



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

## 有關運作上的抵禦能力及遙距工作安排的報告

---

2021年10月

# 目錄

---

引言	3
運作上的抵禦能力	
標準 1：管治	5
標準 2：運作風險管理	6
標準 3：資訊與通訊科技，包括網絡保安	8
標準 4：依賴第三方的風險管理	10
標準 5：業務延續計劃及事故管理	11
遙距工作	
管治	13
在辦事處以外地方進行交易	15
外判及第三方安排	17
資訊保安	18
網絡保安	19
備存紀錄	19
通知的責任	20
在家工作安排	20

## 引言

1. 在 2019 冠狀病毒病（即 COVID-19，簡稱冠狀病毒）疫情爆發期間，證券及期貨事務監察委員會（證監會）與持牌法團曾經就以下事項進行廣泛的監督性討論：
  - 分隔工作安排，藉以在辦事處和營業地點不能使用或出現其他疫情相關干擾的情況下，維持關鍵業務及服務的正常業務運作；
  - 在家工作的安排及操守規定的遵守情況；及
  - 運作上的抵禦能力，藉以應付市場扭曲及冠狀病毒疫情的干擾。
2. 我們注意到，持牌法團展示了高水平的抵禦能力，而這有助它們在疫情期間維持正常業務運作，而遙距工作（尤其是在家工作）是許多持牌法團的業務延續策略的一部分。
3. 我們亦觀察到，證監會的守則、指引和通函<sup>1</sup>中有關網絡保安、業務延續計劃、內部監控及風險管理的相關指導，有助持牌法團維持抵禦能力。
4. 為了確保抵禦能力得以維持，中介人必須按照通用的既定標準採取全面的方針，以達致其運作上的抵禦能力目標（在本文意中，這是指中介人防止、適應和應對業務干擾以及從業務干擾中復原和汲取教訓的能力）。
5. 此外，鑑於遙距工作（尤其是在家工作）在疫情受控後相當可能持續普及，故中介人應該對與遙距工作相關的風險保持警覺，並實施適當的風險管理措施和內部監控以應對這些風險。
6. 為此，除了就本會的監督性觀察所得作出論述外，本報告還：
  - (a) 制訂運作上的抵禦能力標準及所需執行的措施，以補充證監會現行的指引。同時，亦會提供建議的措施和程序，以及本會從檢視某些持牌法團在冠狀病毒疫情及其他干擾事件期間，為了運作上的抵禦能力而採納的計劃及措施中所觀察到的案例和所汲取的教訓；及
  - (b) 就管理遙距工作可能涉及的主要風險方面列出應達到的監管標準，同時亦提供建議的措施和程序，藉以協助中介人遵守這些標準。
7. 雖然也許有其他方法可達致運作上的抵禦能力目標及紓減遙距工作的風險，惟本會鼓勵中介人在任何就其而言屬適當的情況下採納這些建議的措施和程序。

---

<sup>1</sup> 例如，《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》）；《基金經理操守準則》，《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》），在 2017 年 5 月 15 日發出的《致所有持牌法團的通函——勒索軟件威脅警報》，在 2018 年 5 月 4 日發出的《致中介人的通函——透過即時通訊收取客戶交易指示》，及在 2020 年 4 月 29 日發出的《致持牌法團的通函——與遙距工作安排相關的網絡保安風險管理》。



註冊機構應遵守所有適用規定，同時亦應參照香港金融管理局（金管局）不時發出的其他指引。

## 運作上的抵禦能力

1. 中介人所面對的干擾事件形形色色，而且都可能影響其運作，這些事件由單一台電腦出現故障（影響個別員工提供服務的能力），到網絡保安事故或疫情（可導致中介人的活動出現大規模中斷）不等。
2. 某些干擾是無可避免的。因此，中介人應設立適當的框架，以識別、應對及適應干擾事故並就其作好準備。
3. 本章載列了一套運作上的抵禦能力標準及達到這些標準所需執行的措施。
4. 為協助中介人遵守這些運作上的抵禦能力標準及所需執行的措施，我們亦提供了一些建議的措施和程序，以及本會監督性觀察所得的案例和從中汲取的教訓。
5. 中介人應考慮，就其本身的情況而言，本會所建議的措施和程序以及做法是否適用。無論如何，中介人應採納與其業務規模和複雜程度相稱的所有必要政策、程序及監控措施，並且透過這些政策、程序及監控措施有效地遵守運作上的抵禦能力標準及所需執行的措施。

### 運作上的抵禦能力標準 1：管治

#### 運作上的抵禦能力標準 1

中介人應設立有效的管治框架，以訂立其運作上的抵禦能力目標，制訂、實施和監察一些安排及措施以持續識別可能對其業務健全、具效率和有效的運作造成影響的干擾事故<sup>2</sup>，並應對和適應干擾事故。

#### 所需執行的措施

中介人的高級管理層應對訂立運作上的抵禦能力目標，及制訂和執行必要的安排及措施承擔全部責任<sup>3</sup>。

指定員工應監察中介人業務單位在運作上的持續抵禦能力，以支援高級管理層的監督工作。

高級管理層應獲提供充分的資料，讓他們可持續地和及時地評估可能影響中介人在運作上的抵禦能力的事宜<sup>4</sup>，並考慮和批准對中介人對於運作上的抵禦能力方面的工作，進行任何必要的調整。

<sup>2</sup> 《內部監控指引》第 I 部。

<sup>3</sup> 《內部監控指引》第 I(1)段。

<sup>4</sup> 《內部監控指引》第 I(2)段。

## 建議的措施和程序

6. 設立高層管理層監督安排的目的如下：
- (a) 識別可能影響中介人繼續進行業務活動或提供服務的能力，且與內部流程、人員、系統、外來威脅及第三方有關的干擾情境；
  - (b) 由高級管理層檢視及批准中介人對其業務運作受干擾的風險承受能力，當中顧及中介人的風險概況，及就支持在運作上的抵禦能力而言，在不同的運作環境的能力，包括系統、流程、人員、資訊科技基建及風險管理；及
  - (c) 制訂及實施就維持業務活動及服務而言，有效和具抵禦能力且與中介人對受干擾的風險承受能力相符的系統及監控措施。

## 案例

7. 某些公司指派高級管理層、負責人員或部門主管來負責識別和檢視關鍵職能及系統，並每年或當服務、系統或員工有所改變時更新書面業務應變計劃。這些公司亦確保其業務應變計劃適當地涵蓋潛在的干擾事件及相應的應對措施，以及優先考慮關鍵職能及系統（例如與交易及交收有關者）。
8. 一家公司的高級管理層定期檢視有關適應干擾事故的執行措施，以確保該等措施可讓該公司能夠以具效率和效益的方式經營其業務。舉例來說，在冠狀病毒疫情開始時，該公司採取分隔地點運作的安排，使員工在該公司的辦事處、運作復原中心及家居辦公室之間進行實體分隔。員工須在其指定工作地點工作數星期，然後輪換，藉以盡量減低任何該等工作地點中的冠狀病毒感染確診個案的潛在影響。經檢視後，該公司發現分隔地點運作的安排為員工之間的有效溝通造成障礙，於是便迅速地縮短輪換周期。此舉讓管理人員在管理工作量方面具有更大的靈活性，亦促進了更有效的溝通及配合員工的個人需要。
9. 一家公司在疫情期間遭受資源限制，不能如期進行某些審計檢查工作。為此，該公司設立了評估委員會，以識別其業務運作中的主要風險範疇，及為這些範疇的檢查工作排列優先次序，當中包括運作上的抵禦能力及在家工作（包括在辦事處以外地方進行交易）。被列為優先處理的檢查工作因利用了公司第一及第二道防線的可用資源而得以進行，並就該公司在冠狀病毒疫情干擾期間以具效率及效益的方式進行業務的能力，向管理層給予保證。此外，董事會對審計檢查工作延期的申請作出了評估及批准，以確保這些延期具有充分理據，及因延遲進行任何檢查工作而產生的相應風險獲得妥善處理。

## 運作上的抵禦能力標準 2：運作風險管理

### 運作上的抵禦能力標準 2

中介人應訂立有效的運作風險管理框架，以評估干擾對運作（包括人員、流程和系統）及合規事宜的潛在影響，及按照其運作上的抵禦能力目標來管理所產生的風險。

### 所需執行的措施

中介人應制定並維持有效的政策及程序，以確保該中介人所承受的運作風險獲得適當的管理<sup>5</sup>。中介人亦應每隔適當時候進行全面的檢討，以確保該因運作干擾而造成損失的風險維持在可接受的及適當的水平<sup>6</sup>。

### 建議的措施和程序

10. 運作風險管理框架可包含以下各項：

- (a) 可能出現的干擾所帶來的運作和監管風險類別，及監察和紓減這些風險的方針；
- (b) 高級管理層及其他指定員工在制訂和實施風險管理政策及程序方面的角色和責任；及
- (c) 用以確保中介人在運作上的抵禦能力不會受到流程不當、系統不足或任何員工缺勤或離職影響的安排及措施<sup>7</sup>。這些安排及措施包括：
  - 定期檢視各項流程和系統，及評估其在容易受干擾方面的隱憂；
  - 定期檢視當前是否有任何職能由單一名員工或一小組員工執行，及評估該等員工的突然缺勤對該中介人業務運作的不利影響；及
  - 實施適當的措施，以避免、紓減及管理這些隱憂及其影響。舉例來說：
    - 設立後備系統；
    - 安排多名員工在同一團隊內及不同地點工作；或
    - 安排集團公司或第三方提供支援。

### 案例

11. 某些公司設有以下安排，以確保能夠在運作失效或系統無法使用的情況下繼續提供服務：
- 與一家或多家經紀行訂立安排，讓它們可在無法接達本身的交易系統時，仍然能夠將交易指示傳送給交易所；及
  - 設有多個後備數據中心，以盡量減低主要數據中心故障對交易系統造成的影響。
12. 為應付辦事處無法使用的情況，多家公司讓員工可遙距接達（通常是透過流動裝置或公司提供的手提電腦）至其內部系統或交易平台，以便員工可在辦事處以外地方繼續執行其職務。

<sup>5</sup> 《內部監控指引》第 VIII 部。

<sup>6</sup> 《內部監控指引》第 VIII(4)段。

<sup>7</sup> 《操守準則》第 3 項一般原則及《內部監控指引》附錄第 35(d)段。

13. 一家公司實施分隔工作安排後，其中一名員工感染冠狀病毒。由於同組內有部分員工在辦事處工作，而其他員工則在家工作，故並非全組員工同被歸類為該感染員工的密切接觸者及須被強制隔離。因此，該公司能夠繼續向客戶提供服務。

#### 汲取的教訓

14. 一家公司沒有在疫情開始時就其負責交易的員工實施分隔工作安排，而其交易員工全部都在同一個香港辦事處工作。當一名交易員工確診感染冠狀病毒時，由於多名交易員工被強制隔離，導致該公司須暫停其關鍵交易職能。自此，該公司在香港設立了一個後備辦事處，以便安排屬同一交易團隊的員工輪流在不同地點工作。

#### 運作上的抵禦能力標準 3：資訊與通訊科技，包括網絡保安

##### 運作上的抵禦能力標準 3

中介人應確保其資訊與通訊科技系統具抵禦能力，以便在出現干擾事故時維持健全、具效率和有效的業務運作，並應確保這些系統都是在保密及有充分監控的環境下運作<sup>8</sup>。

##### 所需執行的措施

為了確保其資訊與通訊科技系統的運作保密，中介人應制訂各項政策和程序，以保護由其所管有的機密數據和資料，並且持續地管理網絡保安風險。

#### 建議的措施和程序

15. 中介人採取各項步驟，藉以：
- (a) 定期評估就確保在運作方面的抵禦能力而言所需的資訊科技基礎設施、軟件和硬件是否充足及安全。舉例來說，以離線方式將關鍵數據備份及儲存，及進行故障轉換和恢復測試；
  - (b) 防止及偵察出任何錯誤、遺漏或有人未經授權而擅自對中介人的系統及數據進行加插、更改、刪除或侵入等活動；及
  - (c) 識別網絡保安風險，並實施網絡事故管理計劃，從而迅速地應對網絡事故作出。

#### 案例

16. 某些公司採納以下做法，以確保員工可在遙距工作時適當地記錄客戶交易指示的詳情：
- 安裝網絡語音電話系統（IP phone system），讓遙距工作的員工收到或打出的電話通話可被錄音；

<sup>8</sup> 《內部監控指引》第 IV(2)段。



- 要求前線員工只使用公司編配的錄音電話線來為客戶進行交易；及
  - 要求負責交易的員工在通常經營業務的地點以外的地方收到交易指示時，須致電其公司的電話錄音系統以記錄有關交易指示，或以書面方式記錄交易指示的詳情。
17. 多家公司容許員工遙距接達其系統和客戶數據。為了保護這些系統和數據，有些公司：
- 要求多重認證，並就遙距接達公司平台使用 指定用戶名稱和密碼；
  - 規定有關遙距接達權限的申請須由直屬主管批准，並須在其半年一度的授權檢討進行時重新認證；及
  - 監察遙距接達的使用情況，以及移除在任何 30 日內並無使用遙距接達功能的員工的遙距接達權限。
18. 為了偵察及防止機密資料外洩：
- 某公司對經其電腦及流動裝置進行的虛擬會議或電話會議進行抽樣檢查，以確保敏感和機密資料均獲妥善處理，並確保在進行業務活動時已遵循適當流程。
  - 某公司對寄存在其平台上和電郵內的數據應用強效的加密程式。此外，該公司採納了防禦性監控措施，例如阻止非常任員工寄出電郵及歸類為機密的文件被傳送。
  - 某公司已設有政策，確保企業和個人資料及應用程式妥為分隔，以免有關資料從一個環境被轉移至另一個環境。
  - 某公司發出指引，說明其清理辦公桌政策（**clean desk policy**）及有關處理敏感和機密資料的政策，在員工須遙距工作（包括在家工作）的情況下皆適用。為了防止數據及資料外洩，該公司亦建議當交易員工在家工作或在辦事處以外地點工作時，應在另一些並非與其他人共用的房間內執行其職務。
19. 多家公司已積極採取措施，以保護其系統免受網絡攻擊。舉例來說：
- 某公司裝置了軟件，每當有僱員以遙距方式接達其網絡時便會進行系統和防毒檢查。
  - 有些公司向員工發出額外的指引，提醒他們注意網絡威脅及其他與遙距工作相關的技術風險。
  - 某公司密切監察疫情對於全球技術和網絡風險的環境的影響，並實施相應的監控措施應付不斷演變的風險，當中包括僱員短缺造成較大的仿冒詐騙攻擊漏洞，對遙距工作的資訊科技基建的依賴程度上升，以及要求在例外情況下不受限制以便可在家打印及使用 **USB** 裝置來儲存和轉移資料的個案增加。

### 汲取的教訓

20. 某公司為利便在家工作安排而進行系統遷移，但過程中沒有妥善地設置電話錄音的設定值。結果，有些關乎接收交易指示的客戶來電沒有被錄音。

21. 某公司匯報曾出現一次勒索軟件攻擊。首先是後端伺服器中毒，由於防火牆系統無法隔離該受損伺服器以防止進一步受惡意程式感染，故其他伺服器（包括交易平台）其後亦受到影響。業務應變計劃被啟動後，該公司暫停了其在互聯網及流動交易平台上的證券買賣活動，客戶款項提取服務及其部分期貨交易服務。由於該公司已無法取得儲存在後端伺服器內的客戶聯絡名單，因此未能通知客戶上述服務已經暫停。該公司未能對有關事故作出有效應對的根本原因，包括其未能偵察及防止有人未經授權而擅自接達系統，並迅速地隔離受損的伺服器。為了恢復其服務及糾正系統缺失，該公司裝置了新的設備及重建伺服器，加強其網絡保安，以確保能夠迅速且有效率地就惡意軟件感染作出應對，並加強其備份安排，以在離線媒體中備存數據磁帶。

#### 運作上的抵禦能力標準 4：依賴第三方的風險管理

##### 運作上的抵禦能力標準 4

中介人應識別其為維持其業務健全、具效率和有效的運作而須依賴的主要第三方（包括集團內的實體），評核第三方服務供應商的抵禦能力，以及按照其在運作上的抵禦能力目標，管理依賴第三方所產生的風險。

##### 所需執行的措施

中介人應採取適當步驟去識別、規限及管理依賴第三方的風險<sup>9</sup>。中介人亦應每隔適當時候及每當更換主要服務供應商時進行檢討，以確保中介人因依賴第三方而蒙受損失（不論是財務或其他損失）的風險，得以維持在可接受及適當的水平<sup>10</sup>。

#### 建議的措施和程序

22. 中介人採取各項步驟，藉以：

- (a) 評估若主要服務供應商無法提供服務，將會怎樣影響中介人的業務運作；
- (b) 定期檢討各系統和監控措施的報告，以及有關服務供應商的測試結果或其他同等評估，並制定流程和基準，以監察服務供應商在出現干擾時提供服務的能力；及
- (c) 實施適當的安排及措施，以避免、紓減及管理服務供應商無法提供服務的影響。舉例來說：
  - 在與各服務供應商所訂立的協議內，清楚列明在出現任何干擾的情況時的安排；
  - 了解服務供應商的業務延續計劃，包括進行測試及檢討的頻密程度；及

<sup>9</sup> 《內部監控指引》第 VIII 章。尤其是，公司須建立並維持有效的政策及程序，以確保中介人所承受的風險獲得適當的管理。

<sup>10</sup> 《內部監控指引》第 VIII(4)段。

- 指派後備服務供應商，一旦公司委聘的服務供應商未能繼續提供服務時，後備服務供應商便可給予協助。

## 案例

23. 有些中介人在對第三方服務供應商進行盡職審查時，特別注意它們的業務延續計劃或安排，以確保它們能夠處理運作上的干擾。特別是，某公司與多家主要供應商合作，設計適用於在不同干擾情境下可能出現的各種緊急情況的抵禦干擾計劃，並與關鍵供應商制定測試計劃以評估它們的恢復能力。
24. 為紓減供應商的集中風險，多家經紀行已就其主要及後備數據中心委聘不同的互聯網服務供應商。

## 運作上的抵禦能力標準 5：業務延續計劃及事故管理

### 運作上的抵禦能力標準 5

中介人應設有有效的業務延續計劃，以應對及適應干擾事故並從干擾事故中恢復過來<sup>11</sup>，以及應至少每年檢討有關計劃，以評估是否有需要因應中介人在運作、架構或業務方面的任何重大改變而作出修訂。它們亦應採納有效的事故管理流程，以識別、評估及糾正干擾事故並從中汲取教訓，以及避免干擾事故重現或紓減其嚴重性。

### 所需執行的措施

中介人應訂立及維持業務延續計劃，而該計劃應：

- (a) 應對所識別到的不同干擾情境，並載列啟動有關計劃的相應程序；及
- (b) 至少每年及在有需要時進行檢討，並因應中介人在運作、架構或業務方面的改變而作出修訂。檢討結果應妥為記錄在案。

中介人應制訂一套當出現干擾事故時會被啟動的事故管理流程，以處理以下事項：

- (a) 制訂適用的匯報及上報程序；
- (b) 釐定應對有關事故的合適行動；
- (c) 透過分析有關事故來識別根本原因；
- (d) 避免類似事故的出現，及日後若發生類似事故時紓減其嚴重性的需要；及
- (e) 實施通訊計劃，藉以向內部和外部持份者匯報事故，包括向監管機構匯報影響其客戶利益及其繼續進行正常業務運作的能力的重大事故。

<sup>11</sup> 《內部監控指引》附錄第 36 段。

## 案例

25. 有些公司的業務應變計劃涵蓋的情境範圍廣泛，包括交易及非交易系統受到干擾，辦事處無法使用，疫症大流行，網絡故障，電力供應暫停，高級管理層員工流失及喪失建築物。該等計劃亦清楚指明啟動有關計劃需取得的批准，以及就啟動有關計劃通知客戶的方法。
26. 大多數公司定期檢討其業務應變計劃。在冠狀病毒疫情期間，有些公司迅速地檢討其計劃，以顧及因疫情爆發而可能導致的運作干擾。
27. 多家公司對其業務應變計劃進行定期測試，以確保有關計劃在發生干擾事件時能夠妥善地實施。舉例來說：
  - 某公司對遷移至後備辦事處的過程進行測試，以確保員工知道如何到達該處；電腦及打印機的設定正確；以及該辦事處有足夠的工作空間和設施，及其恢復計劃（例如數據的供應情況及系統表現）是有效的。
  - 某公司定期透過互聯網對其多個系統（包括網上交易、莊家活動、結算、財務、會計及電郵）的遙距接達進行測試，以確保有關系統妥善運作。
28. 某公司有一些員工被歸類為受冠狀病毒病感染的人士的密切接觸者，並入住檢疫中心。該公司已即時將流動數據電話智能卡及文具等所需設備送往檢疫中心，讓有關員工能以遙距方式接達該公司的系統，及在有需要時執行主要功能。

## 汲取的教訓

29. 有些公司的業務延續計劃並沒涵蓋可能因其辦事處無法使用而造成的干擾。因此，當其辦事處無法使用時，某些服務亦未能向客戶提供。

## 遙距工作

1. 遙距工作是指員工在中介人辦事處以外的地點執行工作的情况，包括安排員工在他們的“家居辦公室”內工作（即在家工作）。一般來說，遙距工作會帶來風險，原因是為傳統的辦公室工作環境而設的監控和監察措施對遙距工作環境來說未必有效。另外，在家工作亦存在一些獨有的額外風險。
2. 本章所闡述與遙距工作（包括在家工作）相關而可能涉及的主要風險並非詳盡無遺。中介人應評估它們各自的遙距工作安排的風險概況，並確保所有風險都能妥為識別及加以處理。
3. 本章闡述有關管理及紓減該等主要風險應達到的監管標準。本章亦提供了一些建議的措施和程序，儘管中介人可能會因應它們不同的風險概況而採納不同的措施和程序，從而符合上述應達到的監管標準。然而，中介人應設有與其規模和內部架構相稱的妥善管治和監察機制，以確保所採納的措施和程序的成效。

## 管治

### 資源和處理能力

4. 由在辦事處工作轉至遙距工作可能會引起資源（包括人員、硬件、軟件、系統處理能力及連接能力）不足或資源規劃不當的風險，而這些風險會對中介人業務健全、具效率和有效的運作造成不利影響。例如，員工可能未獲提供所需設備，以便有效率地在一個遙距地點履行工作，或可能因互聯網連接速度緩慢而未能以遙距方式接達中介人的系統。
5. 具時間敏感性的交易活動（例如中介人須適時提供報價的上市產品莊家活動）需要高速和低延遲的交易基建。如所使用的網絡設備和軟件差劣及該遙距地點可用的頻寬不足，中介人未能提供報價和無法符合交易所的規定的風險便會上升。
6. 另一個例子是，當辦事處因分隔工作安排而沒有足夠員工收取、檢查和處理實物股票和支票的提存時，提供予某些客戶的交易結算服務便會受到干擾。

### 應達到的監管標準

中介人在安排員工轉為遙距工作前，應確保具備足夠資源，以便在遙距地點妥善地執行工作<sup>12</sup>。

中介人應制定並維持有效的政策、運作程序和監控措施<sup>13</sup>，以切合不同業務部門和運作職能的員工在遙距地點工作時的需要。中介人亦應就被視為高風險或不適合在遙距地點工作執行的業務或運作職能，確保在辦事處內有適當的最低員工數目。有關政策、程序及監控措施應定期及在有需要時進行檢討和作出更新。

<sup>12</sup> 根據《操守準則》第 3 項一般原則，持牌人或註冊人應具備及有效地運用其所需的資源和程序，以便適當地進行其業務活動。

<sup>13</sup> 根據《內部監控指引》第 VII 章，中介人須制定及維持關於其日常業務運作的有效政策、運作程序和監控措施，並確保有關的政策、程序及監控措施獲得遵守。

### 應達到的監管標準

此外，中介人應確保，為支援具效率的遙距工作而提供的資訊科技基建、系統、軟件、硬件、網絡處理能力及連接能力是適當及充足的<sup>14</sup>。

### 建議的措施和程序

7. 中介人採取各項步驟，藉以：
  - (a) 清楚界定可於遙距地點執行的職能，以及可遙距工作而不會阻礙中介人業務健全、具效率和有效地運作的員工的百分比；及
  - (b) 定期檢視中介人的資源和處理能力，從而確保有關資源和處理能力一直維持在充足且合適的水平以支援遙距工作，並在有需要時更新相關政策、運作程序及監控措施。

### 監督或監控流程

8. 合規審查暫停或延遲的情況可能因遙距工作安排而增加，令公司延誤識別出合規方面的問題。
9. 在辦事處以外地方進行交易活動的交易員在欠缺交易團隊主管及負責合規監察的員工親自對其行為作出監督和監控的情況下，不合規行為可能會增加，因而導致出現市場失當行為的風險上升。
10. 某些監控措施失效可能是由於無法以遙距方式取覽所有就進行完整的合規審查而言必需的文件所致。舉例而言，遙距工作的合規員工可能無法及時取覽只有紙本形式並儲存於辦事處的客戶開戶文件，故無法遵守合適性規定或進行打擊洗錢的合規審查。中介人可以將其工序數碼化及淘汰紙本文件，藉以避免發生上述監控措施失效的情況。
11. 其他會阻礙在遙距工作環境進行有效的合規審查或監督的因素可能包括欠缺面對面的互動，這可能對審查質素造成不利影響，因為不能評估有關員工的身體語言。此外管理人員與新入職或經驗較少的合規員工之間因欠缺實體互動，令前者對後者的指導或監督的效益降低。

<sup>14</sup> 《操守準則》第3項一般原則。

### 應達到的監管標準

中介人應制定並維持有效的監督及監控流程，以確保員工即使在遙距工作的環境中，依然符合適用的法律和監管規定以及中介人本身的內部政策和程序<sup>15</sup>，方法包括向員工提供適當培訓<sup>16</sup>，讓他們能以遙距方式履行其監督或監控職能。他們亦應具備在遙距工作環境中執行其職務所需的技能和資源，包括取覽全部所需紀錄和文件<sup>17</sup>。

在轉至遙距工作安排前，中介人應就任何暫時不適用於遙距工作的員工的監控措施，設有充分的替代性監控措施。

中介人應確保員工在遙距工作的環境中執行合規職能時，制定、維持及執行有效的合規程序<sup>18</sup>，包括有關交易、電子通訊及電話的適當監察系統，以偵測不符合法律及監管規定或中介人本身的政策和程序的情況。最易被利用來進行舞弊及欺詐活動的業務或運作職能，應受到密切監察。

### 建議的措施和程序

12. 中介人採取各項步驟，藉以確保：

- (a) 中介人具備所需的物流及技術支援，以實施有效的監督及監控流程。舉例來說，公司實施或加快將它們的工序數碼化及淘汰紙本文件；及
- (b) 按需要配置額外的人力及技術資源，包括外部顧問。

### 在辦事處以外地方進行交易<sup>19</sup>

13. 若遙距工作的員工獲允許在辦事處以外地方進行交易，中介人承擔的監控風險便會增加。除了如上文第 9 段所述欠缺交易團隊主管和負責合規監察的員工親身作出監督和監控外，其他限制（例如有關交易匯報、交易監察及可疑交易監察的系統支援較少）亦可能導致交易員工的不合規行為增加。

14. 與在辦事處以外地方進行交易活動相關的風險及不合規行為可能包括：

- (a) 遙距工作的員工經電話接收的交易指示，並沒有以在辦事處所使用的電話錄音系統記錄下來。結果，交易指示和接收該交易指示的時間的稽核紀錄可能不足以支持有效的交易監察或解決交易糾紛；
- (b) 遙距工作的員工由於無法遙距接達中介人的交易系統，故須將交易指示傳送給其他在辦事處的員工才能執行有關指示，導致在執行交易指示時有所延誤；及
- (c) 遙距工作的員工未能取覽只有在辦事處才能取覽的所需資料，故無法：

<sup>15</sup> 《內部監控指引》第 V 章。

<sup>16</sup> 《內部監控指引》第 III(3)章。

<sup>17</sup> 《內部監控指引》第 V(2)及 V(3)章。

<sup>18</sup> 《內部監控指引》第 V(4)章。

<sup>19</sup> 指員工在中介人辦事處以外的地點進行交易活動的情況。

- 評核市場狀況並釐定為客戶取得最佳條件的最佳執行策略；及
  - 在訂立關於投資產品的背對背交易之前或之時，釐定將向客戶披露的銷售利潤。
15. 在辦事處以外地方進行交易活動的員工任何蓄意或罔顧後果地使用不受監察或非加密的通訊應用程式來分享機密交易資料的行為，都可能不被發現，因而增加不當交易行為及市場失當行為的風險。

#### 應達到的監管標準

中介人在允許員工於辦事處以外地方進行任何交易活動前<sup>20</sup>，應制定並維持有效的政策及程序以及監察機制系統和監控措施，以確保該等活動持正操作並符合所有監管規定<sup>21</sup>。

若員工獲允許於辦事處以外地方就以代理人身分接收的交易指示或公司內部發出的交易指示（例如公司本身的帳戶及職員帳戶）進行交易活動，有關的政策及程序便應確保遙距工作的員工利用錄音電話線接聽以代理人身分接收的交易指示。如中介人尚未於遙距工作地點配置電話錄音系統，相關員工便應即時回電給中介人於辦事處的電話錄音系統，以記錄他們接收來電的時間和該交易指示的詳情<sup>22</sup>。若中介人已採納遙距工作安排並使其成為負責交易的員工的新常態，它便應為那些接收客戶電話交易指示的員工，配備適當的資訊及通訊科技設備，包括電話錄音系統。

若員工獲允許就客戶交易指示在辦事處以外地方進行交易活動，有關政策及程序亦應確保：

- 設有適當的措施以符合載列於在 2018 年 5 月 4 日發出的《致中介人的通函——透過即時通訊收取客戶交易指示》的規定；及
- 員工可接達所需的交易及所有其他系統，讓他們得以管理整體的交易執行流程，並釐定執行策略和參數，以便盡快按最佳條件執行客戶的交易指示<sup>23</sup>。

若員工獲允許在辦事處以外地方進行交易活動，以便替公司本身的帳戶與客戶訂立關於投資產品的背對背交易，有關的政策、程序及監控措施便應確保員工在訂立這些背對背交易之前或之時，能夠接達全部所需的系統，讓他們得以及時取覽所需資料，以便釐定將向客戶披露將賺取的銷售利潤<sup>24</sup>。

獨立的合規或審計職能應與高級管理層、業務運作、風險管理及其他相關監控職能緊密合作<sup>25</sup>，就在辦事處以外地方進行的交易活動積極地執行合規監察的工作。遙距工作的員工遵循各項有關在辦事處以外地方進行交易的合規政策、程序及監控措施的情況，應受到嚴格的檢討流程所規管。

<sup>20</sup> 註冊機構在實施在辦事處以外地方進行交易作為一般做法之前，應與金管局進行討論。

<sup>21</sup> 《內部監控指引》第 VII 章。

<sup>22</sup> 《操守準則》第 3.9 段、《內部監控指引》第 VII(6)段及在 2020 年 3 月 31 日發表的《致中介機構的通函——有關在新冠疫情下順延監管要求的實施期限及提醒業界注意記錄交易指示規定》。

<sup>23</sup> 《操守準則》第 3.1 及 3.2 段。

<sup>24</sup> 《操守準則》第 8.3 段 A(a)(ii) 段段。

<sup>25</sup> 《內部監控指引》第 V 及 VI 章。



## 建議的措施和程序

16. 中介人實施涵蓋以下範疇的監察機制：

- (a) 更頻密地對在辦事處以外地方進行的交易活動進行檢視，並實施經加強的監督性措施，例如由指定的管理人員進行批核，以及借助一套會促致須向高級管理層上報重大風險的違規和事故匯報工具及匯報標準，藉以對在辦事處以外地方進行的交易活動作出監察；及
- (b) 經加強的監察能力，包括在辦事處以外地方的交易環境使用有效的交易和通訊監察工具，以便識別出須處理的潛在問題或趨勢。

## 外判及第三方安排

17. 主要第三方未能提供中介人所需的服務或產品以支援遙距工作安排，是遙距工作的固有風險。當遙距工作的中介人員工依賴第三方及其提供的技術和專業知識來進行核心業務或運作職能時，這項風險便會加劇<sup>26</sup>。
18. 外判及第三方安排可能會產生一些風險，例如第三方經紀行的運作規定與中介人的遙距工作安排互不相容，因而無法向該中介人提供執行服務，或第三方經紀行未能在干擾事件期間執行業務延續計劃。中介人可能會因而未能為其本身或其客戶執行交易。

### 應達到的監管標準

中介人應制定並維持有效的政策及程序，以確保適當地選擇和委任支援遙距工作安排的主要第三方，及適當地管理和監察它們在遙距工作環境中帶來的所有風險<sup>27</sup>。

## 建議的措施和程序

19. 中介人就外判及第三方安排實施以下措施：

- (a) 有關業務延續及抵禦能力的風險
  - 就主要第三方在發生干擾時有效地執行業務延續計劃及向中介人提供所需服務的能力進行定期評估，並定期測試後備設施；
  - 在適當情況下就主要第三方的財務狀況進行檢視，以確保它們並沒有因干擾事件而變得無力償債的風險；及
  - 定期檢視主要第三方對干擾事件的應對策略，以評估它們的資訊科技能力，從而確保它們能夠在須採取遙距工作安排的情況下繼續提供所需的服務。

<sup>26</sup> 例如，執行交易指示及就交易進行結算和交收。

<sup>27</sup> 根據《操守準則》第3項一般原則規定，中介人須有效地運用其所需的（除其他事項外）資源，以便適當地進行其業務活動。有關資源包括其主要第三方向它們提供的服務。

(b) 有關網絡保安及資訊保安的風險

- 就因依賴主要第三方執行業務或運作職能而在網絡保安及資訊保安方面出現的潛在影響進行定期檢視，當中須顧及到該等第三方對干擾事件的應對策略，以確保有關網絡保安及資訊保安的風險在遙距工作環境中獲充分處理。

(c) 有關第三方分判商的風險

- 就主要第三方的名單及其服務協議進行定期檢視，以識別及確認它們賴以提供中介人所需的服務或產品的分判商；
- 定期評估主要第三方紓減風險的措施，以確保該等第三方能夠充分地處理其分判商業務受干擾的潛在影響；及
- 就主要第三方及其分判商進行定期評估，以識別是否存在新的風險及該等風險是否獲適當管理。

## 資訊保安

20. 客戶資料及其他機密資料外洩的風險在遙距工作環境中有所增加，原因是遙距工作的員工可能：

- (a) 將紙本文件帶離辦事處；
- (b) 將文件列印本棄置於辦事處以外的地點；
- (c) 將文件的電子檔案轉寄至個人裝置；
- (d) 就中介人的系統內的文件進行遙距列印或擷取螢幕資料；
- (e) 使用可移除的裝置來儲存數據；或
- (f) 透過個人電郵或不安全的雲端檔案分享服務共用文件及資料。

### 應達到的監管標準

中介人在容許員工遙距工作前，應實施適當及有效的數據保密政策、程序及監控措施，以防止及偵測在遙距工作環境中出現的錯誤或遺漏，或有人未經授權而擅自對其數據處理系統及數據（包括所有由中介人管有的機密資料，例如客戶的個人及財務資料，以及容易引起價格波動的資料）進行加插、更改、刪除或侵入等活動<sup>28</sup>。中介人亦應確保就遙距工作而言，其運作及資料管理系統是安全及受到充分監控的<sup>29</sup>。

中介人應確保員工只有在需要知悉客戶資料及其他機密資料的情況下，才能以遙距方式取覽該等資料，並嚴格執行此一規定。

<sup>28</sup> 《內部監控指引》第 IV(5)部。

<sup>29</sup> 《內部監控指引》第 IV(2)部。

## 建議的措施和程序

21. 中介人採取各項步驟，藉以：
- (a) 向員工就如何在遙距工作時將資料保密提供清楚的指引。舉例來說，尋找私人空間進行電話或視訊通話，及不將實物形式的機密文件帶離辦事處，而是透過安全的遙距接達取覽得這些文件；及
  - (b) 透過定期培訓及由員工聲明其了解並遵守有關政策和程序，提升員工對其維持客戶資料和其他機密資料私隱及保密的責任的認知。

## 網絡保安

22. 中介人面對因資訊科技系統遇襲（例如惡意軟件及勒索軟件的攻擊）而引起的網絡保安風險，而這些風險可能對中介人業務健全、具效率和有效的運作造成不利影響。
23. 接駁互聯網及使用個人裝置來進行遙距工作會增加這項風險。舉例來說，若員工獲准使用除了裝有簡單的防毒程式或防火牆外並不安全的私人電腦或流動裝置來進行其工作，中介人的專屬、機密或客戶數據便可能被人互聯網上截取。

### 應達到的監管標準

中介人應訂立適當的措施以管理及紓減與遙距工作安排相關的網絡保安風險<sup>30</sup>，及防止和偵測網絡保安威脅，並顧及在 2020 年 4 月 29 日發出的《致持牌法團的通函——與遙距工作安排相關的網絡保安風險管理》。

## 建議的措施和程序

24. 中介人採取各項步驟，藉以：
- (a) 制訂及維持網絡保安事故管理計劃，當中涵蓋遙距工作安排引致的保安事故；及
  - (b) 定期向遙距工作的員工提供有關防止網絡事故的培訓。

## 備存紀錄

25. 遙距工作安排導致依據監管規定而須備存的某些類別的紀錄被延誤、受損及零散化的風險增加。特別是，當遙距工作的員工進行的活動並無被載入中央系統所產生的紀錄和文件內，及遙距工作的員工持有的紀錄和文件沒有被送回持牌法團獲批准的辦事處時，持牌法團便可能違反《證券及期貨條例》第 130 條的規定。

<sup>30</sup> 《操守準則》第 4.3 段，及在 2020 年 4 月 29 日發出的《致持牌法團的通函——與遙距工作安排相關的網絡保安風險管理》。

#### 應達到的監管標準

持牌法團應實施及維持適當的內部監控措施，以確保當員工可遙距接達其交易或其他系統時，該員工在這些系統內進行的活動會確實被載入系統所產生的紀錄和文件內。

在容許遙距工作的員工將某些必要的紀錄和文件暫存於其家中，或（就《證券及期貨條例》第 130 條的目的而言）並非獲批准處所的其他遙距工作地點之前，持牌法團應先制訂有效的政策、程序及監控措施，規定員工須在切實可行的情況下盡快將這些紀錄和文件送回獲批准的處所<sup>31</sup>。

### 通知的責任

26. 中介人須將其涵蓋內部監控、組織架構、應變計劃及相關事宜的業務計劃的重大改變通知證監會及（如適用）金管局，包括將員工轉為遙距工作（此舉構成其業務計劃的重大改變）。若遙距工作安排只實施一段短時間的話，中介人可能會忽略這項通知規定。

#### 應達到的監管標準

中介人應推行有關措施，以便將實施遙距工作安排一事（此舉構成其業務計劃的重大改變）及有關安排的任何重大改變從速通知證監會及（如適用）金管局<sup>32</sup>。

### 在家工作安排

27. 在家工作的安排帶來家居辦公室環境獨有的額外風險。
28. 在家人、鄰居及朋友可能頻頻到訪家居辦公室，因而令在家工作的員工可能向這些人士非法披露客戶資料、專屬資料或其他機密資料的風險有所增加。
29. 在家工作的員工亦面對更大的網絡不穩定風險，因為家居網絡設備和軟件（例如無線網絡路由器）的特點深度或寬度，都可能與中介人辦事處所安裝的商用設備和軟件不同。家居網絡亦可能面對較大範圍的威脅，例如惡意軟件。

<sup>31</sup> 有關 2019 冠狀病毒(COVID-19)大流行下的牌照相關事宜的常見問題中問題 8 的答案。

<sup>32</sup> 《證券及期貨條例》第 135(3)及 135(4)條。根據《證券及期貨（發牌及註冊）（資料）規則》附表 3 第 1 部第 9 段及第 2 部第 9 段，如涵蓋內部監控、組織架構、應變計劃及相關事宜的持牌法團及註冊機構的業務計劃出現重大改變，該持牌法團及註冊機構便須作出通知。

### 應達到的監管標準

中介人應為紓減在家工作安排獨有的任何額外風險而建立並維持必需和充分的內部監控措施及運作能力<sup>33</sup>。

中介人亦應制定、維持及嚴格執行有關政策、程序及監控措施，藉以確保在家工作的員工只可在需要知悉客戶資料及其他機密資料的情況下取覽該等資料。

中介人應就在家辦公環境中將機密資料保密的政策及程序，向在家工作的員工提供特定培訓<sup>34</sup>。

### 建議的措施和程序

30. 中介人採取各項步驟，藉以：

- (a) 允許在家工作的員工取覽客戶資料、專屬資料及其他機密資料，惟只有在透過公司提供的安全裝置和系統的情況下才可這樣做；及
- (b) 定期向在家工作的員工取得其了解並遵守有關將機密資料保密的政策及程序的聲明，並定期向他們提供重溫培訓。

<sup>33</sup> 《操守準則》第 3 項一般原則。

<sup>34</sup> 《內部監控指引》第 III(3)部。