得關鍵持份者對系統設計的正式批准。
初步風險分析的更新與變更	初步風險分析反映當前保安要求和設計。	更新風險分析以包含變更；重新驗證保安風險與控制。

7 計劃推行

在計劃推行階段，決策局／部門應循序漸進，首先進行全面的保安風險評估和嚴格的技術性遵行覆檢。這流程在驗證系統功能，識別、分析和評估保安風險以及確保遵行技術標準中發揮關鍵作用。在此階段持續監察對確保隨著系統演化而相應調整保安態勢至關重要。

7.1 活動

計劃推行階段的主要活動如下：

- 保安風險評估
- 技術性遵行覆檢

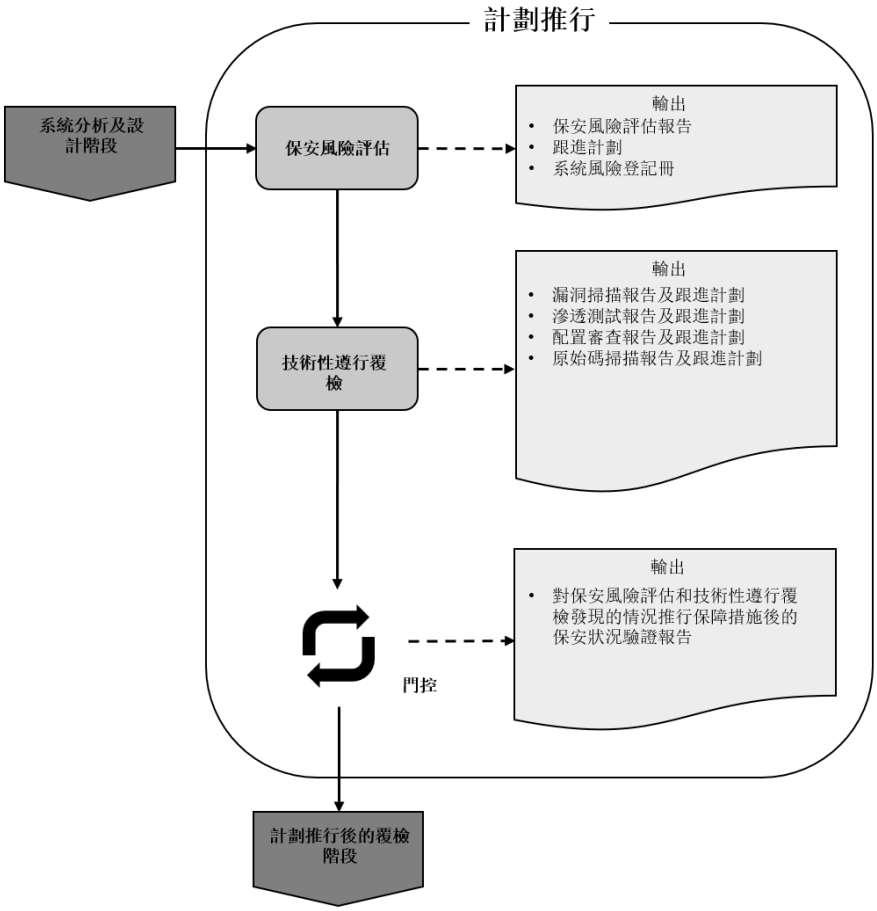

圖 7.1 計劃推行

7.1.1 保安風險評估

決策局／部門應展開保安風險評估，以識別、分析和評估保安風險，並決定風險處理措施，以將風險降至可接受的水平。系統評估的過程應包括識別並分析：

- 系統所有資產和相關流程
- 可能影響系統機密性、完整性或可用性的威脅
- 系統保安漏洞和相關威脅
- 威脅的潛在影響和風險
- 緩解風險的保護要求
- 選擇適當的保安措施並分析風險關係

為使分析結果精確可用，應提供一份系統的完整清單和保安要求，作為識別和分析活動的輸入。與相關者訪談，例如局部區域網絡／系統管理員、資料擁有人、用戶等，也可以為分析提供額外資料。根據評估範圍、要求和方法，分析宜使用自動化的安全評估工具。評估所有收集的資訊後，應報告所發現風險清單。就每項發現的風險，決策局／部門應確定在系統推行前部署適用的保安措施。

有關開展保安風險評估的更多詳細資訊，請參閱以下文件：

- **保安風險評估及審計實務指引**
  可於政府資訊科技情報網獲取。
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

7.1.2 技術性遵行覆檢

決策局／部門應在計劃推行階段進行保安漏洞掃描、滲透測試、配置審查和／或原始碼掃描。在系統運作或提供正式服務前，應評估所確定的保安漏洞及問題，並採取適當修正行動處理。決策局／部門應制定建議跟進計劃，包含計劃推行時間表，並在計劃推行保護措施後，覆檢安全狀況。

有關技術性遵行覆檢的更多詳細資訊，請參閱以下文件：

- **資訊科技保安指引[G3]**
  可於政府資訊科技情報網獲取。
  (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap_tc.shtml)

7.2 職務和職責

7.2.1 資訊科技保安管理組

- 在需要時就系統推行過程中的安全措施和控制提供建議。

7.2.2 項目經理

- 安排保安風險評估和技術性遵行覆檢流程。
- 監察技術性遵行覆檢的執行情況，確保已識別的漏洞得到解決。
- 確保在系統運作前，已採用並驗證評估建議。

7.2.3 資訊科技保安管理員

- 協助進行保安風險評估和技術性遵行覆檢。

7.2.4 局部區域網絡／系統管理員

- 協助進行保安風險評估和技術性遵行覆檢，提供資訊配置詳情，採納變更建議。

7.2.5 應用系統發展及維修小組

- 參與保安風險評估，提供有關系統組件和潛在安全漏洞的資訊。
- 按照既定的時間線修復在技術性遵行覆檢期間發現的任何安全漏洞。

7.2.6 用戶

- 協助開展保安風險評估和技術性遵行覆檢，反饋用戶對系統保安的關注點。

7.3 預期輸出／交付

- 保安風險評估報告及其跟進計劃
- 系統風險記錄冊
- 保安漏洞掃描報告及其跟進計劃和驗證報告
- 滲透測試報告及其跟進計劃和驗證報告
- 配置審查報告及其跟進計劃和驗證報告
- 原始碼掃描報告及其跟進計劃和驗證報告

7.4 門控

在計劃推行階段，建立並測試系統。決策局/部門應評估所推行保安措施的有效性。建議的控制驗證包含以下：

控制驗證	驗證標準	門控操作
記錄保安風險和緩解風險的措施	將所有識別的保安風險和採取的緩解威脅的策略準確記錄在風險記錄冊中。	• 覆檢風險記錄冊，確保資訊完整和準確。 • 在推進前，批准風險記錄冊。
與決策局/部門架構保持一致	根據系統設計階段的要求推行保安控制。	• 根據要求檢查和驗證保安控制。 • 在推進前，確認已正確且完整地推行保安控制。
完成緩解風險工作	妥善處理並記錄在保安風險評估與技術性遵行覆檢中開展的緩解風險工作。	驗證每項緩解風險工作，確保充分緩解保安風險或保安風險可接受，並獲得正式批准。

8 計劃推行後的覆檢

決策局／部門應維持在所部署系統的持續管理、監察及維護的機制，確保解決方案在其整個生命周期內持續安全、穩定和發揮最佳性能。

8.1 活動

測試和計劃推行階段的主要活動如下：

- 持續監察
- 變更管理

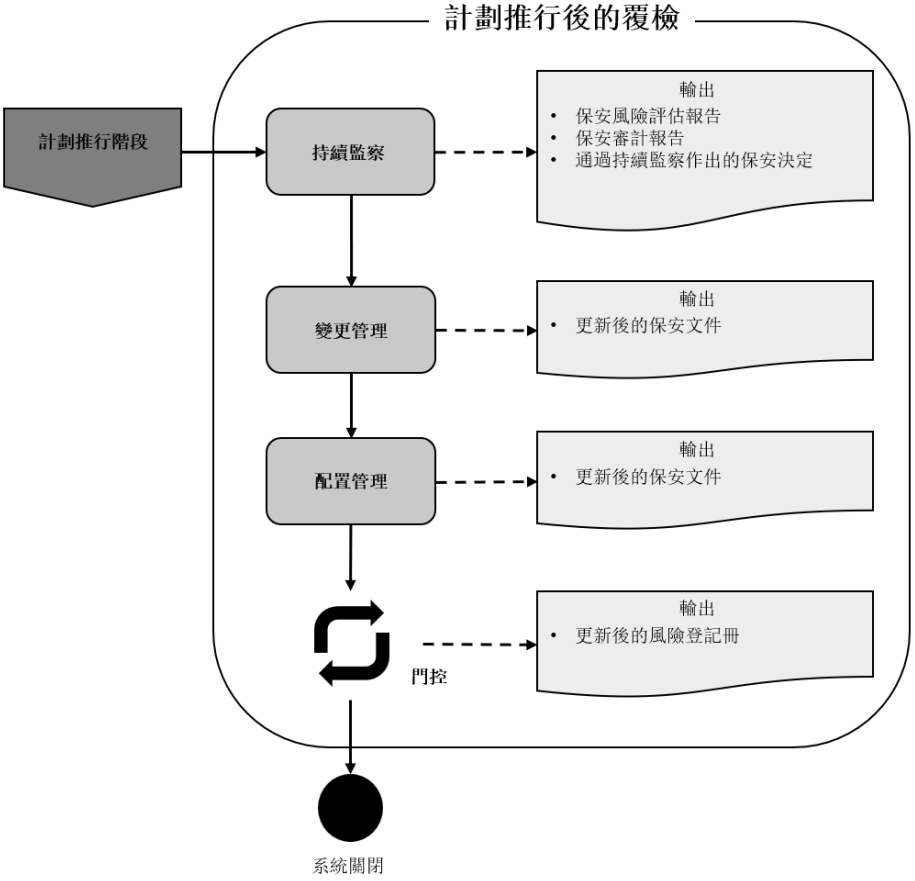

圖 8.1 計劃推行後

8.1.1 持續監察

決策局／部門應定期開展全面的保安風險評估，評估系統保安控制、政策和程序，從而識別潛在保安漏洞或缺陷。持續監察屬於保安審計內容。隨著時間的推移，考慮到系統和環境變更，持續監察是確保保安控制有效性的重要活動。

保安風險評估應包含技術資產、技術保安控制，並涉及對保安政策的全面覆檢，例如與可接受使用和網絡權利相關的政策。這流程將決定行政上保安控制的效力。

通過保安審計，決策局／部門可持續監察保安架構，以驗證保安控制是否按預期運行，並根據任何發現修改或更新保安措施。這種積極主動的方法確保保安措施發展與保安威脅的動態性質和決策局／部門不斷變化的環境保持一致。

8.1.2 變更管理

決策局／部門應以可控且安全的方式管理並執行系統變更，以定期更新保安文件為基礎。系統變更控制不足是系統或安全故障的常見原因。從開發到生產階段，操作環境的任何變更都會顯著影響系統的安全態勢。

為解決此問題，決策局／部門應：

- ***記錄所有建議的變更：***保留所有建議系統變更的詳細記錄，並分析其潛在的安全影響。
- ***更新保安文件：***確保保安文件隨系統的任何變更更新，以反映系統的新狀態以及對保安控制或程序的任何變更。
- ***進行安全影響分析：***在推行變更之前，執行嚴格的安全影響分析，了解變更可能對系統安全性產生的影響。
- ***溝通變更：***與所有持份者溝通任何變更和相關的安全影響，更新培訓材料以補充新的安全實踐。
- ***監察變更推行後：***在推行變更之後，監察系統以驗證保安控制是否依然有效，並且更新的文件是否準確顯示系統的新狀態。

通過此流程，決策局／部門將確保系統安全，及所有持份者可接達最新且準確的安全資訊，從而推動持份者做出明智的決定，並在整個變更管理周期內，維護安全態勢的完整性。

8.1.3 配置管理

配置管理是建立並維護系統保安基準必不可少的環節，可準確控制並保持系統變更清單。鑑於系統配置變更可顯著影響系統保安，因此在配置管理流程中加入更新後的保安文件十分重要。關鍵考量和良好實踐包括：

- ***維持更新後的基準：***建立並記錄配置基準，確保每當發生變更時都會更新此基準。該文件應隨時反映系統配置的當前狀態。

- ***通過文件更新進行持續監察：***持續監察並定期審核配置變更，更新保安文件以擷取系統配置的任何變更。這確保可追蹤和評估所有變更的安全影響。

- ***明文規定的備份和復原程序：***推行並記錄配置備份和復原程序。更新後的保安文件應包括復原程序、職務、職責和時間線，以確保在發生配置相關事故時能迅速復原。

- ***在保安文件中加入配置變更：***確保所有已批准的配置變更及時在保安文件中反映，包括記錄變更理由、保安影響分析，以及推行的任何緩解措施。

- ***自動化工具和人工覆檢：***按照保安程序中的明文規定，利用自動化掃描工具並進行人工覆檢，以驗證配置已正確設置，且符合保安良好實踐。應記錄使用的工具和覆檢的結果，並用於更新保安基準和實踐。

配置管理的目標在於識別和修正可能導致保安漏洞的潛在錯誤配置，進而危及資訊系統保安。在確保配置管理中加入更新的保安文件後，決策局／部門可維持穩健的保安態勢，以回應變化並反映最新的配置狀態

8.2 職務和職責

8.2.1 資訊科技保安管理組

- 對變更管理和配置管理實踐的保安方面提供建議。

8.2.2 資料擁有人

- 確保在持續監察、變更和配置管理活動中考慮資訊的保安分類。

8.2.3 資訊科技保安管理員

- 領導持續監察活動，以識別和評估潛在的漏洞。
- 因系統變更對系統保安產生的潛在影響進行評估。
- 因配置變更對系統保安產生的潛在影響進行評估。
- 協助推行已批准的變更和配置調整。

8.2.4 局部區域網絡／系統管理員

- 執行配置變更和保安修補程式，作為變更管理指令的一部分。
- 通過維護操作保安控制來支援持續的監察工作。

8.2.5 應用系統發展及維修小組

- 確保已安全併入通過持續監察反饋做出的變更。
- 管理應用系統發展和維護中的配置變更。

8.2.6 用戶

- 參與持續監察，報告遇到的任何異常或保安問題。
- 遵行新的配置或變更，作為變更管理溝通的一部分。

8.3 預期輸出／交付

- 保安風險評估報告及其跟進計劃
- 保安審計報告及其跟進計劃
- 通過持續監察作出的保安決定
- 更新保安文件
- 更新風險記錄冊

8.4 門控

使用系統時，決策局／部門應依據用戶反饋、技術變更、政策變更、新出現的威脅和保安漏洞以及其他業務相關問題，定期重新評估系統狀態。建議的控制驗證含：

- 驗證保安風險評估和保安審計報告，確保已處理系統和環境變更。
- 定期覆檢之前的保安風險評估報告和風險記錄冊，確保風險仍然有效並持續處理風險。

控制驗證	**驗證標準**	**門控操作**
持續監察活動	• 內建控制的有效性。 • 監察報告的時間線和準確性。	• 按需要調整監察策略。 • 更新控制配置。 • 提供針對新出現威脅的培訓。
驗證保安風險評估和審計報告	• 風險的相關性和覆蓋範圍。 • 根據系統／環境變更進行充分的控制。	• 更新風險評估方法。 • 修復識別的差距。 • 上報重大風險至高層管理人員。
定期覆檢之前的保安風險評估和風險記錄冊	• 驗證之前的風險評估。 • 風險記錄冊中當前的風險狀態。	• 按照風險的緩急次序採取措施。 • 分配資源作減低風險。 • 更新風險記錄冊。

完