TM-G-1	科技風險管理的一般原則	V.1 – 24.06.03

本章應連同引言與收錄本手冊所用縮寫語及其他術語的辭彙一起細閱。若使用手冊的網上版本，請按動其下面劃了藍線的標題，以接通有關章節。

———————————

目的

就管理科技有關風險時應考慮的一般原則向認可機構提供建議。

分類

金融管理專員以建議文件形式發出的非法定指引

取代舊有指引

本章爲新指引。

適用範圍

所有認可機構

結構

1. 引言
   - 1.1 辭彙
   - 1.2 在附表7下的法律責任
   - 1.3 科技風險管理的一般架構
2. 資訊科技管治
   - 2.1 資訊科技管控政策

---

1. 引言

1.1 辭彙

1.1.1 在本章內，下列用詞涵義如下：

- 「資訊科技」或「科技」指自動化發出、處理、儲存及傳達資訊的方法，包括記錄裝置、通訊網絡、電腦系統（包括硬件與軟件組件及數據）及其他電子裝置；
- 「資訊科技管控措施」指就保安管理、系統 發展與變更管理、資訊處理、通訊網絡及科技服務供應商管理所設的內部管控措施；
- 「資訊科技管治」指機構內的一些組織架構及程序，其作用是使資訊科技的特定任務能配合機構的策略與業務目標，並確保有效利用資訊科技資源及妥善管理科技有關的風險；及

- 「科技風險管理」指能幫助認可機構識別、計算、監察及管控科技有關風險的風險管理系統。

1.2 在附表 7 下的法律責任

1.2.1 認可機構應注意它們有法律責任符合《銀行業條例》附表 7 所訂與其電腦系統有關的最低認可準則。

1.2.2 該附表第 10 段特別規定認可機構要有足夠的會計制度和管控制度；而第 12 段[1]亦規定認可機構須以持正的態度、適度的專業能力，以及無損存戶或準存戶利益的方式經營業務。在這方面，金融管理專員期望認可機構應制定有效的科技風險管理架構，以確保資訊科技管控措施及電腦系統的質素達到足夠的水平。

1.2.3 金管局在現場審查、非現場審查及與認可機構舉行的審慎監管會議期間，將會因應本章所載原則並按適當情況決定認可機構的科技風險管理是否足夠。

1.3 科技風險管理的一般架構

1.3.1 本章的目的是列載金融管理專員要求認可機構的科技風險管理應考慮的一般原則，以補充IC-1「風險管理的一般措施」。有關管理電子銀行的科技有關風險的詳細指引，將於另一章TM-E-1「電子銀行的監管」討論。

[1] 如《認可指引》所載，金融管理專員在判斷某機構是否以審慎及具適度的專業能力的方式經營業務時，將會顧及該機構的電腦系統質素等因素。

1.3.2 由於認可機構愈來愈依賴利用科技來提供銀行服務，認可機構使用科技資源不當可能會構成重大風險，以下爲其中的一些例子：

- 因科技有關投資的錯誤決定而造成的策略性風險；
- 因支援關鍵銀行服務的科技資源遭到未經授權接達或干擾而引致的操作風險；及
- 因處理客戶資訊或交易的電腦系統的保安系統遭到重大破壞或因電腦系統不能使用而造成的信譽風險及法律風險。

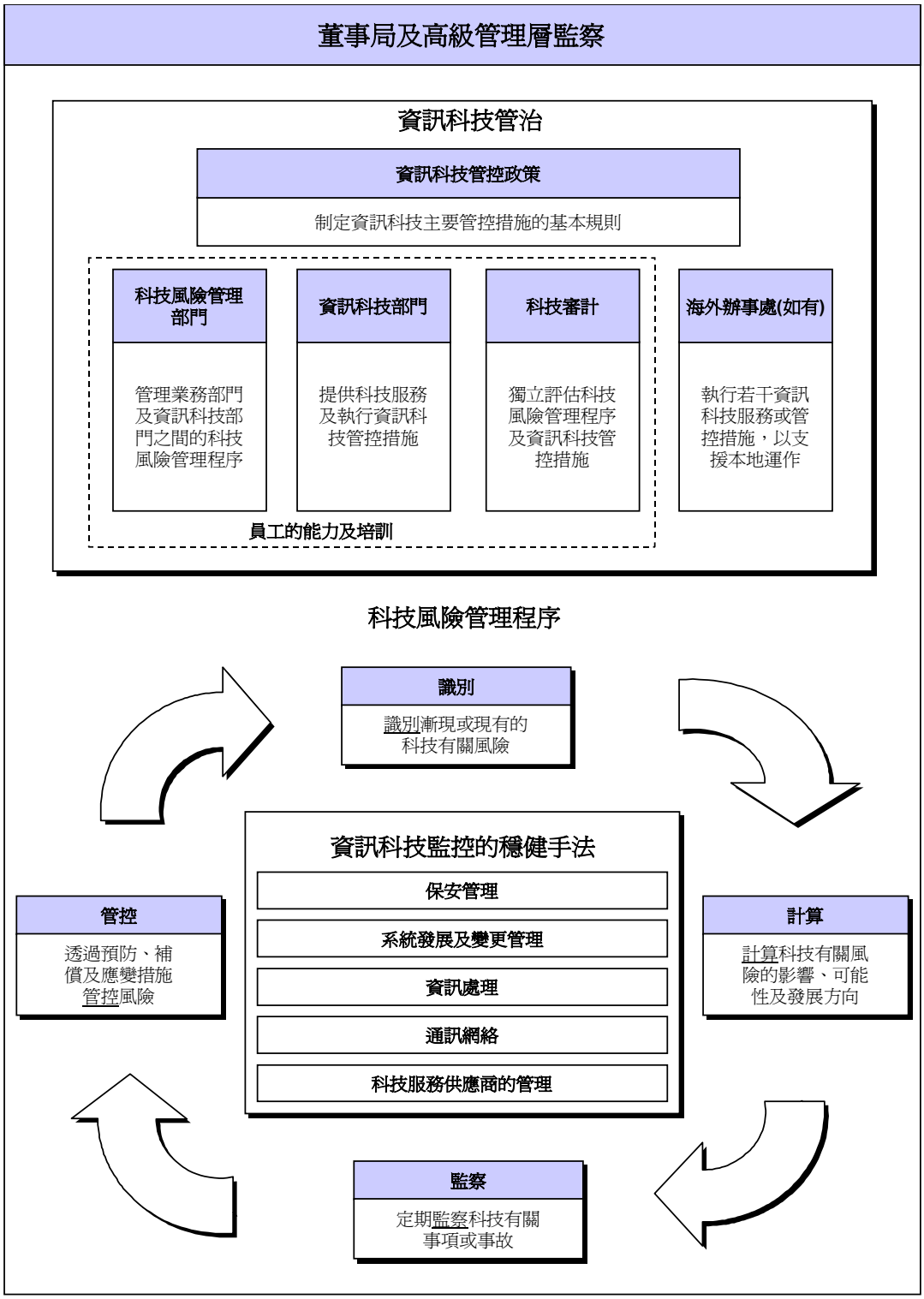
1.3.3 如IC-1「風險管理的一般措施」所載，董事局負有最終責任，了解認可機構所承擔的風險及確保妥善管理有關風險；高級管理層則有責任設計及實施經董事局[2]或其指定委員會核准的風險管理制度。爲達到這個目的，高級管理層應制定有效的科技風險管理架構[3]。一般而言，這個架構包含資訊科技管治、持續科技風險管理程序及就資訊科技管控執行穩健的實務手法。

1.3.4 一般的原則是，認可機構應推行「切合目的」的科技風險管理架構。換言之，該架構應能配合個別認可機構的業務類別所涉及的風險、其所採用的科技及整體

[2] 就本章而言，如爲境外註冊認可機構，董事局對其在香港業務的科技風險管理進行的監察，應由本地高級管理層負責。

[3] 認可機構可從其他資源參考科技風險管理或資訊科技管控措施的資料，如 ISO/IEC 17799:2000《資訊科技—資訊保安管理實務守則》(英文版)(www.iso.ch)、資訊系統審計及管控協會 (www.isaca.org) 、資訊科技管治組織 (www.itgovernance.org) 及資訊保安論壇 (www.securityforum.org)。

風險管理制度。以下概覽科技風險管理的一種穩健架構：


董事局及高級管理層監察
資訊科技管治
資訊科技管控政策
制定資訊科技主要管控措施的基本規則
科技風險管理部門
管理業務部門及資訊科技部門之間的科技風險管理程序
資訊科技部門
提供科技服務及執行資訊科技管控措施
科技審計
獨立評估科技風險管理程序及資訊科技管控措施
海外辦事處(如有)
執行若干資訊科技服務或管控措施，以支援本地運作
員工的能力及培訓
科技風險管理程序
識別
識別漸現或現有的科技有關風險
資訊科技監控的穩健手法
保安管理
系統發展及變更管理
資訊處理
通訊網絡
科技服務供應商的管理
管控
透過預防、補償及應變措施管控風險
計算
計算科技有關風險的影響、可能性及發展方向
監察
定期監察科技有關事項或事故

2. 資訊科技管治

2.1 資訊科技管控政策

2.1.1 若要在整個認可機構內，就資訊科技管控的穩健手法維持貫徹標準，便須得到董事局及高級管理層的明確指示及承擔。在這方面，高級管理層（可由指派的小組委員會協助）應負責制定一套資訊科技管控政策，以便定出資訊科技管控的基本規則。這些政策應經董事局或其指定委員會正式核通，並由各資訊科技及業務部門執行。

2.1.2 一般而言，資訊科技管控政策最低限度應涵蓋本章第3節至第7節所載五方面的資訊科技管控措施。這些政策應定期檢討，如有需要便應更新修訂，以配合不斷改變的操作環境及科技發展。

2.1.3 高級管理層應確保明確制定用以查核有否遵守資訊科技管控政策的程序，以及要求核准豁免遵守資訊科技管控政策的程序。高級管理層亦應訂明未有依從這些程序會帶來的後果。整體而言，個別業務部門及資訊科技部門應在科技風險管理部門（見以下第2.3節）的協助下，負責確保本身遵守資訊科技管控政策及要求核准豁免遵守這些政策的程序。

2.1.4 高級管理層可制定適當機制（如定期發出通告提醒有關員工及爲新入職員工介紹有關政策）以定期提醒有關員工注意資訊科技的管控政策。

2.2 資訊科技部門的監察及組織架構

2.2.1 高級管理層應爲資訊科技部門制定有效的組織架構，以便爲業務部門提供科技服務及日常的科技支援。認可機構應以明文記錄清晰的資訊科技組織架構及個別資訊科技部門的職責，並由高級管理層核准。

2.2.2 適當分隔資訊科技部門內及部門之間的職責[4]，對確保維持有效的資訊科技管控環境具關鍵作用。如認可機構難以分隔某些資訊科技管控的職責，便應制定足夠的管控措施以作補償（如員工之間互相監督），從而減少有關的風險。

2.2.3 認可機構宜設立資訊科技規劃或督導委員會，負責監察認可機構本身是否有效利用資訊科技資源，以支持業務策略。一般而言，這個委員會的成員應包括高級管理層、主要業務部門及資訊科技部門的代表。委員會應定期開會，並向高級管理層匯報與科技有關的主要計劃的進展及資訊科技方面的重大事項。在適當情況下，委員會更應向董事局或其指定委員會作出上述匯報。

2.2.4 整體而言，資訊科技規劃或督導委員會亦應負責制定資訊科技策略，涵蓋與科技有關的短期及長期計劃。資訊科技策略應能顧及新的業務計劃、組織架構變動、科技革新、法規要求、員工及有關管控的事項。這項策略應以明文正式記錄，並經董事局或其指定委

[4] 例如，系統發展人員不得接達生產系統。保安管理的人員不應再被委派執行與其職能有衝突的職責，如系統發展、電腦操作或技術支援。

員會及高級管理層正式認可，同時最少每年檢討及更新一次。

2.3 科技風險管理部門

2.3.1 IC-1 「風險管理的一般措施」指明認可機構應制定有效的風險管理制度，新的產品及服務亦須經過審慎評估（包括詳細的風險評估），推出後再進行檢討。同樣的風險管理管控措施，亦適用於認可機構的科技風險管理工作。

2.3.2 高級管理層應清楚訂明認可機構內哪個部門負責執行及管理科技風險管理程序（即科技風險管理部門）。視乎個別認可機構的業務及操作需要而定，科技風險管理部門可以指認可機構內的一個專責部門，或是多個部門或支援小組共同履行科技風險管理部門的職責。

2.3.3 科技風險管理部門應負責協助業務部門及資訊科技部門執行科技風險管理程序，以識別、計算、監察及管控科技有關的風險。此外，這個部門須協助確保員工注意及遵守認可機構的資訊科技管控政策，並就調查科技有關的詐騙活動及事件提供支援。

2.3.4 科技風險管理部門應確立正式的科技風險確認及接受程序，以檢討、評估及核准不遵守資訊科技管控政策的重大事件。不遵守的常見理由包括科技限制（如某些專有操作系統只可提供簡單的密碼管控措施）、業務限制（如對客戶服務有不利影響）及成本與得益不成比例。這個程序包括：

- 說明由風險擁有人所考慮確認的風險，及評估將會接受的風險；
- 識別用作減輕風險影響的管控措施；
- 制定補救方案以減少風險；及
- 風險擁有人及高級管理層對風險確認的核准。

2.4 科技審計

2.4.1 IC-1「風險管理的一般措施」載述認可機構內部審計部門的一般目標及其獨立性與專業水平的重要。關於科技審計，認可機構應定期評估其科技風險管理程序及資訊科技管控措施。爲確保科技審計涵蓋資訊科技管控環境及關鍵電腦系統，認可機構應制定年度科技審計計劃。認可機構亦應確保適當追溯審計事項，尤其要全面記錄及跟進，以及作出令人滿意的糾正。

2.4.2 部分認可機構的內部審計部門可能較難累積內部的科技審計專業水平。在這些情況下，科技審計支援工作可由外聘專家或同一銀行集團其他辦事處的內部科技審計人員提供支援。

2.5 員工的能力及培訓

2.5.1 鑑於科技發展迅速，高級管理職應確保資訊科技、科技風險管理及內部科技審計部門的員工均具備適當能力，並持續符合所需的專業及經驗水平。此外，確保員工編制足以應付現有及預期的工作量，並能合理地應付員工流失，亦很重要。

2.5.2 爲確保資訊科技員工有足夠的培訓計劃，認可機構必須確立適當程序，辨察負責科技有關職能的員工是否

存在重大的技術差距[5]。認可機構可鼓勵員工（如負責保安管理、科技風險管理及科技審計的員工）考取有關的專業資格，如有需要更應作出適當配合。

2.6 海外辦事處所提供的資訊科技支援

2.6.1 部分認可機構可能倚賴海外辦事處（如母銀行、附屬機構、總辦事處或同一銀行集團其他地區辦事處）或與其合作以執行某些資訊科技管控措施或支援工作。高級管理層應確保在有關文件內（如政策、程序或服務協議）清楚列明本地及海外辦事處在這些環節上的職責。

3. 保安管理

3.1 資訊分類及保障

3.1.1 認可機構宜就每個應用系統指定一位人士爲資訊擁有人[6]。資訊擁有人一般需與科技風險管理及資訊科技部門合作，以確保資訊保密及完整，並依照現有及預計的風險水平保障資訊。

3.1.2 資訊可按敏感程度（如高度敏感、敏感、內部及公開）分爲不同類別，以顯示所需的保障程度。爲協助分類，認可機構最理想的做法是制定每個類別的指引及定義，並闡明按照分類制度制定保障資訊的適當程

[5] 爲識別是否存在技術差距，認可機構可預先訂明某特定職位或崗位的一系列技術要求，包括列出所需具備的知識、資格及經驗，然後以此來評估人員的技術水平。

[6] 資訊擁有人是指獲委派爲某應用系統的業務擁有人，並負責保障這個系統所處理及儲存的資訊。

序。認可機構資訊分類制度的詳細程度，應切實可行及配合認可機構的具體情況。

3.1.3 不論採用哪種媒介（如紙張及電子媒介）備存資訊，認可機構均應制定資訊保密的保障措施。認可機構應確保所有媒介受到適當保護，並確立穩妥的程序，以棄置及銷毀存放在紙張及電子媒介的敏感資訊。

3.1.4 若以加密技術來保障認可機構資訊的保密及完整性，認可機構應採用業內認可的加密解決方案及穩健的密碼匙管理手法，以保護有關的加密密碼匙。一般而言，穩健的密碼匙管理手法包括：

- 就加密密碼匙的產生、分發、儲存、輸入、使用及存檔提供穩妥的管控環境，以免該匙遭到修改及在未經授權下被泄露。特別值得注意是，認可機構宜採用能抵抗擅自改動的儲存方法，以防止加密密碼匙被泄露；及
- 就加密密碼匙制定適當的非現場備份及應變安排，而這些安排須獲得與製造加密密碼匙相同的保安措施保障。

3.2 認證及接達管控

3.2.1 接達資訊及應用系統應以適當的認證機制來限制，並輔以接達管控規則。接達管控規則訂明用戶可以接達何種應用功能、系統資源及數據。每個應用系統均須利用對每一用戶獨有的用戶身分鑑別碼（如用戶識別碼）及適當的認證方法（如密碼）來識別所有用戶，以確保他們就其進行的活動負責。

3.2.2 認可機構應制定有效的密碼規則，以確保不會使用容易被猜中的密碼，並定期更改密碼。較高風險的交易或活動（如支付交易、財務交易訊息及流動資訊處理）[7]應採用更嚴格的認證方法。在這些情況下，用戶認證一般結合多項元素，用戶須憑其所知（如密碼）與所持物件（如聰明卡或硬件保安權標）以證明其身分。

3.2.3 管控特權及緊急用戶身分識別碼[8]的使用及接觸方法應特別審慎。認可機構必須設立的管控措施包括：

- 只是絕對必要的權力才會授予特權及緊急用戶身分識別碼；
- 發放特權及緊急用戶身分識別碼以供使用前，應由適當人員正式核准；
- 以特權或緊急用戶身分識別碼進行的活動均須接受監察（如員工之間互相監督活動記錄）；
- 適當保管特權及緊急用戶身分識別碼及密碼（如收藏於已封口信封及鎖在數據中心內）；及
- 要求使用者交回特權及緊急用戶身分識別碼後，立即更改該密碼。

[7] 流動資訊處理包括從辦公室範圍以外的遙距地點接達到認可機構的電腦資源（如使用筆記簿電腦及其他 流動裝置）。

[8] 特權及緊急用戶身分識別碼，是按特許權力設立並擁有較多的系統資源接達權。一般而言，這些用戶身分識別碼的作用是爲了進行系統管理（即系統管理員身分識別碼），或在生產環境遇到系統問題時，引入緊急解決方案。

3.3 保安管理及監察

3.3.1 認可機構應設立保安管理部門及制定正式程序，以管理系統資源及應用系統接達權的分配，並監察系統資源的使用，以偵測是否有異常或未經授權進行的活動。這個職能尤其應涵蓋下述環節：

- 須經資料擁有人正式核准後，才授予、更改及撤銷接達權。認可機構尤其應制定適當程序，以確保用戶離開該機構或其職責已無需使用接達權時其有關的接達權會被撤銷；
- 確保定期再核證（如每年一次）用戶接達權，以確定用戶接達權仍然切合實際需要，並從系統中撤銷過時用戶戶口；
- 及時檢討保安記錄與違反報告；及
- 進行事故分析、報告及調查。

3.3.2 認可機構應適當分隔保安管理職能內的職責，或採取其他補償管控措施（如員工之間互相監督），以減少保安管理職能未經授權進行活動的風險。

3.3.3 認可機構應制定事故回應及通報程序，以處理在辦公時間或其他時間所發生與資訊保安有關的事故。事故回應及通報程序應包括及時向金管局匯報任何已確定與資訊科技有關的欺詐活動、或保安系統遭到重大破壞的事件。

3.4 系統保安

3.4.1 認可機構應制定管控程序及底線保安規定，以保障應用程式、操作系統、系統軟件及資料庫。例如：

- 應以適當的識別及認證用戶身分的方法，並輔以合適的授權安排，以管控資料及程式的接達；
- 應定期檢查靜態資料（如系統參數）的完整性，以偵測是否有未經授權的更改；
- 應以穩妥方式裝設及設定操作系統、系統軟件、資料庫及伺服器，以符合原擬用途的需要，並確保所有不必要的服務及程式被調校至失效或被移除。應考慮使用保安工具，以加強關鍵系統及伺服器的保安；
- 應制定清晰的員工責任，以確保機構能及時識別、評估及測試有關供應商不時開發的必需修補程式及保安更新程式，並適時地應用於有關系統內；
- 應以明文適當記錄操作系統、系統軟件、資料庫及伺服器所有裝配及設定，並定期核證保安設定（如由科技風險管理部門或科技審計部門負責）；及
- 對於系統及用戶的活動，應制定足夠的記錄，並進行充足的監察，以偵測不正常的活動，有關的記錄資料應穩妥保管，以免遭到篡改。

3.5 終端用戶電腦應用及流動資訊處理

3.5.1 終端用戶電腦應用[9]或可爲認可機構帶來多種好處（如提高生產力），但亦可能令機構更難於管控電腦系統的質素及接達。因此，認可機構應按需要制定終端電腦應用的管控手法及責任，以涵蓋數據保安、文件記錄、數據／檔案儲存及備份、系統復原、審計責任及培訓等環節。

3.5.2 流動資訊處理必須受到管控，以管理在無保護的環境下工作的風險。爲保障認可機構的資訊，認可機構應制定適當的管控措施，包括：

- 用戶要求流動資訊處理的核准程序；
- 遙距式接達網絡、主機數據及／或系統的認證管控措施；
- 流動資訊處理所需設備及裝置的保障（如防範盜竊及惡意軟件的影響）；
- 使用數據加密軟件，以保護在流動環境及傳送期間的敏感資料及業務交易；及
- 爲流動資訊處理設備內的數據及／或系統進行備份。

3.5.3 軟件及資訊處理設施容易受到電腦病毒及其他惡意軟件的攻擊。認可機構應制定程序及責任以偵測及防範這些攻擊。認可機構應制定足夠的管控措施，例如：

[9] 終端用戶電腦應用是把集中式數據中心的資訊處理及系統發展能力，轉移至用戶的桌上 電腦。

- 禁止下載及使用未經許可的檔案及軟件，並禁止接達可疑的網址；
- 裝設由可信賴的供應商提供的抗電腦病毒軟件，並及時更新；
- 禁止下載可執行檔案及流動程式碼[10]，尤其已知容易受攻擊的一類（如透過設立企業防火牆及適當裝設瀏覽器軟件）；及
- 迅速及定期爲所有電腦裝置及流動用戶電腦進行電腦病毒掃描，並設立處理電腦病毒感染的復原程序。

3.6 實體及人員保安

3.6.1 認可機構應制定實體保安措施，以保障電腦設施及設備免受破壞或未經授權接達或接近。關鍵資料處理設施應設置於保安區內，例如設有適當保安屏障及進入管控措施的數據中心及網絡設備室。保安區應只限獲授權人員才可進入，進入權亦應定期檢討及更新。標示有關建築物性質的資料應盡量減少，並且無明顯牌示表明裏面設有資訊處理設施。

3.6.2 認可機構爲數據中心選址時應充分考慮環境風險因素（如鄰近具危險性的工廠）。此外，認可機構應執行實體及環境的管控措施，以監察可能會對資訊處理設施的操作造成不利影響的環境因素（如火災、爆炸品、煙霧、溫度、滲漏及塵污）。設備及設施應受保

[10] 流動程式碼指由瀏覽器從網址自動下載以執行工作的小型程式。

護，例如裝設不間斷電源供應器及後備發電機，以免受到停電及供電干擾影響。

3.6.3 爲管控第三方人員（如服務供應商）進入保安區，認可機構應有正式核准進入的程序，並緊密監察他們的活動。此外，應就聘用長期及臨時性質的科技人員及合約員工設立適當的審查程序（包括核實身分及背景審查）。對與敏感的科技有關職位來說，此舉更爲重要。

4. 系統發展及變更管理

4.1 計劃管理

4.1.1 認可機構應制定管理跟科技有關的主要計劃的整體架構。這架構其中一個目的是要指明這些計劃所應採納及應用的項目管理方法。這套方法最低限度應涵蓋責任分配、活動細分說明、時間及資源預算、主要進程標誌與階段、主要倚賴因素、質量保證、風險評估及批核等環節。

4.2 計劃周期

4.2.1 認可機構應制定及執行一套完整的計劃周期方法，以監管發展、執行及維修主要電腦系統的過程。一般而言，這套方法應涵蓋計劃的開展、可行性研究、訂明需求、系統設計、程式發展、系統及驗收測試、培訓、執行、操作及維修等階段。

4.2.2 計劃周期方法應明確訂明計劃工作小組的角色及責任，以及每個階段應完成的出品。此外，這套方法亦

應制定適當程序，以確保在制定業務需求時能識別適當的保安需求，並在程式發展時建立、然後測試及執行這些需求。

4.2.3 應由無涉及計劃發展的獨立一方（如質素保證部門、科技風險管理部門或科技審計小組）就跟科技有關的主要計劃進行質素保證檢討；如有需要，法律及法規遵行部門宜提供協助。檢討工作的目的是確保遵守計劃周期方法、其他內部政策、管控規定、規例及適用法律條文。

4.2.4 應制定正式的驗收程序，以確保只有經正式測試及核准的系統才可提升至生產環境。系統及用戶驗收測試應在獨立於生產環境以外的環境進行。除非數據的敏感內容已被刪除（即不會透露個人或敏感資料）及事先獲得資訊擁有人核准，否則生產數據不應用於發展或驗收測試。新發展的系統亦應經過性能測試，才可提升至生產環境。

4.2.5 購置套裝軟件是內部發展系統以外的一個方法，並應接受與計劃周期大致接近的管控措施。由於不適當處理軟件使用權可能會使認可機構承受侵犯專利及財政與信譽損失的重大風險，認可機構應制定正式的購置套裝軟件程序。這個程序尤其應包括對套裝軟件（如關於軟件使用權、功能、系統性能及保安規定）及供應商（如關於其財政狀況、信譽及技術能力）的詳細評估。

4.2.6 認可機構應確保軟件供應商提供套裝軟件的持續維修及足夠支援，並以協議正式訂明。至於關鍵的套裝軟

件，認可機構可考慮在合約內加入一項託管的協議，准許認可機構在某些情況下（如軟件供應商終止業務）取得套裝軟件的源碼。

4.3 變更管理

4.3.1 變更管理是規劃、預定、施行、分配及追溯應用系統、系統軟件（如操作系統及實用程式）、硬件、網絡系統及其他資訊科技設施與設備的變更的程序。有效的變更管理程序有助確保生產環境的完整性及可靠性。認可機構應制定正式的變更管理程序，其中包括：

- 將變更分類及安排優先次序，並確定變更的影響；
- 每個有關一方的角色及責任，其中包括資訊科技及終端用戶部門，並適當分隔有關的職責。此舉可確保沒有單一個人可以未經其他授權人員審核及批准而對生產環境造成變動；
- 程式版本管控及審計追蹤記錄；
- 預定、追溯、監察及執行變更，以盡量減少對業務的影響；
- 遇有提升變更至生產環境的問題時，可以把變更還原，以恢復原有的程序、系統裝設或數據；及
- 執行後核實所作的變更（如檢視主要修訂的版本）。

4.3.2 爲了能及時和以受控制的方式處理未有預見的問題，認可機構應制定正式的管理應急變更程序。機構應在

作出應急變更時，由資訊擁有人（就應用系統或生產數據有關的變更而言）及其他有關方面核准這些變更。若需急切作出變更，而徵求資訊擁有人核准並不切實可行，便應在執行變更後盡快（如下一個營業日）徵求資訊擁有人的同意。

4.3.3 應急變更應有記錄及備份安排（包括舊有及變更後的程式版本與數據），以便有需要時復原舊有的程式版本與數據檔案。應急變更應經獨立人員審核，以確保變更適當，並且不會對生產環境造成不利影響。作出應急變更後，應透過正式的驗收測試及變更管理程序以適當的修補來取代。

5. 資訊處理

5.1 資訊科技操作管理及支援

5.1.1 資訊科技部門的管理層最理想的做法，是與業務部門制定服務水平協議，以涵蓋系統的可供使用情況及性能要求、增長容量及向用戶提供支援的水平。負責的資訊科技部門應確保制定適當程序，以管理議定的科技支援及服務的提供。

5.1.2 電腦操作員工作及工作時間安排與執行（如處理資訊、時間安排規定及系統內部管理活動）等詳細操作說明，應於資訊科技操作手冊內明文記錄。資訊科技操作手冊亦應載明生產及發展環境的數據及軟件備份的程序及規定（如備份的頻密次數、範圍及保留期），以涵蓋現場與非現場的備份安排。

5.1.3 認可機構應制定事故管理系統，以就資訊科技操作事故作出迅速回應，向有關的資訊科技管理人員匯報事故，以及記錄、分析與追蹤所有這些事故的發展，直至事故獲得修正爲止。認可機構可成立中央求助台，就與科技有關的所有事故爲用戶提供前線支援，並將事故轉介有關部門調查及解決。

5.2 性能監察及容量規劃

5.2.1 認可機構應制定適當的程序，以確保持續監察應用系統的性能，並及時與全面地匯報例外情況。監察性能的程序應包括預測功能，以防患未然，在問題未對系統性能造成影響時，已能及早識別及糾正。在同時顧及規劃中的業務策略的情況下，這個程序應有助擬備工作量預測，以便識別趨勢，以及提供容量計劃所需的資訊。

5.2.2 除生產環境外，容量規劃應擴展至後備系統及有關設施。

5.3 資訊科技設施及設備維修

5.3.1 爲確保認可機構與科技有關的服務持續可用，認可機構應按照業內手法及供應商建議的檢修頻密次數與規格說明，維修及檢修資訊科技設施與設備（如電腦硬件、網絡裝置、配電、不間斷電源供應器及空調設備）。妥善保存記錄（包括懷疑或實際故障，以及預防與修理性質的維修記錄）是維持有效的設施及設備維修的必要環節。認可機構應備存硬件及設施的詳細清單，以便管控及追溯所有購入及租用的硬件與軟件。這些記錄亦可用作定期盤點庫存。

5.4 災難復原規劃

5.4.1 認可機構應制定資訊科技的災難復原計劃，以確保關鍵應用系統及科技服務可按照業務復原規定恢復正常。有關如何制定應用系統及科技服務的詳細復原程序，以及確保資訊科技資源有適當的保險安排，請參閱TM-G-2「持續業務運作規劃」。

6. 通訊網絡

6.1 網絡管理

6.1.1 通訊網絡負責傳送資訊，及提供接達應用系統及系統資源的渠道。鑑於本身的技術複雜性，通訊網絡有可能很容易被干擾及濫用。保障通訊網必須有穩健的網絡設計、清楚闡明網絡服務及保持良好的網絡管理紀律。

6.1.2 認可機構應明確指定由何人負責網絡管理的整體責任，而這些人須具備適當的知識、技術及資源以履行職責。網絡標準、設計、圖表及操作程序應以明文正式記錄，並且按需要更新及傳達予所有有關網絡員工，另亦應定期作出檢討。

6.1.3 認可機構應識別出對網絡服務的持續不斷性具關鍵作用的通訊設施。並且應設立備用路徑，以備關鍵節點或鏈路失靈時，可自動重訂通訊的路線，從而盡量減少單一點故障（如把關鍵鏈路的路線連接至多於一個對外交換中心，以及預先安排由備用通訊服務供應商提供服務）。

6.1.4 認可機構應持續監察網絡，以減少網絡交通超負荷的機會，及偵測網絡是否有被侵入。監察活動包括：

- 按照預先訂明的目標監察網絡服務及性能；
- 檢討網絡交通量、網絡設施使用情況及任何潛在的交通阻塞點或超負荷情況；及
- 按照常見的攻擊特點偵測異常的網絡活動。

6.1.5 強力的網絡分析及監察工具（如規約分析器、網絡掃描及網絡嗅探工具）通常用作監察網絡性能及偵測潛在或實際的侵入活動。這些強力的網絡工具應受保護以免在未經授權下被使用（如檢視未經加密的敏感資訊）。此外，網絡工具亦應嚴格只限於獲授權員工使用，並依循嚴格的核准及檢討程序。

6.2 網絡保安及核證

6.2.1 爲防止不安全連接接通認可機構的網絡，認可機構應制定及執行有關使用網絡及網絡服務的程序。這些程序應涵蓋：

- 可用的網絡及網絡服務；
- 授權程序，以確定誰人可以接達特定的網絡及網絡服務；及
- 管控措施及程序，以保護接達至網絡接達點、網絡連接及網絡服務。

6.2.2 認可機構應考慮把內部網絡分隔成爲不同部分，而其中應顧及儲存於每個部分的數據，或連接至每個部分的系統所需的接達管控。例如，生產系統應設於獨立於其他部分以外的專用網絡部分，以使生產網絡交通

與其他交易（如連接至互聯網、透過外聯網連接至外方以及市場數據資料）分隔。不同網絡部分之間的敏感數據交通，應予適當管控及保障，以免遭到篡改。

6.2.3 定期檢討網絡裝置（如路由器、防火牆及網絡伺服器）的保安參數設定，以確保這些裝置仍切合當前需要。應備存及定期檢討關鍵網絡裝置每日活動的審計追蹤記錄。網絡操作人員應即時獲通知有關可能出現的破壞保安系統活動。

6.2.4 就要求增補或變動認可機構企業網絡的局部區域網絡（LAN）或寬廣區域網絡（WAN）時，應進行網絡核證[11]。這些增補或變動涵蓋撥入或撥出埠、交換器、終端伺服器、網間連接器／伺服器、路由器、外聯網及公用的互聯網。網絡核證程序包括收集網絡環境的數據、分析容易出現問題的地方及有關的管控措施，以及明文記錄是否已獲得核准，或須符合哪些附加的管控措施才獲核准以進行連接。

6.3 無線局部區域網絡

6.3.1 如設置無線局部區域網絡（WLAN），認可機構應制定核准、裝置、操作及管理無線局部區域網絡的政策及程序。實施無線局部區域網絡前，應制定風險評估程序，以評估可透過無線局部區域網絡接達的資訊的敏感度。認可機構亦應制定有關無線局部區域網絡產品的標準保安裝置設定，並依循網絡核證程序，以確

[11] 網絡核證指一評估程序，其目的是確保網絡裝置及基礎設施的增補或變動，不會導致企業網絡其他部分容易出現問題。網絡核證可爲網絡變更管理程序的一部份。

保以穩妥方式實施無線局部區域網絡，使企業網絡不會面對未受管理的風險。

6.3.2 無線工作站與連線網絡之間可能需要額外的保安措施，以提供較強力的加密安排及互相認證。無線局部區域網絡應從企業網絡中分隔出來（如利用防火牆），以防止在未獲授權的情況下透過無線局部區域網絡接達企業網絡。

7. 科技服務供應商的管理

7.1 科技外判的管理

7.1.1 認可機構管理科技外判[12]時除了須注意SA-2「外判」所載的一般指引外，亦應考慮採用下列的管控措施：

- 科技服務供應商應具備足夠資源及專業知識，以遵守認可機構資訊科技管控政策的實質內容；
- 如外判關鍵科技服務（如數據中心操作），認可機構應詳細評估科技服務供應商的資訊科技管理環境。該估計最理想是由獨立於服務供應商以外的一方進行。獨立評估報告應清楚列明評估的目的、範圍及結果，並提交金管局以供參考。

[12] 與 SA-2「外判」一致，「科技外判」指由另一方承諾向認可機構提供之前由認可機構自行提供的科技服務，或認可機構將會推出的新科技服務的安排。科技服務可外判予香港或海外服務供應商，而服務供應商可以是隸同一認可機構的單位（如總辦事處或海外分行）、認可機構所屬集團的聯繫公司或獨立第三者。

- 外判協議應清楚載明科技服務供應商的表現標準及其他責任[13]，以及軟件與硬件擁有權的事項等。由於科技服務供應商可能會進一步把服務分包由其他方負責，認可機構應考慮加入一項條文，規定科技服務供應商把服務的重大部分分包時，須向認可機構發出通知或獲得核准，以及規定原有的科技服務供應商仍須就分包服務負責。
- 除SA-2「外判」所載的定期監察外，認可機構亦應進行年度評估，以確保關鍵的科技服務供應商有足夠的資訊科技管控環境；
- 認可機構應盡量避免過度倚賴由單一個外方服務供應商提供關鍵的科技服務；及
- 認可機構應就已外判的關鍵科技服務制定應變計劃，以免因未料到的科技服務供應商問題，而導致服務無法可用[14]。這可以包括制定退出管理計劃及物色額外或候補的科技服務供應商，以提供這些支援及服務。

7.2 其他科技服務供應商的管理

7.2.1 除科技外判外，認可機構可能會倚賴一些外聘的科技服務供應商，提供跟科技有關的支援及服務（如電訊及網絡操作）。認可機構應制定有關如何管理各類主要外聘科技服務供應商的指引。與SA-2「外判」

[13] 這些責任可包括：科技服務供應商須確保其職員或代理人所取得的認可機構的資訊得到保密，以及遵守認可機構有關的資訊科技管控政策與程序。

[14] 服務供應商可能會變成無力償還債項，或因其他困難而無法繼續提供有關服務及支援。

及上文第7.1節所載的一般原則接近，這些指引或需包括揀選服務供應商的程序、核准重大例外情況的程序，以及注意避免過度倚賴單一個科技服務供應商提供關鍵科技服務。

———————————

目錄	辭彙	首頁	引言