SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

有關涉及交易活動的運作和離岸入帳風險以及數據風險的風險管理作業手法的主題檢視報告

2023 年 3 月 30 日

目錄

A. 引言

1. 證券及期貨事務監察委員會（證監會）認為，穩健的風險管理是持牌法團在面對市場不明朗因素及波動時，維持抵禦能力的關鍵。

2. 為向持牌法團提供進一步指引以應對新冒起的風險，證監會進行了一項主題檢視，以評估選定的持牌法團的風險管治及監督框架，以及它們在以下範疇的風險管理作業手法。

   (i) **有關交易活動的運作風險管理**——運作風險指由於內部程序、人員及系統不足或缺失而導致損失的風險。此範疇的主題檢視聚焦於有關交易活動的運作風險，涵蓋持牌法團實施的管理層監督、監控和監察措施。

   (ii) **有關交易活動的離岸入帳風險管理**——離岸入帳是一種業務模式，當中作為交易發起或執行實體的持牌法團透過集團層面的離岸入帳安排，將交易風險（例如市場或信貸風險）轉移至負責為風險入帳的離岸聯屬公司。此安排可能包括在集團聯屬公司之間進行成本分擔或損益分配的轉移定價安排。此範疇的主題檢視涵蓋持牌法團採用的離岸入帳和轉移定價安排，以及為應對潛在風險而實施的相關監控和監察措施。

   (iii) **數據風險管理**——數據風險指因持牌法團對數據生命周期（包括數據收集、分類、使用、保留、轉移和處置）管理不善而導致運作受干擾和聲譽或財務受損的風險。此範疇的主題檢視涵蓋為紓減數據生命周期各階段的風險而實施的管理層監督、監控和監察措施，特別是從數據保護的角度來看。

3. 是次主題檢視首先透過問卷向 48 家持牌法團或金融集團[1]（統稱“集團”）收集資料。在較後階段，本會與該等集團進行深入討論及對其作出現場視察，以檢視它們在上述風險範疇的管理層監督、監控和監察措施。

4. 本報告撮述業界在上述三個風險範疇中的風險管治、監督及管理的作業手法，以及從主題檢視和其他監管活動所觀察到的良好作業手法例子及有待改善之處。證監會期望持牌法團在紓減這些特定風險時應達到的標準亦載於本報告。

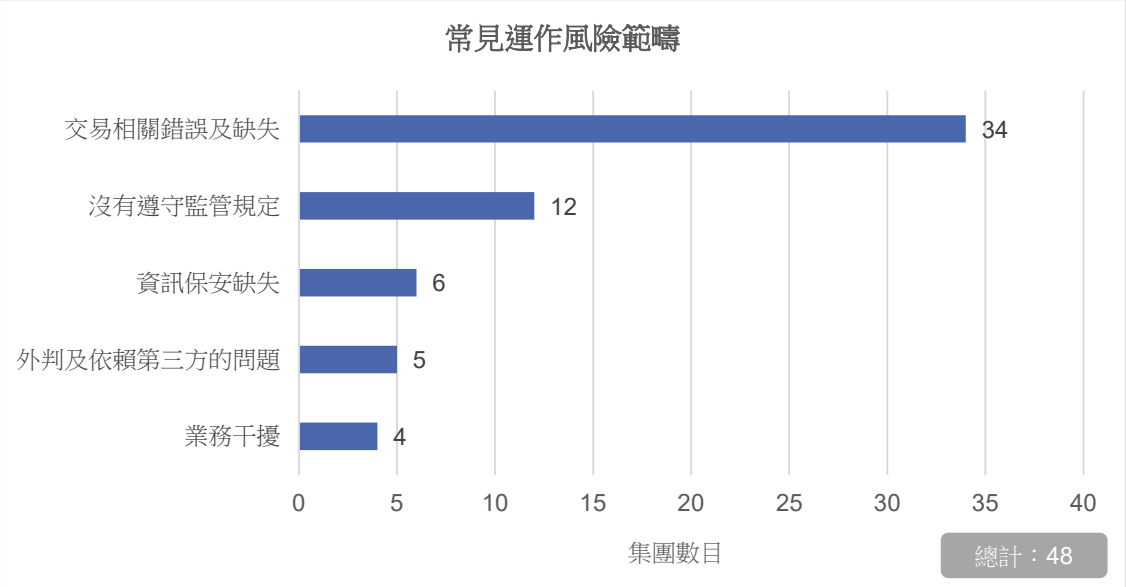
5. 證監會將緊貼本地和全球在管理運作、離岸入帳及數據的風險時的作業手法方面的發展，並會在必要時為業界提供額外指引。

[1] 同一金融集團可由多於一家持牌法團所代表。

B. 有關交易活動的運作風險管理

背景

6. 在是次檢視中，運作風險指由於內部程序、人員及系統不足或缺失而導致損失的風險。雖然持牌法團在其所有業務活動中均面對運作風險，但是次主題檢視乃聚焦於持牌法團進行的交易活動所引致的運作風險。調查結果顯示，該等集團中大部分都依照嚴重程度（例如頻率及財務影響）將“交易相關錯誤及缺失”（例如輸入不正確交易指示和不慎地違反交易或持倉限額）認定為常見運作風險中首要關注的範疇[2]。



7. 近年來，有持牌法團的交易活動所引致的運作風險事故對公司及其客戶造成重大損失，在某些情況下還影響了市場運作。持牌法團如要充分管理其交易活動中的運作風險，健全的風險管治及監控框架至關重要。

I. 運作風險管治

8. 風險管治指有界定責任及問責性的組織架構安排，讓持牌法團能夠妥善制定和實施措施來識別、評估、紓減及匯報風險。

9. 運作風險管治不足可能會導致以下問題，繼而可能阻礙持牌法團有效識別和紓減運作風險：

- 各職能之間的角色及責任並不明確，可能會降低持牌法團在應對運作風險事故和防止過度承擔風險方面的成效；及
- 沒有定期檢視風險管理框架的成效，可能進一步令持牌法團面臨運作漏洞或新冒起的運作風險種類。

[2] 回答問卷時，該等集團可選擇一個或多個運作風險範疇（如相關）。

應達到的標準
為了應付交易活動所涉及的運作風險，持牌法團應制定穩健的風險管治框架[3]，當中應涵蓋不同方面，其中包括下列範疇： (a) 清楚地界定高級管理層及相關職能的角色、責任及問責性[4]，以確保能妥善實施運作風險管理框架（包括上報規程）和在持牌法團內培育優良的風險文化；及 (b) 設有因應持牌法團的業務性質、規模、運作複雜程度及風險狀況而對運作風險管理框架的充足性和成效進行定期檢視的機制。

<u>市場作業手法</u>

(a) 在管理運作風險方面的角色及責任

高級管理層的責任及問責性

10. 一般而言，該等集團實施了運作風險管治框架，並將管治運作風險管理方面的特定角色及責任指派予高級管理層。

11. 除了負責風險管理職能的核心職能主管外，大部分集團還指定了負責其他職能（例如營運監控與檢討及／或主要業務）的核心職能主管，以監督運作風險管理政策及程序（包括處理運作風險事故的程序）的實施和定期檢視。

12. 部分集團設立了風險管治委員會或小組（由核心職能主管及其他高級管理層組成），定期召開會議，以檢視運作風險事故的趨勢及補救狀況，並評估該等集團目前的風險承擔水平是否仍可接受。

13. 一些集團考慮到其資本及風險狀況，從定量（例如風險限額及損失金額）和定性（例如不能容忍某些種類的風險及行為）兩方面界定了它們的運作風險胃納（即公司願意接受的運作風險水平）。這些集團亦制定了風險策略（即制定和實施風險管理政策的方向及重點），以應對運作風險並與其風險胃納保持一致。

相關職能在運作層面上的角色及責任

14. 大部分集團透過採取“三道防線”方針，將運作風險管理的角色指定由不同的職能來負責。

    (i) 第一道防線指進行交易活動和承擔風險的前線人員（即交易單位）。一些集團主要交由負責監管交易活動的人員（例如交易主管）來進行相關監察，而其他集團則在交易單位內指派特定的監督職能（即前線辦公室監督）來監察交易活動。前線辦公室監督

[3] 《證券及期貨事務監察委員會持牌人或註冊人操守準則》（《操守準則》）第 9 項一般原則和第 14.1 段，以及《適用於證券及期貨事務監察委員會持牌人或註冊人的管理、監督及內部監控指引》（《內部監控指引》）第 I 部。

[4] 證監會於 2016 年 12 月 16 日發出的《致持牌法團有關加強高級管理層問責性的措施的通函》。

職能負責進行日常監控和監察，以偵測和防止運作風險、員工失當行為及不合規問題。

(ii) 第二道防線指獨立的風險管理及合規職能。這些職能負責進行風險識別及評估程序，管理公司層面的風險承擔，以及實施監控和監察措施，以確保遵從相關規例。

(iii) 第三道防線指獨立審核職能，負責評估該等集團運作風險管理框架的成效並確保獲識別的風險得以化解。

運作風險事故的匯報及上報

15. 該等集團普遍表示，它們會向高級管理層提交事故報告及風險指標監察儀表板等管理層資訊，以便監督運作風險評估及事故補救程序。

16. 當發生運作風險事故時，大部分集團會檢視事件時序表，識別根本原因（例如內部監控缺失或系統失靈），並評估對其客戶、市場及公司的影響程度。根據檢視結果，這些集團會對所受到的影響採取補救行動，並制定防止事故再次發生的必要措施，例如加強內部監控措施和為員工提供複修培訓。這些集團亦制定了書面規程，藉此向高級管理層匯報運作風險事故，以及向監管機構匯報重大或涉及違反監管規定的事故。

17. 有待改善之處

- 某集團並無在其內部政策中清楚訂明運作風險事故的上報規定（例如上報的門檻及時間表）。至於另一集團，其交易人員沒有遵循內部政策訂明的運作風險事故匯報時間表。這些作業手法都可能會削弱管理層監督的成效和阻礙補救計劃的迅速實施。

良好作業手法

- 有些集團建立了有系統性的要求，以便根據風險事故的性質、嚴重程度及所帶來的財務影響，對事故作出評估和將其上報至適當的管理層。評估為高風險的事故（包括對客戶、財務、聲譽或遵守監管規定方面有重大影響的事故）需要職級較高的高級管理層更迅速的關注（例如立即上報至行政總裁）。

培育風險文化

18. 風險文化指機構內所有層面對風險管治的接受程度[5]，對有效實施公司的風險管理框架而言，不可或缺。

19. 大部分集團的高級管理層均意識到透過訂立正確的上層基調來為員工樹立行為榜樣的重要性，以強調誠實、品格及負責任的風險管理。

20. 有些集團為員工提供監督指引及培訓，以提高他們的風險意識。

[5] 有關風險文化的詳情，可參閱證監會於 2013 年 12 月發表的《業界風險研討會議系列：全球系統重要性金融機構風險及緩解措施趨勢》報告。

21. 部分集團會考慮員工的合規紀錄來評核員工表現，並採用適當的賞罰分明制度，以引導員工的行為。

(b) 運作風險管理框架的持續檢視

22. 大部分集團至少每年對其風險管理框架（包括運作監控措施（見本節第 II 部））的充足性和成效進行定期檢視。當交易活動的風險狀況有變（例如在推出新產品後）或從風險事故中識別到運作漏洞時，這些集團亦會進行特別檢視。

23. 為了利便對運作風險管理框架的持續檢視，這些集團通常使用一種或多種以下工具。

- 風險與監控自我評估——這涉及對該等集團運作風險承擔的全面評估，以及對其現有監控措施成效的評估，讓它們能夠及早制定改善措施，以應對任何已識別的新風險種類或潛在監控漏洞。風險與監控自我評估通常由前線辦公室監督職能進行，並由獨立職能（例如風險管理）核實，結果會提交予高級管理層，以便對任何風險紓減計劃作出認可。

- 主要風險指標——主要風險指標的使用涉及追蹤和分析各種風險因素（例如重複違反限額要求或異常損益變動）的趨勢及影響。該等集團採用主要風險指標來監察其風險管理框架下的運作監控措施的表現。它們定期向高級管理層提交主要風險指標報告及相關交易詳情，藉以就不合規事宜收緊監控措施、作出進一步調查或採取紀律行動的潛在需要進行決議。

- 情境分析——這些集團進行定期情境分析，以評估其現有風險管理框架對潛在運作風險事件的抵禦能力。它們利用內部模型及來自過往或假設的運作風險事件（例如錯誤交易招致的損失）的數據來預測潛在的運作損失。

24. 有待改善之處

- 某集團僅遵從集團層面的運作風險管理框架，而沒有在公司層面進行任何檢視，以確保該框架充分且有效地防止和紓減源自於本地情況的運作風險（例如違反本地賣空規定的風險）。

- 某集團利用主要風險指標作為風險監察工具來識別具有高運作風險的範疇，但並沒有就其主要風險指標所採用的門檻的適當性及成效，進行充分的持續評估。在其中一個例子中，該集團有關場外產品交易的警示水平與其過往交易量並不相稱。該集團承認在設定門檻時出錯，而有關錯誤在本會查詢後才識別出來。

II. 運作監控和監察措施

25. 運作監控和監察措施指為了偵測及防止交易活動中可能對持牌法團造成財務損失或其他損害的錯誤、遺漏或失當行為而實施的內部監控措施。持牌法團通常會實施交易前或交易後措施，以確保符合其風險胃納、交易及客戶授權和監管規定。

應達到的標準
持牌法團應設立適當的運作監控和監察[6]作業手法，以偵測及防止在交易活動中的錯誤、遺漏或失當行為。它們應確保： (a) 交易前及交易後監控和監察措施得以妥善實施，並獲定期檢視及調整，使交易活動符合監管規定及與持牌法團的風險狀況相符；及 (b) 從運作監控和監察過程中識別到的例外交易情況獲妥善評估及跟進，以便能及早採取適當行動，以減少在交易活動中的任何運作漏洞或失當行為。

<u>市場作業手法</u>

(a) 交易前及交易後監控和監察措施

26. 大部分集團在交易前或交易後層面採取人手或自動化監控和監察措施，及有時雙管齊下，以確保遵循交易授權、交易及持倉限額，以及適用的監管規定。

交易監控和監察措施所應對的運作風險指標例子	
交易前層面	**交易後層面**
▪ 違反交易及持倉限額 ▪ 就受限制產品或在受限制市場或與受限制對手方進行交易 ▪ 進行未經授權交易，違反交易授權 ▪ 無擔保股票賣空活動 ▪ 輸入錯誤交易指示（例如沒有按市場價格發出交易指示、重複發出交易指示）	▪ 高度使用交易及持倉限額 ▪ 不尋常地修改或取消交易 ▪ 不尋常的交易模式及異常情況 ▪ 異常大的交易量或交易規模 ▪ 未經批准或無合理依據而凌駕交易前監控措施

27. 就自動化監控和監察措施而言，相關集團設立了當達到預定準則及門檻時，對各類例外交易情況的不同系統反應。

- 警告或軟封鎖——所輸入的交易指示會被擱置，並在相關風險警示獲有關人員確認、證實為合理和批准後才能被處理。這種反應通常用來提醒人員可能輸入了錯誤交易指示（例如交易指示金額超過現有可用資金或重複發出交易指示）；及

- 硬封鎖——所輸入的交易指示會被完全封鎖。這種反應通常用來防止輸入不符合監管規定（例如有關無擔保賣空的交易指示）或違反交易及客戶授權（例如有關受限制產品的交易指示）的交易指示。

28. 有待改善之處

- 部分集團沒有進行定期檢視，以確保交易監控措施全面涵蓋所有交易活動（例如包括涉及場外衍生工具的交易活動），因而增加了未必能及時或根本無法識別顯示為承擔過度風險的不尋常交易模式及異常情況的風險。

[6] 《操守準則》第 3 項一般原則及第 4.3 段和《內部監控指引》第 VIII 部及附錄第 35 段。

- 某集團實施了交易前監控措施，將客戶的賣盤指示與客戶的可用股票結餘互相進行對比，以防出現無擔保賣空活動。然而，該集團無法及時識別一項涉及延遲反映客戶股票結餘減少（因股份合併或股份提取而引致）的系統限制。這引起了因交易人員不慎地為客戶超賣股票而導致的多宗交收失誤事故。

(b) 例外交易情況的處理

29. 大部分集團制定了規程，藉此檢視和處理從交易前及交易後監控和監察措施中識別到的例外交易情況（例如違反交易授權、交易對帳問題及交易錯誤）。例外交易情況最先由第一道防線（例如前線辦公室監督職能）根據人員交易行為、違規的根本原因及對客戶造成的影響進行評估。第二道防線（例如風險管理職能）會要求交易人員及時採取補救行動，然後向相關交易人員發出提示或警告，以防止違規情況再次發生。合規職能可能會參與評估在遵守監管規定方面所構成的影響和考慮是否需要向監管機構匯報。

30. 有些集團亦設有獨立團隊來進行質素保證檢視，以確保所有例外交易情況均獲妥善處理，並有足夠的稽查線索。

31. 有待改善之處

- 儘管出現經常重複違反交易授權的情況，而所涉及的未經批准產品交易造成了超乎預期的損失，但某集團並沒有採取適當的跟進行動，例如對相關交易人員的操守進行評估，以及實施經優化的監控措施來防止這種違規情況再次發生。這可能會削弱交易監控措施的成效，並縱容不合規作業手法。

良好作業手法

- 某集團不但透過了解相關交易人員所提供的依據並評估對損益所構成的影響，還通過分析交易人員的過往交易和合規紀錄所識別到的風險指標，對例外交易情況（例如不尋常地取消和修改交易）進行檢視，以揭發任何顯示有更嚴重運作漏洞的異常情況和防止有進一步違規情況。

C. 有關交易活動的離岸入帳風險管理

背景

32. 離岸入帳通常是一種業務模式，當中交易發起或執行實體透過集團層面的離岸入帳安排，將交易風險（例如市場或信貸風險）轉移至負責為風險入帳的離岸聯屬公司，再由負責為風險入帳的聯屬公司與交易發起或執行實體訂立轉移定價安排，以分配成本、利潤或損失。

33. 在 48 家選定的集團中，有 20 家表示它們有採取離岸入帳安排，以便由負責為風險入帳的聯屬公司集中管理交易投資組合風險（例如透過交易淨額結算[7]及對沖[8]），以及有效率地管理集團聯屬公司的資本。該等集團同時亦設有轉移定價安排，以便在集團聯屬公司之間進行成本分擔或損益分配。

離岸入帳模式

34. 該等集團採用了兩種離岸入帳模式。

- 直接入帳模式——將交易直接記入負責為風險入帳的離岸實體的帳冊內。負責為風險入帳的實體（而非交易發起或執行實體）是面對交易對手方的訂約方，而交易所引致的信貸風險[9]及市場風險[10]均由負責為風險入帳的實體承擔。

- 背對背入帳模式——將交易初步記入交易發起或執行實體的帳冊內。交易發起或執行實體是面對交易對手方的訂約方。它會保留交易對手方的信貸風險，但以鏡像背對背交易的方式將交易所引致的市場風險轉移至負責為風險入帳的離岸實體。

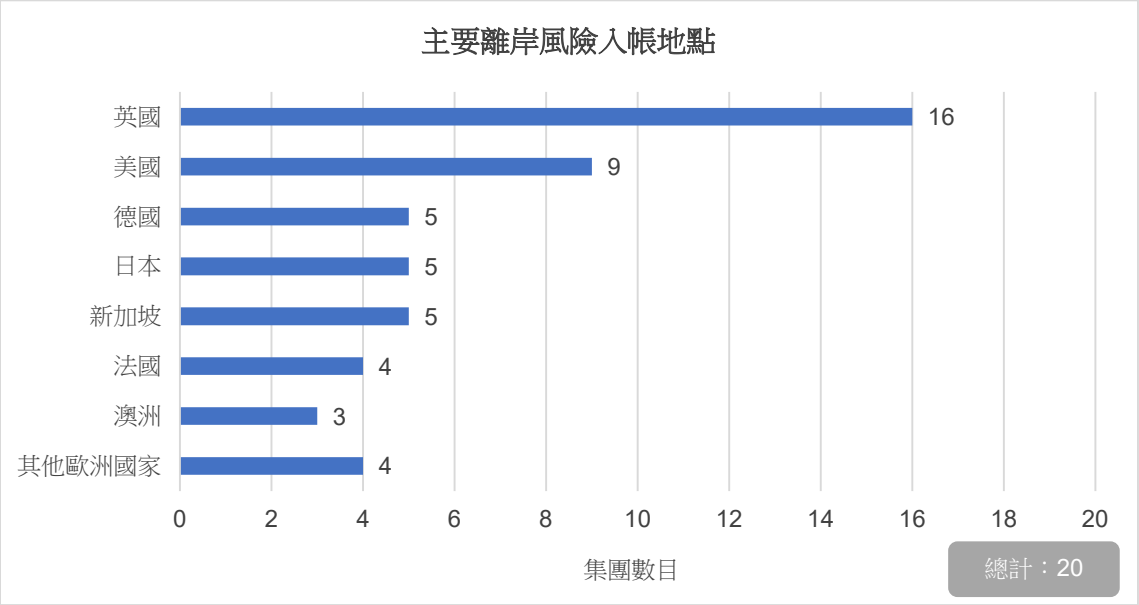
14 / 20 家集團僅採用直接入帳模式。

6 / 20 家集團同時採用直接及背對背入帳模式。

[7] 淨額結算是一種透過結合同一相關資產的相反交易持倉來抵消風險承擔的安排。
[8] 對沖是一種透過就同一相關資產或其他高度相關的資產持有相反交易持倉來抵消風險承擔的安排。
[9] 信貸風險指交易對手方未必能履行其對公司負有的責任的風險。
[10] 市場風險指價格或價值的走勢可能導致公司蒙受損失的風險。

風險入帳地點

35. 下圖顯示上述 20 家集團[11]所採用的主要離岸風險入帳地點(即由香港持牌法團將交易風險以離岸方式入帳的離岸地點），而首選的地點為英國及美國。上述 20 家集團表示，選擇特定風險入帳地點的主要決定因素是(i)集團或地區風險管理職能的所在之處，以及(ii)監管資本制度對交易活動施加較寬鬆的資本規定的地點。英國脫歐後，部分集團將其風險入帳地點從英國遷移至德國及法國等歐洲國家。



36. 部分集團表示，由海外聯屬實體發起或執行的交易可在香港入帳，但與由香港持牌法團發起或執行並記入海外聯屬公司的帳冊內的交易相比，交易量較低。是次主題檢視主要聚焦於作為交易發起或執行實體的持牌法團在離岸入帳安排下所面對的風險。

I. 離岸入帳風險管治

37. 離岸入帳安排通常涉及橫跨不同司法管轄區的多個集團聯屬公司及程序。集團聯屬公司之間的風險分配及財務聯繫可能很複雜。持牌法團須實施充足的風險管治，以確保具備健全的管理架構及在集團層面的妥善協調，藉以應對離岸入帳安排所涉及的風險（詳見第 47 至 48 段）。

應達到的標準
持牌法團應就離岸入帳安排設立穩健的風險管治框架[12]。該框架應涵蓋不同方面，其中包括下列範疇： (a) 清楚地界定高級管理層在管理離岸入帳安排的相關風險方面的責任及問責性[13]；及

[11] 一家集團可能有一個或多個風險入帳地點。

[12] 《操守準則》第 9 項一般原則和第 14.1 段，以及《內部監控指引》第 I 部。

[13] 證監會於 2016 年 12 月 16 日發出的《致持牌法團有關加強高級管理層問責性的措施的通函》。

(b) 就制定風險管理政策和評估離岸入帳安排所涉及的潛在風險（例如累積風險承擔或入帳失誤），設有與集團聯屬公司進行協調的機制。

市場作業手法

(a) 高級管理層在離岸入帳風險管理方面的監督及責任

38. 該等集團指定了負責風險管理職能的核心職能主管及負責其他職能（例如整體管理監督、主要業務、財務與會計、營運監控與檢討、合規）的核心職能主管，以監督離岸入帳安排，包括風險事故的處理。

39. 這些集團的高級管理層定期召開會議，以檢視該等集團在離岸入帳安排下的交易風險承擔，風險事故（例如延誤或沒有將交易記入聯屬公司的帳冊內）的根本原因及處理風險事故的進展，並討論業務發展（例如推出新產品）對目前離岸入帳安排的影響。

40. 有待改善之處

- 某集團沒有就重大的交易入帳事故制定上報規程和時限。在其中一個例子中，該集團的其中一名交易人員沒有根據離岸入帳安排將交易持倉記入集團聯屬公司的帳冊內。然而，該事故在八個月後才被上報至相關管理委員會，阻礙了該集團及時改善監控措施來堵塞運作漏洞。

(b) 與集團聯屬公司在離岸入帳的運作及風險管理方面的協調

集團層面的管治小組或委員會

41. 該等集團普遍認為，為參與離岸入帳安排的聯屬公司制定結構清晰的通訊協議，是提高該等集團的風險管理程序透明度和完善風險策略的有效途徑。

42. 有些集團在集團、地區及／或地方層面定期舉行管治小組會議，以討論和協調任何離岸入帳事宜（例如過度的交易風險承擔或入帳缺失或錯誤）。

43. 有待改善之處

- 某集團的一些擔任集團層面管理委員會（負責協調離岸入帳事宜）的核心成員的高層人員，曾多次缺席委員會會議，而與該集團相關的重大交易入帳事宜（例如將交易記入錯誤的離岸交易帳冊內）乃是會議上的討論項目。這令人質疑他們就履行與集團聯屬公司協調和解決潛在風險問題的責任所作出的承諾。

良好作業手法

- 在集團層面的離岸入帳安排中作為交易發起實體的一些集團，經常與負責為風險入帳的離岸實體舉行會議，討論和解決交易及入帳事宜（例如涉及違反交易授權[14]的交易入帳、市場風險限額的使用率及損益分配的對帳），而這些事宜可能對交易發起實體及負責為風險入帳的實體造成風險。

政策及程序

44. 一般而言，該等集團的風險管理中心建立了集團層面的框架，並與地方風險管理團隊協調，以制定地方政策來管治離岸入帳安排。

45. 這些政策及程序通常涵蓋高級管理層與相關職能的風險管理角色和責任，風險或入帳事故的上報程序，以及監控和監察措施，以確保離岸入帳安排的有效運作。

46. 有待改善之處

- 部分集團只依賴集團層面的政策來管治離岸入帳安排。這些政策沒有充分界定高級管理層在地方層面的責任及問責性。此外，離岸入帳事故的上報程序及設定地方風險限額的權限均不夠明確。

II. 離岸入帳的監控和監察措施

47. 根據集團層面的離岸入帳安排，持牌法團可以離岸方式將交易入帳，因而將風險轉移至其集團聯屬公司。如持牌法團因運作問題而未能妥善地將交易持倉記入集團聯屬公司的帳冊內（例如在未經授權或超出預定限額的情況下將交易入帳），所產生的損失便可能由持牌法團承擔。

48. 此外，集團聯屬公司可能會將成本或交易損失分配予涉及集團層面的轉移定價安排的持牌法團。如所分配的損失的比例過高或較預期多，持牌法團或會面臨迫切的財務風險。

應達到的標準

持牌法團應確保實施適當的監控和監察措施[15]，以管理由與其集團聯屬公司之間的離岸入帳安排所引致的風險[16]。有關監控和監察措施應涵蓋不同方面，其中包括下列範疇。

(a) 有關將持倉記入集團聯屬公司的帳冊內的監控和監察措施

(i) **交易授權** —— 持牌法團應設立交易授權，以清楚地列明交易人員的責任及權限，包括根據離岸入帳安排所進行的交易及入帳活動，並應實施適當的監控和監察措施，以確保其人員遵循交易授權。

[14] 有關交易授權的更多詳情，請參閱下文第(C)(II)節。

[15] 《操守準則》第 3 項一般原則及第 4.3 段和《內部監控指引》第 VIII 部。

[16] 持牌法團應遵從：(i)《操守準則》第 20.1 段，當中列明當出現對集團聯屬公司的財務風險承擔時應採納的風險管理標準；及(ii)《操守準則》第 20.3 至 20.5 段，當中列明當把場外衍生工具交易記入並非在可資比較的場外衍生工具司法管轄區內受到規管的集團聯屬公司的帳冊時應遵守的準則。

(ii) **系統接達監控措施** —— 持牌法團應實施適當的系統接達監控措施，以確保只有獲授權的人員才可進行離岸入帳活動。

(iii) **風險限額** —— 持牌法團應確保設有風險限額，以監控和管理所承擔的交易風險，並應實施適當的監控和監察措施，以確保其人員遵循風險限額。

(b) 有關轉移定價安排的損失分配監控和監察措施

持牌法團應實施充足的監控措施，以監察根據轉移定價安排獲分配的任何損失的規模，並應採取適當措施，以防止可能會損害其財政能力的重大損失分配。

<u>市場作業手法</u>

(a) 有關將持倉記入集團聯屬公司的帳冊內的監控和監察措施

交易授權

49. 所有集團均設立交易授權，以界定其交易單位或人員所進行的交易及入帳活動，作為離岸入帳安排的一部分。有關授權可能包括一系列獲許可的產品及集團的交易和對沖策略。

50. 關於對交易授權所作的任何更新，大部分集團均設立機制，要求須就涉及更高風險承擔的授權取得交易單位中較高級的主管人員及／或獨立職能（例如風險管理或合規）的批准。

51. 有些集團要求其前線辦公室監督職能監察其人員是否遵從交易授權。

52. 有待改善之處

- 某集團的一名交易人員在將交易記入集團聯屬公司的帳冊內方面，被賦予過多權限，包括可就超出其交易授權範圍的產品類別入帳。然而，該集團因缺乏審查機制而未能及時發現此事，而該人員無心地進行了多項違反其交易授權的交易。

系統接達監控措施

53. 大部分集團已按需要將系統接達權授予其人員，以便他們進行離岸入帳活動。舉例來說，交易人員及負責監管交易活動的人員獲授予“讀寫”權限，即他們獲准查看交易持倉，以及將交易在境外入帳或將風險轉移至境外，而僅出於監察目的（例如風險管理和合規）而需查看交易持倉的人員則獲授予“唯讀”權限。

54. 有些集團要求其前線辦公室監督職能定期審視交易帳冊的接達權，以確保它們仍屬恰當。

55. 有些集團亦制定偵測性監控措施，以識別任何未經授權而取覽交易帳冊的情況。

56. 有待改善之處

- 某集團的前線辦公室監督職能發現，雖然一名交易人員不再需要有關將交易記入離岸集團聯屬公司的帳冊內的接達權，但該接達權在一段長時間後才從系統中移除。這導致該集團在此期間內，可能承受著人員在未被發現的情況下未經授權而將交易記入離岸實體的帳冊內的風險。

風險限額

57. 一般來說，該等集團在不同層面（例如個別交易人員、交易櫃枱、實體和集團層面）設有風險限額以管理其離岸入帳活動的風險承擔，並持續監察他們遵循風險限額的情況。

58. 部分集團設置了自動化監控措施（例如向交易人員和風險管理團隊發出系統警示），以助偵測當日風險限額使用率為高的情況，而有些集團則在當日結束時利用特殊報告來識別違反風險限額的情況。

59. 部分集團允許交易人員申請臨時提高風險限額，但須取得負責監管交易活動的人員或前線辦公室監督職能的批准。他們須以文件記錄提高風險限額的詳情，包括其額度、有效期和理由。

60. 有待改善之處

- 某集團允許其交易人員出於某些理由而執行超出其內部交易限額的交易指示。然而，我們發現，在一些情況下，所需要提供的理由並不完整或不存在。這會影響該集團為評估臨時提高風險限額是否合理和適當而進行的任何交易後檢視的成效。

良好作業手法

- 某集團制定了交易授權和限額，並利用自動化系統封鎖和警示機制來處理不合規交易，以確保其交易和入帳活動符合集團層面的風險管理政策和離岸入帳安排。該集團定期檢視和核實其所有交易授權和限額是否適當。在作出修訂時，該集團要求相關交易人員確認並承諾遵守經修訂的交易授權和限額。

(b) 有關轉移定價安排的損失分配監控和監察措施

61. 採取離岸入帳安排的 20 家集團均與其交易發起或執行實體和負責為風險入帳的實體訂立了轉移定價安排。

62. 在大多數情況下，轉移定價安排要求負責為風險入帳的實體承擔交易損失。在其他情況下，有關安排允許負責為風險入帳的實體因應產品類別與交易發起或執行實體分擔全部或部分的交易損失。

63. 大多訂立轉移定價安排的集團均表示，它們透過書面協議來管治這些安排的實施。為利便遵守海外和當地稅務匯報規定，該等集團擬備了轉移定價文件報告，從而將價值驅動因素、所履行的職能的相互依存性及金融集團內各實體所承擔的風險以文件記錄下來。

64. 部分集團經考慮其轉移定價安排下的過往損益分配模式及任何超乎預期的損失分配預測（例如因集團聯屬公司表現欠佳所致）後，擬備了有關其財政能力的年度預算。

65. 一些集團制定程序，以定期監察所面臨的風險及其轉移，並評估所構成的影響。它們亦設有機制，以監察流動資金和及時將任何財務風險上報予高級管理層。

66. 有待改善之處

- 根據集團層面的轉移定價安排，分配予某集團的損失可能為異常大額，並可導致資不抵債的情況。然而，該集團並沒有妥善地評估有關的財務影響或採取足以應對風險的措施。

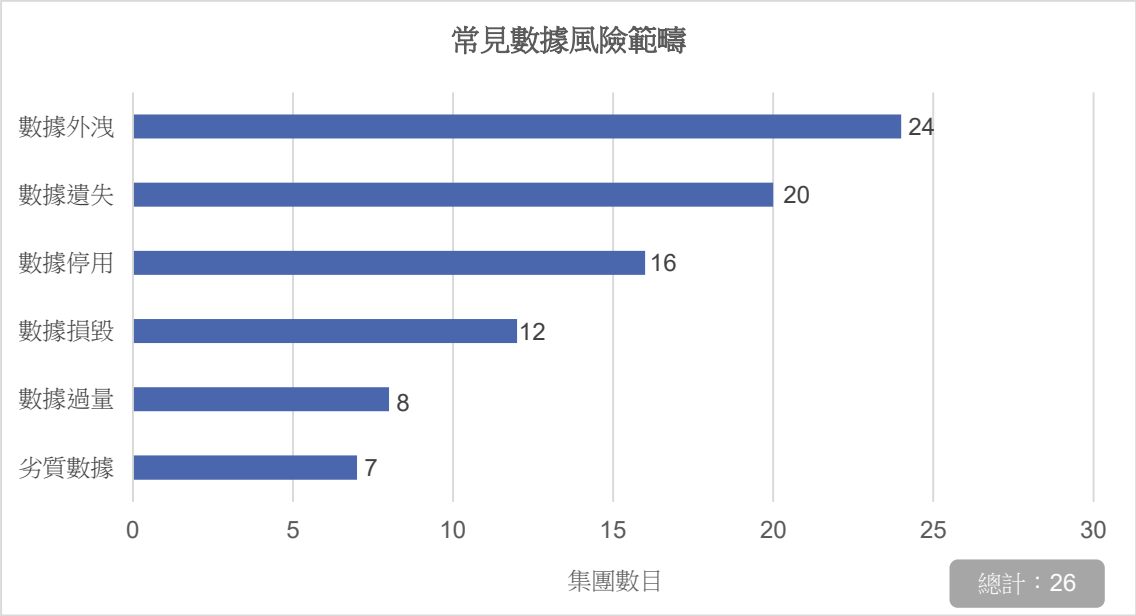
良好作業手法
▪ 某集團與海外集團聯屬公司訂立了應急財務安排，以在出現使該集團的流動資金減至不穩定水平的潛在重大損失時，允許其金融集團注資或將有關損失重新分配予其他集團聯屬公司。

D. 數據風險管理

背景

67. 一般來說，數據風險指因持牌法團對數據生命周期（包括數據收集、分類、使用、保留、轉移和處置）管理不善而導致運作受干擾和聲譽或財務受損的風險。

68. 在 48 家接受檢視的集團中，有 26 家表示曾經歷與數據風險有關的事故。該等集團所識別的三大數據風險範疇[17]分別是數據外洩[18]、數據遺失[19]和數據停用[20]；其他風險範疇則包括數據損毀[21]、數據過量[22]和劣質數據[23]。



69. 鑑於持牌法團在業務營運過程中會收集及使用愈來愈大量的數據，故數據風險備受高度關注。持牌法團必須對數據風險管理進行足夠的管理層監督，在數據生命周期的各個階段制定適當的監控和監察措施，並實施充分的保護措施，以防止數據外洩、遺失或被擅自取覽。

I. 數據風險管治

70. 持牌法團如要迅速應對因其業務作業手法和新技術出現而引致的數據風險，確保遵從適用的法律和規例（包括《個人資料（私隱）條例》（第 486 章）（《私隱條例》）），及有效地提高員工對數據風險的認知，健全的風險管治架構及獲清楚界定的風險管理角色及責任至關重要。

---

17 回答問卷時，該等集團可選擇一個或多個數據風險範疇（如相關）。
18 數據外洩屬保安漏洞，即機密或敏感數據在有關情況下被盜或未經數據擁有人授權而被處理。
19 數據遺失指有意或無意地銷毀數據。
20 數據停用指在某特定時間內暫時無法取覽數據。
21 數據損毀指令數據無法使用的損壞。
22 數據過量指不必要地收集和處理數據，因而可能引致私隱問題。
23 劣質數據指數據不完整、不準確或不一致。

應達到的標準
持牌法團應制定穩健的風險管治框架[24]，以便有效地管理數據風險和遵從適用的法律及監管規定[25]。該框架應涵蓋不同方面，其中包括下列範疇： (a) 清楚地界定高級管理層在監督數據風險管理方面的責任及問責性[26]；及 (b) 制定結構完善的規程，以便及時處理並向高級管理層和有關當局（如適當）匯報數據風險事故。

<u>市場作業手法</u>

(a) 高級管理層對數據風險管理的監督及責任

71. 大部分集團制定了數據風險管治框架，以便管理層進行監督及就與數據風險有關的事故進行上報。以書面訂立的框架主要述明負責監督數據風險管理和確保在數據生命周期內實施監控和監察措施的指定人員（例如負責風險管理職能的核心職能主管、負責資訊科技職能的核心職能主管）及委員會的角色和責任。

72. 大部分集團的高級管理層均了解提高員工對數據風險事宜的認知和遵從與數據風險有關的政策的重要性，方法是就如何處理敏感資料和匯報數據風險事故，提供入職培訓和定期培訓。

73. 有待改善之處

- 部分集團對數據風險沒有充分的了解，故無法清晰地劃分管理層責任。舉例來說，它們無法清楚說明監督數據風險及相關事故的責任應屬於負責風險管理職能的核心職能主管或負責資訊科技職能的核心職能主管，還是由該兩名主管共同承擔。

良好作業手法
▪ 部分集團指定成立一個由資訊保安或數據管理、合規、法律及運作風險職能的代表所組成的數據管治委員會。該委員會負責監督在數據風險管理框架及有關識別和處理數據風險事宜的監控措施方面的實施。該委員會獲提供有關重大數據相關事宜的管理層報告，並定期在會議上就此進行討論。

(b) 數據風險事故的處理

74. 大部分集團均指定重大數據風險事故在訂明時限內須匯報予特定人員或委員會，有些集團亦會成立特別工作小組，以加快有關識別該等事故的根本原因及在其發生後紓減風險承擔的流程。特別工作小組因應事故的性質和嚴重程度，可能會由不同持份者（例如各主要業務的主管及資訊科技、風險管理和合規職能）所組成。

---

24 《操守準則》第 9 項一般原則和第 14.1 段，以及《內部監控指引》第 I 部。

25 包括《私隱條例》。

26 證監會於 2016 年 12 月 16 日發出的《致持牌法團有關加強高級管理層問責性的措施的通函》。

75. 如出現數據遺失或洩露的情況，該等集團的負責各方一般會評估潛在的影響，釐定適當的措施來遏止相關風險，並負責作出任何所需的匯報，以履行遵守法律和監管規定的責任。

76. 有待改善之處

- 部分集團沒有訂明上報規程及時限。有些事故（例如數據遺失）沒有及時匯報予高級管理層，因而削弱了管理層監督的成效。

良好作業手法
▪ 有些集團採用了中央系統，以有系統的方式追踪它們就數據風險事故所採取對策的進度及實施補救措施。此舉可利便相關的獨立職能進行監察及向高級管理層匯報。 ▪ 某集團與其員工進行年度演習，模擬發生數據風險事故的情況，讓員工充分了解處理事故的方法和上報規程，及評估其流程的成效。

II. 有關數據生命周期的監控和監察措施

77. 適當的監控和監察措施[27]至關重要，讓持牌法團得以管理數據生命周期，及紓減因劣質數據、未經授權取覽數據或敏感數據洩露或遺失而引起的相關風險[28]。

(a) 數據收集

78. 持牌法團十分依賴高質素的數據來作出商業決定及進行業務運作。

應達到的標準
持牌法團應從可靠的來源收集數據，並採取適當步驟，以確保所收集數據的質素。

市場作業手法

79. 在收集數據作特定商業用途（例如符合認識你的客戶規定，進行市場調查及分析員工行為）時，該等集團一般會遵守《私隱條例》及其他適用的法律和規例。

80. 該等集團會從各種來源取得資料和數據。一般來說，它們在取覽任何客戶數據前，會事先取得客戶的同意，及向他們披露收集數據的目的。大部分集團均設法從經認可且可靠的來源（例如商業數據庫）取得市場數據等其他類別的數據。

81. 該等集團為確保數據質素而採用的一些常見方法包括評估數據來源的可靠性（例如對數據提供者進行盡職審查），及進行以風險為本的數據驗證（例如核實關鍵數據的準確性和完整性）。

---

27 《操守準則》第 3 項一般原則及第 4.3 段和《內部監控指引》第 IV 部。

28 就針對網絡保安風險的數據保護措施而言，從事互聯網交易的持牌法團亦應參考《降低及紓減與互聯網交易相關的黑客入侵風險指引》所載的指引，證監會在 2017 年 10 月 27 日發出的《致持牌法團的通函 —— 有關資訊科技風險管理及網絡保安的良好業界作業方式》所載的良好作業手法，及證監會在 2020 年 9 月 23 日發出的《2019-20 年互聯網經紀行網絡保安主題檢視報告》所載的額外指引。

(b) 數據分類

82. 根據以風險為本的方針，持牌法團通常會識別敏感數據及採取更嚴格的保障措施，以防止數據遺失或洩露。

應達到的標準
持牌法團應按照數據的敏感程度，將所處理的數據合理地分類，並實施相稱的保護措施。

<u>市場作業手法</u>

83. 該等集團已制定按照數據的敏感程度和相關風險將數據分類的流程。常見的數據類別包括“高度機密”、“機密”、“內部”及“公開”。

84. 數據分類旨在利便該等集團因應有關以風險為本的考慮因素而制定監控措施。一般來說，它們對機密數據採取了更嚴格的保障措施，例如數據加密、數據屏蔽[29]及實體和邏輯[30]接達監控措施。

85. 部分集團更進一步實施系統，以保護和保障在不同端點、網絡和通訊渠道（例如電子郵件和共用磁碟）的數據。它們在有關系統內訂立規則或準則，以偵測任何未經授權而轉移數據或通訊內容載有任何敏感資料的情況，並在適當情況下對數據傳輸（例如對外發出的電子郵件）採用軟封鎖或硬封鎖。當有關系統識別到警示情況時，指定團隊便會審查有關警示情況，並釐定是否發生了數據洩露及是否需向高級管理層上報。

(c) 數據使用

86. 持牌法團如要限制數據只可由獲持牌法團授權的適當人員及外聘人士使用，及偵測和防止未經授權取覽數據的情況，便須實施數據取覽監控措施。

應達到的標準
持牌法團應確保敏感數據只可由獲授權人士取覽、使用或更改。

<u>市場作業手法</u>

87. 為了避免數據遭未經授權使用，大部分集團依照機密類別，按需要向其員工授予數據取覽權，並實施數據取覽監控和監察機制，確保相關數據只可由獲授權人士取覽和使用。

88. 部分集團已備存各部門存入和取用機密資料的紀錄，當中包括對資料的描述、數據擁有人、數據接收人和機密程度，並由指定部門進行審查，以識別是否有任何不當處理機密數據的情況。

---

29 數據屏蔽是一項透過掩藏或修改原始數據來保護敏感數據的技術。

30 邏輯接達監控措施包括對接達系統的人員進行身分識別、認證和授權（例如使用密碼或生物特徵）。

89. 有待改善之處

- 某集團不但將所有未公布的研究材料（被歸類為“機密”數據）儲存在一個共用磁碟內，而且沒有限制有關材料只可由員工在有需要的情況下取覽。在沒有制定適當的數據取覽監控措施的情況下，研究材料所載的價格敏感資料容易在公布前遭洩露和不當使用。

(d) 數據保留

90. 為了同時符合監管期望和滿足業務需要，持牌法團需為各類數據釐定適當的保留期限和儲存媒體。

應達到的標準
持牌法團應訂立數據保留及後備政策，以確保在指定的期限內妥善保管及提供數據，藉此遵從有關備存紀錄的監管規定和滿足自身的業務需要。

<u>市場作業手法</u>

91. 一般來說，該等集團為不同種類的數據（例如個人身分資料及交易數據）設定最短的保留期限，以同時滿足業務需要和符合監管規定。

92. 大部分集團將機密數據（例如客戶、交易和僱員資料）保留在加密儲存媒體內。

93. 有些集團除了在香港，還在多個境外地點保留其數據，特別是在其集團公司的營運所在地，以符合集團層面的數據備份及業務抵禦能力規定。

94. 有待改善之處

- 部分集團沒有為某些種類的數據（例如從認識你的客戶程序或其他業務運作中取得的客戶個人資料）設定最短的保留期限，以致過早處置須根據《證券及期貨（備存紀錄）規則》備存的紀錄。

- 即使客戶的帳戶可能已被取消逾十年，而且已再無需要為了符合備存紀錄的監管規定而保留其個人資料紀錄，但有些集團永久保留了該等客戶的紀錄。這做法可能有違《私隱條例》的規定[31]，當中訂明資料使用者須採取所有切實可行的步驟，以刪除不再需要的個人資料。

- 某些集團沒有制定充足的保障措施以妥善保留機密文件。由於有關員工未有妥善存置若干客戶或內部紀錄，或備份過程失敗，以致遺失不少相關紀錄，因而違反了《證券及期貨（備存紀錄）規則》的規定。

[31] 保障資料的第 2 原則 —— 個人資料的準確性及保留期間。

(e) 數據轉移及處置

95. 持牌法團在轉移[32]及處置數據時需保持警覺，以應對當中涉及的較高數據遺失及洩露風險。

應達到的標準
持牌法團應實施充足的保障措施，以防止數據在傳輸時洩露至非擬定人士，及被棄置的數據遭惡意取覽或修復。

<u>市場作業手法</u>

96. 大部分集團表示，它們會在公司內部及與位於香港境內外的第三方服務提供者和集團聯屬公司轉移數據。數據可透過電子郵件、外置便攜式儲存裝置、共用磁碟或系統界面傳輸。加密技術是確保數據轉移過程安全的最常用方法。

97. 一些集團禁止在其電腦系統上安裝未經授權的軟件和硬件（例如 USB 裝置和外置硬碟），而部分集團亦採用防止數據遺失軟件，以紓減因內部或外部因素而導致數據洩露或遺失的風險。

98. 在處置敏感數據時，該等集團通常會將紙本形式的數據或資料輾碎，使人無法再讀取內容。媒體銷毀和消磁是清除電子數據的常用方法。

99. 某些集團規定須由指定職能（例如合規）或第三方服務提供者監察敏感數據的處置過程。

100. 部分集團參考了各類數據的內部紀錄保留期限表，以釐定應何時處置數據。該等集團會指派人員進行定期審查，以評估有關期限表是否獲及時更新，以及數據是否已按照期限表妥為處置。

101. 有待改善之處

- 某些集團的僱員在離職前，將載有高度機密數據（例如客戶或專利資料）的電子郵件發送至他們的個人電郵帳戶，但該等集團並沒有制定充足的監控措施，以有效和及時地偵測或防止此類數據洩露。

(f) 聘用第三方服務提供者

102. 如持牌法團在數據生命周期中委聘第三方服務提供者[33]進行某些活動，而該服務提供者可取覽其專利和敏感數據，持牌法團便較容易受到多項風險和隱憂所影響。

---

[32] 持牌法團亦應參閱證監會於 2022 年 3 月 24 日發出的《致持牌法團的通函 —— 管理商業電郵騙案的風險》，以實施適當的監控措施，避免洩露客戶資料。

[33] 持牌法團如使用外間電子數據儲存提供者，以根據《證券及期貨條例》（第 571 章）或《打擊洗錢及恐怖分子資金籌集條例》（第 615 章）的規定備存紀錄，亦應同時遵循證監會在 2019 年 10 月 31 日發出的《致持牌法團的通函 —— 外間電子數據儲存的使用》所載的適用規定和應達到的監管標準。

應達到的標準
凡在數據生命周期中委聘服務提供者，持牌法團應執行妥善的盡職審查及持續監察，以確保服務提供者有能力保護數據和遵從適用的法律及監管規定。

市場作業手法

103. 部分集團表示，它們在數據生命周期中委聘了第三方服務提供者進行某些活動。該等集團對服務提供者的監控情況進行了盡職審查及持續監察，以確保它們實施充足的數據保障措施。

104. 數據轉移一般受到該等集團與其第三方服務提供者之間的服務水平協議所約束，特別是在處理機密資料及於服務終止時處置數據方面。服務水平協議訂明了相關各方的責任、數據的擁有權和合規要求。

105. 有待改善之處

- 某集團委聘了第三方服務提供者，以將機密客戶數據移至新硬件，但卻沒有對該服務提供者的能力執行盡職審查或對其服務表現進行持續監察，以致該集團可能面臨較高的數據洩露風險。

良好作業手法
▪ 在終止服務時，某集團透過以下措施，指示服務提供者處置相關數據：(i)指派該集團的適當人員來見證和核實數據處置的過程；及(ii)要求該服務提供者確認相關數據已獲妥善處置。