OR-1 業務操作風險管理

V.2 – 25.07.2022

本單元應連同引言及收錄本手冊所用縮寫語及其他術語的辭彙一起細閱。若使用本手冊的網上版本，可按動其下面劃了藍線的標題，以接通有關單元。

目的

列載金管局在監管認可機構的業務操作風險時將會採用的模式，並就有效的業務操作風險管理的主要元素向認可機構提供指引。

分類

金融管理專員以建議文件形式發出的非法定指引

取代舊指引

2005年11月28日發出的單元OR-1「業務操作風險管理」(v.1)

適用範圍

所有認可機構

結構

1. 引言

1.1 背景

1.1.1 正如單元SA-1《風險為本監管制度》第2節所載，認可機構一般面對8大類風險：信貸、市場、利率、流動性、業務操作、信譽、法律及策略風險。認可機構應制定穩健及有效的制度以管理每類風險。

1.1.2 所有銀行產品、活動、程序及制度都存在業務操作風險。根據巴塞爾銀行監管委員會(巴塞爾委員會)發出的資本標準，業務操作風險的定義是「因內部程序、人員及制度的不足之處或缺失，或因外部事件而引致虧損的風險」。上述定義涵蓋法律風險，但不包括策略及信譽風險。然而，認可機構的業務操作風險管理架構應按情況所需顧及策略與信譽風險。

1.1.3 業務操作風險越來越受關注，原因是銀行：

(a) 日益倚賴越趨複雜的自動化科技；

(b) 開發日趨複雜的產品；

(c) 參與大型併購活動；

(d) 進行整固及內部重組；

(e) 運用某些方法(如抵押安排、信用衍生產品、淨額結算及資產證券化等)以緩減某些風險，但卻可能因此而引致其他風險(如法律風險)；以及

(f) 外判某些職能。

某些銀行由於未能實施妥善的程序及流程以管控業務操作風險，因而蒙受重大的業務操作虧損。

1.1.4 本單元主要以巴塞爾委員會於2021年3月發出題為《經修訂穩健業務操作風險管理原則》[1]的文件為依據。2021年的修訂取代巴塞爾委員會於2003年發出(並因應2007至09年的全球金融危機所汲取的教訓而於2011年作出修訂)的《穩

[1] https://www.bis.org/bcbs/publ/d515.pdf。

健業務操作風險管理原則》，併入進一步指引，以協助銀行落實有關原則、納入其他重要的業務操作風險來源、反映《巴塞爾協定三》改革方案內的全新業務操作風險框架，以及強調確保銀行運作穩健性的原則[2] 的重要性。

1.2 範圍

1.2.1 本單元：

(a) 列載金管局對業務操作風險的監管方法；以及

(b) 就建立穩健的業務操作風險管理架構的主要元素提供指引。

1.2.2 金管局在制定本單元時，參考了以下資料：

(a) 第1.1.4段及附註2提及巴塞爾委員會於2021年發布的兩套原則；

(b) 《有效監管銀行業的主要原則》[3] 第25項原則；以及

(c) 部分國際銀行採納的業務操作風險管理政策及方法。

1.3 法定架構

1.3.1 《銀行業條例》附表7第10段規定認可機構在獲認可之時及之後須繼續備有足夠的會計制度及管控制度。有關制度是確保認可機構審慎及有效率地經營業務、保障機構資產、減低詐騙風險、監察機構所承受的風險，以及遵守法律及監管規定的關鍵。

1.3.2 附表7第12段進一步規定認可機構要以持正、審慎、具專業能力，以及無損存款人或潛在存款人利益的方式經營業

[2] 見巴塞爾委員會於2021年3月發出題為《運作穩健性原則》的文件 (https://www.bis.org/bcbs/publ/d516.htm)。

[3] https://www.bis.org/basel_framework/standard/bcp.htm。

務。正如《認可指引》所載，金管局在評估機構遵守本段的情況時所考慮的因素，其中包括業務操作風險方面的事項，例如應付外來衝擊及突發事件的能力、抵禦內部與外部詐騙事件及避免運作失誤的能力，以及資訊及通訊科技[4]與員工的質素。

1.3.3 此外，《銀行業(資本)規則》(《資本規則》)規定所有在香港註冊成立的認可機構均須在計及其業務操作風險下，維持按照《資本規則》計算的充足的監管資本。

1.4 實施

1.4.1 認可機構應在切實可行情況下盡快制定及實施業務操作風險管理架構，而有關架構應符合本單元所載指引，並與其業務性質、規模、複雜程度及風險狀況相稱。認可機構應定期檢討業務操作風險管理架構，並因應不斷演變的經營環境及業務操作風險管理方法作出更新。

1.4.2 一般而言，本地註冊認可機構的業務操作風險管理架構應涵蓋其附屬公司，並在適當情況下亦涵蓋其他有關連實體(例如有聯繫公司)。在香港經營的國際銀行集團(不論是本地附屬公司或分行形式)可倚賴集團業務操作風險管理架構/政策，並按需要作出修訂，惟須確保就本地業務的規模、性質及複雜程度而言，本地業務的內在業務操作風險得到充分處理。若與銀行集團的香港業務相關的某些業務操作風險管理職能集中於集團或地區層面，有關認可機構在金管局提出要求時應能證明該等在集團或地區層面執行的相關職能就本地業務的規模、性質及複雜程度而言屬適當，並在各重要範疇符合本單元列載的標準。

[4] 資訊及通訊科技指資訊科技及通訊系統的相關實體及邏輯設計、個別硬件及軟件組件、數據及操作環境。

1.5 運作穩健性

1.5.1 運作穩健性指認可機構即使遇到干擾仍能繼續維持關鍵運作[5]。這項能力讓認可機構能夠識別相關威脅及潛在故障，從而保障本身免受影響，並因應有關干擾事件作出應對、變通、復原，以及汲取經驗，盡量減少干擾對維持關鍵運作的影響。在考慮其運作穩健性時，認可機構應假設干擾會發生，並計及在一系列嚴峻但可能發生的情景[6]下其整體風險取向及可承受影響上限[7]。

1.5.2 雖然業務操作風險管理及運作穩健性要達到的目標不同，但兩者關係密切。有效的業務操作風險管理制度及高水平的運作穩健性能發揮共同作用，減低業務操作風險事件的發生次數及造成的影響。認可機構在實施本單元所載指引時，應參考金管局發出載於《監管政策手冊》單元OR-2「運作穩健性」的相關指引。將認可機構的業務操作風險管理架構與其運作穩健性 / 確保遇到干擾仍繼續維持關鍵運作的能力連繫起來的具體指引，載於第2.2.4、5.2.1(g)、7.1.1、7.2.4(f)、7.2.6、7.4.7(a)及(d)、8.1.3、8.3.1(附註23)及8.3.2(a)段。

2. 業務操作風險的監管方法

2.1 目標及原則

2.1.1 每間認可機構應因應其複雜程度、產品及服務範圍、組織架構及風險管理文化，制定及維持具成效及效率的適當業務操作風險管理架構，以識別、評估、監察及管控 / 緩減業務操作風險。

---

[5] 「關鍵運作」此一用語的涵義與單元OR-2「運作穩健性」所界定的相同。

[6] 「嚴峻但可能發生的情景」此一用語的涵義與單元OR-2「運作穩健性」所界定的相同。

[7] 「可承受影響上限」此一用語的涵義與單元OR-2「運作穩健性」所界定的相同。

2.1.2 金管局採用風險為本監管方法(見SA-1《風險為本監管制度》)，透過現場審查、非現場審查及審慎監管會議持續監管認可機構的業務操作風險。目的包括在計及本單元所載的指引之下，評估認可機構的業務操作風險承擔及虧損的程度及趨勢，以及業務操作風險管理架構是否足夠及具成效。如屬本地註冊認可機構，金管局亦會評估相對於其業務操作風險承擔的規模而言，其資本是否足夠。

2.1.3 金管局在評估認可機構的業務操作風險承擔及管理時，會特別留意以下因素：

(a) 認可機構的業務操作風險管理架構是否適合，包括董事局及高級管理層進行監察的程度，以及風險文化；

(b) 管理業務操作風險的策略、政策及流程(包括業務操作風險的定義)是否足夠；

(c) 識別、評估、監察及管控業務操作風險的業務操作風險管理程序是否足夠；

(d) 認可機構緩減業務操作風險的措施是否具成效；

(e) 認可機構對業務操作風險的內部檢討及審計是否足夠，以及有關結果；

(f) 認可機構的外聘核數師致管理層函件中所提出的結果及建議；

(g) 認可機構的重大業務操作風險事件的成因及影響；

(h) 認可機構及時與有效地解決業務操作風險事件及潛在問題所用的流程；以及

(i) 認可機構的災難事故復原及持續業務運作計劃的質素及全面性。

2.1.4 如有需要，金管局會與其他相關監管機構協調及交換資料，以助評估認可機構的業務操作風險管理架構。

2.2 監管程序

2.2.1 每間認可機構都須接受金管局審查其業務操作風險管理架構是否具成效。此外，根據《銀行業條例》第59(2)條，金管局有權要求認可機構提交由外聘核數師編製有關認可機構的內部管控制度的個別報告。

2.2.2 金管局亦會在計及認可機構的業務操作風險承擔下，監察本地註冊認可機構遵守《資本規則》下的資本規定的情況。業務操作風險資本要求的計算方法載於《資本規則》。

2.2.3 若有任何事件可能對認可機構的運作構成重大影響，認可機構應通知金管局。有關事件可能包括：

(a) 已發生 / 識別的重大業務操作虧損 / 風險承擔；

(b) 制度或管控措施的重大缺失；

(c) 擬就銀行業務相關範疇(包括後勤辦事處的業務活動)訂立內包或外判安排，或擬更改該等範疇的內包或外判安排或修訂有關的內包或外判安排的涵蓋範圍；

(d) 組織架構、基建或經營環境的任何重大變化；以及

(e) 啟動持續業務運作計劃。

2.2.4 金管局在接到有關上述事件的通知後，如認為有需要，可要求有關認可機構提交報告，分析事件的成因 / 目的及影響，並列明糾正所識別的任何弱點的行動計劃，或應對因所擬訂的轉變引起的問題的應變計劃。無論如何，在發生第2.2.3節所提及的事件後，認可機構須考慮所汲取的教訓及引致該事件的新威脅和問題，再次評估影響其維持關鍵運作的威脅及潛在風險。金管局亦預期有關認可機構不時檢討為應對該等威脅及潛在風險而實施的任何管控措施與流程，以確保該等措施與流程繼續有效。

2.2.5 若機構的內部管控制度存在嚴重失誤或缺失，可構成不安全及不穩健的做法，並可能引致重大虧損或損害機構的財

政穩健情況。若威脅機構安全穩健地進行業務活動的嚴重缺失或情況未能及時得到妥善處理，金融管理專員如認為適合會採取監管行動。該等監管行動可包括要求就有問題範疇提交獨立特別檢討報告；對認可的同意附加條件以限制所涉及的業務活動水平或完全終止有關業務活動、對機構及 / 或其負責董事及經理採取執法行動，以及即時實施所有必要糾正措施。

2.2.6 認可機構應力求持續改進其業務操風險管理架構，如有需要，金管局會在其風險為本監管過程中監察、比較及評估認可機構所作出的改進及其未來發展計劃。

3. 業務操作風險管理架構

3.1 概覽

3.1.1 認可機構應制定、實施及維持與其整體風險管理程序全面融合的業務操作風險管理架構。有關的業務操作風險管理架構應融入機構各個層面，包括集團及業務單位[8]，以及全新的業務項目、產品、活動、程序及制度。此外，認可機構的業務操作風險評估結果應併入其整體業務策略制定過程。

3.2 合適的架構

3.2.1 業務操作風險管理架構的目的是確保一致及全面地識別、評估、緩減 / 管控、監察及匯報業務操作風險。

3.2.2 就本單元的目的而言，合適的業務操作風險管理架構應包含以下主要元素：

(a) 風險管治(包括董事局及高級管理層監察)及風險文化——見第4節；

[8] 「業務單位」一詞在廣義層面指包括所有相關的輔助、企業及 / 或共享的服務職能，例如財務、人力資源及運作與科技。然而，除非另有說明，風險管理及內部審計並不包括在內。

(b) 風險管理結構由三道防線組成，即業務單位管理層(第一道防線)、獨立的企業業務操作風險管理職能(第二道防線[9])，以及獨立核證(第三道防線)——見第5節；

(c) 業務操作風險管理策略、政策及流程——見第6節；

(d) 識別、評估、監察、管控 / 緩減及匯報業務操作風險的業務操作風險管理程序——見第7節；

(e) 業務操作風險管理的特定環節，包括轉變管理、資訊及通訊科技及持續業務運作規劃——見第8節；以及

(f) 披露——見第9節。

3.2.3 實際上，認可機構的業務操作風險管理架構必須反映業務單位、產品及服務範圍、企業組織架構及風險管理文化的涵蓋範圍及複雜程度。每間認可機構的業務操作風險狀況都有其獨特性，需要特別制定適合其所面對風險的程度與嚴重性及機構規模的風險管理方法。

3.2.4 然而，上述三道防線模型已廣為業界採納，並有不同程度的落實形式。認可機構應充分及按適合程度採納此模型，以管理每類業務操作風險子類別，包括資訊及通訊科技風險，並能證明該模型的運作良好，以及能說明董事局(或獨立的董事局委員會)及高級管理層如何確保以適合的方式實施及運作該模型。認可機構應確保每道防線[10]：

(a) 有充足的預算、工具及人手；

(b) 有清楚界定的角色及責任；

(c) 有持續及充足的訓練；

(d) 在認可機構各個層面促進良好的風險管理文化；以

[9] 除企業業務操作風險管理職能外，第二道防線一般亦包括合規職能。

[10] 除就本節第(d)及(e)項外，高級管理層的責任並不涵蓋內部審計職能(第三道防線)，此職能通常直接向董事局匯報。

及

(e) 與其餘兩道防線溝通聯繫以鞏固業務操作風險管理架構。

3.2.5 業務操作風險管理架構的組成部分應由第一道防線完全併入認可機構的整體風險管理程序，並由第二道防線充分覆檢及提出質疑，以及由第三道防線進行獨立覆檢。

3.2.6 若某一業務單位同時執行第一道及第二道防線的職能，認可機構應記錄及區分該等第一道及第二道防線的職能的責任，並要強調第二道防線的獨立性。

4. 風險管治

4.1 概覽

4.1.1 業務操作風險管理需要組織架構中的不同組成部分的關注及參與，而每部分都有不同責任。組織架構中的每個組成部分都必須清楚了解本身在機構的組織及風險管理架構中的角色、權限及問責關係。所有業務及輔助職能都應該是整體業務操作風險管理架構的重要部分。設立企業業務操作風險管理職能可協助董事局及高級管理層履行了解及管理業務操作風險的責任。此外，儘管某些員工專門負責與業務操作風險相關的特定責任，機構的全體員工都應有責任識別及管理業務操作風險。

4.2 董事局監察

4.2.1 認可機構的董事局對業務操作風險管理負有最終責任。為履行這項責任，董事局(或其授權委員會)應批准及定期檢討：

(a) 業務操作風險管理架構；以及

(b) 業務操作風險的風險取向與可承受風險限度說明文

件及業務操作風險限額[11]。

業務操作風險管理架構

4.2.2 為確保業務操作風險管理架構適合，並對認可機構有效，董事局或其授權委員會應：

(a) 了解認可機構的產品、服務、活動及制度的組合的內在風險的性質及複雜程度；

(b) 建立風險文化，確保認可機構有足夠程序以了解其現有及已計劃的策略及活動的內在業務操作風險的性質及涵蓋範圍[12]；

(c) 建立清晰的管理層責任分配及問責關係，以落實穩固的內部管控環境，同時企業業務操作風險管理職能、業務單位及輔助職能之間保持適當的獨立性 / 分隔；

(d) 確保業務操作風險管理程序受到全面及靈活的監察，並與管理認可機構各個層面的所有風險的整體架構全面融合或協調；

(e) 為高級管理層提供有關業務操作風險管理架構的基本原則的清晰指引，並批准高級管理層根據該等原則制定的相應政策；

(f) 定期檢討及評估業務操作風險管理架構的成效，以確保認可機構已識別並正在管理由外在市場變化及其他環境因素所引致的業務操作風險，以及涉及新產品、活動、程序或制度，包括風險狀況及重要項目的轉變(如營業額的轉變)的業務操作風險(包括與應用資訊及通訊科技相關的業務操作風險——見第

[11] 本單元所提及的風險取向與可承受風險限度說明文件僅指關乎業務操作風險的。海外註冊認可機構的本地分行亦可借助集團的業務操作風險取向與可承受風險限度說明文件，但須確保在考慮到有關分行的業務規模、性質及複雜程度後，該分行的內在業務操作風險得到充分應對(例如透過相應的風險監察指標)。

[12] 認可機構可在整體實體層面處理風險文化，但應確保實體所培養的風險文化符合第4.4節列載的標準。

8.2節)；

(g) 確保認可機構的業務操作風險管理架構受到第三道防線(審計或其他曾接受適當訓練的外聘獨立第三方)有效的獨立檢討；以及

(h) 隨着最佳做法不斷演進，確保管理層掌握有關改進。

風險取向與可承受風險限度說明文件及風險限額

4.2.3 業務操作風險的風險取向與可承受風險限度說明文件應清楚說明銀行願意承受的業務操作風險性質、類別及水平。有關文件應在董事局授權下制定，並與認可機構的短期及長期策略及財務計劃相連。在計及認可機構的客戶及股東利益，以及監管規定下，有效的風險取向與可承受風險限度說明文件應：

(a) 易於傳達，亦因此能讓所有持份者易於理解；

(b) 包含認可機構的業務計劃獲批核時所依據的主要背景資料及假設；

(c) 包含清楚說明承受或避免某些類別風險的原因的陳述，並設定界限或指標(不論是否量化的界限或指標)以能監察有關風險；

(d) 確保業務單位及法律實體(如適用)的策略及風險限額與銀行的整體風險取向說明文件一致；以及

(e) 具前瞻性，並在適用情況下進行情景及壓力測試，以確保認可機構明白哪些事件可能引致超越其風險取向與可承受風險限度說明文件。

4.2.4 董事局應定期檢討其風險取向與可承受風險限度說明文件，以及業務操作風險限額是否適合。有關檢討應考慮外圍環境當前及預期的變化(包括機構提供服務的所有地區的監管環境)、業務或活動量一直或將會大幅增加；管控環境的質素、風險管理或緩減策略的成效、虧損經驗，以及違

反限額的次數、數量或性質。董事局亦應監察管理層遵守風險取向與可承受風險限度說明文件的情況，並就及時偵測及糾正違反情況作出規定。

4.3 高級管理層責任

4.3.1 高級管理層應制定清晰、有效及穩健的管治架構，並經董事局批准，其中應有清楚界定、具透明度及一致的業務操作風險管理責任分配。

4.3.2 認可機構的管治架構應與其活動的性質、規模、複雜程度及風險狀況相稱。在制定業務操作風險管治架構時，認可機構應顧及以下的穩健業內做法：

- **委員會的架構** —— 大型及較為複雜的認可機構會設立一個或以上的業務操作風險管理委員會，向董事局層面的風險管理委員會匯報。視乎認可機構的性質、規模及複雜程度，可按國家、業務或職能範疇設立業務操作風險委員會。規模較小及較簡單的認可機構可以只設立一個風險管理委員會監察所有風險，而不必另行設立獨立的業務操作風險管理委員會；
- **委員會的組成** —— 業務操作風險管理委員會(或規模較小的認可機構的風險管理委員會)包括具備不同專門知識的成員，涵蓋業務活動、財務活動、法律、技術及監管事宜以及獨立風險管理等範疇；
- **委員會的運作** —— 委員會應按適當周期舉行會議，並有充足會議時間及資源，以能進行具建設性的討論及決策。委員會的運作記錄應足以就委員會的成效進行檢討及評估。

4.3.3 高級管理層有責任藉制定具體政策、程序及流程以落實董事局(或獲授權委員會)所批准的業務操作風險管理架構，而

該等政策、程序及流程應可在業務單位內實施及核實，以管理業務操作風險。該等政策、程序及流程應在整個機構內貫徹實施及維持，以按照認可機構的風險取向與可承受風險限度說明文件管理所有重要產品、活動、程序及制度的業務操作風險。

4.3.4 為確保員工清楚了解及執行業務操作風險管理政策及流程，高級管理層應釐定認可機構的業務操作風險管理組織架構，並交代個別人員的角色及責任。機構內各級員工必須清楚了解其各自在業務操作風險管理程序中的角色。

4.3.5 儘管各級管理人員都對其職責範圍內的政策、程序、流程及管控措施是否適合及具成效負責，高級管理層應清楚分配職權、責任及匯報關係，以鼓勵及維持問責性，並確保投放必要資源以按照認可機構的風險取向與可承受風險限度說明文件有效管理業務操作風險。高級管理層亦應確保負責監察遵守認可機構的業務操作風險政策的情況及落實遵守有關政策的員工具有的權力，與接受其監察的單位保持獨立。此外，高級管理層應參考業務單位的活動的內在風險來評估及確保業務操作風險管理程序的適合性。

4.3.6 高級管理層有責任確保投入足夠人力及技術資源以管理業務操作風險，使認可機構的活動由合資格員工進行，該等員工須具備必要經驗與技術能力，並能取得資源。

4.3.7 高級管理層應確保負責管理業務操作風險的員工與負責管理信用、市場等其他風險的員工，以及負責採購保險風險轉移及其他第三方安排(如外判)等外聘服務的員工有效協調及溝通。如未能有效協調及溝通，可引致認可機構的整體風險管理計劃存在重大漏洞或重疊的情況。

4.3.8 高級管理層應負責設立及維持穩健的質疑機制及程序，以解決業務操作問題，包括匯報、追踪及上報問題的程序，以確保問題得到解決。

4.3.9 鑑於業務操作風險管理不斷演變，而經營環境亦持續轉變，高級管理層應確保業務操作風險管理架構(尤其政策、程序及制度)仍然具備充足的穩健性，以管理業務操作風險虧損，並確保有關虧損及時得到充分處理。業務操作風險的改善主要有賴於高級管理層是否願意採取主動，迅速及適當地應對業務操作風險經理所關注的事宜。

4.3.10 有關企業管治的一般指引，另見單元CG-1「本地註冊認可機構的企業管治」。

4.4 風險文化

4.4.1 認可機構的董事局及高級管理層亦肩負起培養正面的風險文化的重任，這是業務操作風險管理架構(尤其架構內的程序的成效)賴以成功的重要因素。一般而言，董事局應帶頭為認可機構建立良好的風險管理文化，並應由高級管理層落實。

4.4.2 認可機構的風險文化涵蓋僱員對風險的一般認知、態度及行為，以及機構內的風險管理。構成正面風險文化的因素包括：

(a) 高級管理層必須清楚訂明並向認可機構各級員工清晰傳達機構的業務目標及風險取向、業務操作風險管理架構及相關員工就落實該架構的有關角色、責任及權限，使員工能了解其就業務操作風險管理的責任。

(b) 董事局及高級管理層應堅定及貫徹地支持業務操作風險管理及道德行為，以具說服力的方式加強行為及道德守則、薪酬福利策略及培訓計劃。高級管理層必須持續參與整個風險管理程序，並向整個機構傳達一致的訊息，透過行動與說話表明董事局及高級管理層全力支持機構的風險管理架構。

(c) 董事局及高級管理層所傳達的文化應強調認可機構各級員工都要有高水平的道德行為標準，以及禁止認可機構各級員工有任何利益衝突的情況或不適當地提供金融服務(不論是故意或疏忽)。就此，認可機構可制定適用於員工及董事局成員的行為守則或道德政策，並由董事局(或其獲授權委員會)及高級管理層成員以身作則，遵行有關守則。董事局應定期檢討及批核有關守則或政策，並經僱員認證。有關守則或政策的實施應由董事局層面的委員會監察，並應可供公眾查閱(例如在認可機構網站)。認可機構可就特定崗位(例如財資部門交易人員及高級管理層)另行制定行為守則。

(d) 高級管理層應確保為機構各級員工(如業務單位主管、內部管控主管及高級經理等)提供適當的業務操作風險管理及道德行為培訓。所提供的培訓應反映相關員工的角色及責任。

(e) 認可機構薪酬政策必須與其風險取向與可承受風險限度以及整體安全與穩健程度一致。認可機構亦必須適當地平衡風險與回報[13]。對表現的獎勵應考慮風險管理，而制度的設計亦不應對其運作方式與所期望的風險管理價值觀(例如設定的持倉限額)相反的人員提供獎勵。

(f) 認可機構必須營造適當環境，讓員工可公開討論及提出業務操作風險問題而無需擔心會帶來不利後果。

[13] 另見巴塞爾委員會於 2011年5月發出的《風險及工作表現與薪酬掛鈎的一系列方法》報告；金融穩定論壇於2009年4月發出的《穩健的薪酬制度原則》；金融穩定理事會於2009年9月發出的《穩健的薪酬制度原則——實施準則》以及金融穩定理事會於2018年4月發出的工具「加強管治架構以緩減不當行為風險」。

4.4.3 認可機構亦應就穩健風險管理文化的一般指引參考以下《監管政策手冊》單元：

(a) CG-1「本地註冊認可機構的企業管治」；

(b) IC-1「風險管理架構」；

(c) CG-3「行為守則」；以及

(d) CG-5「穩健的薪酬制度指引」。

5. 三道防線

5.1 業務單位管理層(第一道防線)

5.1.1 業務單位管理層負責日常識別、管理及匯報其業務單位特有的業務操作風險。在每個業務單位內實施的業務操作風險管理架構應反映有關業務單位的範疇及其內在運作複雜性及業務操作風險情況[14]。業務單位管理層必須與認可機構的整體企業業務操作風險管理職能保持獨立。

5.1.2 為方便管理每個業務單位的業務操作風險，良好做法是有關業務單位應設有專責的業務操作風險員工。這些員工通常都有兩重的匯報安排。一方面他們在有關業務單位內有直接的匯報關係，另一方面他們與企業業務操作風險管理職能緊密合作，確保政策與工具保持一致，並匯報成果與問題。第一道防線的責任應包括：

(a) 透過運用業務操作風險管理工具識別及評估其相關業務單位的內在業務操作風險的重大程度；

(b) 設立適當管控措施，包括業務特定政策 / 標準、程序、流程及制度，以緩減內在業務操作風險，並透過運用業務操作風險管理工具評估相關管控措施的設計及成效；

[14] 業務操作風險狀況指業務單位的業務運作風險承擔及管控環境評估，並根據預期至嚴峻虧損的估計考慮可能產生的一系列潛在影響。有關狀況一般向管理層及董事所反映的業務操作風險承擔的程度，足以讓其據以作出決策及履行監察責任。

(c) 匯報業務單位是否缺乏足夠資源、工具及培訓，以確保能識別及評估業務操作風險；

(d) 監察及匯報業務單位的業務操作風險狀況，以及確保遵守既定的業務操作風險取向與可承受風險限度說明文件；以及

(e) 匯報管控措施未能緩減的剩餘業務操作風險，包括業務操作虧損事件、管控缺失、程序的不足之處，以及違反業務操作風險可承受限度的情況。

5.2 業務操作風險管理職能(第二道防線)

5.2.1 銀行界一個主流做法是以類似信用及市場風險管理職能的方式，設立企業業務操作風險管理職能(在集團及/或機構層面)。這個職能的主要角色是協助高級管理層履行了解及管理業務操作風險的責任，並確保制定及在機構各層面貫徹執行業務操作風險政策、程序及流程(第7節)。就此，企業業務操作風險管理職能履行多項職責，包括：

(a) 在企業層面制定及維持業務操作風險管理及管控的政策、流程及指引；

(b) 設計及實施機構的業務操作風險評估方法、工具及風險匯報系統；

(c) 就業務單位的以下三方面得出獨立看法：(i)已識別的重大業務操作風險；(ii)主要管控措施的設計及成效，以及(iii)可承受風險限度；

(d) 質疑業務單位所實施的業務操作風險管理工具、計量活動及匯報制度的適切性及一致性，並提供證據證明有關質疑有利於評估其成效；

(e) 建立劃一的業務操作風險管理分類、方法及流程；

(f) 檢討及參與監察業務操作風險狀況，並向董事局及高級管理層匯報業務操作風險狀況；

(g) 與其他負責管理及應對任何對維持關鍵運作構成威脅的風險，以及負責協調持續業務運作規劃、第三方倚賴關係管理、復原及處置規劃及其他相關風險管理架構的有關職能合作，以加強機構整體的運作穩健性；

(h) 設計及提供業務操作風險管理培訓，包括培養風險意識，以及就業務操作風險管理問題向業務單位提供意見，例如有關業務操作風險工具的運用；以及

(i) 與內部及外聘核數師聯絡。

5.2.2 企業業務操作風險管理職能的經理在認可機構內的地位應足以讓其有效履行職責。他們獲分配的職銜最理想的是與信用、市場及流動性風險等其他風險管理職能的職級與崗位相若。

5.2.3 金管局明白認可機構的經營方式各有不同，並採用不同的業務操作風險管理制度及方法。因此，金管局不打算訂明企業業務操作風險管理職能的正式定義。然而，在任何情況下，認可機構都應因應其業務規模與複雜程度制定政策，清楚界定企業業務操作風險管理職能的角色及責任。

5.2.4 一般而言，規模較大的認可機構的企業業務操作風險管理職能的匯報制度應與產生風險的業務單位保持獨立，並負責設計、維持及持續發展認可機構的企業業務操作風險管理職能。規模較小的認可機構可透過職責分隔及獨立檢討程序與職能，以達致企業業務操作風險管理職能保持獨立。

5.2.5 事實上，部分認可機構的內部審計職能可能會在某方面參與制定業務操作風險管理計劃的初步工作。若屬這種情況，認可機構應確保適時將日常的業務操作風險管理責任轉交其他職能負責。此舉是確保內部審計職能保持獨立。

5.2.6 如屬在集團及 / 或企業層面設有企業業務操作風險管理職

能的認可機構的分行、附屬公司或個別業務單位，通常應在分行、附屬公司或業務單位設有專責的業務操作風險員工，以確保政策及工具的一致性，以及匯報成果及問題。

5.2.7 如有需要，業務操作風險管理架構文件應清楚提述相關業務操作風險管理政策及流程。

5.3 其他業務操作風險相關職能

5.3.1 企業業務操作風險管理職能一般邀請相關企業管控小組支援其對業務操作風險及管控的評估。認可機構內還有多個其他業務操作風險相關的輔助職能，應在認可機構的業務操作風險管理中就企業業務操作風險管理職能發揮支援作用。這些職能包括法律及合規、人力資源、資訊及通訊科技與財務等專家部門，這些部門應對業務操作風險的某些特定範疇及相關問題負責。例如人力資源職能應為「人事」風險管理方面的主要參與者，而並非僅分享資訊及提供專家意見。這些其他業務操作風險相關職能應一方面負責管理其本身範疇內的業務操作風險，另一方面向業務操作風險管理的組織架構內的其他方提供支援。

5.4 獨立核證(第三道防線)

5.4.1 董事局應就認可機構的業務操作風險管理架構是否適合獲提供獨立核證。有關評估應由並無參與制定及實施日常業務操作風險管理程序或另外兩道防線的運作的內部核數師、外聘核數師或其他具備合適資格的獨立第三方等進行。認可機構的審計所涵蓋的範疇應足以核實業務操作風險管理政策與流程在整個認可機構內得到有效實施。董事局應(直接或透過其審計委員會)確保審計計劃的範圍及次數與其風險承擔相符。

5.4.2 有效的獨立評估應：

(a) 審視透過第一及第二道防線設計及實施業務操作風險管理制度及相關管治程序的情況(包括第二道防線的獨立性)；

(b) 審視核實[15]程序，以確保有關程序獨立及按符合既定政策的方式實施；

(c) 確保業務單位管理層迅速、準確及充分地就所提出的問題作出回應，並定期向董事或其相關委員會匯報尚待處理及已處理完畢的問題；以及

(d) 就業務操作風險管理架構及認可機構各個層面的相關管治程序的整體適合性與足夠程度提出意見，包括業務操作風險管理架構是否符合組織架構需要與期望(例如有關企業風險取向與可承受風險限度，以及架構因應不斷轉變的運作環境作出調整的需要)，以及有否遵守法定及法例規定、合約安排、內部規則及道德操守。

5.4.3 在評估程序中所識別及匯報的任何業務操作問題應按情況而定由高級管理層及時有效地應對，或通知董事局。

5.4.4 如單元IC-2「內部審計職能」所述，獨立檢討可涵蓋內部審計職能(第三道防線)的內在業務操作風險，有關檢討可由外聘核數師或其他合資格獨立檢討人員或審計委員會等獨立方進行。

6. 業務操作風險管理策略、政策及流程

6.1 策略

6.1.1 業務操作風險管理的第一步是制定機構的整體策略與目標。一經制定，機構便可識別其策略與目標的相關內在風險，從而制定業務操作風險管理策略。董事局有責任釐定

[15] 核實是有效運作的業務操作風險管理架構的關鍵，可確保認可機構所用的量化系統具備足夠穩健性，能為進項、假設、方法、程序及出項提供核證，從而讓業務操作風險評估能可靠反映認可機構的業務操作風險狀況。

業務操作風險管理策略，並確保有關策略與整體業務目標相稱。就此，董事局應就認可機構的風險取向與可承受風險限度提供清晰指引，即認可機構為達致其業務目標而願意承受哪些風險及不能接受哪些風險。

6.2 政策

6.2.1 認可機構應以書面記錄其管理業務操作風險的政策，列明其所有主要相關業務及支援程序的業務操作風險管理的策略與目標，以及為達致有關目標而打算採用的程序。認可機構應以書面記錄其企業業務操作風險政策，並向各級員工清楚傳達。

6.2.2 認可機構管理業務操作風險的政策應包括：

(a) 機構對業務操作風險及業務操作虧損的定義(見第6.3節)，包括認可機構及其客戶所面對而認可機構會監察的業務操作風險類別；

(b) 管治架構，此架構界定董事局、委員會[16]、高級管理層、風險管理職能、業務單位管理層及其他業務操作風險相關職能的業務操作風險管理角色、責任及匯報安排；

(c) 認可機構接受的業務操作風險取向與可承受風險限度；內在業務操作風險(即計及管控措施前的風險)及剩餘(即計及管控措施後的風險承擔)業務操作風險的門檻、重大活動觸發點或限額，以及經批准的風險緩減策略及工具；

(d) 識別及評估風險及管控的工具，以及三道防線在運用有關工具方面的角色及責任；

(e) 設立及監察內在及剩餘風險承擔的門檻或限額的方法，以及確保管控措施的設計、實施及運作有效；

[16] 另亦應載有相關委員會的職權範圍及成員。

(f) 所有業務單位的存貨風險及實施的管控措施(例如在管控庫)；

(g) 業務操作風險用語的通用分類目錄(詳見第6.3.1段)；

(h) 為編製及時與準確的數據 / 資訊的管理匯報架構的概要，以及列入風險管理報告的數據 / 資訊類別；

(i) 獨立檢討及質疑業務操作風險管理程序的結果的機制；以及

(j) 根據有關應對內部及外圍環境變化的管控環境質素的持續評估，或在認可機構的業務操作風險狀況出現重大轉變時，按情況所需檢討及修訂有關政策的規定。

6.2.3 有關政策應由一組適用於業務操作風險的特定組成項目的原則配合，例如新客戶批核、新產品批核、資訊及通訊科技系統批核、外判、持續業務運作規劃、危機管理及洗錢(詳細指引見第7.4.7段)等。

6.2.4 業務單位管理層負責管理特定業務單位的風險。因此，業務單位管理層須根據企業業務操作風險管理政策，制定針對其業務的補充政策及流程，有關的補充政策及流程應與企業業務操作風險管理政策一致。

6.3 業務操作風險定義

6.3.1 為能有效識別、評估、監察及匯報認可機構的業務操作風險，有必要界定業務操作風險的基本組成項目。就此而言，有關政策應提供業務操作風險用語的通用分類目錄，以確保各業務單位在風險識別、風險承擔評級及風險管理目標保持一致[17]。分類目錄應按事件類別、成因、重大程

[17] 若業務操作風險用語的分類目錄存在不一致的情況，有可能增加未能識別風險及將風險分類，或未能就評估、監察、管控及緩減風險分配責任的可能性。

度及涉事的業務單位區分業務操作風險承擔。分類目錄亦應標示部分或全部反映法律、操守、模型、資訊及通訊科技(包括網絡)風險，以及信用或市場風險範圍內的風險承擔。

6.3.2 業務操作風險的定義應考慮機構所面對的所有重大業務操作風險，並涵蓋嚴重業務操作虧損的最重要成因。正式及詳盡的定義亦極為重要，有助改進溝通、釐定問責關係、分析事件特徵及累積事件以制定模式及進行分析，以及貫徹進行經驗及意見交流。

6.3.3 巴塞爾委員會參考業務操作風險的四項基本成因——程序、人員、系統及外部事件(或環境)來界定業務操作風險(見第1.1.2段)。有關定義旨在依據銀行營運中可單獨或共同引致業務操作虧損的主要內部及外在因素，將業務操作風險與其他風險區分。下表列載在業務操作風險的四項基本成因下各項風險成因分類的例子：

風險成因	風險成因分類
程序	• 指引、政策及流程不足 / 不適合； • 溝通不足 / 失效； • 數據輸入失誤； • 對帳不足； • 客戶 / 法律文件欠妥善； • 保安管控不足； • 違反監管及法定規定 / 要求； • 變動管理程序不足；以及 • 後備 / 應變計劃不足

人員	• 違反內部指引、政策及流程； • 越權； • 犯罪行為(內部)； • 職責區分 / 雙重控制不足； • 職員經驗不足； • 職員疏忽；以及 • 角色及責任不明確
系統	• 硬件 / 網絡 / 伺服器維修保養不足
外在因素	• 犯罪行為； • 銷售商表現欠佳； • 人為災難事故； • 自然災害；及 • 政治 / 法律 / 監管成因

6.3.4 此外，為促進管理及計量業務操作風險，以及評估業務操作虧損事件的潛在影響，認可機構應按預設的事件類別將該等事件分類。巴塞爾委員會已制定距陣，將業務操作虧損事件類別分為七大類，然後再細分為附件所載的子分類及相關活動例子[18]。認可機構的內部分類制度若有別於巴塞爾委員會的制度，應以文件記錄將其內部分類與附件所載的各大事件類別(第一級)配對的準則。認可機構應在金管局要求時提供其虧損數據及該等數據與附件所載的各大事件類別的配對。

7. 業務操作風險管理程序

7.1 概覽

7.1.1 認可機構應具備有效方法定期及適時地識別、評估、監察

[18] 見巴塞爾委員會綜合架構OPE25.17表2。

及管控其主要產品、活動、程序及制度的內在業務操作風險，從而確保在可能範圍內防範潛在風險(尤其可能影響維持關鍵運作的威脅及潛在問題)。認可機構應採取合理措施確保就該等目的而言，有關程序及工具為足夠及有效。

7.2 風險識別及評估

7.2.1 為能更充分了解其業務操作風險狀況及有效調配風險管理資源，認可機構應盡可能識別所承受的業務操作風險類別，並評估其受該等風險影響的可能性。認可機構應根據其本身對業務操作風險的定義及分類，識別及評估所有現有或新的重要產品、活動、程序及制度的內在業務操作風險。有效的業務操作風險識別及評估，是有效的業務操作風險管理制度的基本特徵，並可直接提升運作穩健能力。

7.2.2 認可機構在識別其業務操作風險時，應同時考慮可能對達致其目標構成不利影響的內在及外在因素，例如：

(a) 認可機構的管理架構、風險文化、人力資源管理手法、組織架構變動及僱員流失；

(b) 認可機構的客戶、產品及活動的性質，包括業務來源、分銷機制及交易的複雜程度與交易額；

(c) 認可機構的產品及活動在運作周期中所用的程序及系統的設計、推行及運作；以及

(d) 外圍經營環境及行業趨勢，包括政治、法律、技術及經濟因素、競爭環境及市場結構。

7.2.3 認可機構在識別風險後，需要訂明評估每項所識別風險的適當方法、藉考慮所識別風險的成因估計該等風險真正發生的可能性，以及透過參考對實現企業目標造成的潛在影響以評估該等風險的影響。

7.2.4 以下是識別及評估業務操作風險的多項常用工具：

(a) **事件管理** (按照一套預設的方法識別、分析、進行端

對端管理及匯報業務操作風險事件的程序)——穩健的事件管理方法一般包括分析事件以識別新的業務操作風險、了解基本成因及管控弱點，以及制定適當回應以防止類似事件再次發生。有關資料是自我評估(見下文(c))，特別是管控措施成效的評估的進項。

(b) **業務操作風險事件數據**(收集認可機構遇到的所有重大事件的全面業務操作風險事件數據庫，作為業務操作風險評估的基礎)——事件數據庫一般包括內部虧損數據及幾乎出現虧損的情況。事件數據一般按照業務操作風險管理架構政策所界定的分類目錄來分類，並在整個認可機構內貫徹應用。事件數據一般包括事件日期(發生日期、發現日期及會計日期)，以及(如屬虧損事件)財務影響。如能取得有關資料，業務操作風險數據庫亦最好能包括有關事件的事故成因的資料。如屬可行，認可機構亦應尋求收集外部業務操作風險事件數據，並將有關數據用於其內部分析，原因是這類數據往往能提供有關整體業界經常面對的風險的資訊。

(c) **自我評估**(認可機構對不同層面的業務操作風險及管控措施進行評估)——有關評估一般評核內在風險(即計及管控措施前的風險)、管控環境的成效，以及剩餘風險(即計及管控措施後的風險承擔)，並兼具計量及質量元素。質量元素反映在銀行釐定其內在及剩餘風險評級時，對發生風險事件的可能性及後果的考慮。有關評估可運用業務程序配對，以識別業務程序、活動及組織架構職能的主要步驟，以及相關風險及存在管控不足的地方。有關評估應包含有關經營環境、業務操作風險、基本成因、管控

措施及對管控成效的評核的詳盡完備的資料，讓獨立檢討人員能決定銀行如何得出有關評級。認可機構可備存風險記錄冊，以檢核有關資料，從而對管控措施的整體成效得出具參考價值的看法，以及方便高級管理層、風險委員會及董事局進行監察。

(d) **管控監察及核證架構**(有系統地評核、檢討及持續監察與測試主要管控措施的方法)——對管控措施的分析確保有關措施的設計適合所識別的風險並能有效運作。分析亦應考慮管控的涵蓋範圍是否足夠，包括在考慮到各業務範疇的不同業務操作風險後，是否有充足的防範、偵測及回應策略。

(e) **指標** (運用業務操作風險事件數據及風險與管控評核結果制定的計量指標，以評估及監察業務操作風險承擔)——指標主要是被認為適合用作啟動管理追踪及上報程序而選取的運作 / 管控指標。有關指標可以是由機構不同職能認定及定期追踪的簡單指標，例如事件發生次數，或按需要由較先進精密的風險承擔模型得出的出項。指標的作用是提供預警資訊，以監察業務及管控環境的持續表現，並匯報業務操作風險狀況，讓管理層得以在問題演變為機構的重大問題前採取行動。有效的指標與相關業務操作風險及管控措施有清晰聯繫。參照商定的門檻或限額持續監察指標及相關趨勢，能為風險管理及匯報目的提供極具參考價值的資訊。

(f) **情景分析**(識別、分析及計量一系列情景的方法，包括發生可能性低但極為嚴峻的事件(例如疫症、自然災害及第三方或第三方的供應鏈失效或受到干擾)，而部分事件可引致嚴重的業務操作風險虧損)——情景分析一般包含由有關主題的專家(包括高級管理

層、業務管理層及負責業務操作風險管理及合規、人力資源及資訊科技風險管理等其他職能範疇的高級職員)舉行工作坊，以制定及分析引致潛在事件的因素及一系列的後果。情景分析的進項一般包括相關內部及外部虧損數據，以及來自自我評估、管控監察及核證架構、具前瞻性指標、根本成因分析及程序架構(如有運用)的資訊。情境分析程序可用作制定潛在事件的一系列後果，包括就風險管理目的進行的影響評估，以補足以歷史數據為依據的其他工具或當前的風險評估。情景分析程序亦可納入災難事故復原及持續業務運作計劃，在運作穩健性的測試中使用(另見單元OR-2「運作穩健性」)。鑑於情景分析程序存在主觀因素，因此應有穩健有效的管治架構及獨立檢討，以確保程序的完整性及一致性。

(g) **基準及比較分析**(比較認可機構所運用的不同風險計量及管理工具的結果，以及將認可機構及業內其他企業採用的指標作比較)——進行該等比較可加深對認可機構的業務操作風險狀況的了解。例如將內部虧損的次數及嚴峻程度與自我評估結果比較，有助認可機構決定其自我評估程序是否有效運作。情景數據可與內部及外部虧損數據比較，藉以加深對認可機構對潛在風險事件的風險承擔的嚴峻程度的了解。

7.2.5 認可機構應確保業務操作風險評估工具的出項：

(a) 根據準確數據得出，並以穩健的管治及核實與確認流程確保有關數據的完整性；

(b) 被充分計及在內部訂價及表現評估機制，以及業務機會評估之內；以及

(c) 如有需要，受企業業務操作風險管理職能監察的行動計劃或補救計劃的規限。

7.2.6 第7.2.4段提及的業務操作風險評估工具亦可直接用於認可機構維持運作穩健性的方法。尤其是事件管理、自我評估及情景分析程序讓認可機構可識別其關鍵運作面對的威脅及潛在問題。認可機構應利用有關工具的出項改進其運作穩健性的管控措施及流程[19]。

7.3 風險監察及匯報

7.3.1 認可機構應實施程序，以持續監察其業務操作風險狀況及對虧損的重大風險承擔。有關程序應包括對認可機構的各類業務操作風險承擔的計量及質量評估；評估糾正 / 緩減措施的質素及適合程度，以及確保有充足的管控措施及制度以及早識別及處理問題，以免問題轉趨嚴重。有關措施應與認可機構所承受的風險及所進行的活動的規模相稱。

7.3.2 認可機構在監察其業務操作風險時應運用適合的指標(見第7.2.4(e)段)。透過就指標設定適當的「目標或限額」或「上報程序啟動點」，監察有關指標便能就業務操作風險增加或業務操作風險管理失效提供預警，以便向上級管理層通報潛在問題。

7.3.3 風險監察應為認可機構的活動的一部分，監察的次數應反映認可機構的活動所涉及的風險，以及經營環境轉變的步伐及性質。

7.3.4 認可機構監察活動的結果、內部 / 外聘審計及 / 或業務操作風險管理職能對業務操作風險管理架構進行的評估、外聘核數師致管理層的函件，以及監管當局編製的報告(如適

[19] 有關管控措施及流程應與威脅及潛在問題的識別一致並一併進行，作為認可機構維持運作穩健性的方法的一部分。

用)應載入向董事及高級管理層提交的報告，為主動積極的管理提供支持。

7.3.5 認可機構應在正常及受壓的市況下都能及時擬備報告[20]。有關報告應全面、準確、一致，並可據以就各業務單位及產品採取行動。為此，第一道防線應確保就任何剩餘業務操作風險作出匯報，涵蓋業務操作風險事件、管控缺失、程序的不足之處及違反業務操作風險可承受限度的情況。報告的篇幅應易於處理，就認可機構的業務操作風險狀況及遵守業務操作風險取向與可承受風險限度說明文件提供概覽。數據過多及不足都會妨礙有效的決策。

7.3.6 一般而言，董事局應收到充足的高層次資料，以能了解認可機構的整體業務操作風險狀況，以及聚焦於對業務造成的重大及策略性影響。

7.3.7 管理報告一般應透過提供內部財務、業務操作及合規指標，以及與決策相關的外圍市場或環境事件及情況的資料，以交代認可機構的業務操作風險狀況。有關報告應提供如下文所載的資料：

(a) 機構正面對或可能面對的主要及新出現的業務操作風險(例如如指標及其趨勢數據所示的、風險及管控措施自我評估的變動、審計 / 合規檢討報告提出的意見等)；

(b) 重大內部業務操作風險事件及虧損(包括事故成因、所採取補救措施的狀況及 / 或成效)；

(c) 相關外部事件或監管變動，以及對認可機構的任何潛在影響；以及

(d) 例外情況匯報(其中包括經授權及未經授權的偏離認可機構的業務操作風險政策的情況(包括風險取向與

[20] 匯報應符合巴爾委員的「有效的風險數據整合及風險匯報的原則」(https://www.bis.org/publ/bcbs239.pdf)。

可承受風險限度)，以及可能或實際違反預設業務操作風險承擔及虧損的門檻、限額或質量要求的情況)。

7.3.8 數據掌握及風險匯報程序應定期予以分析，目標是能藉此提升風險管理表現及改進風險管理政策、流程及做法。

7.3.9 為確保所收到的報告具參考價值及可靠，管理層應定期核實整體匯報制度及內部管控措施的及時性、準確性及適切性。

7.3.10 認可機構可考慮記錄報告所提供的資料，特別是虧損數據，以建立一套有系統地追踪及記錄虧損事件的次數、嚴峻程度及其他相關資料的架構。

7.4 風險管控及緩減

7.4.1 認可機構對業務操作風險的管控的一項關鍵元素是穩健的內部管控制度。若內部管控制度設計妥善及貫徹實施，將有助管理層確保運作具效率及成效、保障機構資源、編製可靠財務報告，以及遵守法律及規例。穩健的內部管控措施亦會減低內部程序及系統出現重大人為失誤及異常情況的機會，並會有助及時偵測該等失誤及異常情況的發生。

7.4.2 就已識別的所有重大業務操作風險而言，認可機構應決定是否運用適當的政策、程序、流程及 / 或制度以管控及 / 或緩減有關風險或承擔有關風險。對於無法管控或緩減的風險，認可機構應決定是否接受該等風險、減低涉及的業務活動程度，或全面撤出有關活動。

7.4.3 穩健的內部管控計劃包括風險評估、活動監察及管控、溝通及資訊[21]，而上述各項亦是風險管理程序的重要組成部分。認可機構管控業務操作風險的方法一般包括：

[21] 管理層應向個別職能清楚說明內部管控要求，而個別職能又持續向管理層提供資料及反饋意見，以提升管控要求。

(a) 明確定立的批核權限及 / 或程序；

(b) 分隔職責——應識別、避免或盡可能減低個別職員的責任出現利益衝突(會令對虧損的隱瞞、失誤或不當行為較易發生)。若實行上某些利益衝突無法避免，則應實施雙重管控(例如程序上要求由兩個或以上獨立實體 / 人士一致行動，以保障敏感職能或資料)或其他反制措施、獨立監察及檢討，以防範隱瞞虧損、失誤或其他不當行為的情況；

(c) 密切監察遵守指定風險限額或門檻的情況及對違規進行調查；

(d) 獲取及運用銀行資產及記錄的保障措施；

(e) 適量的職員人手及培訓以維持專門技術知識；

(f) 持續進行識別回報偏離合理預期的業務單位或產品的程序(例如應屬低風險、低利潤幅度的買賣活動卻帶來高回報，可能令人懷疑是否因違反了內部管控才取得有關回報)；

(g) 定期就交易及帳目進行核實及對帳；以及

(h) 規定僱員需要暫停履行職責一段時間的假期政策，應暫停不少於一星期或與有關僱員的角色及認可機構的風險狀況 / 複雜程度相符的其他日數的期間。

7.4.4 管控程序及流程應包括確保遵守政策、規例及法律的制度。有關制度的主要元素可包括：

(a) 對認可機構在達致所定目標方面的進度的高層次檢討；

(b) 核實遵守管控措施的情況；

(c) 檢討對違規情況的處理及解決方法；

(d) 評估必須的批核及授權，以確保對適當級別管理層具問責性；以及

(e) 追踪有關批准偏離門檻或限額、管理層干預及其他

偏離政策、規例及法律的情況的報告。

7.4.5 認可機構應確保風險管理管控基建能跟上業務活動的增長或變化(例如新產品、遠離總公司的分行 / 附屬公司的運作及進入不熟悉的市場)。

7.4.6 管控程序及流程應與認可機構維持運作穩健性的方法一致，從而透過相關職能(即有關的三道防線)進行的盡職審查，在正常情況下及遇到干擾事件時都可維持認可機構的運作穩健性。

7.4.7 認可機構的業務操作風險特別受以下因素影響，因此認可機構應制定相關政策及程序以控制有關的風險承擔：

(a) **轉變計劃**

若認可機構計劃作出轉變，例如從事新活動或開發新產品 / 服務、進入不熟識的市場 / 司法管轄區、實施新的或經修訂的業務程序或技術系統，及 / 或在地理上遠離總公司的地方經營業務等，都可能帶來較顯著的業務操作風險。因此，認可機構應設有政策及流程，訂明識別、管理、質疑、批准及監察轉變的程序，以及說明有關各方在轉變管理過程中的角色及責任。該等政策應列明有關批准實行轉變項目的客觀準則。

此舉目的是確保轉變計劃以受控的方式推行，同時業務單位及輔助職能都作好充分準備應對擬作出的轉變。此外，認可機構應利用其轉變管理能力，評估所計劃進行的轉變對維持關鍵運作的任何相關組成部分，以及其互連與互倚關係的潛在影響。

有關轉變管理程序的進一步指引，見第8.1節，另就新產品及服務的管控措施的一般指引，見單元IC-1「風險管理架構」第4.3節。

(b) **資訊及通訊科技的運用**

有關政策應旨在確保透過充足的資訊及通訊科技管治及管控措施，包括保安管理、系統開發及轉變管理、資訊處理、通訊網絡及技術服務供應商的管理，應對與運用資訊及通訊科技相關的風險。有關一般原則的指引，見單元TM-G-1「科技風險管理的一般原則」，有關資訊及通訊科技風險管理的進一步指引，見下文第8.2節。

(c) **電子銀行服務**

電子銀行風險管理是認可機構科技風險管理的重要部分，應涵蓋客戶身分認證、資料保密及完整性、應用程式保安、互聯網基建及安全監察等方面的管控措施，以及有關欺詐銀行網站、偽冒電郵或類似騙案的管控措施等客戶保安方面的措施。有關電子銀行風險管理原則的一般指引，見單元TM-E-1「電子銀行的風險管理」。

(d) **對第三方的倚賴**

雖然借助第三方服務供應商等實體有助控制成本、提供專門知識、擴大產品銷售及改善服務，但這亦帶來風險。董事局及高級管理層應了解該等風險，並確保有妥善的政策及流程以應對與第三方服務供應商相關的風險，而不論目前是否有外判安排或認可機構是藉其他途徑倚賴服務供應商進行其業務運作。就外判活動而言，風險管理程序應涵蓋因應擬外判的活動的重要性及關鍵程度、風險集中情況、對服務供應商的盡職審查、對外判活動的管控措施及應變規劃，而對建議的外判安排進行的全面風險評估。有關金管局建議認可機構考慮外判其活動時應處理的要點，見單元SA-2「外判」。此外，認可

機構的外判安排應顧及處置機制當局的查閱權。外判的相關服務供應商的風險管理政策及活動，應與維持運作穩健性方面的關鍵運作管理及對倚賴關係的管理一致，並一併進行。至於其他類型的對第三方的倚賴，認可機構應在計及所涉及的風險後，考慮是否需要採用上文詳述的相若風險管理程序。

(e) **清洗黑錢**

認可機構應根據「認識你的客戶」、遵守法律規定、與執法機關合作及持續培訓職員的原則，制定政策、流程及管控措施，以打擊清洗黑錢及恐怖分子資金籌集活動。有關管理清洗黑錢及恐怖分子資金籌集活動的指引，見單元AML-1「打擊洗錢及恐怖分子資金籌集的監管方法」。

(f) **客戶的適合性**

認可機構應制定政策及流程，以識別它們認為適合向其銷售某些複雜及高風險產品的客戶。目標客戶應被認為有能力了解及承擔有關產品可能引致的潛在財務風險。

(g) **海外分行／附屬公司**

海外分行或附屬公司的操作系統及程序可能會改變認可機構的業務操作風險狀況。因此認可機構應了解每間海外分行及附屬公司的程序及系統上的差異所造成的影響，並就海外分行及附屬公司的運作制定適當的管控措施。

(h) **客戶資料保密**

正如《銀行營運守則》所列明，認可機構在收集、使用及保存客戶資料方面，應遵守《個人資料(私隱)條例》。

(i) 外部文件

外部文件指由認可機構編製及提供予客戶及對手方或第三方的文件，例如合約、交易結單或宣傳單張。這些文件若含有不當或不準確資料，可能會引致法律及業務操作風險。

認可機構應備有足夠的程序及制度，以在發出外部文件前先加以審閱。有關程序及制度可包括考慮以下因素：

- 是否符合適用的監管及法律規定；
- 有關文件在多大程度上運用標準或非標準條款；
- 發出有關文件的渠道或方式；以及
- 是否需要確認收妥文件。

7.4.8 在內部管控措施並未充分應對風險，但退出有關風險並非合理選項時，高級管理層可尋求透過保險等風險緩減產品將風險轉移予另一方，以補足管控措施。然而，認可機構不應以風險緩減工具取代內部業務操作風險管控措施。同時，認可機構亦需要仔細考慮保險等風險緩減工具在多大程度上能真正緩減風險，或會否將風險轉移至另一個業務範疇，甚或構成新的風險(如法律或對手方風險)。董事局應決定認可機構願意及有財政能力承擔的最高虧損風險承擔額，並應每年檢討認可機構的風險及保險管理計劃。雖然認可機構應在個別基準上決定具體保險或風險轉移需要，但應留意適用監管規定。

8. 業務操作風險管理的特定範疇

8.1 轉變管理

8.1.1 轉變管理應評估認可機構的轉變計劃(如第7.4.7(a)段所述)的相關風險由推出至終止的時段(例如某項產品的整個有效

周期)的演變情況。轉變管理的政策及流程應根據商定的客觀準則界定識別、管理、質疑、批准及監察轉變的程序。轉變的實施應按照具體監察管控措施予以監察。轉變管理政策及流程應進行獨立及定期檢討與更新，並按三道防線模型清楚分配角色及責任，尤其：

(a) 第一道防線應對新產品、活動、程序及制度進行業務操作風險及管控評估，包括在決策及規劃階段至實施及實施後檢討期間對所需轉變的識別及評核。

(b) 第二道防線(即企業業務操作風險管理職能)應對第一道防線的業務操作風險及管控評估提出質疑，以及監察適當管控措施或補救行動的落實情況。企業業務操作風險管理職能應覆蓋此程序的所有階段。此外，企業業務操作風險管理職能應確保所有相關管控組別(例如財務、合規、法律、業務、資訊及通訊科技、風險管理)按需要參與有關程序。

8.1.2 認可機構應有檢討及批准轉變計劃的政策及程序，涵蓋：

(a) 內在風險，包括法律、資訊及通訊科技及模型風險(尤其是涉及外判的情況)；

(b) 對認可機構的業務操作風險狀況、取向與可承受風險限度的轉變，包括現有產品或活動的風險轉變；

(c) 必要的管控措施、風險管理程序及風險緩減策略；

(d) 剩餘風險；

(e) 相關風險管理門檻或限額的轉變；以及

(f) 評估、監察及管理風險的流程及指標。

8.1.3 檢討及批准過程應包括確保在引入轉變前已就人力資源及技術基建作出適當投資。在落實轉變期間及之後應監察轉變，以識別與預期業務操作風險狀況的任何重大差異，並管理任何意料之外的風險。在關鍵運作的任何相關組成部分有所轉變後，應就識別及評估威脅 / 潛在問題及業務操

作風險的管控措施與程序作出評估，以確保有關管控措施與程序繼續有效。

8.1.4 為有助對轉變的監察，認可機構應盡可能備存有關其產品及服務(包括外判的職能或活動)的中央記錄。

8.1.5 認可機構亦應參閱單元IC-1「風險管理架構」第4.3節有關新產品及服務的風險管理的一般指引。

8.2 資訊及通訊科技

8.2.1 認可機構在業務運作中應用資訊及通訊科技，同時存在內在風險及效益。雖然相對人手操作程序，自動化程序較少機會出現失誤，但亦帶來風險，必須透過穩健的科技管治及基建風險[22]管理計劃應對。此外，科技相關產品、活動、程序及交付渠道的運用令認可機構面對業務操作風險，以及出現重大財務虧損的可能性。因此，認可機構的業務操作風險管理架構應對資訊及通訊科技風險採取綜合管理方法。資訊及通訊科技風險管理應確保有效的資訊及通訊科技表現及資訊及通訊科技保安，從而協助締造對達致認可機構的策略目標所必須的有效的運作及管控環境。穩健的資訊及通訊科技風險管理可減低認可機構對直接虧損、法律申索、信譽損害、資訊及通訊科技干擾及不當使用科技的業務操作風險承擔，與其風險取向與可承受風險限度說明文件相稱。

8.2.2 為確保數據及系統的保密、完整及可用性，董事局應定期監察認可機構的資訊及通訊科技風險管理的成效，高級管理層應經常評估認可機構的資訊及通訊科技風險管理的設計、實施情況及成效。為達到此目的，須經常調整業務、風險管理及資訊及通訊科技策略，以確保與認可機構的風

[22] 「基建風險」此用語涵蓋與資訊科技基建有關的風險，不僅限於涉及資訊科技基建的故障的風險。關於應用程式及數據保安等其他資訊科技風險亦包括在內。

險取向與可承受風險限度說明文件一致，並符合私隱及其他適用法律。

8.2.3 有效的資訊及通訊科技風險管理應包括以下程序：

(a) 界定資訊及通訊科技風險；

(b) 識別面對資訊及通訊科技風險的運作及評估相關風險承擔的程度(例如高、中、低)；

(c) 實施與所評估風險水平相稱的資訊及通訊科技風險緩減措施。常見的措施包括網絡保安、回應與復原計劃、資訊及通訊科技轉變管理程序、資訊及通訊科技事故管理程序(包括及時向用戶傳遞相關資訊)；

(d) 監察緩減措施的成效(包括定期測試)；

(e) 定期向高級管理層匯報資訊及通訊科技風險、管控措施及事件。

8.2.4 認可機構制定的資訊及通訊科技風險管理連同輔助程序應：

(a) 參照相關業內標準及最佳做法，以及因應不斷演變的威脅(如網絡威脅)及不斷發展或新的科技定期作出檢討，以確保完備；

(b) 定期作出測試以識別是否與所列明的可承受風險限度的指標存在差距，並促進提升資訊及通訊科技風險識別、防範、偵測及事件管理；以及

(c) 運用可據以採取行動的情報持續加強對資訊及通訊科技系統、網絡及應用程式的潛在問題的狀況的了解，並促進就風險或轉變管理的有效決策。

8.2.5 認可機構應就會造成干擾的外部事件引起的受壓情景制定方法以能在資訊及通訊科技方面作好準備，例如促進實施大規模的遠程存取、急速調配實體資產及 / 或大幅擴充頻寬以支援遙距用戶聯繫及客戶數據保障的需要。就此而

言，認可機構應確保：

(a) 就資訊及通訊科技系統、網絡及應用程式受到干擾或攻擊的相關潛在風險制定適當的風險緩減策略。認可機構應評估有關風險連同相關緩減策略是否在其風險取向與可承受風險限度之內；

(b) 備有清楚界定的管理特選用戶及應用程式開發的程序；以及

(c) 定期更新資訊及通訊科技，包括網絡保安，以維持適當的保安狀況。

8.2.6 另見單元TM-E-1「電子銀行的風險管理」及TM-G-1「科技風管理的一般原則」的相關指引。

8.3 持續業務運作管理及災難事故復原計劃

8.3.1 所有認可機構應有正式的應變及持續業務運作計劃(持續運作計劃)[23]，以確保其在嚴峻的業務干擾下有能力繼續運作及限制虧損。董事局批准及其後檢討持續運作計劃時，應確保應變策略繼續與當前的運作、風險與威脅及認可機構的業務操作風險管理架構一致。穩健的持續運作計劃需要第一及第二道防線投入計劃的設計；高級管理層及業務單位主管大力參與計劃的實施，以及第三道防線定期作出檢討。

8.3.2 此外，持續運作計劃對干擾情景應具前瞻性，並有相關影響評估及復原程序：

(a) 持續運作計劃應以對認可機構運作的潛在干擾情景分析為依據。為作出分析，應涵蓋認可機構的所有業務單位及關鍵服務供應商與主要第三方(如中央銀行、結算所)，並識別關鍵運作及主要內部與外部倚

[23] 持續運作計劃應與單元OR-2所載關鍵運作的持續運作計劃一致並與其測試同時進行。

賴關係及予以分類；

(b) 每個情景都應就其財務、業務操作、法律及信譽後果接受計量及質量影響評估或業務影響分析；以及

(c) 持續業務運作流程應按干擾情景的門檻或限額(例如可接受停運上限)的規限而啟動。有關流程應處理恢復運作方面的事宜、設定復原時間目標及復原點目標，以及知會管理層、僱員、監管當局、客戶、供應商及(如適用)民政當局的通訊指引。

8.3.3 認可機構應根據員工的具體角色為員工提供訂造的培訓及認知計劃，以確保員工能有效執行應變計劃。持續業務運作程序應定期予以測試，確保萬一發生嚴峻的業務干擾情況，認可機構仍能符合復原及恢復目標與時限。在可行情況下，認可機構應參與與主要服務供應商進行的持續業務運作測試。正式測試及檢討活動結果應向高級管理層及董事局匯報。

8.3.4 有關金管局預期認可機構就持續業務運作規劃採用的穩健方法，另見單元TM-G-2「持續業務運作規劃」。

9. 披露

9.1 《銀行業(披露)規則》(第155M章)訂明認可機構須遵守的監管披露規定(包括與業務操作風險承擔及業務操作風險管理相關的)。單元CA-D-1「《銀行業(披露)規則》的應用指引」列載詮釋指引，以補足有關規則。

9.2 下文概述預期認可機構會遵守的幾項一般原則，尤其是從而可讓其持份者評估其業務操作風險管理方法及業務操作風險承擔：

(a) 認可機構應公開披露有關其業務操作風險管理的資訊。披露的數量及類型應與認可機構的運作規模、風險狀況及複雜程度相符，並應顧及不斷轉變的業界做法；

(b) 認可機構亦應向其持份者披露相關業務操作風險承擔(包括重

大業務操作虧損事件[24])，但同時避免因作出有關披露而造成業務操作風險(例如提述尚未處理的潛在管控問題)。認可機構披露其業務操作風險管理架構的方式應能讓持份者決定認可機構是否有效地識別、評估、監察及管控 / 緩減業務操作風險；以及

(c) 認可機構應有正式的披露政策，而高級管理層及董事局會定期及獨立檢討與批准有關政策。有關政策應列明認可機構決定會作出哪些業務操作風險披露的方法，以及披露程序的內部管控措施。此外，認可機構應實施程序以評估其作出的披露及披露政策是否合適。

[24] 披露重大業務操作虧損事件的建議並不包括披露機密及專有資料(包括有關法定儲備的資料)。

附件：虧損事件的詳細分類

事件類別 (第1級)	定義	分類 (第2級)	活動舉例 (第3級)
內部欺詐	因旨在騙取、挪用財產或繞過規例、法律或公司政策的一類行為所引致的虧損，而涉及至少一名內部人員，不包括多元文化 / 歧視事件	未經授權活動	• 沒有匯報交易 (故意) • 交易種類未經授權 (有金錢損失) • 倉盤計價錯誤 (故意)
		盜竊及欺詐	• 欺詐 / 信貸欺詐 / 假存款 • 盜竊 / 勒索 / 挪用公款 / 搶劫 • 挪用資產 • 惡意損毀資產 • 偽造 • 支票輪 • 走私 • 竊取帳戶資金 / 偽冒帳戶持有人等 • 違反稅務規例 / 逃稅 (蓄意) • 賄賂 / 回佣 • 內幕交易 (非經本行帳戶)
外部欺詐	由第三方作出旨在騙取、挪用財產或繞過法律的一類行為所引致的虧損	盜竊及欺詐	• 盜竊 / 搶劫 • 偽造 • 支票輪
		系統保安	• 黑客造成的破壞 • 竊取資訊 (有金錢損失)

事件類別 (第1級)	定義	分類 (第2級)	活動舉例 (第3級)
僱傭措施及工作環境安全	因違反僱傭、健康或安全法例或協議的行為、支付人身傷害賠償、或多元文化 / 歧視事件所引致的虧損	勞資關係	• 薪酬、福利、終止僱傭合約相關事宜 • 有組織的勞工行動
		安全環境	• 一般責任 (滑倒等) • 僱員健康及安全規則事件 • 勞工補償
		多元文化及歧視	• 所有類別的歧視
客戶、產品及經營手法	因無意或疏忽而未能履行對特定客戶的專業義務 (包括受信義務及產品適合性規定) 或某項產品的性質或設計所引致的虧損	適合性、披露及受信	• 違反受信責任 / 指引 • 適合性 / 披露事宜 (認識你的客戶等) • 違反零售客戶披露規定 • 違反私隱規定 • 激進推銷 • 反覆操作客戶帳戶 • 不當使用保密資訊 • 貸款人責任
		不良經營手法或市場行為	• 壟斷 • 不良交易手法 / 市場行為 • 操控市場 • 內幕交易 (經本行帳戶) • 未經許可活動 • 洗錢
		產品缺點	• 產品問題 (未經授權等) • 模型錯誤

事件類別 (第1級)	定義	分類 (第2級)	活動舉例 (第3級)
		殷選、保薦安排及風險承擔	• 未有按指引調查客戶 • 超越客戶風險承擔限額
		諮詢活動	• 有關諮詢業務表現的糾紛
實體資產損壞	因自然災害或其他事件造成的實體資產的損失或損壞所引致的虧損	災害事故及其他事件	• 自然災害損失 • 外部原因造成的人員傷亡 (恐怖活動、故意破壞)
業務受干擾及系統故障	因業務受干擾或系統故障所引致虧損	系統	• 硬件 • 軟件 • 電訊 • 公用事業服務中斷 / 受干擾
執行、交付及程序管理	因失效的交易處理或程序管理，或因與交易對手方及銷售商的關係所引致的虧損	交易確認、執行及記錄備存	• 溝通出現問題 • 數據輸入、備存或載入錯誤 • 錯過限期或未履行責任 • 模型 / 系統操作失誤 • 會計錯誤 / 實體歸屬錯誤 • 其他任務表現欠佳 • 交付失敗 • 抵押品管理問題 • 參考數據備存
		監察及匯報	• 並未有效履行強制匯報責任 • 外部報告不準確 (引致虧損)

事件類別 (第1級)	定義	分類 (第2級)	活動舉例 (第3級)
		接收客戶及文件記錄	• 遺漏客戶許可 / 免責聲明 • 法律文件遺漏 / 不全
		客戶帳戶管理	• 未經批准取得帳戶 • 客戶記錄錯誤 (引致虧損) • 因疏忽導致客戶資產損失或損壞
		交易對手方	• 非客戶對手方表現失誤 • 其他與非客戶對手方的糾紛
		銷售商及供應商	• 外判 • 與銷售商的糾紛