OR-1	業務操作風險管理	V.1 – 28.11.05

本章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，以接通有關章節。

——————————

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 背景
   - 1.2 範圍
   - 1.3 法定架構
   - 1.4 實施
2. 業務操作風險的監管方法
   - 2.1 目標及原則
   - 2.2 監管程序

1. 引言

1.1 背景

1.1.1 金管局在SA-1《風險爲本監管制度》的第2節指出，認可機構一般面對8大類風險：信貸、市場、利率、流動資金、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操作系統來管理每類風險。

1.1.2 幾乎所有銀行交易及業務活動都存在業務操作風險。根據巴塞爾委員會發出適用於銀行資本標準的經修訂架構（「資本協定二」），業務操作風險的定義是：「因內部程序、人員及操作系統的不足之處或缺陷，或因外在事件而引致虧損的風險」。這個定義包括法律風險，但不包括策略及信譽風險。

1.1.3 過去幾年，業務操作風險越來越受關注，原因是銀行：

- 越來越倚賴日趨複雜的自動化技術；
- 開發日趨複雜的產品；
- 參與大型的合併及收購活動；
- 進行整固及內部重組；
- 採用某些技術（如抵押、信用衍生產品、淨額結算及資產證券化等）以減低某些風險，但此舉卻可能會引致其他風險（如法律風險）；及
- 外判某些工序。

近年某些銀行由於未能實施妥善的程序以控制業務操作風險，因而蒙受重大的業務操作虧損。

1.1.4 巴塞爾委員會於2003年2月發出一份文件，題爲《業務操作風險管理與監管的穩健做法》，以供銀行及監管當局用作評估業務操作風險管理政策及方法。巴塞爾委員會相信有關文件所列載的原則是建立穩健做法

的基礎，並適用於任何規模及業務範圍的銀行。因此，委員會建議採用《資本協定二》內任何一種計算業務操作風險的資本要求的方法的銀行都應符合該有關文件所載的指引。巴塞爾委員會亦規定銀行如採用較先進的計算方法，即標準(業務操作風險)計算法(「STO計算法」)（及替代標準計算法(「ASA計算法」）或高級計算法(「AMA計算法」)，必須先符合指定的業務操作風險管理準則。

1.2 範圍

1.2.1 本章：

- 列載金管局對業務操作風險的監管方法；
- 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；及
- 就認可機構如何符合採用STO計算法（或ASA計算法）計算在《資本協定二》內業務操作風險的資本要求的質量準則，提供進一步指引。

1.2.2 金管局在制定本章時，參考了以下各項：

- 上文第1.1.4段提及巴塞爾委員會發出的文件；
- 採用STO計算法（或ASA計算法）計算在《資本協定二》內業務操作風險的資本要求需符合的質量準則；
- 一些國際銀行採用的業務操作風險管理政策與方法；及
- 《有效監管銀行業的主要原則》第13項原則，內容涉及銀行控制其他重大風險（包括業務操作風險）的風險管理程序（有關資料載於巴塞爾委員會發出的文件《主要原則方法》(1999)）。

1.2.3 就本建議文件而言，由於對不同認可機構來說，某項業務操作事故或風險的關鍵程度、嚴重程度或重要性

都不同，因此金管局沒有定出劃一的評估方法。在決定某項業務操作事故或風險的相對重要性時，認可機構可考慮與其本身的情況相關的質量及數據因素，及評估這些因素目前及未來對資本、盈利、專營權或信譽造成的影響。

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前及之後須繼續備有足夠的會計制度和足夠的管控制度。這是確保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、審慎及專業能力，以及無損存款人或可能的存款人的利益的方式經營。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，其中包括業務操作事宜，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操作失誤的能力，以及電腦系統與員工的質素。

1.3.3 此外，《銀行業條例》第98條規定所有在香港註冊成立的認可機構的資本充足比率不得少於8%。在香港實施《資本協定二》後，除了信貸風險及市場風險外，這個比率還會計及業務操作風險。

1.4 實施

1.4.1 金管局明白相對其他風險管理環節，業務操作風險作爲一個獨立項目仍然處於發展初階。用於識辨、評估、監察及報告業務操作風險的各種技術和工具仍在演變。因此本建議文件僅列出管理業務操作風險的「穩健做法」，而不是「法定規定」。認可機構所制定的業務操作風險管理架構應符合本章所提供的指引，並與其規模、業務複雜程度及風險狀況相稱。

1.4.2 認可機構若打算採用STO計算法（或ASA計算法）計算業務操作風險的資本要求，在評估是否符合採用這些方法的質量準則時，需要考慮本指引內適用的部分。

2. 業務操作風險的監管方法

2.1 目標及原則

2.1.1 每間認可機構應制定及維持具成效及有效率的適當業務操作風險管理架構，以識辨、評估、監察及控制／減低業務操作風險。每間認可機構在制定其業務操作風險管理架構時，需要考慮其業務的複雜程度、產品及服務範圍、組織結構及風險管理文化。

2.1.2 金管局採用風險爲本監管制度（見SA-1《風險爲本監管制度》），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，目的是評估認可機構的業務操作風險承擔及虧損的程度及趨向，以及其業務操作風險管理架構是否足夠及有效。如屬本地註冊認可機構，金管局亦會評估其資本相對其風險承擔是否足夠。

2.1.3 在評估認可機構所承擔的業務操作風險及對業務操作風險的管理時，金管局會特別留意以下因素：

- 認可機構的業務操作風險管理架構是否合適，包括董事局及高級管理人員進行監察的程度，以及風險文化；
- 管理業務操作風險的策略、政策及程序，包括業務操作風險的定義是否合適；
- 識辨、評估、監察及控制業務操作風險的業務操作風險管理程序是否足夠；
- 認可機構減低業務操作風險的措施的成效；

- 認可機構對業務操作風險的內部檢討及審核是否足夠，以及內部檢討及審核的結果；
- 認可機構的外聘核數師發出的管理函件中所提出的審核結果及建議；
- 認可機構的重大業務操作風險事故的成因及影響；
- 認可機構用以及時及有效地解決業務操作風險事故及問題的程序；及
- 認可機構的災難事故後運作復原及持續業務運作計劃的質素及全面性。

2.1.4 金管局亦會確保認可機構公開披露足夠的資料，以供市場人士評估它們對業務操作風險的管理方法。就此而言，爲實施《資本協定二》而對認可機構發出的披露資料要求的監管指引將會列載更多指引。

2.2 監管程序

2.2.1 金管局會審查每間認可機構的業務操作風險管理架構的成效。此外，《銀行業條例》第59(2)條賦予金管局權力，可特別要求認可機構呈交由外聘核數師擬備的報告書，內容關乎認可機構的內部管控制度。

2.2.2 金管局目前在決定本地註冊認可機構根據《銀行業條例》第98條須遵守的最低資本充足比率時，會考慮到認可機構所承擔的業務操作風險。計算本地註冊認可機構的業務操作風險的指定資本要求的方法，將會列載於金融管理專員根據《銀行業條例》訂立的《銀行業(資本)規則》內。

2.2.3 如有任何事件可能會對認可機構的業務操作構成重大影響，認可機構應通知金管局。有關事件可能包括：

- 已發生或已識辨的重大業務操作虧損／風險承擔；
- 操作系統或管控措施嚴重的缺陷；

- 就銀行業務有關的範疇（包括後勤辦事處的業務活動）訂立內包／外判安排的計劃，或修訂內包／外判安排或修改內包／外判安排的範圍的計劃；
- 組織結構、基礎設施或業務操作環境的任何重大轉變；及
- 啓動持續業務運作計劃。

2.2.4 金管局在接到認可機構有關上述事件的通知後，若認爲情況有需要，可能會要求有關認可機構呈交報告，分析事件的成因／目的及影響，並列明糾正所識辨的問題的行動計劃，或應付擬進行的變更實施失敗而設的應變計劃。

2.2.5 機構的內部管控的嚴重失誤或缺失，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。若重大的缺失或情況對機構安全及穩健地經營業務構成威脅，而機構未能及時妥善處理，金融管理專員將會採取監管行動。這些監管行動可能包括要求就有問題的範疇呈交獨立的特別檢討報告；就同意認可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；對機構或/及其負責董事及經理採取強制行動；及要求認可機構即時實施所有必要的糾正措施。

3. 業務操作風險管理架構

3.1 概覽

3.1.1 過去認可機構主要倚賴設於業務單位內的內部管控機制並輔以審核職能來管理業務操作風險。近來，穩健的業務操作風險管理正發展爲由指定人員負責的職務，按照既定的正式政策及程序來進行。促成這個發展的原因，是董事局及高級管理人員日漸意識到需要將業務操作風險定爲獨立的風險類別，就如信貸風險

及市場風險一樣，以提高風險意識、保障信譽、減少損失，以及提高股東價值。

3.2 適合的架構

3.2.1 無論認可機構的規模及業務複雜程度是怎樣，每間認可機構都應制定適合的架構，以管理業務操作風險。業務操作風險管理架構的目的，是確保能以一致及全面的方式識辨、評估、減低／控制、監察及報告業務操作風險。

3.2.2 就本建議文件而言，合適的業務操作風險管理架構應具備以下元素：

- 組織結構（包括董事局的監察、高級管理人員的責任、業務單位管理層的職責，以及一個業務操作風險管理職能和內部審核）；
- 風險文化；
- 策略及政策（業務操作風險管理策略、政策及程序）；及
- 業務操作風險管理程序（識辨、評估、減低／控制、監察及報告業務操作風險的程序）。

3.2.3 實際上，認可機構的業務操作風險架構必須反映業務單位的業務範圍及複雜程度，以及其公司組織結構。每間認可機構的業務操作風險狀況都是獨特的，需要特別定出適合其規模及所面對的風險程度與嚴重性的風險管理方法。不同機構需要不同的方法，亦沒有一套特定的架構可配合每間機構的需要。事實上，銀行業及監管機構正繼續發展它們就業務操作風險的組織模式及技巧。

4. 組織結構

4.1 概覽

4.1.1 管理業務操作風險，需要組織架構中的不同組成部分的關注及參與，而每部分都需負起不同的責任。組織架構中的每個組成部分都必須清楚理解本身在機構的組織及風險管理架構中的職能、權限及問責關係。所有業務單位及支援部門都應該是整體業務操作風險管理架構中不可或缺的部分。成立獨立的中央風險管理職能，可協助董事局及高級管理人員履行他們需了解及管理業務操作風險的責任。此外，雖然機構會就業務操作風險指定專責人員，但機構的所有人員都有責任識辨及管理業務操作風險。

4.2 董事局的監察

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。爲履行這項職責，董事局或其下設委員會應：

- 從業務操作風險爲一項應予管理的獨立風險類別的角度，來了解認可機構的業務操作風險的主要範疇；
- 訂明業務操作風險策略，並確保有關策略與認可機構的整體業務目標相稱；
- 批核及定期檢討認可機構的公司架構，以明確地管理業務操作風險，目的是要確立認可機構的業務操作風險的通用定義、管理業務操作風險的原則及共同的風險管理架構，以及制定清晰的業務操作風險管治及報告制度，包括職能與責任、標準及工具；
- 定期審閱機構整體業務操作風險狀況的高層次報告，有關報告內容識辨重大風險及這些風險對機構策略的影響；
- 確保高級管理人員採取必要措施，根據經董事局批准的風險管理架構下的原則，在機構的不同業務單位推行適當的政策及程序；

- 定期檢討風險管理架構，以確保認可機構持續管理來自外圍市場變化及其他環境因素引致的業務操作風險，以及與新產品、活動或操作系統有關的業務操作風險；
- 確保認可機構的業務操作風險管理架構得到在操作上獨立、受過適當訓練及具備適當能力的人員進行有效及全面的內部審核；及
- 確保遵守有關披露業務操作風險的監管要求。

4.3 高級管理人員的責任

4.3.1 高級管理人員應有責任推行經董事局批准的業務操作風險管理架構。具體來說，他們需負責制定管理認可機構所有重要產品、活動、程序及操作系統的業務操作風險的具體政策、方法及程序。

4.3.2 爲確保員工清楚了解及執行業務操作風險管理的政策與程序，高級管理人員應釐定認可機構的業務操作風險管理組織架構，並清楚傳達個別人員的職能及責任。機構內各級職員必須清楚了解其在業務操作風險管理程序中的職責。

4.3.3 雖然各級管理人員都對其職責範圍內的政策、程序及管控是否適合及其成效負責，但高級管理人員應清楚分配職權、責任及匯報關係，以激勵及維持問責性，以及確保投放必需的資源以有效管理業務操作風險。高級管理人員也應確保負責對認可機構的業務操作風險政策的執行進行監察和維持合規的人員具有的權力，與接受其監察的部門保持獨立。此外，高級管理人員應因應業務單位的活動的固有風險，來評估業務操作風險管理的程序是否適合。

4.3.4 高級管理人員亦有責任確保對業務操作風險管理投放足夠的人力及技術資源，從而令認可機構的業務由具備必要經驗與能力的合資格人員進行。

4.4 業務操作風險管理職能

4.4.1 銀行界一個領導性的做法，是以類似信貸及市場風險管理職能的方式，成立中央業務操作風險管理職能（在集團及／或公司層面）。這個職能的主要職責是協助管理人員履行了解及管理業務操作風險的責任，以及確保制定業務操作風險管理政策及程序，及機構整體一致執行有關政策及程序。爲此，這個職能履行多項職責，包括：

- 在公司層面釐定有關業務操作風險的管理及控制政策及程序；
- 設計及實施機構的業務操作風險評估方法、工具及風險報告系統；
- 協調整個機構的風險管理；
- 向董事局及高級管理人員作綜合報告；
- 提供業務操作風險管理培訓，並向業務單位就業務操作風險管理事項（例如使用業務操作風險管理工具）提供意見；及
- 與內部及外聘核數師聯絡。

4.4.2 如屬在集團及／或公司層面設有中央風險管理職能的銀行，其分行、附屬公司或個別業務單位通常會設有專責業務操作風險管理的人員，以確保政策及工具的一致性，以及成效及問題的通報。

4.4.3 若業務操作風險管理職能與市場及信貸風險管理職能類似，是屬於一個獨立的風險管理職能，便能更有效履行其職務。事實上，部分機構的審核部門可能負有制定業務操作風險管理計劃的初步責任。若屬此情況，認可機構應確保日常管理業務操作風險的責任及時轉交由其他部門負責，以確保審核部門保持獨立。

4.4.4 金管局明白每間認可機構的經營方式都不同，並採用不同的業務操作風險管理結構與方法。因此，金管局並不打算規定獨立的業務操作風險管理職能的正式定

義。然而，認可機構在制定其本身的業務操作風險管理組織結構時，應考慮結構中不同部門的地位、職能、責任及工作程序，可如何確保整體業務操作風險管理的一致性及完整性。

4.5 業務單位管理人員的職責

4.5.1 業務單位管理人員負責日常管理及報告其業務單位特有的業務操作風險。他們必須確保其業務單位的內部管控及做法與認可機構管理整個機構的業務操作風險的整體政策及程序一致。他們應確保就有關業務備有特定政策、程序及人員，以管理所有重要產品、活動及程序的業務操作風險。每個業務單位推行的業務操作風險管理架構應反映其業務範疇，以及其固有的業務操作的複雜性及業務操作風險狀況。業務單位管理人員必須與認可機構的整體業務操作風險管理職能保持獨立。

4.5.2 爲促進各業務單位管理業務操作風險，根據良好的做法，業務單位應有專責的業務操作風險管理人員。這些人員通常都有兩條的報告路線。一方面他們在其部門內有直接的報告關係，另一方面他們又與中央風險管理職能緊密合作，確保政策與工具保持一致，並報告成效與問題。他們的責任可能包括制定風險指標、釐定觸發需要升級處理風險的事項，以及提供管理報告。爲能有效運作，這些人員應獲授予足夠權力與資源，以履行其責任。

4.6 其他與業務操作風險有關的職能

4.6.1 認可機構內還有一些其他部門參與業務操作風險的管理。這些部門包括專業部門如法律及合規、人力資源、資訊科技及財務，這些部門應對業務操作風險的一些特定範疇及相關事項負責，例如人力資源職能在管理涉及「人員」的風險上應作爲主要參與者，而不僅是交流資訊及提供專家建議。與業務操作風險有關的其他職能應一方面負責管理其本身範疇內的業務操

作風險，另一方面就業務操作風險管理向組織結構內的其他各方提供支援。

4.7 內部審核的職責

4.7.1 內部審核應提供對業務操作風險管理架構的獨立評估，包括中央業務操作風險管理職能的運作情況。因此，內部審核不應有直接的業務操作風險管理責任。認可機構的審核所涵蓋的範圍應足以核實在整個認可機構內，業務操作風險管理政策及程序都得到有效實施。董事局應（直接或透過其審核委員會間接地）確保審核計劃的範圍及次數與機構的風險承擔相符。在審核程序中識辨及報告的任何業務操作事項應按情況而定由高級管理人員及時及有效地予以處理，或通知董事局。

5. 風險文化

一個成功的業務操作風險管理架構，尤其是架構內的程序的成效，有賴良好的風險文化。認可機構的風險文化包括其僱員對風險的一般意識、態度及行爲，以及機構內的風險管理。構成良好的風險文化的因素包括：

- 認可機構的業務目標及承受風險的能力、業務操作風險管理架構以及實施該架構的有關職責與責任必須清晰傳達予各級員工，員工亦應了解他們在業務操作風險管理方面的責任。
- 高級管理人員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信息，即透過行動與說話全力支持機構的風險管理架構。
- 董事局及高級管理人員向認可機構各級員工傳達的文化，應強調高水平的道德行爲標準。爲此，認可機構可採納行爲守則[1]，並在遵行有關守則方面，管理人員應以身作則。

[1] 有關行爲守則的詳細規定，請參閱 CG-3 《行爲守則》。

- 認可機構的業務及風險管理活動必須由合資格的員工執行，這些員工應具備必需的經驗、技術能力及獲取足夠資源。
- 認可機構的薪酬政策必須與其承受風險的能力相符。對表現的獎勵應顧及風險管理因素，而且有關制度的設計不應鼓勵員工採用與期望的風險管理價值觀（例如設定的持倉限額）相反的方式運作。
- 認可機構必須營造適當環境，讓職員可公開提出業務操作風險的問題而不用擔心會帶來不良後果。

6. 業務操作風險管理策略、政策與程序

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，機構便可識辨與其策略與目標有關的固有風險，從而制定業務操作風險管理策略。董事局有責任釐定業務操作風險管理策略，及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承受風險的能力或程度提供清晰指引，即認可機構爲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，並列明其對所有主要相關業務及支援程序的業務操作風險的管理策略與目標，以及爲達到有關目標而打算採用的程序。認可機構應以書面記錄其公司業務操作風險政策，並由董事局（或其屬下委員會）批准，及清楚傳達予各級員工。

6.2.2 認可機構管理業務操作風險的整體公司政策應包括：

- 機構對業務操作風險的定義，包括認可機構及客戶所面對而機構會監察的業務操作風險類別；

- 認可機構承受業務操作風險的能力與程度；
- 識辨、評估、監察及控制其業務操作風險的方法；
- 報告制度的簡介及風險管理報告會涵蓋的數據／資料類別；及
- 組織結構，界定以董事局、委員會、高級管理人員、風險管理職能、業務單位管理人員及與業務操作風險管理有關的其他部門在業務操作風險管理方面的職能、責任及匯報方式。

6.2.3 公司政策應由一套應用於特定的業務操作風險組成項目的原則提供支持，例如新客戶批核、新產品批核、新資訊科技系統批核、外判、持續業務運作規劃、危機管理及清洗黑錢等（詳盡指引見第7.4.7段）。

6.2.4 業務單位管理人員負責管理其本身業務單位的風險。因此，業務單位管理人員須根據公司業務操作風險管理政策，制定針對其業務的補充政策及程序，有關的補充政策及程序應符合公司的整體業務操作風險管理政策。

6.3 業務操作風險的定義

6.3.1 爲能有效識辨、評估、監察及匯報認可機構的業務操作風險，認可機構必須闡明業務操作風險的相關組成項目，並在整個機構內貫徹採用。有關定義應考慮機構所面對的一整套的主要業務操作風險，及反映引致嚴重業務操作虧損的最主要原因。正式及詳盡的定義亦是必要的，以改進溝通、釐定問責關係、將事故分類及累積以制定模式及進行分析，以及貫徹地交流經驗與意見。

6.3.2 巴塞爾委員會參考業務操作風險的4項基本成因——程序、人員、操作系統及外在事件（或環境）來界定業務操作風險。這個定義是要透過指出銀行的業務操作中可能引致業務操作虧損的主要內部及外來因素

（單獨或多個因素），來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4項成因下各項的風險成因分類：

風險成因	風險成因分類
程序	• 指引、政策及程序不足／不適合； • 溝通不足／失效； • 數據輸入失誤； • 對帳不足； • 客戶／法律文件不足或不當； • 保安控制不足； • 違反監管及法定規定／要求； • 變動管理程序不足；及 • 後備／應變計劃不足
人員	• 違反內部指引、政策及程序； • 越權； • 犯罪行爲（內部）； • 職責區分／雙重控制不足； • 職員經驗不足； • 職員疏忽；及 • 職能與責任不明確
操作系統	• 硬件／網絡／伺服器維修保養不足
外來因素	• 犯罪行爲； • 供應商表現欠佳； • 人爲事故； • 自然災害；及 • 政治／法律／監管問題

6.3.3 此外，爲評估業務操作風險及其潛在影響，許多銀行的業務操作風險定義已包含風險事故分類（即實際虧損或虧損事故）及影響（即財政影響的類別），以補充成因分類的定義。巴塞爾委員會制定了一個矩陣，將業務操作虧損事故類別分爲7大類，然後再細分爲從屬類別及相關活動例子[2]。根據《資本協定二》下AMA計算法的要求，須按這些虧損事故類別收集及分析業務操作風險虧損數據。認可機構在政策中考慮及列明其對業務操作風險的定義時，可採用巴塞爾委員會的矩陣作爲一般範圍。對業務操作風險定出更詳盡的定義，會有助機構以一致的方式及在整體（即集團／機構層面）基礎上評估、監察及報告業務操作風險。

7. 業務操作風險管理程序

7.1 概覽

7.1.1 認可機構應備有程序及工具以定期識辨、評估、監察及控制其主要產品、活動、程序及操作系統的固有業務操作風險。它們應採取合理措施，以確保所制定用作識辨、評估、監察及控制業務操作風險的風險管理系統足以達到有關目的。

7.2 風險識辨及評估

7.2.1 爲能更深入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辨所承受的業務操作風險類別，並評估機構受這些風險影響的可能性及程度。認可機構應根據本身對業務操作風險的定義及分類，識辨及評估所有現有或新的主要產品、活動、程序及操作系統的固有業務操作風險。有效的風險識辨及評估程序是其後制定可行的業務操作風險監察及管控制度的關鍵。

[2] 見附件 7 – 《巴塞爾協定二》的詳盡虧損事故類別分類。

7.2.2 認可機構在識辨業務操作風險時，應考慮可能影響認可機構達致其目標的內部及外來因素，例如：

- 認可機構的管理結構、風險文化、人力資源管理做法、組織架構變動及僱員流失率；
- 認可機構的客戶、產品及活動的性質，包括業務來源、分銷機制以及交易的複雜程度及交易額；
- 認可機構的產品及活動在運作周期中所用的程序及操作系統的設計、推行及運作；及
- 外圍經營環境及業內趨勢，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 認可機構在識辨風險後，需要闡明評估每項已識辨風險的適當方法，透過考慮風險的成因以估計已識辨風險真正發生的可能性，以及從對達致公司目標的潛在影響角度來評估這些風險的影響。

7.2.4 以下是多項常用於識辨及評估業務操作風險的工具：

- 自我或風險評估——銀行根據一個潛在風險清單評估其業務操作及活動。這個程序是由內部發起，通常結合核對清單及／或研討會來識辨業務操作風險環境的優勢及弱點。
- 風險圖表——在這個程序中，各業務單位、機構職能或工作流程會按不同的風險類別標出。這個程序可突顯有問題的地方，有助安排其後的管理行動的先後次序。
- 風險指標——風險指標是指統計數據及／或矩陣（通常是財政方面的），它們有助了解認可機構的風險狀況。認可機構通常會定期（例如每季或每月）檢討這些指標，使認可機構警覺到一些轉變可能帶來的風險。這些指標包括未

能完成的交易宗數、職員流失率及失誤與遺漏的次數及／或嚴重程度。

7.2.5 自我評估若能有效進行，認可機構應能識辨管控方面的漏洞，及最終應採取的適當糾正行動（或具體註明接受有關風險），並有清晰指示，列明負責採取有關糾正行動的部門及目標完成日期。因此，有關程序應明確指明機構須進行風險分析，清楚界定各業務範圍的問責關係，以及確保高級管理人員進行監察。

7.2.6 爲了解機構所承擔的業務操作風險對機構的影響，認可機構應持續評估其業務操作風險，並計及以下因素：

- 已發生的業務操作風險事故或會引致重大業務操作虧損但得以避免出現的事故（例如幾乎發生的失誤或交易對手因示好而豁免收取罰款）；
- 風險及控制措施的內部評估結果；
- 風險指標顯示的數字或趨勢（即可反映業務操作效率的數量數據（如未能交收的交易宗數、職員流失率、操作系統停止運作持續的時間、處理量及失誤次數），或控制措施的成效（如審核評分或審核提出的關注事項、超越限額情況）；
- 已報告的外來業務操作虧損及風險承擔；及
- 業務經營環境的變化。

7.2.7 業務操作風險的計量方法尚在發展中。認可機構如希望採用較爲先進的業務操作風險計量方法，便需要收集業務操作風險事故的完整及準確數據（按風險分類）以及業務操作虧損的潛在來源。一個已確立及整全的虧損事故數據庫可用作業務操作風險的實證分析及模型擬定，以及計算有關虧損的數額。這對於有效評估及管理業務操作風險的重要性已被肯定。

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重大虧損承擔。有關程序應包括對認可機構的各類業務操作風險承擔的質量及數量評估、評估糾正／減低業務操作風險行動的質素及合適性，以及確保備有足夠的控制措施及操作系統，以能及早識辨及處理問題，以免問題演變爲嚴重事件。有關程序應與認可機構的風險及活動規模相稱。

7.3.2 在監察業務操作風險時，認可機構應識辨或制定適當的指標，以能及早就業務操作風險向管理人員發出提示（通常稱爲「主要風險指標」）。認可機構採用的主要風險指標應能爲管理人員提供預測性的資料，並應反映業務操作風險的潛在來源，以便管理人員可以及早採取行動，避免事件演變爲嚴重問題。主要風險指標基本上是選自由銀行的不同職能用以識辨及定期記錄的業務操作／監控指標，有關指標被視爲適用於管理人員進行監察及觸發提升處理層面的事件。透過對主要風險指標設定適合的「目標或限額」或「提升處理層面觸發點」，監察主要風險指標可就業務操作風險的增加或業務操作風險管理的失效提供預警，以便將潛在問題傳達至高級管理人員。

7.3.3 風險監察應屬認可機構活動的一個組成部分，監察的頻密程度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經常性與性質。

7.3.4 認可機構監察活動的結果、內部審核及／或風險管理職能的合規檢討結果、外聘核數師發出的管理函件，以及監管機構編製的報告應(在適當情況下)包括在定期呈交予董事局及高級管理人員的報告內，以支持董事局及高級管理人員進行主動管理。

7.3.5 一般而言，董事局應收到足夠的高層次資料，以能了解認可機構的整體業務操作風險狀況，以及集中注意對業務有重大及策略性影響的地方。

7.3.6 高級管理人員應確保有關級別的管理人員按時收到定期的業務操作風險管理報告，而報告的內容與格式應有助有關管理人員監察及控制其業務範圍。呈交予高級管理人員的風險報告應來自適當環節，如業務單位、支援部門、業務操作風險管理部門及內部審核。

7.3.7 一般而言，管理報告應載有有關內部財政、業務操作與合規數據，以及與決策有關的外部市場事件及情況資料。這些報告應提供如下文所載的資料：

- 機構正面對或可能面對的主要業務操作風險（如主要風險指標及其趨勢數據、對風險及控制措施的自我評估的轉變、審核／合規檢討報告列載的意見所顯示的業務操作風險）；
- 主要風險事故／虧損經驗、所識辨的問題及擬採取的補救行動；
- 所採取的行動的狀況及／或成效；及
- 異常情況報告（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，以及可能或實際違反預設業務操作風險承擔額及虧損限額的情況）。

7.3.8 管理人員分析報告時，應務求能改進現有的管理表現，以及制定新的風險管理政策、程序及做法。

7.3.9 爲確保收到的報告具參考價值及可靠，管理人員應定期核實整體報告操作系統與內部管控的及時性、準確性及適切性。

7.3.10 認可機構可考慮儲存報告所提供的資料，特別是虧損數據，以建立一個架構有系統地記錄及觀察虧損事件的次數、嚴重程度及其他相關資料。

7.4 風險控制及減低

7.4.1 認可機構應備有政策及程序，以控制及／或減低業務操作風險。認可機構也應備有操作系統，以確保遵守

有正式文件列載有關認可機構的風險管理操作系統的內部政策。有關系統的主要元素可包括：

- 高層次檢討認可機構在達成所定目標方面的進度；
- 查核遵從管控措施的情況；
- 有關檢討、處理及解決違反管控措施事項的政策及程序；及
- 有正式文件列載的批核及授權操作系統，以確保對適當級別的管理人員的問責性。

7.4.2 認可機構應確保風險管理的管控結構能配合業務活動的增長或轉變（如新產品、遠離總行的分行／附屬公司的業務操作及進入不熟悉的市場）。

7.4.3 認可機構控制業務操作風險的一項關鍵元素，是備有穩健的內部管控制度。若內部管控制度設計妥善及得到貫徹實施，有助管理人員保障機構的資源、編製可靠的財務報告，以及遵守法例與規例。穩健的內部管控制度亦可減低內部程序及操作系統出現嚴重的人爲失誤及不當的情況，並有助及時偵察失誤及不當情況。

7.4.4 認可機構控制業務操作風險的方法一般包括：

- 分隔職責，以避免個別職員的責任出現利益衝突而有利隱瞞虧損、失誤或不當行爲；
- 緊密監察指定風險限額的遵從情況及調查超越限額的事件；
- 就獲取及使用銀行資產及記錄維持保障措施；
- 確保職員備有適當專業知識及訓練；
- 識辨似乎偏離合理預期回報的業務單位或產品（如應屬低風險、低邊際利潤的交易活動卻帶

來高回報，應質疑是否因爲違反內部管控才獲得有關回報）；及

- 定期就交易及帳目進行核實及對帳。

7.4.5 就所有已識辨的重大業務操作風險而言，認可機構應決定是否運用適當程序以控制及／或減低有關風險，或承擔該等風險。如屬無法控制或減低的風險，認可機構應決定是否接受該等風險、或減低有關的業務活動水平，甚至完全退出有關業務活動。

7.4.6 認可機構可透過保險等風險減低工具，將一定程度的業務操作風險轉移予第三方。然而，認可機構不應以風險減低工具取代對業務操作風險的內部管控。認可機構也需仔細考慮保險等風險減低工具能真正減低風險的程度，或會否將風險轉移至另一個業務範疇，甚或構成新的風險（如法律或交易對手風險）。

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：

- **新產品及活動**

  銀行若從事新活動或發展新產品，尤其若有關活動或產品與認可機構的核心業務策略不一致，業務操作風險便可能會更顯著。因此，認可機構應備有政策，定明認可機構新產品批核程序的標準，以及說明有關程序中的職能與責任。

  以上措施，是要確保新業務及認可機構現有業務的轉變是以受控制的方式進行，同時業務單位及支援職能都能作好充分準備，應付擬進行的新業務或現有業務的轉變。有關新產品／服務的措施的一般指引，見 IC-1 《風險管理的一般措施》。

- **資訊科技能力及保安以及資訊科技操作系統、設施及設備的變動**

  有關政策應旨在透過足夠的資訊科技管控，包括保安管理、操作系統開發及變動管理、資訊處理、通訊網絡及管理技術服務供應商等，確保資訊科技方面的高風險事項得到處理。有關認可機構在管理科技有關風險時應考慮的一般原則，見 TM-G-1《科技風險管理的一般原則》。

- **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不可或缺的部分，其中應涵蓋客戶認證、資料的保密及完整性、應用保安、互聯網基建及保安監察等方面管控，以及在客戶保安方面如防範虛假電郵及網站等的措施。有關電子銀行風險管理一般原則的指引，見 TM-E-1 《電子銀行的監管》。

- **外判**

  外判的風險管理應包括對外判安排計劃進行全面的風險評估，所考慮的因素包括擬外判的活動的重要性及關鍵性、對服務供應商的盡職審查、對外判活動的控制措施以及應變計劃。有關金管局建議認可機構在外判業務時需處理的主要事項，見SA-2 《外判》。

- **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、程序及控制措施，以打擊清洗黑錢及恐怖分子籌資活動。爲向認可機構提供有關打擊清洗黑錢及恐怖分子籌資活動的基本政策及原則，金管局發出了《防止清洗黑錢活

動指引》（2000年修訂）、《防止清洗黑錢活動指引補充文件》（2004年修訂）及有關的《闡釋備註》。

- **適合的客戶**

  認可機構應備有政策及程序，以識辨它們認爲適合向其銷售某些複雜及高風險產品的客戶。目標客戶應被認爲有能力了解及承擔有關產品可能會引致的潛在財務風險。

- **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操作系統上的差異所造成的影響，並就海外分行及附屬公司的業務操作制定適當的管控。

- **客戶資料保密**

  《銀行營運守則》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》。有關客戶資料保密的原則的詳情，請參閱就《個人資料（私隱）條例》發出的指引第 3.7 號。

- **外部文件**

  外部文件指由認可機構編製及提供予客戶及交易對手或第三方的文件，例如合約、交易情況表或宣傳單張。這些文件如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操作系統，在發出外部文件前先加以審閱。有關程序及操作系統包括考慮以下因素：

  - 是否符合有關監管及法律規定；

- 有關文件運用標準條款或非標準條款的情況；
- 發出有關文件的渠道或方式；及
- 文件需要確認收妥的情況。

8. 持續業務運作管理及災難事故後的復原計劃

所有認可機構都應備有正式的應變及持續業務運作計劃，以確保能持續運作，以及在業務受到嚴重干擾時限制損失。管理人員應定期檢討有關計劃，確保計劃與認可機構目前的運作情況及業務策略一致。此外，這些計劃應定期受到測試，以確保認可機構在業務一旦受到嚴重干擾時能執行這些計劃。有關金管局預期認可機構在進行持續業務運作規劃時會考慮的穩健手法，見TM-G-2《持續業務運作規劃》。

目錄	辭彙	主頁	引言