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

列載金管局對認可機構的電子銀行服務的監管模式，以及向認可機構提供有關電子銀行風險管理一般原則的指引。

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

第15.1號指引「電子銀行業務」，發出日期爲1997年7月7日

第15.1.1號指引「在互聯網進行銀行交易的保安」，發出日期爲1997年11月25日

第 15.3 號指引「有關網上銀行業發展的公開密碼匙基礎建設及法律環境」，發出日期爲 1998 年 10 月 7 日

「電子銀行服務的保安風險管理建議文件」通告，發出日期爲2000年7月6日

「電子銀行交易的保安事宜獨立評估建議文件」通告，發出日期爲2000年9月20日

「有關涉及虛假電郵或網站的海外騙案」通告，發出日期爲2003年5月19日

適用範圍

所有認可機構

結構

1. 引言

    1.1 詞彙

附件A： 獨立評估的範疇及報告

附件B： 設立互聯網基礎建設的穩健方法

————————————

1. 引言

1.1 詞彙

1.1.1 本章所用的詞彙釋義如下：

- 「非武裝區」指在可信的內部網絡與外部網絡（如互聯網）之間插入的網絡分段，以防止他人從外部網絡直接進入可信的內部網絡，反之亦然；
- 「電子銀行」指利用互聯網傳送保密客戶資料（包括進行交易）的銀行服務[1]。就本章而言，電子銀行包括提供予個人、公司及機構客戶的服務；
- 「防火牆」指用作檢查在兩個或以上網絡（例如可信的內部網絡、非武裝區及互聯網）之間流通的信息小包、信息小包模式及網絡的服務，以確定應否准許信息小包及網絡的服務進入上述網絡或在網絡之間通過；
- 「入侵偵測系統」指由主機、伺服器或網絡收集有關信息的系統，以偵測入侵及濫用電腦資源的跡象，以及將該等活動通知有關人員；及
- 「路由器」指用作引導網絡間之交通的網絡設備。路由器經常被用作電腦網絡的保安設備，使網絡系統只容許來自某個網絡的某些類別信息小包及網絡服務進入另一個網絡。

[1] 電子銀行不包括：(i) 自動櫃員機或經私人網絡連接的自助服務機；(ii)電話銀行服務；(iii)經撥號電話線連接的個人電腦銀行；及(iv)不涉及經互聯網連接的流動電話銀行服務。

1.2 背景

1.2.1 電子銀行服務的發展爲認可機構帶來風險，亦帶來益處。雖然一般來說認可機構對電子銀行服務所帶來的風險類別並不陌生，但電子銀行的特性可能會在某程度上令認可機構的風險狀況有所改變，在風險管理方面帶來新的挑戰。特別是：

- 互聯網是全球性的開放式網絡，任何人士都可以從世界任何地方進入互聯網。認可機構不能夠直接控制互聯網及客戶用以連接電子銀行的設備的保安措施，因此認可機構在保安事故及服務中斷方面會承受更大的業務操作風險；
- 由於認可機構日益倚賴電子銀行技術以及技術越趨複雜，可能令認可機構越加倚重外聘技術服務供應商（例如電訊公司及應用程式與保安設備供應商），最終增加認可機構的業務操作風險及信譽風險；
- 認可機構決定應否及應在何時推出電子銀行服務項目，可能是一項策略性挑戰，尤其是當認可機構不能確定提供或維持有關服務的效益會否超過初期投資及維持適當水平的保安所需的持續支出；及
- 若海外監管當局認爲有關服務是以海外人士爲對象，並規定認可機構須申請在有關地區的認可資格，電子銀行便可能會令認可機構面對信譽及法律風險。

2. 監管模式

2.1 監管目的

2.1.1 金管局的監管目的是要建立及維持安全與穩健的環境，以促進電子銀行在香港的發展，但同時又不會構成阻礙。

2.1.2 爲達到這個目的，金管局認爲在科技方面保持中立是非常重要，使認可機構能靈活選擇及運用與其電子銀行服務配合的科技。就電子銀行定下絕對的風險管理

要求或一成不變的科技標準，是不切實際及會帶來反效果。

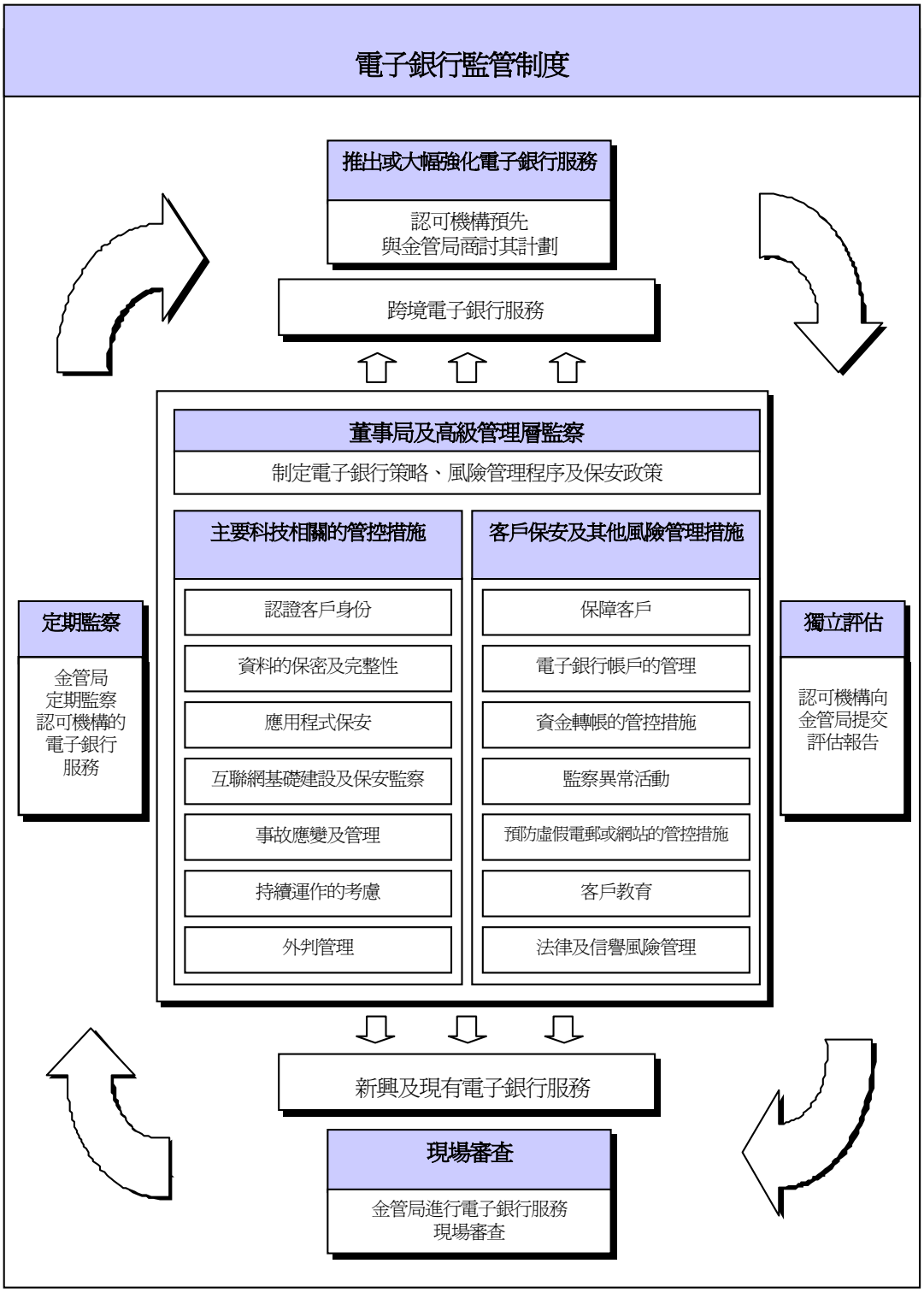
2.1.3 大原則是認可機構應實施「適合」的風險管理措施，即能配合個別認可機構許可的交易類型及金額所涉及的風險、採用的電子傳遞渠道及風險管理系統。

2.1.4 金管局在編製本章時，已考慮到國際監管機構，特別是巴塞爾銀行監管委員會[2]建議的監管模式及指引。然而，認可機構應注意，本章的目的並不是要就管理各類電子銀行服務所引起的風險指定劃一或鉅細無遺的原則與方法。

2.2 電子銀行監管制度

2.2.1 金管局的電子銀行監管制度是依據風險爲本的監管方法，對認可機構的電子銀行業務作出適當水平的持續監管。這套監管制度包含了有效的電子銀行持續監管模式，及確保認可機構的管理層對電子銀行服務進行適當的風險管理（見下文第3至5節）。以下內容列載電子銀行監管制度概覽。

[2] 巴塞爾銀行監管委員會發出了多份有關電子銀行的文件，特別是 2003 年 7 月發出的《電子銀行風險管理原則》(http://www.bis.org/publ/bcbs98.htm)及 2003 年 7 月發出的《跨境電子銀行業務的管理與監管》 (http://www.bis.org/publ/bcbs99.htm)。


電子銀行監管制度
推出或大幅強化電子銀行服務
認可機構預先與金管局商討其計劃
跨境電子銀行服務
董事局及高級管理層監察
制定電子銀行策略、風險管理程序及保安政策
主要科技相關的管控措施
認證客戶身份
資料的保密及完整性
應用程式保安
互聯網基礎建設及保安監察
事故應變及管理
持續運作的考慮
外判管理
客戶保安及其他風險管理措施
保障客戶
電子銀行帳戶的管理
資金轉帳的管控措施
監察異常活動
預防虛假電郵或網站的管控措施
客戶教育
法律及信譽風險管理
定期監察
金管局定期監察認可機構的電子銀行服務
獨立評估
認可機構向金管局提交評估報告
新興及現有電子銀行服務
現場審查
金管局進行電子銀行服務現場審查

2.3 推出或大幅強化電子銀行服務

2.3.1 雖然認可機構在推出新的電子銀行服務前不須取得金管局的正式批准，但認可機構應事先與金管局商討其計劃。此外，認可機構亦應與金管局商討論其大幅強化現有銀行服務[3]的計劃。一般而言，在有關商討中，認可機構應能令金管局相信下述事項已得到妥善處理：

- 董事局及高級管理層的監察（見第3節）；
- 與電子銀行有關的主要科技相關的管控措施（見第4節），特別是電子銀行服務的獨立評估結果（見下文第2.4分節）；
- 客戶保安及其他風險管理措施（見第5節），特別是若向個人客戶提供服務，有關的服務條款及章則是否符合《銀行營運守則》的規定；及
- 與外判（見SA-2 「外判」）、經互聯網進行《證券及期貨條例》指明的若干受監管活動（見SB-1「對獲得證監會註冊的認可機構進行的受規管活動的監管」）及跨境電子銀行業務（見下文第2.6分節）等有關的任可其他相關監管事項。

2.4 獨立評估

2.4.1 認可機構在推出新的電子銀行服務或大幅強化現有服務前，其高級管理層須委任可靠的獨立專家（評估人員）進行獨立評估。獨立評估的範疇及須予匯報的項目最少應包括附件A所指明的範圍。獨立評估報告應提交金管局作爲參考。若認可機構聘請了不同人士（例如內部審計師、外聘審計師或保安顧問）分別就其電子銀行服務的不同範疇進行獨立評估，該認可機構可向金管局提交合併報告或向金管局提交所有個別有關報告。

2.4.2 認可機構應於其後至少每年進行一次正式風險評估，以確定是否需要再進行任何獨立評估，如有需要，則

[3] 這是指對有關認可機構或其客戶有重大風險影響的主要服務提升或科技修改項目。

亦要確定獨立評估的次數及範疇。風險評估應考慮到所提供的服務的風險狀況的重大轉變、認可機構的互聯網基礎設施（包括系統修補程式）及電子銀行應用程式的重大修改、嚴重的系統弱點或重大系統保安事故。在適當情況下，金管局會審閱該等獨立保安評估報告，以作爲金管局的現場審查及非現場審查的一部分。

2.4.3 評估人員應具備及能證明其具備所需的專門知識，以進行獨立評估。爲確保公正，評估人員應與發展、實施或操作有關服務的各方保持獨立，並且不應參與需檢討的業務操作，或參與挑選或實施需予檢討的相關管控措施。如有需要，評估人員應可自由及直接地向認可機構的高級管理層匯報其評估結果。

2.4.4 評估人員可以是外聘人士（例如外聘審計師或第三方保安顧問）或認可機構的內部人員（例如內部審計師），但評估人員須符合上述的專門知識及獨立性的要求。

2.5 現場審查及其他監察程序

2.5.1 金管局將會在現場審查及非現場審查過程中根據本章所列原則，按情況決定認可機構的電子銀行服務風險管理是否足夠（見下文第3至5節）。

2.5.2 認可機構應迅速向金管局匯報有關電子銀行的任何懷疑或已確定的騙案、重大保安事故、任何嚴重的服務中斷情況或與其電子銀行服務有關的其他重大事項。金管局亦可能會實施其他監察程序（例如監管控制自我評估），以便對電子銀行進行持續監察。

2.6 跨境電子銀行服務的監管

2.6.1 金管局會遵照巴塞爾委員會的協定[4]、補充文件及2003年6月的《跨境電子銀行業務的管理及監管》文件內的指引，就監管跨境電子銀行服務，與有關的註冊地及所在地監管機構作出監管合作及交換資料。

[4] 見巴塞爾銀行監管委員會於 1983 年 5 月發出的《銀行的海外機構的監管原則》，亦普遍稱爲《協定》。

2.6.2 一般而言，本地註冊認可機構如計劃在其沒有實體辦事處的另一個地區推出跨境電子銀行服務，應預先與金管局商討。認可機構須要令金管局相信其已進行充份的嚴格調查（例如認可機構已諮詢適當的當地監管機構），以確定有關的海外地區的法例、規例及監管標準的適用情況。此外，認可機構應具備有效及持續的風險管理程序，以管理其跨境電子銀行業務的風險。

3. 董事局及高級管理層監察

3.1 規劃及組織

3.1.1 電子銀行服務的獨有特色以及其相對偏高的首次投資可能會對認可機構造成重大風險影響。就此而言，金管局要求認可機構的董事局[5]或其指定委員會及高級管理層確保會詳細評估對機構而言是全新的電子銀行服務（有關新產品及服務的風險管理，另見 IC-1「風險管理的一般措施」）。

3.1.2 評估的目的是要確保董事局或其指定委員會及高級管理層完全明白有關的風險特點，及機構具備足夠人手、專門知識、技術及財政資源，以推出及維持有關服務。

3.1.3 若新的電子銀行服務可能會對認可機構的風險狀況造成重大影響，認可機構的董事局或其指定委員會應獲知會。一般來說，董事會或其指定委員會應先確保，其認可機構具備所需的專門知識以進行有效的風險管理監察，才會推出有關服務。

3.1.4 董事局或其指定委員會及高級管理層亦應確保就其推出新電子銀行服務，制定正式業務策略。此外，電子銀行策略亦應成爲認可機構的整體業務策略的一部分。

3.2 風險管理程序

[5] 就本章而言，如屬海外註冊認可機構，其本地管理層負有監察其香港業務的電子銀行環節的責任。

3.2.1 董事局或其指定委員會應確保電子銀行風險管理是認可機構的風險管理制度不可分割的部分（見IC-1「風險管理的一般措施」及TM-G-1「科技風險管理的一般原則」）。因此，認可機構應按其銀行服務的需要實施及推行適當的風險管理政策及程序，以及其風險管理制度規定的相關內部管控措施及審核程序。

3.2.2 此外，董事局或其指定委員會應確保認可機構的風險管理措施及制度會按需要作出修訂及強化，以應付與電子銀行有關的風險管理事故。電子銀行有關的風險管理措施一般至少包含本章第4及第5節提及的措施。

3.3 制定資訊保安政策

3.3.1 高級管理層應確保認可機構定期制定及更新與其電子銀行服務有關的全面資訊保安政策。有關政策應由高級管理層批准及發出。政策文件應列明有關的政策、程序及措施，以保障認可機構的業務運作免受保安及入侵事故影響。政策文件亦應界定個別人員的責任，以及說明執行方法及針對不遵守有關政策、程序及措施情況下的紀律處分。

3.3.2 除了發出及更新資訊保安政策外，高級管理層亦應表明會致力維持高水平的電子銀行資訊保安，並向所有有關人員廣泛傳達這項信息，從而在機構內培養保安文化。

4. 涉及電子銀行的主要科技相關管控措施

4.1 認證客戶身份

4.1.1 認可機構應挑選可靠及有效的認可技術，以核實電子銀行客戶的身份及權限。認證客戶身份程序若能集合以下兩項因素，通常會比較有效：

- 客戶所知（例如用戶名稱及密碼）；及
- 客戶所持物件（例如由保安權標或認可機構的保安系統提供的一次性密碼[6]、硬件式電子鑰

[6] 「一次性密碼」是指只可用作單一次有效連接或在指定時限內（例如大約 60 秒）使用，以認證身份的密碼。這樣即使一次性密碼被黑客盜取，亦不能再使用有關密碼以認證身份。

匙、或儲存在聰明卡或客戶所持的其他裝置的客戶私人密碼匙[7]）。

4.1.2 認可機構須要仔細評估某種認證方法是否已成熟，以及即使客戶的個人電腦已被入侵時（例如是被特洛伊木馬軟件[8]侵襲），有關方法是否仍能發揮效用。一般來說，金管局要求認可機構會運用比較有效的認證客戶身份方法（例如合併使用上文提及的因素[9]），來認證風險較高的客戶交易（例如未登記的第三方過戶，及公司或機構客戶的大額交易）。

4.1.3 若認可機構仔細考慮過其他相關因素後，決定只利用用戶名稱及密碼認證其電子銀行客戶的身份，便應實施足夠的客戶保安措施，以保障客戶的密碼，並要採納有效的監察機制，以偵測任何異常活動（見下文.第 5 節）。

4.1.4 除了實施認證客戶身份的措施外，認可機構亦要實行適當方法（例如在電子銀行伺服器安裝數碼證書及其相關密碼匙鑰），讓客戶核實網站的身份及其真確性（另見下文第 5.5.1 段）。

4.2 資料的保密及完整性

4.2.1 由於電子銀行服務涉及經互聯網及認可機構的內部網絡傳送敏感資料（例如電子銀行密碼），因此認可機構應採取適當方法，使敏感資料通過內部及外部網絡期間以及儲存在認可機構內部網絡時，仍維持其保密及完整性。

---

7 簡單來說，「私人密碼匙」是指只提供予客戶的專用密碼匙，利用公開密碼匙加密技術認證客戶的身份。

8 特洛伊木馬軟件是電腦程式的一類，該程式表面看來並無不妥（例如看似是電腦遊戲），但內含有害的程式。特洛伊木馬軟件傳染個人電腦的方法，包括入侵者利用某些操作系統的弱點，當受害者開啓受感染電郵附件或到訪帶有病毒的網站，受害人的電腦便會受到侵襲。特洛伊木馬軟件可記錄屏幕所顯示的畫面及用戶所按的鍵，盜取受害人的個人電腦所儲存的資料，或控制受害人的個人電腦。

9 舉例來說，利用雙重因素認證身份方法（如密碼及數碼證書合併方法等）就高風險交易認證客戶身份，會比單一因素認證方法有效。認可機構可考慮利用本港（例如香港郵政）開發及發出的的公用密碼匙基礎建設及數碼證書，以加強其認證客戶身份程序的可行性。

4.2.2 加密技術可以用作保護敏感資料的保密及完整性。認可機構應跟據資料的敏感程度及重要性，選擇與保障程度相符的加密技術。金管局建議認可機構採用國際認可的加密技術，而有關計算法的加密強度已經過廣泛測試。認可機構應實施穩健的密碼匙管理方法，以保障其加密密碼匙。

4.2.3 認可機構應考慮是否需要就傳送敏感資料（例如電子銀行密碼）採用強勁的「端對端」加密方法，以確保敏感資料在客戶的裝置與認可機構的可信內部網絡之間傳送時，都受到加密保護。這個安排可減低在認可機構的網站伺服器[10]或非武裝區受到入侵時，敏感資料外泄的風險。

4.2.4 若認可機構選用的科技並不容許進行「端對端」加密，而在客戶的裝置與認可機構的可信內部網絡之間的某一處會進行資料解密程序，認可機構便應採取適當措施[11]保障敏感資料。

4.2.5 除加密技術外，認可機構亦應實施其他必要措施，以維護其電子銀行系統所處理的資料的保密及完整性。例如，這些措施包括：

- 把檢查與管控措施併入應用程式內，以便在處理交易後核對數據檔案結餘，以及查核在不同系統之間傳送的數據的完整性；
- 將處理及監察電子銀行交易的部門分開，使任何一名職員在沒有其他部門合作時，不能同時進行、授權、處理及刪除電子銀行交易或帳戶，以制衡有關人員的行動；及
- 監察異常活動，包括任何銀行交易或記錄有否被篡改（見下文第5.4分節）。

4.3 應用程式保安

[10] 互聯網伺服器是專門連接互聯網及儲存組成網頁的檔案，以便用戶可經互聯網連接到該網頁。

[11] 其中一項可能的措施是，任何密碼程序（例如解密和加密）均應在一個能高度抵抗擅自改動的安全環境中進行。

4.3.1 電子銀行系統的應用程式保安不足，會增加系統被成功入侵或受到襲擊的風險。因此，認可機構應參考以下穩健的方法[12]，確保其電子銀行系統的應用程式具備適當的保安水平：

- 當認可機構選擇系統開發工具或程式編製語言以開發電子銀行應用系統時，應評估不同的工具或語言可以提供的保安功能，以確保能實施有效的應用程式保安措施。若選用第三方開發的電子銀行系統，認可機構應考慮到有關系統的應用程式保安措施是否適合；
- 伺服器應全面及有效地核實輸入參數（包括用戶輸入的資料及可由用戶電腦提交的數據庫查詢）。此舉可防止電子銀行系統處理了刻意提供的不正確輸入的參數，以免出現未經授權存取數據、執行嵌入參數的命令的情況、或引起緩衝區滿溢襲擊[13]。此外，電子銀行系統應以最少所需的系統特權的形式操作；
- 電子銀行客戶使用的應用程式系統產生的錯誤信息不應透露系統的敏感細節，同時應適當地記錄有關錯誤。同樣，生產式網頁伺服器上的HTML[14]源碼不應載有敏感資料，例如有關網頁應用程式的設計特點的任何提述或說明；
- 須用可靠的保安機制以管理所用的電子銀行通訊對話。例如，在一段指定時間內若沒有活動，便應該終止有關的通訊對話。載有敏感資料的網頁不應儲存在瀏覽器的臨時檔案內；

---

12 認可機構可參考有關應用程式保安的其他參考資料，例如 Open Web Application Security Project (www.owasp.org) 及 SANS (SysAdmin, Audit, Network, Security) Institute (www.sans.org)。

13 緩衝區滿溢襲擊專門針對不小心編寫出來的程式，這些程式可以讀入的輸入數據比其可以處理的多，引致部分電腦記憶體被所接受的數據重寫。這些過量的輸入數據可被操控，引致程式非正常地終止或在目標電腦內執行一些未經授權的敏感指示。

14 HTML 指超文本標記語言（Hypertext Markup Language），是製作網頁的標準描述語言。

- 最理想是應用程式能禁止客戶的瀏覽器記錄或展示客戶以往輸入的電子銀行用戶名稱及密碼以及客戶以往接達的電子銀行網頁；
- 在發現或接獲舉報有關電子銀行應用程式的問題後，應按情況檢查有關程式的源碼，確保有關問題得到適當處理。認可機構可以就系統開發及源碼檢查定下保安標準。如屬第三方開發的系統，認可機構應適當地爲系統安裝由供應商不時提供的修補程式；
- 載有網站的管理網頁或敏感資料的隱藏目錄應從生產網站伺服器中移除，或以有效的認證及接達管控機制保護。備用檔案及共用檔案[15]應從生產網站伺服器或檔案目錄的結構中移除，以免被未經授權用戶接達；及
- 認可機構必須對檔案目錄結構及檔案的接達控制進行定期的保安檢討，以確保所有敏感檔案都受到適當保護，沒有因網頁應用程式的漏洞而遭泄露。

4.4 互聯網基礎建設及保安監察

4.4.1 認可機構應建立適當的操作環境，以支援及保護其電子銀行系統。適當的操作環境通常包含安全可靠的互聯網基礎建設（包括非武裝區的設計及伺服器、入侵偵測系統、防火牆及路由器的設定）以及內部網絡及與外部各方的網絡連接的適當保安措施（另見TM-G-1「科技風險管理的一般原則」）。

4.4.2 認可機構應主動及持續地監察其電子銀行系統及互聯網基礎建設，以偵測及記錄任何保安事故、懷疑入侵事故或漏洞[16]。全面的審計記錄及適當的實時保安警報（例如入侵偵測系統警報）應提交予有關負責人員或小組，以及時審閱。審計記錄應予以保護，免受未

15 備用檔案及共用檔案可能載有網站的檔案記錄、網頁、手稿程式或舊版本的網頁。攻擊者通常會搜尋每個檔案目錄，以找出這些備用及共用檔案名稱及文件擴展名，以取得網站的敏感資料。

16 一般而言，認可機構應至少每日一次監察有關機構(例如香港電腦保安事故協調中心(www.hkcert.org)、防電腦病毒供應商及系統供應商)所公布的保安漏洞及電腦病毒預警。

經授權刪改，並應保留一段合理期間（例如3個月），以便在有需要時協助任何騙案調查及糾紛調解。

4.4.3 認可機構應參閱附件B有關設計、建立及監察其互聯網基礎建設的穩健方法。

4.5 事故應變及管理

4.5.1 認可機構應備有正式的事故應變及管理程序，以便及時舉報及處理懷疑或證實的保安事故、騙案或電子銀行服務中斷的情況（包括在辦公時間以內或以外）。事故應變及管理程序應容許認可機構：

- 迅速發現引起事故的源頭（特別是事故是否因爲認可機構本身的保安管控措施或操作環境的問題引致）；
- 評估事故的規模及影響；
- 若事故可能會引致信譽受損或重大財政損失，應迅速將事故提升至高級管理層的層面處理；
- 在適當情況下迅速知會受影響客戶；
- 控制對認可機構的資產、數據、信譽、以及尤其是客戶所造成的損害；
- 按情況收集及保存司法證據，以便日後有需要時進行調查及起訴疑犯及入侵者之用；及
- 檢討事故。

4.5.2 認可機構應制定通訊策略，以適當處理事故可能引起的對外各方（例如客戶、傳媒及業務夥伴）的關注。

4.5.3 認可機構應設立事故應變小組（可由來自科技風險管理部門或其他有關部門的人員組成），以按照上述程序管理事故及作出回應。該小組應獲賦予權力在緊急情況下採取行動，並應受過充足訓練，能使用入侵偵測系統、闡釋審計記錄的相關數據的重要性及決定須採取的適當行動（例如封鎖特定的網絡交通或關閉部分服務）。

4.6 持續運作的考慮

4.6.1 認可機構應持續提供電子銀行服務，其系統並有合理的回應時間，符合機構的章則及條款以及預計的客戶期望。關鍵電子銀行服務的可用程度極之倚賴認可機構的處理能力（例如包括電子銀行系統、關聯網絡以及與內部系統的界面的處理能力）、轉用備用系統（確保不受相關的干擾影響）的能力及其他電子銀行服務傳送渠道的效率。

4.6.2 認可機構應制定每項關鍵電子銀行服務的表現準則，並應根據有關準則評估服務水平。認可機構應採取適當措施，確保電子銀行系統及與內部系統的界面能應付電子銀行的預計交易量及日後的增長。

4.6.3 認可機構在制定電子銀行持續業務運作計劃時，除了應參考TM-G-1「科技風險管理的一般原則」及**TM-G-2**「持續業務運作規劃」所訂明的一般指引外，亦應考慮以下做法：

- 電子銀行持續業務運作計劃應列明遇有業務受干擾的情況，如何恢復或取代電子銀行處理能力及在有需要時重建交易檔案的程序；
- 電子銀行持續業務運作計劃應能處理對外聘服務供應商（例如互聯網服務供應商）的任何相關倚賴；及
- 若關鍵電子銀行服務的應變安排會利用其他服務傳送渠道，認可機構要考慮到客戶的需求與期望，確保該服務傳送渠道可向其客戶提供適當水平的持續服務。

4.7 外判管理

4.7.1 由於互聯網的技術相當複雜，加上其全球性質，部分認可機構可能會倚賴銀行集團內的另一個單位（例如總行）或外聘服務供應商，操作及維持與其電子銀行服務有關的資訊科技系統或業務程序。在這些情況下，認可機構應參考TM-G-1「科技風險管理的一般原則」及SA-2「外判」所訂明有關科技外判管理的管控措施；及

4.7.2 認可機構應定期進行嚴格調查，評估外聘服務供應商的財政穩健情況及能力，以維持適當的保安水平及趕

上快速轉變的科技。金管局亦要求認可機構會特別留意：

- 調配足夠資源（並有所需知識與明確責任配合），以便有效監察外判予外聘技術服務供應商的電子銀行服務；
- 確保對外判服務進行獨立評估（參第2.4分節及附件A）；及
- 如屬跨境外判，確保有關安排符合適用法律、規例及監管標準的規定。

5. 客戶保安及其他風險管理措施

5.1 保障客戶

5.1.1 至於提供予個人客戶的其他銀行服務，認可機構須遵守《銀行營運守則》內有關向個人客戶提供電子銀行服務的規定。

5.1.2 認可機構必須在其章則與條款內清楚列明機構與客戶之間各自的權利與義務。有關的章則與條款對機構與客戶雙方都應該公正中肯。根據《銀行營運守則》的原則，金管局認爲除非客戶作出欺詐或嚴重疏忽行爲，否則客戶無須對因經其帳戶進行的任何未經授權交易引致而蒙受的直接損失負責。

5.2 電子銀行帳戶的管理

5.2.1 若認可機構容許其現有客戶在網上開設電子銀行帳戶，機構便應確保備有足夠管控措施，以減低騙徒在真正客戶不知情的情況下，開設電子銀行帳戶的風險。

5.2.2 認可機構應採用可靠的認證方法[17]，以核實在網上開設電子銀行帳戶的人士的身份。此外，認可機構 應

[17] 若認證方法涉及客戶輸入其信用卡／提款卡或電話銀行帳戶的個人密碼及有關的信用卡／帳戶號碼，認可機構應就重設或重發個人密碼實施足夠的管控措施。特別要留意的是，新個人密碼應以安全的渠道送交予客戶，例如經分行網絡發給客戶或以郵遞方式寄往客戶的登記地址。認可機構一般不應容許客戶經電話或其他電子渠道輸入個人資料的方法來重設個人密碼，除非認可機構採用更有效的認證客戶身份方法（例如多重因素認證方法）或施行更嚴格的管控措施（例如暫時停止客戶的電子銀行戶口的運作，直到認可機構能從其他

向有關客戶發出確認書。認可機構亦可考慮在認可機構相信有關客戶已收到確認書之前，禁止有關的電子銀行帳戶在網上轉帳至任可未經註冊第三方（參下文第 5.3 分節）。

5.2.3 遇有客戶要求更改其電子銀行帳戶資料或其他可用作監察帳戶活動的聯絡資料，認可機構應核實客戶的身份。有關的更改包括重設或重發客戶的電子銀行密碼，及更改聯絡資料（例如電郵地址、通訊地址或聯絡電話號碼）。認可機構在處理這些更改時，應考慮以下措施：

- 如客戶親身在分行提出更改資料申請，應核對客戶簽名，及如有需要，應查核客戶的身份證或護照；
- 評估以郵遞或投放於分行收集箱的更改資料申請（如更改通訊地址）所涉及的風險，如有需要，應透過適當渠道（如電話）與客戶確認有關申請，才作出更改；
- 如更改申請是經電子銀行服務或其他渠道提出，應確保備有有效監察機制（見下文第 5.4 分節）；
- 避免郵寄重要文件（如新密碼、新支票簿及更換損毀信用卡）至最近才更改的通訊地址，尤其是當機構並沒有類似上文所述的 3 項措施。在這些情況下，機構應要求有關客戶前往分行，並於核對其身份證或護照後領取有關文件；及
- 對於客戶以電話要求郵寄新密碼或其他重要文件的情況，機構應採取額外措施核實客戶身份，例如除一般個人資料外，詢問客戶一些會隨着時間而改變的資料，包括大約的帳戶結餘及近期交易。

渠道核實客戶的身份）。認可機構亦應定有程序以減低騙徒透過盜取郵件等方法獲得有關的敏感資料的風險。例如，認可機構在發出個人密碼前，應先行確保客戶已收妥信用卡／提款卡。若認可機構發信通知客戶親身領取信用卡／提款卡，有關通知不應載有信用卡／帳戶號碼。

5.3 資金轉帳的管控措施

5.3.1 若認可機構純粹倚靠用戶名稱及密碼核實電子銀行服務的客戶身份，應考慮將第三方資金轉帳限制於客戶已預先登記的帳戶[18]。爲確保該項措施的成效，認可機構應要求客戶經安全渠道（例如親身或以郵寄方式）登記第三方帳戶及確保適當核實客戶的登記申請（見第5.2.3段）。

5.3.2 另一個方法是客戶可在網上辦理登記第三方帳戶的手續，但有關登記只會在一段期間後才生效，使客戶能有足夠時間收到確認書。

5.3.3 若認可機構在權衡利弊後決定接受資金轉帳至未登記第三方帳戶[19]，機構應備有適當保障措施以管理未經授權的第三方資金轉帳的風險，例如：

- 在電子銀行帳戶剛啓動時，網上轉帳至未登記第三方（包括本地及海外收款人）的設定交易限額應定爲零；
- 認可機構應確保客戶只能透過安全渠道（例如在分行或以郵寄方式）調高限額，並要有足夠的身份核實措施（另見第5.2.3段）；
- 應向客戶適當披露與該等資金轉帳有關的風險；
- 現有客戶如其未登記第三方資金轉帳的設定限額並非零，而該客戶很久沒有轉帳至未登記第三方，認可機構可考慮調低該客戶的有關限額；
- 應對未登記第三方資金轉帳設定每日或每宗交易最高限額。而該等限額應低於轉帳至登記第三方的適用限額；

---

18 認可機構亦應評估網上轉撥至商號無需預先登記的做法的風險，並按需要實施類似的 管控措施。

19 這些帳戶可能包括支付帳單、款項支付至非公用事業公司（例如珠寶店、證券買賣及第三方信用卡帳戶）。

- 認可機構可考慮在客戶進行網上未登記第三方資金轉帳前，作出第二項因素身份核證（見上文第4.1.2段）；及
- 最理想的做法是認可機構應於容許轉帳至未登記第三方帳戶的公司或機構電子銀行服務上，實施雙重因素身份核證。

5.4 監察異常活動

5.4.1 認可機構應具備有效的監察機制，以及時察覺可疑的網上交易及異常活動。尤其是個人電子銀行服務的監察機制應能察覺類似以下的個案：

- 在一段短時間內，有多次網上資金轉帳至同一個未登記第三方帳戶，特別是若轉帳金額接近所容許的最高限額，或金額超過某個數額；及
- 客戶更改通訊地址[20]後不久即出現可能潛有欺詐成分的活動，例如開設網上電子銀行帳戶、要求郵寄重要文件至該地址（例如支票簿、新電子銀行密碼、信用卡／提款卡密碼）、提高資金轉帳限額或資金轉帳至未經登記第三方的情況突然增加。

5.4.2 若出現可疑網上資金轉帳及異常活動，認可機構的監察機制應迅速通知其監察人員。遇有這些情況，認可機構應盡快與有關交易或活動的帳戶持有人查核。

5.4.3 認可機構亦應可考慮一旦發現個人客戶的帳戶對未經登記第三方作出網上資金轉帳、網上資金轉帳超過某個限額或察覺到與其帳戶有關異常活動，便立即以其他自動化渠道（例如將信息傳遞至客戶的流動電話或電子郵箱）通知有關客戶。

5.5 預防虛假電子郵件或網站的管控措施

[20] 若認可機構大約在同一時間收到通過郵遞方式提交的更改聯絡資料的申請（例如通訊地址、電話號碼及電郵地址），認可機構便應特別留意有關情況。

5.5.1 認可機構應管理涉及騙取客戶個人資料（例如帳戶號碼或電子銀行密碼）的虛假電郵或網站[21]所帶來的風險。爲此，認可機構應考慮採取下列措施：

- 讓客戶知道認可機構或其代理／商業夥伴絕不會以電子郵件的方式要求他們提供敏感帳戶資料（例如個人密碼）。若客戶有懷疑，應與認可機構聯絡；
- 教育客戶如何可確保他們是與認可機構的正式網站聯繫，例如在瀏覽器的細小扣鎖或鑰匙標誌上連按兩次滑鼠，以查閱電子銀行交易網站的數碼證書的有關資料[22]，或在確定儲存在瀏覽器的書簽功能上的認可機構網站是真確後，才使用該書簽功能登入網站。認可機構應要求客戶不要經電子郵件內的超連結登入認可機構的電子銀行交易網站，除非客戶已核實網站是真確的，例如網站的數碼證書是否有效；及
- 定期在網上搜尋，查看是否有任何第三方網站的域名可能會被誤會是認可機構的域名，或是否有網站與認可機構的網站建立了超連結。若該等網站的意圖有可疑，認可機構應考慮封鎖（例如用防火牆或路由器）由這些網站轉駁至認可機構網站的任何網上交通、就使用該等域名提出爭議，及向警方或金管局尋求協助。此外，認可機構可考慮按需要，主動登記與其正式域名類似或會被誤會爲其正式域名的域名。

5.6 客戶教育

5.6.1 由於客戶用作連接電子銀行服務的裝置是在認可機構的控制範圍以外，因此若客戶不知道或不了解使用電子銀行服務所需的保安措施，保安風險可能會增加。

---

21 虛假電郵或網站（例如經載於虛假電郵的超連結連接）會利用不同方法使有關電郵或網站看似真實，這些方法包括：(i) 套用真實網站的圖像； (ii)將客戶轉駁至真正的網站，讓客戶與有關的真正認可機構接通，而不知道其個人資料可能正在經過虛假網站；及(iii)利用一些域名，其與有關認可機構的域名很接近，或可能會被視作爲認可機構的域名。

22 一般來說，認可機構應通知客戶如何查核發出證書的機構、證書是否發給有關認可機構，及證書是否仍然有效。

因此，認可機構應特別留意向客戶就電子銀行保安措施提供容易理解及顯著的建議。特別是《銀行營運守則》規定認可機構應提醒其個人電子銀行客戶有關採取合理保安措施的責任。

5.6.2 視乎電子銀行客戶類型及所提供的電子銀行服務性質，認可機構一般應至少給予客戶下述的各項保安預防措施建議：

- 電子銀行密碼（如客戶可選擇用戶名稱，則亦應包括這些用戶名稱）的選擇及保護。例如認可機構應建議客戶不要選用出生日期、電話號碼或客戶姓名中易於認出的部分等資料作爲密碼。認可機構亦應建議客戶避免使用同一個密碼登入其他網上服務（例如用作連接互聯網）；
- 對社會工程技巧[23]的防範措施。認可機構應提醒客戶切勿向任何未能核實其身份或任何可疑網站提供個人資料（例如有關其身份證或護照上的資料、地址或銀行帳戶）。尤其是認可機構應提醒客戶切勿向任何人士（包括認可機構的職員或警方）透露其密碼；
- 提醒客戶不要經公用或共用電腦（例如可供上網的咖啡室或公共圖書館內的電腦）使用電子銀行服務；
- 採取預防措施保障客戶，免被欺詐電郵或網站混淆或欺騙（見上文第5.5分節）；及
- 建議客戶要確保其個人電腦的設定是安全的，並適當地保護其電腦（例如安裝個人防火牆軟件及定期更新防電腦病毒軟件），以免被電腦病毒及惡性程式入侵。

5.6.3 認可機構亦可參考香港銀行公會（www.hkab.org.hk）不時提供的銀行客戶保安提示。此外，認可機構應定期檢討其保安建議，以確保

[23] 社會工程是指利用社交技巧試圖取得資料或接達途徑的計謀。例如不法分子可能會自稱是某認可機構的人員，試圖誘騙受害人透露其個人資料、用戶名稱或密碼。

隨着科技及電子銀行服務不斷改變，有關建議仍然適用。

5.6.4 由於客戶可能會覺得難以吸收冗長及複雜的建議，因此認可機構應定出有效的方法及渠道，以便能就保安措施與客戶溝通。認可機構可使用多種渠道（例如認可機構的網站、印刷在客戶月結單上的信息、宣傳單張、認可機構前線人員與客戶聯絡的機會），以加強某些主要預防措施。

5.7 法律及信譽風險管理

5.7.1 認可機構應適當地評估其電子銀行服務涉及的法律及信譽風險。若電子銀行服務是提供予另一個地區或可能被視作以另一個地區爲目標，這個評估便特別重要。

5.7.2 根據風險評估結果，認可機構應備有妥善的管控措施，以管理法律及信譽風險。例如，這些管控措施可包括：

- 妥善的電子銀行章則與條款；
- 在電子銀行網站或其他有關文件上的當眼處列載適當的資料披露及免責聲明，以符合適用的法律規定（例如《個人資料（私隱）條例及海外地區的保障消費者規例）及應付潛在的信譽問題；及
- 考慮是否須要就剩餘法律風險購買適當的保險。

5.7.3 若認可機構打算推出新的電子銀行服務（例如支付服務），而現有傳送渠道並沒有提供，則金管局要求認可機構應考慮本章所列的相同的監管規定及風險管理原則，包括法律及信譽風險。

5.7.4 例如，帳戶匯集服務[24]通常涉及檢索客戶於其他機構開設的網上帳戶的有關資料（例如帳戶結餘）。認可

[24] 帳戶匯集服務讓客戶可以用一個用戶登入的名稱及密碼，在單一網站檢視其在不同機構開設的網上帳戶。某些海外帳戶匯合服務要求客戶向匯集商提供其網上帳戶的用戶名稱及密碼，以便匯集商可檢索到客戶的有關資料，並將有關資料綜合在單一網站上。視乎服務的推行方法，認可機構可能需要解決有關保障客戶密碼及保密資料的安全問題。

機構向客戶提供有關服務前，應仔細評估這項服務所帶來的保安、法律及信譽風險。視乎檢索過程的機制而定（尤其是認可機構及客戶在檢索資料時所扮演的角色），這項服務所帶來的法律及信譽影響可能會不同，認可機構需要作出適當評估。

附件 A: 獨立評估的範圍及報告

A1. 在考慮到本章第3至5節所載的指引後，獨立評估一般應至少包括以下範疇：

<u>董事局及高級管理層監察</u>

A1.1 評估認可機構的高級管理層是否已核准及發出與電子銀行服務有關的全面資訊保安政策，及制定有效的管理架構以確保有關政策在機構內得到實施、執行及定期修訂；

<u>認證客戶身份及資料保密</u>

A1.2 評估是否已推行適當措施，讓認可機構能認證客戶身份及客戶使用電子銀行服務的權限；

A1.3 評估是否已推行適當措施，以確保儲存或經過外部及內部網絡的資料的保密及完整性；

<u>應用程式保安、互聯網基礎建設及保安監察</u>

A1.4 評估是否已在電子銀行系統內實施適當的應用應程式保安措施，包括運用能夠提共有效保安功能的適當系統開發工具、適當設計、檢討及保護應用程式代碼及檔案目錄，以及全面核實輸入參數；

A1.5 評估是否已實施適當保安措施[25]（包括伺服器[26]、防火牆及路由器的系統設計與設定，以及網絡保安），以合理地保證認可機構的非武裝區、電子銀行系統、內部網絡及與公用網絡或遠程各方的網絡連接部分受到保障；

A1.6 評估是否已推出適當措施，以持續偵測及記錄異常活動、入侵事故或系統漏洞，包括保存及審查審計追蹤

---

25 獨立評估不僅應包括外部公用網絡（如互聯網）與認可機構本身的伺服器或防火牆的網絡連繫的保安事項，還應包括這些伺服器／防火牆與認可機構內部系統及數據庫的網絡連繫及系統界面的保安事項。

26 認可機構應留意，某些涉及連接公用網絡的服務（例如與電子銀行客戶聯繫的電郵服務及將網站名稱轉爲網站地址及將網站地址轉爲網站名稱的域名服務）的妥善保安安排亦相當重要，以防止利用這些服務襲擊電子銀行系統。因此，獨立評估亦應涵蓋該等服務的有關伺服器（域名服務伺服器、電郵伺服器）的保安事項。

記錄或交易記錄，以及是否定有適當程序以匯報該等事件及作出回應；

A1.7 評估是否已實施適當的實體保安措施，以防止他人未經授權而可接觸到關鍵電腦或網絡設備；

A1.8 評估是否已備有有關應用程式、系統及網絡組成部分的適當變更控制政策及程序，以確保生產系統及網絡的所有變動都經適當批准、測試及實施；

事故應變及業務持續運作管理

A1.9 評估是否已實施足夠的業務運作及表現監察程序，並定明表現準則，以確保能及時分析表現監察統計數據，以及已採取適當措施以處理任何相關問題；

A1.10 評估是否已在設計電子銀行系統及互聯網基礎建設時，併入適當措施（例如主要系統組成部分的冗餘度），以合理地保證可防止系統受干擾、減輕干擾造成的影響及／或對干擾作出適當的回應；

A1.11 評估是否已制定適當的持續業務運作計劃及程序，以應付對認可機構的電子銀行服務的嚴重干擾的情況及恢復電子銀行服務；

A1.12 評估是否備有適當安排，至少每年一次檢討、核實及排練持續業務運作計劃；

客戶保安

A1.13 評估是否已採取適當措施，就客戶的需要提供電子銀行服務的保安措施顯著的意見；

A1.14 評估電子銀行帳戶管理的管控程序的成效（包括開立帳戶、發出或重設密碼、第三方帳戶登記及更改帳戶資料等）；及

A1.15 評估是否已實施適當措施，以處理高風險交易（ 例如未經登記第三方資金轉帳及網上付款等）。

A2. 獨立評估報告的內容

評估期

A2.1 報告應列明進行獨立評估的時間以及當時系統的發展階段（例如設計階段或測試階段）。

範圍及方法

A2.2 報告應說明評估的範圍及所採用的方法。尤其是評估範圍應清楚列出獨立評估涵蓋哪些系統組成部分，以及認可機構的內部網絡及網絡設備中的哪些部分（例如網間連接器及路由器）。

A2.3 評估人員應對高風險環節進行更爲徹底的審查。如認可機構提供高風險電子銀行服務（例如容許向未經登記第三方帳戶進行大額資金轉帳的服務），它們便應考慮因應不同類型的網上襲擊，在獨立評估中加入滲透測試。

評估結果概要

A2.4 報告應包括以下資料：

- 評估結果，其中可包括就所發現的問題對保安的影響的闡釋，以及評估人員對有關問題所涉及的風險水平的評估；
- 評估人員就解決有關問題而提出的建議；及
- 管理層對有關問題及建議的回應，包括爲解決有關問題而將會採取的措施、完成有關措施的預定日期，以及將會採取的任可臨時措施（管理層的回應可載於另一份報告內）。

A2.5 若管理層採取其他方法以解決評估人員所發現的問題，或如評估結果顯示出機構的電子銀行服務存在嚴重問題，有關認可機構可要求該評估人員或其他獨立專家進行跟進檢討。

A3. 外判業務之獨立評估

A3.1 若認可機構的電子銀行服務已外判（部分或全部）予外聘服務供應商，認可機構的高級管理層應確保該外聘服務供應商委托獨立專家就該服務進行足夠的獨立評估，並向認可機構提供有關的評估結果，以及在獨立評估之間定期檢討其保安安排是否足夠。

A3.2 外聘服務供應商選用的評估人員，以及委托評估人員進行獨立評估的次數與範圍應與第2.4分節及本附件所建議的相若，並要考慮到最新的科技發展及業內的穩健運作方法。

附件 B: 設立互聯網基礎建設的穩健方法

B1. 背景

B1.1 本附件爲認可機構提供有關設立互聯網基礎建設的穩健方法，包括非武裝區的伺服器的設計與設定、防火牆及路由器，以及入侵偵測系統的使用。要強調一點，本附件不擬列載所有穩健方法，認可機構亦應參考業內的穩健方法[27]及裝設與其電子銀行服務涉及的風險相符的互聯網基礎建設。

B2. 非武裝區的伺服器

B2.1 互聯網基礎建設或非武裝區通常都裝設有各種不同類別的伺服器，包括應用程式伺服器、網頁伺服器、域名服務伺服器及電郵伺服器。視乎實施形式而定，部分伺服器會處理網上電子銀行系統的前端處理程序，例如核實客戶輸入的數據或回應客戶。由於這些伺服器會經互聯網受到任何互聯網用戶的襲擊，因此這些伺服器不應儲存任何機密數據。

B3. 防火牆及路由器

B3.1 認可機構應適當選擇、設定及安裝防火牆及路由器。此外，認可機構應安裝「外部防火牆」，以控制互聯網與非武裝區內的伺服器之間的交通，確保只有認可通訊方法才可連接這些伺服器，以免攻擊者會利用某些通訊方法[28]來對這些伺服器構成威脅。當防火牆對來自互聯網的惡意網絡交通作出回應時，不應泄露任何敏感或系統資料。

B3.2 爲確保只讓許可類別的交通可以經非武裝區的伺服器連接至認可機構可信內部網絡，理想的做法是認可機

---

27 認可機構可參考其他有關互聯網基礎建設保安的資料（例如 SANS (System Administration, Networking and Security) Institute (www.sans.org) 及 the Computer Emergency Response Team (www.cert.org)）。

28 舉例來說，「Telnet」是容許遠程用戶登入伺服器的通訊方法（除瀏覽器以外），因而增加用戶可佔用這些伺服器的風險。

構應安裝另一層「內部防火牆」，以控制非武裝區的伺服器與認可機構的可信內部網絡之間的交通。此外，若使用兩層或以上的防火牆，認可機構可考慮使用不同類型的防火牆，以防止各防火牆存在的類似保安漏洞被利用。

B3.3 防火牆及路由器作爲保安工具的成效主要視乎它們的設定，以及認可機構是否制定有關其設定與更新的政策。認可機構必須制定及記錄有關其防火牆及路由器的設定、監察及更新的正式政策，才能確保設定的所有變更都受到妥善的控制、測試及記錄。

B3.4 認可機構應經常檢查防火牆及路由器設定，並在適當時候予以更新，以就新發現的問題及系統弱點加強保護。由於這個程序相當複雜，因此認可機構必須小心選擇信譽良好的供應商，這些供應商應能掌握防火牆與路由器的最新發展，以防範最新的襲擊方法。

B3.5 一般而言，認可機構應禁止任何無需經過防火牆而利用直接撥號或其他網絡連接的方法連接到第三方。若爲進行某項工作而需撥號連接，便須要得到適當批准及監察，並要在完成有關工作後立即終止連接。

B3.6 與管理防火牆有關的網絡交通應限於認可機構內部的系統管理網絡分段，該分段應與連接至生產系統的網絡分段分開，因而生產網絡與系統就不會因防火牆的管理活動而受到影響。

B4. 其他保安措施

B4.1 認可機構應停用或移除伺服器、防火牆及路由器上任何未有應用到的程式及電腦程序。認可機構應安排人員負責適時檢查、測試及應用伺服器、防火牆及路由器的適當修補程式。此外，認可機構應按需要在伺服器及防火牆安裝及更新防電腦病毒軟件。認可機構只應維持路由器、防火牆及伺服器的運作所需的最低數目的用戶帳戶。

B4.2 認可機構應只准許由經過嚴格認證身份的用戶帳戶或獲授權的電腦程序，更新伺服器、防火牆及路由器所載的程式及其他資料。同時，伺服器、防火牆及路由器亦應受到嚴格的變更控制程序管理。認可機構應運用適當的掃描工具，以定期鑒別運作環境中的任何潛

在保安問題。認可機構應定期檢查伺服器與防火牆所保載的程式與靜態數據（例如設定）的完整性，以核實有關程式及數據有否曾被更改。

B4.3 所有利用特權或緊急帳戶（例如系統管理員或「超級用戶」）接入伺服器、防火牆及路由器的情況都應受到嚴格控制、記錄及監察（例如員工之間互相審查）。例如，應只准許這些帳戶由有足夠的實體保安的終端機登入，或若伺服器、防火牆及路由器是由遠程管理的，則應有嚴格的系統資料認證及加密，以防範未經授權的接達。

B4.4 互聯網基礎建設的關鍵組成部分應預留備用部份，以防止任何單一故障令整個網絡及基礎建設無法運作。

B5. 入侵偵測與有關系統的使用

B5.1 認可機構應小心辨別所需的資料，以偵測互聯網基礎建設是否被入侵。這些資料有助認可機構決定記錄伺服器、防火牆及路由器的哪些審計資料，以及如有需要還應監察哪些數據（例如系統資源運用、網絡交通）。

B5.2 認可機構應定有適當的控制措施，以保護審計記錄及編製備份，並確保編製記錄的系統的時鐘都是同步的。審計記錄一般應每日檢查一次。由於記錄檔案通常都相當龐大，難以用人手處理，因此認可機構應考慮使用入侵偵測系統，以分析審計記錄及收集其他相關但審計記錄未能提供的資料。

B5.3 在挑選入侵偵測系統產品時，認可機構應考慮有關產品能否提供所需的資料以偵測可能的入侵情況，以及供應商能否適時提供最新的襲擊特徵（即可偵測可能的入侵情況的預設活動模式）。

B5.4 主機入侵偵測系統可偵測到主機（例如互聯網伺服器及防火牆）可能受到的入侵情況，其方法是透過鑒別審計記錄所記錄的未經授權活動或其有關設定或其他重要檔案的更改。至於網絡入侵偵測系統則可監察及偵查傳遞至及來自電腦、以及在網絡分段的異常交通。

B5.5 認可機構應測試入侵偵測系統，並應定期調校其襲擊特徵及預警設定，以提高其成效及減少虛報的情況。認可機構應備有程序，以確保有關的支援人員應每週 7 日，每日 24 小時就入侵偵測系統發出的重要警報作出回應。

———————————

目錄	辭彙	主頁	引言