澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

傳閱文件 005/B/2023-DSB/AMCM
（日期：二零二三年六月二十六日）

電子銀行風險管理指引

澳門金融管理局（AMCM）根據三月十一日第 14/96/M 號法令第九條和七月五日第 32/93/M 號法令核准之《金融體系法律制度》第六條所賦予的權限，制定本指引。

1. 背景

1.1 資訊科技的發展和創新正在改變獲許可機構的運作方式，也使其能透過私人或公共的網絡，並通過電子及互動通訊渠道，例如互聯網（如網頁、移動設備）、互動終端、固定電話網絡或其他電子終端／設備，為客戶提供產品和服務。就本指引而言，電子銀行是指通過網上銀行[1]、自助服務終端[2]以及電話銀行[3]渠道向客戶提供的金融產品和服務[4]。

1.2 電子銀行帶來效益但也伴隨着風險。因此，獲許可機構須根據風險的種類、複雜性、允許的交易金額及其使用的電子渠道採取相應的風險管理控制。

1.3 本指引的目的是制定主要原則，並從技術和運營的角度，為獲許可機構就識別、評估和管理與電子銀行相關的風險提供指導。

---

1 網上銀行是指通過互聯網向客戶的設備（包括個人電腦和移動設備）提供金融服務。

2 自助服務終端是指獲許可機構用於向其客戶提供金融服務的互動終端（包括但不限於自動取款機、現金存款機、支票存款機和虛擬櫃員機）。

3 電話銀行是指通過電話線路或移動通訊網絡提供的金融服務（包括專人接聽和互動式話音回應的電話銀行服務）。就本指引而言，電話銀行不包括以銷售推廣，活動通知／回撥確認，或客戶關係管理為目的所提供的銀行服務。

4 金融產品和服務包括但不限於以下內容：申請新產品和服務，查看貸款和存款帳戶的餘額及交易，進行電子銀行的交易（包括電子錢包和預付卡），帳戶轉帳，認購股票和投資產品，提交信息，查看或管理聚合帳戶，通過手機銀行應用程式進行零售支付，電子錢包或預付卡的資金存入和使用，接入自助服務終端，以及接入提供電子支付服務的第三方支付平台等。

1.4 本指引適用於在本地註冊的信用機構，也適用於外地信用機構在澳門開設的分行。所有正在或準備開展電子銀行業務的信用機構須採用本指引的主要原則，建立穩健、有效的風險管理程序；強化系統的運行可用性、安全和恢復能力；以及實施嚴格的保密制度和關鍵的管理守則以保護客戶資料。在適用的情況下，本指引也適用於已使用或將使用電子通訊渠道提供服務的其他機構[5]：

(a) 根據第 15/83/M 號法令獲許可經營的金融公司；

(b) 根據第 25/99/M 號法令獲許可經營的資產管理活動的機構；

(c) 根據第 83/99/M 號法令獲許可經營的投資基金管理公司；及

(d) 根據《金融體系法律制度》獲許可經營的金融中介機構和其他金融機構。

1.5 下文各段列出電子銀行對獲許可機構所帶來風險管理的挑戰、期望獲許可機構須實施的關鍵風險管理程序，以及對電子銀行系統進行相關評估的監管要求。須注意的是，由於科技的不斷快速發展，本指引所列舉的建議並非決定性的。獲許可機構須適當參照其他相關及適用的行業標準和做法，以保證電子銀行的風險管理程序合時和適用。

1.6 AMCM 認同巴塞爾銀行監察委員會（下稱“巴塞爾委員會”）2003年7月頒佈的文件《電子銀行風險管理原則》(http://www.bis.org/publ/bcbs98.htm)和《跨境電子銀行活動管理和監管》(http://www.bis.org/publ/bcbs99.htm)做法，並鼓勵獲許可機構閱讀和理解這些文件定出的主要原則。

2. 電子銀行所帶來的風險及相關風險管理挑戰

2.1 巴塞爾委員會認為，電子銀行的基本特性對銀行機構構成了很多風險管理挑戰：

第一，科技和客戶服務創新方面的急速變化，對機構而言，需要在很短的時間內推出新的業務應用軟件，產生了競爭壓力。競爭也增加了機構在實施新電子銀行應用軟件前，進行足夠的策略評估、風險分析及安全檢查的

[5] 信用機構及在此處所指的其他金融機構，以下簡稱為“獲許可機構”。

必要性。

第二，交易性電子銀行網頁及相關的零售及批發業務功能，與舊電腦系統的整合，使機構更加依賴於健全的系統設計和架構，以及系統的互通能力和營運可擴展性。

第三，隨着對資訊科技依賴程度的提高，與不受監管的第三方機構建立夥伴聯盟和外判安排的趨勢越來越明顯。

第四，公開電子網絡的普遍性和全球性使得安全控制、客戶身份認證、資料保護、審計軌迹和客戶私隱等都變得更加重要。

2.2 儘管電子銀行所涉及的風險種類不是新的，但當中一些風險的產生方式、規模和潛在後果都出現了新的維度。為着監管之目的，AMCM列出以下幾種常見的電子銀行相關風險，獲許可機構瞭解後將有助其識別、計量、監測和控制這些風險：

(a) 策略風險。這是指因為不利的業務決策、執行決策不當或缺乏對行業變化作出反應，而產生的對現時及未來盈利和資本的影響。管理層在決定開發某種特定的電子銀行產品前，須瞭解與電子銀行相關的風險，同時也須考慮此產品和科技與獲許可機構的策略計劃是否相吻合，有否配置適當的專業人員和資源以識別、監測和控制這些風險。

(b) 操作風險。這是指錯誤或欺詐風險，或系統未能對交易或狀況進行適當記錄、監測和記帳的風險。如果業務操作未有經過仔細規劃、實施和監測，可能存在較高的電子銀行操作風險。獲許可機構提供電子銀行產品既要滿足客戶要求，也要確保自身有適當的產品組合和提供準確、及時和可靠服務的能力。使用電子渠道進行業務的客戶通常都難以容忍錯誤和遺漏的出現。獲許可機構的電腦和網絡系統受到網絡攻擊或入侵是操作風險主要關注之一，獲許可機構須建立健全的預防和偵查控制手段，保護其電子銀行系統以免遭受網絡攻擊。此外，獲許可機構須備有應急方案和業務恢復計劃，以確保在非常情況下能夠繼續提供不間斷的電子銀行產品和服務。

(c) 法律風險。這是指違反或不遵守法律、法規或職業道德標準而對盈利和資本產生的風險。法律風險將使獲許可機構受到處罰、賠償損

失、合約無效、信譽受損、業務機會及擴展潛力受限等影響。大部份電子銀行客戶會同時選用非電子（如實體分行）及電子銀行渠道，獲許可機構須向客戶保證使用這些渠道傳輸的資訊是一致和準確的，以及符合法律和法規的要求。

(d) 信譽風險。這是指由於負面的公眾意見而對現時或未來盈利和資本產生的影響。獲許可機構的信譽可能因電子銀行服務不佳而受損，損失客戶，引起公衆不滿。通過精心設計的營銷，包括資訊披露，是一種可教育潛在客戶的方法，有助減少信譽風險。獲許可機構須確保客戶了解電子銀行所提供的產品或服務，以及使用電子銀行系統可能產生的效益和需承擔的風險，同時，在營銷過程中，對產品的宣傳要公正和準確。

(e) 流動性風險。這是指由於無法及時提供足夠資金以滿足贖回和結算需求，而對運營造成影響，從而對獲許可機構的收益或資本帶來的風險。對於提供電子銀行業務的獲許可機構，資金流動性風險可能很大，因為與傳統銀行業務方式相比，電子銀行業務可以讓客戶更便利地將大量資金轉移到其他機構。獲許可機構在執行超出預設的流動性風險承受能力的大額或大量交易之前，須注意並制定適當的流動性風險管理政策和程序。更多有關流動性風險的穩健管理實踐，可查閱 AMCM的《流動性風險管理指引》。

(f) 信用風險。這是指由於借款人無法在到期時或其後的任何時間全額清償債務，而對獲許可機構的持續經營能力和盈利能力產生的影響。無論通過何種渠道提供服務，獲許可機構須有適足的程序評估信貸申請和借款人的信用狀況，以妥善管理相關信貸風險。

3. 董事會和管理層的監督

3.1 董事會和高級管理層有責任和義務管理及控制與電子銀行相關的風險。董事會和高級管理層要充分認識電子銀行的基本特徵及其所帶來的挑戰，建立穩健的電子銀行風險管理機制，同時也須具有管理其機構電子銀行所使用技術和產品的知識和技能，以便可適時修改既有的風險控制體系，以確保有關體系能充分識別、評估、監測和控制電子銀行相關的風險。為此，董事會和高級管理層須：

(a) 在進行下列事項前，作出適當的策略評估和全面的成本、效益和風

險分析：

- 將電子銀行業務納入公司策略目標的決定；
- 確定獲許可機構的風險取向；及
- 確定電子銀行服務的複雜程度及支援此類服務的技術。

(b) 評價業務計劃的可行性，並確保機構具有開展電子銀行業務所需的財務、人力、技術資源、專業能力（包括內部或從第三方獲取的），以及適當的風險管理及內部控制程序；

(c) 制定切合目的的政策和程序，以對電子銀行風險進行及時的評估、監測和控制，這包括：

- 建立主要授權和報告機制，包括上報有關影響機構安全、穩健或信譽事件的必要程序；
- 在適用情況下，根據相關監管指引（如 AMCM《反洗錢及反恐怖融資指引》和相關補充說明），制定措施以確保非面對面的客戶符合有關盡職調查的要求；及
- 制定其他必要措施，以解決為確保電子銀行產品和服務的完整性及可用性的相關特有風險因素。

(d) 為電子銀行相關活動建立健全的安全控制系統，以管理和儘量減少由於潛在的內部和外部安全威脅而帶來的安全風險（參見第 4 段）；

(e) 建立監控機制、流程和程序，以有效地檢測並應對可疑和異常的交易或活動（參見第 5 段）；

(f) 建立有效的業務持續管理控制，如業務持續和應急計劃、處理內部和外部風險的事故響應計劃、以及在服務中斷時進行必要通知等，以管理影響服務可用性的突發事件（參見第 6 段）；

(g) 建立全面及持續的盡職調查和監控程序，以管理有關支持電子銀行業務的外判關係及其他第三方服務（參見第 7 段）；及

(h) 為倘有的跨境電子銀行服務建立有效的管理控制措施（參見第 8 段）。

3.2 鑑於電子銀行業務環境的不斷變化，董事會和高級管理層須定期審查相關政策和程序，以確保政策和程序合時並適用於電子銀行業務的性質和範

圍。董事會和高級管理層須評估及持續監測和分析，因應推行和日常維護電子銀行業務而對機構所產生的財務影響，並考慮有關業務對客戶基礎、貸款質量和組成、存款量及其波動性、流動資金來源、交易量等的潛在影響，以及因採用新的渠道而對其他相關方面的影響，以確保所有相關影響得到適當的管理和控制。

3.3 董事會和高級管理層可通過審查客戶使用量、投訴、故障時間、未對帳交易及系統使用率等定期報告，以監測電子銀行業務。另外，適當和獨立的審計也是監測電子銀行業務的重要組成部分。審計的範圍須與電子銀行的複雜性和風險相匹配，而且須包括整個電子銀行業務流程（如網絡配置及安全、與舊系統的連接、監管合規性、內部控制及由第三方所提供的支持活動等）。

4. 安全控制

網上銀行

4.1 獲許可機構須意識到網上銀行必須安全，才可獲得客戶和企業的高度信任。銀行管理層有責任確保通過電子渠道所處理的交易和資訊是受到妥善保護。為此，獲許可機構須擁有穩建而全面的網上銀行安全控制系統。

4.2 為處理和控制網上銀行相關風險和安全威脅，獲許可機構的安全控制系統須符合下列目標：

(a) **身份認證**。獲許可機構須使用可靠和適當的認證方法來確定和核驗其網上銀行客戶的身份和授權，並應考慮管理層對相關場景／交易風險的評估結果而採用適當和合理的身份認證方法。同時要對身份認證方法的成本（包括涉及的科技和內部程序），與有關方法所提供的保護程度、機構自身和客戶交易及資料的價值和敏感度等進行權衡。此外，還須注意的是，一個合理系統的組成要素，將隨着科技和標準的演進而改變。

一般情況下，身份認證的過程是通過認證三個因素中的一個或多個因素而確定客戶所宣稱的身份，它們是：“客戶知道的”（如密碼或個人身份號碼）、“客戶持有的”（如智能卡、安全密碼器或電子證書）及“客戶獨有的”（如指紋、虹膜紋理或面部圖像等生物

特徵）。

通常情況下，多因素的身份認證方法要比單一因素[6]更難被破解，故具有更高的可靠性。因此，對於允許高風險交易[7,8]的電子銀行渠道，須實施雙因素認證方式（"2FA"，例如要求客戶使用另一種因素如一次性密碼（OTP）[9]、交易簽名[10]或生物認證）。在登入網上銀行時，獲許可機構須考慮採用 2FA 認證客戶的身份。此外，獲許可機構須在進行每筆高風險交易前採用 2FA，以重新認證客戶的身份。然而，對於價格頻繁波動的金融產品認購和交易，獲許可機構可選擇在執行此類高風險交易前，在每個登錄會話只要求進行一次 2FA 以認證客戶身份，而無須每筆交易都要求 2FA。

與此同時，獲許可機構須對網上銀行服務所採用的身份認證方法進行持續的評估和評價，以確保身份認證機制的有效性。用於保持客戶身份認證機制有效性的常見做法包括：

- 對身份認證方法進行風險評估，包括在(i)採用該等方法之前；(ii)實施方法後；以及(iii)發生了影響所採用方法的整體安全狀況的重大事故時；
- 為 OTP 設置合理的有效期[11]，使 OTP 在指定有效期限過後無法用於身份認證；

---

6 使用客戶身份標識和密碼進行確認屬於單因素確認，因爲這兩項信息都是"客戶知道的"。

7 高風險交易至少應涵蓋高風險資金轉帳，包括 (i) 轉帳到未登記的第三方收款人；(ii) 向未登記的高風險商戶支付帳單；以及 (iii) 向未登記的第三方進行金錢或非金錢利益相關（例如信用卡獎勵積分）的網上轉帳。

8 除上述的高風險資金轉帳外，高風險交易還包括 (i) 網上登記第三方收款人或高風險商戶；(ii) 建立新的帳戶綁定（如將銀行帳戶與社交媒體帳戶綁定以接收重要信息，或將銀行帳戶或支付卡與移動支付應用程式綁定）；(iii) 上提交易限額；(iv) 更改帳戶聯繫信息（如電子郵件地址、聯繫電話號碼、郵寄地址）；(v) 在網上銀行應用介面上披露客戶帳戶的全部聯繫信息；(vi) 管理銀行帳戶（如創建用戶帳戶）；(vii)金融產品認購和交易。

9 OTP 是一種密碼，僅可單次使用於訪問的身份認證。即使該一次性密碼被騙徒獲取，也無法重複用於後續的身份認證。

10 交易簽名是由獲許可機構通過預先登記的渠道（如電子簽名）創建的一次性驗證碼，以用於身份認證。

11 一般而言，OTP的有效期不應超過100秒。

- 當變更現有的身份認證因素（例如密碼、認證密碼器、記錄在電子設備上的生物辨識資料如指紋／ 虹膜紋理／面部圖像）時，須以安全方式進行充分的客戶身份認證（例如，使用 2FA 和安全問題認證客戶身份）。而在變更用於身份認證的敏感信息時，須及時透過不同渠道向客戶發送通知；
- 採用密碼學和系統完整性控制措施，以保護用於身份認證的敏感數據；及
- 實施用戶會話控制措施，阻止併發會話及終止在一段時間內未作任何響應的登錄會話，以防止已經過身份認證的會話受攻擊（例如，會話劫持）。

(b) **不可否定**。不可否定包括建立電子信息的來源或傳送的證明，保障發送人免受接收人虛假地否認曾接收資料，或保障接收人免受發送人虛假地否認曾發送資料。獲許可機構須根據網上銀行交易的重要性和種類，採取適當措施，以保障經外部和內部網絡傳送的電子資訊的準確性和完整性，以建立網上銀行交易的不可否定性及確保交易的保密性和真實性。例如，使用公匙密碼術、電子簽名和電子證書等安排，能有效識別始發交易的人，而對交易附加電子簽名，能偵查未經授權的修改和防止隨後的否認。

(c) **資料和交易的真實性**。資料真實是指保證所傳送、處理及儲存的資訊沒有被未經授權修改。若未能保證交易、記錄和資料的完整性，獲許可機構將遭受財務損失和面臨巨大的法律和信譽風險。獲許可機構須確保已採取適當措施，保證所傳送、處理和儲存資訊的準確性、完整性和可靠性。在網上銀行系統環境中，保持資料真實性的通常做法有：

- 在處理網上銀行交易的整個過程中須具備高度防篡改的控制；
- 在儲存、訪問和修改網上銀行的記錄時須具備高度防篡改的控制；
- 在設計網上銀行交易和記錄保存過程，須確保所有未經授權的更改能被偵測；

- 建立適當的更改控制政策，包括監測和測試程序，以防止網上銀行系統的變更可能錯誤地或無意地損害有關的控制或資料的可靠性；及
- 任何對網上銀行交易或記錄的篡改，須可以被交易處理、監測和記錄保存功能所偵測。

(d) **職責分離**。職責分離是內部控制的基本要素，旨在減低在操作過程和系統內的欺詐風險，並保證交易和資產均獲得適當授權。須作分離及由不同人員進行的職責包括系統功能操作、系統設計和開發、應用系統維護、電腦系統運維、資料庫管理、安全管理、數據安全、整理和備份資料檔案保管等。對於安全管理職能，最好實行輪崗及交叉培訓。對於交易流程，須防止同一人員可以在系統中發起、批准、執行及輸入交易，以防止欺詐行為得以實施與隱瞞。

(e) **授權控制**。獲許可機構須嚴格控制授權和特權訪問，不適當的授權控制將會讓用戶更改其授權、避開職責分離控制及進入無權訪問的網上銀行系統、網絡、數據庫或應用程式。授權和訪問許可須以工作職責及履行該等職責的必要性為基礎，並遵守以下基本原則：

- 須根據僅需使用原則授予用戶訪問權限。不論職務或職能的高低，任何人均無固有權利擁有機密資料、應用程式、系統資源或設施的權限，只有獲得適當授權的用戶才可以訪問機密資料和使用系統資源，且僅用於合法目的；及
- 須採取適當措施，以確保不再需要的訪問權限得以及時撤銷或停用。

(f) **審計軌迹的保留**。獲許可機構如不能對網上銀行活動保留清楚的審計軌迹，其內部控制可能會被削弱。獲許可機構須確保所有網上銀行交易均留有清楚的審計軌迹，以對所有重要的網上銀行活動和應用程式進行獨立審計。這特別適用於下列種類的網上銀行交易：

- 客戶帳戶的開立、修改和關閉[12]；

[12] 獲許可機構須在與客戶建立業務關係之初，根據AMCM 的《反洗錢及反恐融資指引》及相關補充說明，進行嚴謹的客戶身份識別、認證和盡職調查程序。

- 任何有財務後果的交易；
- 任何容許客戶超出限額的授權；及
- 任何系統存取權限或特權的授予、修改和撤銷。

(g) **敏感資訊的保密**。保密是保證敏感資訊只有得到授權的人方能獲取。誤用或未經授權披露敏感資料和記錄，將使獲許可機構面臨信譽和法律風險。因此，獲許可機構須採用適當的技術（如密碼學技術），以確保敏感資訊在內網及外網傳送時，以及在內部系統儲存時的保密性和完整性。同時，須採用經過廣泛測試並獲得國際認可的安全密碼學演算法，以保護通過外網（包括互聯網）傳輸的客戶資訊，以及於內網中儲存和傳輸的高度敏感資訊（如客戶登錄憑證）。

4.3 獲許可機構的安全控制可包括使用硬體和軟體工具及其他的安全措施，來阻止所有關鍵網上銀行系統、伺服器、網絡、數據庫和應用程式的未經授權訪問。獲許可機構除須履行第 4.2 段所述有關保障資料及運作流程的真實性和保密性的目標外，亦須確保應用系統的安全達到適當水平，並建立與行業最佳做法相吻合的基礎設施，以及實施其他足夠的控制，以有效管控機構所面臨的安全風險。須考慮的相關控制包括但不限於：

(a) 持續對攻擊源頭、情景和技巧進行瞭解；

(b) 部署非軍事區（DMZ）和多層防火牆以確保網絡基礎設施的安全；

(c) 保持最新的資訊設備庫存清單和網絡圖；

(d) 快速識別和緩解系統的漏洞；

(e) 實施對外部連接的網絡訪問控制；

(f) 使用系統入侵檢測工具及備有相關的應對程序；及

(g) 確保所有網上銀行電腦設備和媒介的物理安全。

4.4 獲許可機構對網上銀行系統進行任何重大變更或大幅提升[13]前，須進行技

[13] 重大改變或大幅提升是指系統基礎設施或功能的變化，但不包括任何維護工作或日常／常規運營服務，例如安裝補丁、硬件更換等。

術安全評估，以驗證安全控制的有效性。此外，須定期對現有網上銀行系統（即使未有進行任何重大變更）進行技術安全評估（例如，至少每年進行漏洞掃描和滲透測試），以評估安全控制的持續有效性。相關的技術安全評估須包括但不限於：

(a) **配置審查。**獲許可機構須對網絡組件，如防火牆、伺服器及任何其他支援網上銀行系統的相關設備，進行配置審查，藉着網絡組件來限制未經授權的活動及縮小攻擊面，以降低安全風險；

(b) **源代碼審查。**獲許可機構須對任何源代碼變更進行源代碼審查，尤其在對網上銀行系統推出重大變更或大幅提升前，以識別由於編碼錯誤、不安全的編碼慣例或惡意嘗試而引致的安全缺陷。源代碼審查的範圍、方法和結果須作出正式記錄。對於由第三方服務提供者開發及／或維護的網上銀行系統，獲許可機構須要求其服務提供者提供獨立的評估報告及／或相關測試的證明，以驗證服務提供者在作出任何源代碼變更後已進行源代碼審查。獲許可機構須審閱有關評估結果；

(c) **漏洞掃描。**獲許可機構須定期對支援網上銀行系統的外部和內部網絡組件進行漏洞掃描，以識別安全漏洞和相關潛在風險。經評估潛在的影響和風險程度後，須及時採取補救措施（如安裝補丁），以修復已識別的安全漏洞；及

(d) **滲透測試。**須定期及在系統架構或資產發生重大變更後，由合資格的獨立方以風險為本的原則對網上銀行系統進行滲透測試。滲透測試須模擬實際攻擊情景，覆蓋所有支援網上銀行系統的組件，以識別漏洞和潛在威脅。

4.5 獲許可機構須定期評估其安全控制系統以保證其持續有效，並持續對不同層級的員工提供培訓，使員工具備必要的技能，以遵守安全控制體系的要求，並瞭解相關技術和行業的最新發展。對負責監督網絡安全、虛擬化安全、數據庫安全和終端安全等重要技術控制的人員，技術培訓更尤其重要。

4.6 隨着網上銀行的使用日益增加，為客戶提供的線上服務種類不斷擴展。獲許可機構須識別特定網上銀行服務所附帶的風險，並實施足夠的控制措施以儘量減低相關風險。為此，在適用情況下，獲許可機構須執行下

列第 4.7 至 4.12 段所述的額外安全措施，以應對**資金轉帳、線上提交資料、遙距開戶服務、帳戶聚合服務**[14]及**開放應用程式介面（開放API）**所附帶的風險。

4.7 為確保**資金轉帳**功能已實施充分的安全控制，獲許可機構在進行第 4.2（a）段所述的高風險資金轉帳前，須採取適當的身份認證措施。然而，如轉帳金額不超過客戶和獲許可機構設定的交易限額，獲許可機構可對未登記收款人的小額資金轉帳選擇豁免進行 2FA 的要求。客戶設定的交易限額須受獲許可機構設定的限額所約束。獲許可機構須：

(a) 制定審慎的政策和有效的保護措施，包括制定恰當的交易限額，以減低向未登記收款人進行未經授權的大額資金轉帳的風險。開設新的網上銀行帳戶時，獲許可機構須先關閉高風險資金轉帳功能或將相關的交易限額預設為零。此外，若帳戶在一段時間內未被使用（該期限通常不超過18個月），獲許可機構須考慮重置向未登記收款人進行大額資金轉帳的交易限額為零；

(b) 採取適當的控制措施，如要求客戶需事先申請或激活，才能使用小額資金轉帳功能，以防止客戶在不知悉的情況下使用有關轉帳功能。在任何情況下，一旦客戶進行資金轉帳，須通過客戶預先登記的渠道及時向客戶發送通知；

(c) 當客戶激活資金轉帳功能、設置或增加轉帳限額時，須明確地告知客戶當中所涉及的風險；

(d) 為企業客戶提供雙重授權控制的選項；及

(e) 須確保機構的流動性風險管理系統，能夠有效地監控、評估、控制和管理在正常和壓力情景下的流動性風險，特別是當客戶在短時間內通過網上銀行渠道轉出大量資金的情況。

4.8 獲許可機構須實施充分的安全控制，減低客戶通過互聯網提交資料和文檔，即**線上提交資料**服務，所產生的風險。獲許可機構須考慮數據的敏感性和常見攻擊媒介，建立適當的系統措施。獲許可機構須：

[14] 帳戶聚合服務是指將不同機構的信息匯集在一個平台上，讓客戶無需分別登錄這些機構的服務，即可訪問該客戶在其他機構的帳戶信息。

(a) 部署先進的密碼學機制和其他保護控制，以保持客戶提交的敏感資訊和文檔的保密性和完整性；

(b) 對網上銀行系統實施足夠的保護控制，以防止透過系統提交的文檔被惡意軟件攻擊；

(c) 建立監控系統，以檢測並應對上傳的惡意文檔；及

(d) 執行額外的檢查以認證客戶身份。

4.9 獲許可機構須採取適當且有效的流程和技術，以控制**遙距開戶服務**[15]的冒充風險、洗錢和恐怖主義融資風險。當客戶未能親臨進行身份識別時，獲許可機構較難核查文檔的真確性和客戶的身份。獲許可機構須：

(a) 妥善認證身份資料，例如檢查所提交身份文件的安全特徵，使用可靠且獨立的技術（如光學字型辨識技術）提取身份資料。提取的身份資料須與透過適當且有效的流程和技術（如面容識別、指紋、虹膜掃描、肢體活動偵測或實時視訊會議）所取得的客戶實時生物辨識資料進行比對；

(b) 妥善保存在遙距開戶過程中涉及客戶的相關文件及資料，以確保能在被要求時可迅速地檢索；

(c) 在遙距開戶服務應用新技術前進行評估，並持續監控所應用技術的有效性，尤其是在技術應用及運作初期。

4.10 獲許可機構在與其他機構合作推出**帳戶聚合服務**前，須部署適當的控制措施。獲許可機構須：

(a) 根據適用的本地或海外法律和監管要求，包括但不限於個人資料私隱，反洗錢及反恐融資的要求，對服務範圍進行審查；

(b) 評估業務模式並實施適當的措施，以應對服務所衍生的潛在風險（例如，信譽風險，法律和合規風險，操作風險）；

(c) 與合作機構建立適當的程序，以處理客戶查詢或投訴及任何財務

[15] 在適用時，獲許可機構須採取AMCM《反洗錢及反恐融資措施的補充說明 - 客戶遙距開戶》中的額外控制措施。

糾紛；

(d) 實施網絡和應用程式安全控制，以減低任何與合作機構的連接而對網上銀行系統帶來的入侵風險；及

(e) 預先獲得客戶對服務的同意，並向客戶充分披露服務的條款、風險和限制。

4.11 應用程式介面（API）是指不同軟件應用程式之間的接口，以實現應用程式之間的數據傳輸或功能調用。**開放APIs**是由一個組織對外開放的API，允許第三方（如客戶、業務夥伴[16]）訪問其資訊系統。

一般而言，開放API可以分為交易型和信息型API，這些API可便利獲許可機構提供不同的網上銀行服務（如帳戶資訊查詢、資金轉帳、交易執行等）。

允許公眾使用開放API可能產生額外的安全風險，獲許可機構須考慮根據開放API功能的性質、複雜性和重要性，實施額外的安全措施。獲許可機構須：

(a) 在任何新的開放API服務投入到生產環境前，進行充足的功能、性能和安全測試；

(b) 對開放API規範的任何變更，保留正式的文件和記錄；

(c) 對於涉及處理敏感客戶資料和高風險交易的開放API服務[17]，應對業務夥伴進行全面的盡職調查。獲許可機構須透過其正式渠道公開業務夥伴及其相關產品（如移動應用程式或網站）的名單，以確保公眾信任和消費者保障；

(d) 在將任何客戶資料共享給業務夥伴前，需預先獲得客戶的同意，並向客戶充分披露有關條款及風險；及

(e) 建立風險為本的持續監控機制，持續審查系統架構、安全性和數據標準，確保正在使用的開放API持續符合相關監管要求和行業最佳

16 包括金融機構。

17 服務包括但不限於：(i) 線上提交／申請信用卡、貸款或其他產品或服務；(ii) 客戶檢索和修改其帳戶資訊；(iii) 客戶發起交易、支付和預定付款／轉帳。

實踐。

4.12 **手機銀行（包括移動支付）**正成為提供金融服務的重要平台。手機銀行平台涉及特定的風險，包括但不限於對手機銀行客戶的身份認證不足、移動設備惡意軟件和病毒、移動設備的不安全數據傳輸和儲存等。因此，除了滿足網上銀行的安全措施外，獲許可機構須：

(a) 對手機銀行實施嚴格的身份認證控制。由於使用同一移動設備訪問網上銀行並接收或生成 OTP 可能削弱 2FA 的有效性，獲許可機構須實施額外的風險緩解措施。例如，客戶更改手機號碼須僅可通過具備適當身份認證（不包括僅以SMS OTP 作為2FA）的安全渠道進行，以及高風險交易須在考慮相關交易風險、身份認證機制的嚴謹程度及監控欺詐能力後，合理延遲後才生效。此外，須採取額外措施以加強對 OTP 身份認證控制，包括限制 OTP 的有效期、實施穩健的加密金鑰管理實踐，以及定期評估採用 OTP 進行客戶身份認證的有效性；

(b) 制定有效的安全控制措施，保護在客戶移動設備處理和儲存的數據。獲許可機構須在可行的情況下，確保手機銀行會話結束後，客戶敏感資料不會儲存或緩存在移動設備；

(c) 實施監控機制和處理流程，以檢測與移動設備相關的潛在安全風險（如已破解／越獄的設備）並觸發警示。獲許可機構須在允許客戶訪問手機銀行服務前，明確警告客戶使用有潛在安全風險設備訪問手機銀行服務的風險，甚至考慮限制此類設備訪問手機銀行服務；及

(d) 在客戶發起高風險交易或小額資金轉帳至未登記收款人時，當原交易通知可通過移動設備查閱，立即透過不同於原通訊渠道的其他已登記通訊渠道，向客戶發送額外通知。

特定電子銀行渠道

4.13 除適用於網上銀行的一般控制措施（第 4.1 至 4.12 段）外，如獲許可機構有透過**社交媒體平台**、**自助服務終端**和**電話銀行**向客戶提供服務，須實施下列第 4.14 至 4.16 段所述的安全措施，以應對上述特定電子銀行渠道所產生的風險。

4.14 當允許通過**社交媒體平台**訪問銀行服務時，獲許可機構將面對多種風險，包括但不限於由不安全的介面或連接導致客戶資料外洩，因平台的安全漏洞導致系統被入侵，因平台服務中斷和客戶糾紛處理不當而引致的信譽風險。獲許可機構與社交媒體平台／網站合作前，須採取以下措施：

(a) 評估與平台／網站合作的合適性，包括其財務狀況、風險管理控制的充分性及防止資料外洩的記錄；

(b) 進行法律盡職調查，以確保符合所適用的本地或海外法律和監管要求；

(c) 實施適當的安全控制措施並進行定期評估，以減低入侵機構的電子銀行系統和網絡的風險，以及在數據傳輸過程中客戶數據洩露的風險；及

(d) 確保有適當的安排，以妥善跟進客戶投訴，以及因平台／網站問題而引起的可能財務損失作出責任分配。

4.15 當允許通過**自助服務終端**使用銀行服務時，獲許可機構須進行定期評估，以識別和評估包括但不限於銀行卡資料竊用攻擊、終端被未經授權訪問和控制，以及未能檢測和處理偽鈔等風險，並須實施適當的風險管理措施以應對有關風險。此外，獲許可機構須密切監察與自助服務終端相關的新興網絡攻擊和漏洞，並採取適當措施以應對相關風險。

4.16 在**電話銀行**業務中須實施適當的客戶身份認證控制，以減低客戶身份被冒充的風險。常見的身份認證方法包括電話銀行密碼、生物認證技術和身份確認問題。獲許可機構須注意可能減弱身份認證方法有效性的風險（例如，身份確認問題的答案可從公開渠道獲得），並在需要時採取額外的措施，包括詢問具有動態答案的問題，例如與最近交易相關的信息。如果電話銀行服務允許高風險交易，須採用 2FA 認證客戶身份。此外，獲許可機構須實施適當的控制措施（例如，按僅需知悉原則提供客戶資料的訪問權限，以及保存有關訪問身份認證問題和答案的記錄），以應對可訪問身份認證問題答案的員工（或服務提供者）可能使用該資訊冒充客戶身份的風險。

客戶安全

4.17 獲許可機構的首要責任，是確保客戶在使用電子銀行渠道的安全性與傳統銀行服務渠道的安全水平保持一致。特別地，獲許可機構須根據第 4.18 至 4.22 段所述的要求，提升客戶安全性，如透過充分的提示和提高認知的活動、及時的通知、對可疑或欺詐來源採取有效的預防措施、適當的資訊披露和客戶私隱資料保護等措施。

4.18 倘若客戶不知道或不瞭解使用電子銀行服務的必要安全預防措施，獲許可機構的安全風險可能會更高。作為上述安全控制措施的補充，獲許可機構須通過各種渠道[18]，定期向客戶提供易於理解的電子銀行安全預防措施提示（例如，密碼的選擇和保護、電子銀行欺詐的防範、避免使用公共或共用電腦及不安全網絡訪問電子銀行的客戶提示、欺詐電郵／網站／短信／流動應用程式的防範，以及病毒及惡意程式的防護等），並向客戶說明應採取適當電子銀行安全預防措施[19]的責任。獲許可機構須制定客戶教育和認知計劃，以減少客戶因誤用特定渠道（如移動設備）所帶來的風險。

4.19 通過電子銀行系統進行任何高風險交易，須及時透過預先登記的渠道向客戶發送通知，以便客戶檢測未經授權的交易。每條通知消息須包含與該交易相關的明細，包括交易類型、收款人的部分信息、交易金額等（如相關資訊適用於有關交易）。客戶可選擇不接收“交易執行”的通知，惟在此情況下，獲許可機構須向客戶提供充分的風險披露，並請客戶確認知悉所涉及風險。

4.20 採取預防措施以防範欺詐網站、電郵、短信、流動應用程式、社交媒體帳戶或電話的風險，這包括提醒客戶，獲許可機構不會透過網絡渠道（如電郵、超連結、短信、附件）或電話向客戶索取敏感的帳戶和個人資料；以及提醒客戶不要通過電郵、短信或互聯網搜索器內的超連結登入電子銀行帳戶。獲許可機構須主動和定期搜尋欺詐網頁和流動應用程式，以對有關的存在保持警惕。獲許可機構亦須建立恆常的通訊渠道，向客戶通報任何欺詐或不可靠的來源。如發現與自身相類似的欺詐網頁或流動應用程式，獲許可機構須：

---

18 渠道可包括當面溝通、社交媒體平台、正式網頁、流動應用程式、短信、電子郵件、宣傳視頻或單張等。

19 例如，在個人電腦和移動設備上安裝防病毒、防間諜和防火牆軟件，定期更新防病毒和防火牆產品的安全補丁或新版本等。

(a) 向司法警察／網絡安全事故預警及應急中心（CARIC）和AMCM報告；

(b) 採取適當的補救措施，包括嘗試移除欺詐或虛假物；

(c) 通過各種渠道及時通知客戶有關欺詐或虛假物，並澄清與該網頁或流動應用程式無關；如發現含有該網頁或流動應用程式超連結的電郵或短信，須同時澄清沒有發出此等電郵或短信；及

(d) 請曾經透過該網頁或流動應用程式進行交易的客戶，聯繫獲許可機構[20]以便採取補救措施。

4.21 **資訊披露**。為避免客戶混淆，以及讓潛在客戶在使用電子銀行服務前對獲許可機構的身份和法律地位作出判斷，獲許可機構須確保在其網頁或流動應用程式內，向客戶／潛在客戶披露足夠資訊，例如，提供的資訊包括但不限於：

(a) 機構的名稱和總行的所在地（如適用，分行所在地）；

(b) 對機構總行進行監管的主要監管機構的身份（就澳門註冊的獲許可機構而言，即 AMCM）；

(c) 有關客戶如何聯繫客戶服務中心的說明，以解決服務問題、查詢、投訴、懷疑帳戶被不當使用等事宜；

(d) 適用於電子銀行產品和服務的條款，該等條款須明確列出有關服務的費用、獲許可機構與其客戶之間的權利、義務和責任；

(e) 機構的客戶私隱及安全政策，以及客戶在訪問其電子銀行帳戶時須採取的安全措施和合理的預防措施（參見 4.22 段）；

(f) 機構計劃提供或不提供電子銀行服務的地區；及

(g) 其他適當、或特定地區所要求的資料。

4.22 **客戶私隱和保密**。維護客戶資料的私隱是獲許可機構的重要職責。獲許可機構須確保其私隱政策和規範符合適用的相關法律和法規，並須盡力確保：

[20] 獲許可機構應確保其職員具備必要的資訊和知識，以有效地回答客戶的查詢。

(a) 機構的客戶私隱政策和規範，已考慮並符合有關其提供電子銀行產品和服務所在地區適用的所有私隱法規和法律；

(b) 提示使用電子銀行產品和服務的客戶有關私隱政策和相關私隱關注事項；

(c) 披露有關機構查閱和／或處理敏感信息（例如指紋／虹膜紋理／面部影像等生物辨識資料）的相關風險；

(d) 客戶可不允許機構以交叉營銷為目的，與第三方分享客戶聯繫信息、敏感資料（如身份證號碼、信用卡／扣帳卡卡號、銀行帳戶信息）、個人需求、興趣、財務狀況、支付和銀行交易活動等資料；

(e) 客戶資料不會用於超出客戶授權的用途；及

(f) 當提供外判服務的第三方接觸客戶資料時，必須遵守機構所制定的客戶資料使用規範。

有關更多電子銀行客戶私隱保護的最佳實踐，可查閱巴塞爾委員會的《電子銀行風險管理原則》附件V（http://www.bis.org/publ/bcbs98.htm）。

5. 欺詐監控

5.1 由於欺詐技術和策略越趨複雜，欺詐監控對於保護客戶免受欺詐行為和活動所引致的潛在損失具有重要作用。獲許可機構須建立有效的欺詐監控機制[21]，以及時預防、檢測和阻止異常交易或不規則的活動。此外，獲許可機構須密切監測欺詐技巧的趨勢和發展，按需要定期優化欺詐監控機制，並在優化過程中須考慮任何從內部和外部來源所收集的欺詐事件報告、最新威脅和情報等。

5.2 獲許可機構須正式確定並記錄欺詐處理流程和程序，以及時探明和應對欺詐事件。欺詐處理流程和程序須涵蓋預防欺詐行為及對欺詐事件的補救措施，這包括處理懷疑欺詐個案、異常交易，以及由欺詐監控系統觸發的警

[21] 該機制須包括考慮來自可疑的服務訪問來源（如互聯網協議(IP)地址）、異常客戶行為（如用戶通過不常用的設備訪問服務、短時間內在不同國家或地區的自動櫃員機提取現金、短時間內頻繁地向同一收款人轉帳或提取現金）、異常的後續活動（如開通網上銀行／手機銀行帳戶後短時間內更改聯繫方式、更改客戶的手機號碼後短時間內進行大額轉帳至未登記收款人）和其他已知的欺詐案例。

報（如暫停高風險或可疑交易以進行篩查和評估、確定可能的根本原因、及時將事件上報管理層等）。此外，獲許可機構須在必要時透過可靠渠道及時聯繫客戶以確認交易或活動。

5.3 獲許可機構須配置足夠的資源和具有相關知識的專責人員進行欺詐監控和應對。負責欺詐監控和應對的人員須持續接受培訓，使其知識和技能水平能跟上有關新興威脅、趨勢和技巧，以做好欺詐風險管理。

6. 業務持續計劃

6.1 **有效的容量、業務持續與應急計劃**。電子銀行客戶通常期望有關服務7x24小時可用，任何服務中斷均對客戶產生很大影響。正因為這對客戶和客戶服務的潛在影響（如帳單和其他支付交易不能按時執行），獲許可機構須分析服務間斷的後果，採取措施降低間斷的概率，並減少系統恢復時間。為此，獲許可機構須：

- 根據預計未來電子銀行系統的交易量或業務增長情況，定期進行容量規劃工作；透過審查電子銀行系統的網絡和系統架構設計，從而識別出支持有關系統運作所需組件之間的依賴關係；
- 實施措施（如高可用性架構、流量控制），以確保電子銀行系統的可用性；
- 在推出新的電子銀行服務和重大系統變更前，通過模擬各種負載情境，對關鍵電子銀行系統和支援相關系統的網絡及系統基礎設施進行端到端性能測試[22]，以識別潛在的性能瓶頸；
- 對所有關鍵電子銀行系統和支援相關系統的網絡及系統設施，實施自動化性能監控和警報機制，以及時檢測和處理任何可能的服務中斷或性能下降；及
- 就關鍵電子銀行業務處理和交付系統，制定適當的業務持續和應急計劃[23]，並定期對有關計劃進行測試。

---

22 在某些情況下，如果現有服務正在進行重大提升或需要提供7x24服務，則可在“類似生產”的測試環境中進行測試。

23 某些機構鑑於業務交易量、受影響客戶數量和可用的替代服務渠道，可能沒有將電子銀行服務視爲“關鍵業務”，因而在業務持續計劃中未給予高度優先考慮。管理層須定期對此決定進行

有關更多電子銀行的容量、業務持續和應急計劃等方面的最佳實踐，可查閱巴塞爾委員會的《電子銀行風險管理原則》附件 VI（http://www.bis.org/publ/bcbs98.htm）。

6.2 **事故的應對和管理**。獲許可機構須建立適當的事故應對計劃和程序，以管理、遏制及減少突發事件引起的問題，包括可影響電子銀行系統和服務可用性的內部及外部攻擊。有效的事故應對機制須包括：

- 恢復電子銀行系統和服務的計劃；
- 能夠儘早識別及評估有關事故或危機發生時的嚴重性和影響的機制；
- 成立在緊急情況下有權採取行動的事故應對小組，且相關小組人員須獲足夠的培訓，以分析事故檢測／應對系統的內容、理解相關結果的含義及確定需採取的適當行動；
- 涵蓋內部及外判運作的清晰通報程序（如事故升級和內部通報高級管理層的程序）；
- 當出現重大安全問題或破壞性事件時通報AMCM、網絡安全事故預警及應急中心（CARIC）和其他相關監管機構的程序；
- 可充分應對外部各方（如客戶、媒體和業務夥伴）關切的溝通策略；
- 可收集和保留電腦取證的程序，以助後續的審查和對攻擊者的起訴；及
- 定期對電子銀行系統事故應對計劃進行演練，以確保計劃的有效性並熟悉計劃中所定的處理程序。

6.3 **機構面臨服務中斷時的通知**。獲許可機構在檢測到事故後，須主動通過有效渠道通知受影響或可能受影響的客戶。當服務中斷[24]預計會持續一段較長時間時，機構須採取更有效的措施，如發佈新聞稿並持續向客戶提供事故的更新告示（如估計的影響、受影響服務、預計恢復時間、其他可提供

再評估，以確保作出決定的理由仍符合電子銀行服務的實際增長及發展和／或擴展策略。

[24] 在適用的情況下，獲許可機構須實施AMCM《業務持續管理指引》中的相關通報控制要求。

服務的渠道等）。

7. 外判管理

7.1 獲許可機構將部分或全部的電子銀行業務外判[25]予關聯機構或第三方服務提供者已變得相當普遍。不論外判理由為何，機構須清楚其責任和義務並沒有因此而降低和減輕。特別地，機構在外判後仍須遵守《金融體系法律制度》、《個人資料保護法》及其他法規有關保密的規定。因此，機構須對服務提供者的活動進行有效的監督，以識別和控制由此而生的風險，並確保其外判安排符合有關法定要求。機構須按照下列 7.2至7.7 段[26]所述的要求進行外判管理。有關更多電子銀行系統外判管理的最佳實踐，可參閱巴塞爾委員會的《電子銀行風險管理原則》附件 II（http://www.bis.org/publ/bcbs98.htm）。

7.2 獲許可機構須充分瞭解進行外判安排的相關風險。聘用服務提供者前須對其進行盡職調查，以瞭解服務提供者的財務狀況、風險概況、經驗、專業知識、技術的兼容性和客戶滿意度。

7.3 獲許可機構和服務提供者須簽訂正式外判合約，條款須仔細及妥善地以書面形式訂明各方的角色、關係、義務和責任，包括：

(a) 服務提供者所收集或儲存非公開客戶資料的使用限制；

(b) 要求服務提供者採取適當的控制措施，以保障其所持有的客戶資料的安全性，並規範在合約到期或終止後對客戶資料的擁有權；

(c) 網頁／流動應用程式的運行時間、超連結性能、客戶服務反應時間等服務水平標準；

(d) 事故應對計劃，包括通知責任，以及就網頁／流動應用程式的停運、篡改、未經授權訪問或惡意編碼作出的應對；

---

25 外判的業務範圍可包括資訊系統管理（如軟件應用、網頁）、資訊系統運營和維護（如系統或應用程式數據的處理；數據中心、硬件或區域網絡的監控和維護）、中後台運營（如電子資金轉帳、客戶服務、電話中心的維護）、白標安排、業務持續和災難恢復功能。

26 在適用的情況下，獲許可機構須實施AMCM《外判管理指引》和相關的補充說明中的額外控制要求。

(e) 電子銀行服務的業務持續計劃，包括備用處理線路、備份伺服器、緊急操作程序等；

(f) 針對安全、內部控制、業務持續和應急計劃而進行的獨立審查及／或審計的條款；

(g) 在本地或外地進行外判服務分包的限制；及

(h) 有關解決爭議、獲許可機構和相關監管機構索取資料所適用的法律和管轄權。

7.4 獲許可機構須要求服務提供者，實施至少與其自身營運同樣嚴謹的安全政策、程序和控制，同時制定和實施可行的應急和業務持續計劃，以確保其所提供的服務和績效的持續性。服務提供者須隨着技術環境和操作要求的改變，對有關計劃作出定期審查、更新和測試。

7.5 獲許可機構須對服務提供者進行定期（按實際需要）盡職調查，以評估其是否有能力提供所需的服務水平、可保持足夠的安全水平和跟上科技的快速變化。同時，須建立適當的程序，以監督服務提供者的財務狀況、風險概況和合約遵守情況，以及須透過由服務提供者提供的線上或定期書面報告，跟踪其服務表現及／或安全問題、其財務狀況及風險概況等。向服務提供者索要的資料須包括但不限於以下內容：

(a) **服務的可用性**，如服務中斷的頻率和時間長短（包括中斷原因）、正常運行時間和故障時間的比例、客戶所報的登入問題的次數和種類等統計；

(b) **活動的水平和數量**，如透過不同電子銀行渠道（如網絡應用程式、流動應用程式等）獲取電子銀行服務的帳戶數量、API請求的頻率、新的、活躍或停用帳戶的數量和百分比、交易的種類、數量和金額等；

(c) **服務的效率**，如每天按時段的平均應答時間、伺服器容量的使用情況、客戶服務查詢的種類和平均解決時間等；

(d) **安全事故**，如被拒絕的登錄嘗試、密碼重設、企圖和成功滲透的次數、已檢測的病毒或其他惡意編碼的數量和種類，以及任何物理安全控制的違反情況；

(e) **服務提供者的穩健性**，如季度或年度財務報告、新客戶和流失客戶

的數量、系統的變更、員工的流失率和管理層的變化等；及

(f) **質量保證**，如績效報告、審計結果、滲透測試和漏洞評估。

7.6 在整個外判過程中，獲許可機構須有應急方案，以應對現有服務提供者不能繼續運作或提供所需服務。有關方案須考慮由於服務提供者的服務不能達到既定要求、或在盡職調查過程發現其他問題，而需變更服務提供者或服務關係的情況。

7.7 對外判業務的定期審計，將有助確保相關控制是否適當且正常運作。除上述的監察程序外，獲許可機構還須確保對外判業務的定期獨立內部及／或外部審計範圍，至少與其內部開展同類業務時的審計範圍一致。

8. 跨境活動管理

8.1 利用互聯網公開、普及和自動化的特點，許多國際性機構透過其在不同國家／地區的分行或附屬機構的網頁／流動應用程式，為其所在國家／地區客戶提供電子銀行產品和服務。而一些其他機構從其所在地區，通過遠程方式，向另一個其尚未獲取牌照設立機構的地區的居民，提供電子銀行服務。

8.2 巴塞爾委員會定義跨境電子銀行業務為“某機構在一個地區向另一地區的居民，提供**交易性**在線產品或服務”。鑑於進行跨境商業往來將涉及不同的司法管轄權及適用法律的問題，開展跨境電子銀行業務的機構可能面臨更大的法律風險。如不進行充分的盡職調查，機構將有可能面臨違反不同法律和法規的風險，如適用於境外司法管轄區的消費者保護法、廣告和披露法、記錄保存和報告要求、私隱條例和反洗錢法等。

8.3 在開展**跨境**電子銀行業務前，所有在澳門運作的獲許可機構須**事先徵詢 AMCM 的意見**，以確定獲許可機構已滿足下列條件：

(a) 進行了充分和適當的風險評估與盡職調查，以確保能適當管理跨境電子銀行業務相關風險及符合電子銀行業務所觸及的境外司法管轄區的法律和法規；及

(b) 建立有效和持續的風險管理程序，以對開展跨境電子銀行業務所產生的風險進行評估、控制和監測。

8.4 獲許可機構須在其網頁／流動應用程式上作出聲明，清楚指出其所提供的網上銀行產品及服務的對象僅限於指定司法管轄區的居民[27]。雖然這一聲明的法律效果並不確定，但可明確及緩解其盡職調查義務。此外，獲許可機構還須在其網頁／流動應用程式內作出充分的披露，以便潛在客戶能對獲許可機構的身份、註冊地和法律地位作出判斷(參見 4.21(a))。

9. 獨立評估

9.1 鑑於管理電子銀行業務風險的重要性，獲許可機構須在推出相關服務或大幅提升現有服務前，對電子銀行系統進行獨立評估。獨立評估須根據本指引第 3 至 8 段的要求及至少涵蓋以下方面：

(a) 董事會和管理層的監督；

(b) 安全控制；

(c) 欺詐監控；

(d) 業務持續計劃；

(e) 外判管理；及

(f) 跨境活動管理。

9.2 作為第 9.1 段所述獨立評估安排的一部分，第 4.4 段所述的技術安全評估須由合資格的評估人員進行，以在推出網上銀行服務或大幅提升現有服務前，評估網上銀行系統所實施的安全控制的持續有效性。

9.3 此外，根據第 4.4 段中的要求，獲許可機構須至少每年進行一次滲透測試和漏洞掃描。滲透測試的範圍須至少涵蓋機構的網上銀行及通過互聯網或無線網絡提供的任何金融服務。有關評估結果須按 AMCM要求提交，同時，機構須就評估結果採取迅速和適當的跟進行動。

9.4 由機構任命進行獨立評估和技術安全評估的人員（評估者），須具備並展示執行相關工作所需的專業技能，且獨立於開發或管理電子銀行系統的各方、沒有參與被審查的業務運作、或沒有參與選擇或實施相關控制措施，

[27] 或反過來說，獲許可機構應公告其不提供電子銀行產品和服務的司法管轄區。

以及能直接和自由地向機構的高級管理層報告審查的發現。只要符合上述條件，評估者可以是機構的內部職員（如內部審計人員）或外部人員（如外部審計師或其他第三方服務提供者）。

9.5 在首次獨立評估後，獲許可機構須至少每兩年，或當出現重大變更時，進行一次風險評估，以確定是否需要進行獨立評估，以及獨立評估的範圍和頻率。風險評估須充份考慮所提供服務的風險狀況的重大改變、網絡設施和應用系統的重大變更、關鍵系統漏洞或重大的安全隱患等。

9.6 獨立評估的報告須提交予 AMCM，以作現場和非現場審查的參考。如獲許可機構委托不同方分別對其電子銀行服務的不同部分進行獨立評估，向 AMCM 提交的報告可以是合併報告或所有的分項報告。獨立評估報告須至少包括下列內容：

(a) 進行評估的時間段和相關系統的開發階段（如設計或測試階段），以及在評估後有關系統投入運作的跟進安排（如有）；

(b) 評估範圍，包括系統組成、內部網絡、網絡設備、營運和控制程序的描述；

(c) 評估過程中所採用的方法（如訪談、抽樣、技術測試）；

(d) 評估者於獨立評估和技術安全評估的發現（如未解決問題和影響）和改善建議（如補救措施）；及

(e) 管理層的回應，包括已實施的風險控制措施或已制定的整改計劃，以處理未解決的問題。

9.7 在向客戶提供新的電子銀行服務前，獲許可機構須審慎評估與此服務相關的風險，尤其是法律和信譽風險。同時，須進行定期評估，以確保有關管理法律和信譽風險的措施保持適足妥當。在可能和適當的情況下，獲許可機構可為其電子銀行業務購買保險。

10. 監管方式

10.1 鑑於操作、信譽和其他相關風險可能帶來的影響，獲許可機構在開展新的電子銀行服務或對現有服務進行重大變更前，須通知及與 AMCM 討論有關計劃。特別地，在開展跨境電子銀行業務前（參見 8.3 段），須事先諮

詢 AMCM。

10.2 AMCM一般會要求獲許可機構須清楚陳述開展電子銀行業務的策略、前景及其與整體經營策略的配合、相關項目的風險分析與詳細的風險／回報研究。獲許可機構的管理層須表明已審視了目前營運的風險狀況，並考慮了開展電子業務的影響，且董事會（如屬海外機構分行，則為其總行）認為在現有資源、風險管理系統和技術能力條件下，開展電子銀行業務將不會對運營的安全性和穩健性帶來不可接受的不利影響。

10.3 具體而言，獲許可機構須向AMCM證明以下關注點已得到妥善解決：

(a) 董事會和高級管理層有適當的監督；

(b) 與電子銀行業務相關的主要科技控制措施已得到處理；

(c) 已採取適當（包括物理和邏輯）的安全措施及其他必要的風險管理控制措施；

(d) 與外判和跨境電子銀行業務相關的問題已解決；

(e) 就提供新的電子銀行服務，已進行了成本效益分析；

(f) 已建立和記錄電子銀行業務的策略，以明確說明為應對和控制與電子銀行業務相關的所有風險而制定的政策、實踐和程序；

(g) 因應科技、法律和業務環境（包括對資訊安全的外部和內部威脅）的變化，將持續監測電子銀行業務執行計劃的有效性，並定期對計劃進行更新；及

(h) 將持續監測電子銀行業務相關風險。

10.4 在現場和非現場審查中，AMCM將根據本指引的要求，對獲許可機構的電子銀行業務風險管理是否適足作出判斷。對於在本指引公佈實施之前已開展電子銀行業務的獲許可機構，須確保其現行的風險管理系統（包括獨立評估和技術安全評估的安排），儘快或在本指引公佈後的 12 個月內，符合本指引的有關規定。