強制性公積金計劃管理局

I.1 電子強積金系統運作的規管監督框架

目錄

I. 引言

《強制性公積金計劃條例》（《條例》）第6E條訂定強制性公積金計劃管理局（管理局）的職能。根據《條例》第6E(1)(ec)條，管理局獲賦權監督電子強積金系統的運作，包括：(i)審批《條例》第19K(2)(a)條所描述的守則；(ii)向有關系統營運者及核准受託人，發出管理局認為對保障該系統的完整及穩定屬適當的指示或指令；以及(iii)監察該系統營運者遵守運作守則和遵從第(ii)項所述的指示及指令。

2. 根據《條例》第19K(2)(b)條，有關系統營運者須確保電子強積金系統以安全及有效率的方式管理和運作，以期把發生可預見的、對該系統發揮功能的干擾的可能性，盡量減低。

3. 管理局現於本框架（規管監督框架）列明監督規定，藉以：(a)作為管理局根據《條例》第6E(1)(ec)(ii)條，為保障積金易平台的完整和穩定而向系統營運者發出的指示及指令，以及(b)根據《條例》第6E(1)(ec)(iii)條，監察系統營運者有否遵守運作守則和遵從《條例》第6E(1)(ec)(ii)條所述的指示及指令。具體而言，規管監督框架旨在闡釋與系統營運者在《條例》第19K條下的責任相關的監督規定，以及管理局在監督積金易平台時所依循的程序。為免生疑問，本規管監督框架並不縮減或減損相關各方在《條例》及其附屬法例下對積金易平台負有的責任及義務。

II. 生效日期

4. 本規管監督框架由財經事務及庫務局局長根據《條例》第19I(1)條藉於憲報刊登的公告指定積金易平台為電子強積金系統當日（即2024年6月13日）起生效。

III. 用詞定義

5. 本規管監督框架中的用詞凡在《條例》或其附屬法例已有定義，則該詞的涵義與《條例》或其附屬法例為該詞所下的定義相同。規管監督框架如另有訂明，則作別論。

6. 除本規管監督框架另有訂明外，規管監督框架的用詞的定義如下：

(a) ***「應用程式介面」***指一種用於系統對系統數據傳輸的途徑，藉以促進在不同電腦系統之間交換信息和執行指令。

(b) ***「核准受託人」***指獲管理局按照《條例》第20條核准為受託人的公司或自然人，而就任何由兩名或多於兩名核准受託人管理的註冊計劃而言，指（除在《條例》第33至33B條中）共同及各別的受託人。

(c) ***「特訂平台設定」***指就提出要求的核准受託人所管理的註冊計劃，由核准受託人不時提出並由系統營運者根據服務協議的條款接納並執行的對積金易平台所作的任何改動或增補。

(d) ***「承辦商」***指系統營運者不時聘用以執行系統營運者與積金易平台有關的業務或職能的一名或多於一名人士。

(e) ***「資料保障法例」***就系統營運者及每名核准受託人而言，指《個人資料（私隱）條例》（《私隱條例》）及個人資料私隱專員發出或批准的任何相關實務守則、規則或指引，以及與使用和處理個人資料有關的任何其他適用法例。

(f) ***「積金易平台」***指由系統營運者不時提供的電子強積金系統（根據《條例》第19I(1)條指定的電子系統）及計劃管理服務（詳情載於運作守則和運作手冊），而視乎適用於個別核准受託人的特訂平台設定而定，核准受託人、其服務提供者、參與僱主及成員，以及其他獲准接觸該平台的人士，可透過服務中心及／或以多種電子方式接觸該平台。

(g) *「《強積金（一般）規例》」*指《強制性公積金計劃（一般）規例》（第485A章）。

(h) *「經合組織」*指經濟合作與發展組織。

(i) *「資科辦」*指政府資訊科技總監辦公室。

(j) *「運作手冊」*指由系統營運者根據運作守則不時制訂、發出及備存的手冊，當中載述計劃管理服務的範圍及詳情、相關工作流程和使用積金易平台的詳細運作規定。

(k) *「運作守則」*指《條例》第19K(2)(a)條所述由系統營運者制訂並經管理局審批的守則。

(l) *「《條例》」*指《強制性公積金計劃條例》（第485章）。

(m) *「《私隱條例》」*指《個人資料（私隱）條例》（第486章）。

(n) *「個人資料」*指在《私隱條例》所賦予的涵義。

(o) *「處理」*就個人資料而言，指就各項或各組個人資料進行的任何操作或一組操作，不論有關操作是否以自動化方法進行。

(p) *「計劃管理服務」*指系統營運者不時向核准受託人提供的一如在運作守則及運作手冊中所載述的服務及設施。

(q) *「服務協議」*就每名核准受託人而言，指系統營運者與核准受託人簽訂的有關系統營運者向核准受託人提供積金易平台的協議。

(r) *「指明實體」*指(a)積金易平台有限公司；或(b)根據《條例》第6DA條為下述目的而設立的全資附屬公司：(i)利便執行管理局的職能；以及(ii)為施行《條例》新訂第3B部，管理和營運電子系統，以及為施行第3B部，為核准受託人提供計劃管理服務。

(s) *「職員」*指系統營運者、承辦商或其分判商就系統營運者執行積金易平台的相關業務或職能而不時僱用的一名或多於一名人士。

(t) *「系統營運者」*指根據《條例》第19I(1)條獲指定，管理和營運某電子系統的指明實體。

(u) *「工作日」*指並非以下日子的日子：(a)公眾假日；或(b)《釋義及通則條例》（第1章）第71(2)條所界定的烈風警告日或黑色暴雨警告日。

IV. 監督標準

7. 根據《國際退休金監管機構組織私營退休金監管原則》[1]，私營退休金監管目標的重點在於促進退休基金的穩定、安全和良好管治，從而保障退休基金成員及受益人的利益。在國際上，退休金的規管越來越着重管治及風險管理事宜，世界各地的退休金監管機構亦跟隨其他金融界別的做法，相繼採用風險為本的方式監管退休金。

8. 在2011年1月，經合組織與國際退休金監管機構組織發布了《經合組織／國際退休金監管機構組織退休基金風險管理制度良好作業守則》[2]。具體而言，該作業守則涵蓋了退休基金風險管理制度的各主要範疇，包括管治安排、運作及外判工作的風險和管控，以及在監察、匯報和溝通上的風險管理機制。

9. 因應上述國際標準，管理局在制訂積金易平台的監督標準時，已考慮了相關的監管目標及良好作業守則。下文載述有關規定的各部分，訂明了各項監督標準。管理局認為這些規定對保障積金易平台的完整及穩定是適當的，系統營運者須持續遵守這些規定。具體而言，下文載述有關規定的各個部分，會進一步闡述為符合《條例》第19K條而實施的監督規定。管理局將會定期根據該等規定評核系統營運者，以監督系統營運者在管理和營運電子強積金系統及交付計劃管理服務方面，營運積金易平台的情況。

IV.1 管治

10. 根據《條例》第19K(2)(b)條，有關系統營運者須確保電子強積金系統以安全及有效率的方式管理和運作，以期把發生可預見的、對該系統發揮功能的干擾的可能性，盡量減低。

---

[1] 《國際退休金監管機構組織私營退休金監管原則》，請瀏覽 https://www.iopsweb.org/principlesguidelines/IOPS-principles-private-pension-supervision.pdf

[2] 《經合組織／國際退休金監管機構組織退休基金風險管理制度良好作業守則》，請參閱 http://www.iopsweb.org/principlesguidelines/46864307.pdf

11. 一般而言，系統營運者應設有妥善、清晰及具透明度的管治安排，並促進積金易平台能安全、有效率地運作。就此，系統營運者的董事局和高層管理人員應制訂有效的監督計劃，當中包括（但不限於）以下各項：

(a) 清楚訂明管理、營運及監察積金易平台的角色及責任；

(b) 配備具有適當知識、技能和經驗的合適各方，以履行其角色及責任；

(c) 訂立管控政策（包括但不限於有關利益衝突及操守守則的政策），確保積金易平台以安全及有效率的方式管理和運作；

(d) 妥善分配足夠的技術資源和其他資源，以支援及監察積金易平台運作；

(e) 配備適當的管理資訊系統，以助進行有效的管理監督；

(f) 制訂有效的風險管理框架，確保各方遵守管控政策、運作守則、服務協議，以及管理局發出的適當指示或指令；及

(g) 確保系統營運者及承辦商有能力勝任管理和營運積金易平台的工作，以及設有足夠的培訓計劃。

12. 系統營運者應制訂有效的風險管理框架，包括制訂風險接受程度和風險承受能力的政策、指派作出風險決定的責任、訂定問責安排，以及處理不同危機及緊急情況的決策。系統營運者的董事局和高層管理人員應就積金易平台的運作釐定適當的風險承受水平，並訂立符合該風險承受水平的政策、程序和管控措施。管治安排應能為風險管理及內部控制職能提供充足的獨立性、授權和資源。

13. 管治安排（包括風險管理框架）應妥為記錄，並傳達予所有相關職員，確保他們遵守當中的規定。系統營運者的董事局及高層管理人員應定期檢討和核准管治安排。

IV.2 安全

i. 系統運作的可靠性及健全度

表現管理

14. 系統營運者應就積金易平台運作的可靠性及健全度清楚訂明表現目標，並設計及制訂相關政策，以達到該等目標。系統營運者應定期評估積金易平台的運作是否符合既定目標。

15. 系統營運者應識別對積金易平台發揮功能具關鍵作用的運作程序，並充分監察該等程序的表現。此外，系統營運者亦應制訂協助偵測該等程序有否出現異常活動、詐騙行為及事故的安排，以便迅速採取行動，應對這些活動構成的風險。

16. 由於積金易平台很可能會處理大量交易，系統營運者應確保積金易平台有足夠能力處理交易，特別是在高峰時間或高峰日子。系統營運者應定期監察及測試積金易平台的實際能力和表現，並因應交易量或業務模式轉變而導致的需求增加，制訂提升能力的計劃，藉以維持積金易平台管理及運作所需的程序。系統營運者亦應定期進行系統能力壓力測試，以核實積金易平台能否在極端情況下處理異常龐大的交易量。如發現系統能力有任何不足之處，系統營運者應制訂補救措施，以解決系統能力問題。

持續業務運作計劃

17. 系統營運者應制訂可行、周全及備有全面文件紀錄的持續業務運作計劃，以應對及管理危機，並確保在發生緊急情況時可及時恢復和持續運作。一般而言，系統營運者須：

(a) 進行業務影響分析，以識別對持續業務運作構成威脅的各種不同風險，並量化業務中斷（包括可能引致積金易平台的運作出現廣泛或嚴重中斷的事件）造成的影響；

(b) 清楚訂明目標（包括恢復運作時間及具體恢復點）、政策及程序，以便在服務中斷後迅速恢復整體運作，並及時恢復關鍵運作；

(c) 識別可能構成運作中斷重大風險的事件，並制訂處理該等事件的緩解措施；

(d) 制訂危機及事故處理程序以處理及遏止緊急事故繼續惡化，防止事故影響機構的整體業務。有關程序須包括應付潛在資料遺失的程序，並且包括及時而有效的通訊策略，以諮詢及通知所有相關各方（例如核准受託人）、管理局及其他有關方面（例如關鍵服務提供者）；

(e) 設立配備適當網絡及基礎設施設計、足夠資源、能力、功能及適當人手安排的備用場地（即復原場地），使其不受系統營運者在主要場地的運作廣泛或嚴重中斷所影響，並在有需要時由備用場地接掌主要場地的運作；

(f) 定期測試其業務及資訊科技系統的復原安排。有關測試應包括與其業務及風險狀況相關的不同性質、嚴重程度和持續時間的各種假設情景。舉例而言，系統營運者可考慮的假設情景，包括但不限於疫情、自然災害及第三方或其供應鏈出現故障或中斷的情景。相關各方（例如核准受託人）和關鍵服務提供者（按適用情況及在可能範圍內）均應參與測試；及

(g) 定期檢討有關安排是否足夠及具成效，並說明所識別的任何漏洞或不足之處，以及記錄已計劃採取的補救措施。

外判安排

18. 如系統營運者擬外判某些業務運作，應確保外判安排不會損害積金易平台的安全及效率。系統營運者應對建議的外判安排進行全面風險評估（包括運作風險、法律風險、合規風險及信譽風險），並在作出有關安排前適當處理已識別的所有風險。具體而言，風險評估應包括以下各項：

(a) 將予外判服務的重要性及關鍵程度；

(b) 外判的理據（例如成本效益分析）；及

(c) 外判對系統營運者風險狀況的影響。

19. 為管理外判風險，在簽立任何書面外判協議前，系統營運者的高層管理人員須在盡職審查及招標過程中，查核承辦商是否具備交付所需服務的適當財政及技術能力。

20. 在任何外判安排中，系統營運者的高層管理人員對所外判的業務或職能均負有最終責任。外判安排只是讓高層管理人員把某項業務或職能的日常管理責任轉移予承辦商，而非其問責性。就此，系統營運者應訂立有效的管控程序，以監察其外判業務或職能。

21. 系統營運者與承辦商簽訂的外判協議，應清楚列明所提供的外判服務種類和水平，以及承辦商在合約下的責任和義務。此外，協議須訂明終止協議的條件，以及延續／移交條款。系統營運者應定期（例如每年）檢討外判協議，並因應運作需要和外在環境的轉變，評估應否重新議訂及延續該等協議。

22. 系統營運者應確保在任何外判安排中具備有效的程序，以監察承辦商的表現，以及管理與承辦商的關係和外判業務或職能涉及的風險。系統營運者亦應制訂匯報程序，使有關外判業務或職能的問題能迅速上報至高層管理人員和承辦商處理，以及把重大事件上報至管理局。系統營運者應定期檢討外判安排的管控程序。

23. 若有關資料由承辦商或位於香港境外的辦事處備存，系統營運者應根據下文第IV.2部第iv節「資料保護及安全」載列的管控規定，考慮該等實體所設的資料安全措施是否令其滿意，並應定期檢討該等實體是否有效執

行該等措施。相關各方簽訂的協議（包括承辦商協議）應列明資料保護的義務及責任，確保在聘用期或委任期內設有資料安全措施。

24. 外判安排不應妨礙管理局、系統營運者的內部及外聘核數師和按合理要求提供第三方評估報告的人士或機構接觸有關資料。系統營運者應確保與承辦商簽訂的外判協議載有條款，容許有關人士或機構對承辦商涉及的外判業務或職能的運作及管控措施作出審查或檢討。

25. 為確保系統營運者所聘用的承辦商具備所需的技能、資歷、經驗及資源，以能符合《條例》及其附屬法例訂明的法定要求，並能執行系統營運者外判的職務，系統營運者應制訂正式政策，列明選聘承辦商的準則。系統營運者亦應要求承辦商遵守《條例》下的所有適用保密規定（例如《條例》第41、41A及41B條）以及資料保障法例。

<u>系統開發及變更管理</u>

26. 在系統開發及變更管理方面，系統營運者應設立一個整體框架，管理與科技相關的主要項目及系統變更。在這個框架中，應指明積金易平台的開發及變更所應採取及應用的管理方法，當中最低限度應涵蓋職責分配、業務詳情、預算計劃、影響分析、風險評估、工作里程、工作進程標誌、主要倚賴因素、質素保證與測試、核准、實施後的驗證和監察工作，以及問題管理等環節。如對積金易平台作出任何重大變更（例如積金易平台主要功能的變更、對積金易平台的安全或效率有重大影響的變更等），系統營運者應在實施有關變更前預先通知管理局。

27. 為能及時處理突發情況，系統營運者應制訂正式的程序，以管理應急變更，包括評估影響、核准變更、進行測試以及在實施變更後進行檢討。一般而言，如發生事故導致或可能導致積金易平台運作中斷、性能顯著

下降，或出現監管合規問題，均可能須啟動應急變更。系統營運者應在實施應急變更後通知管理局。

28. 各項應急變更應妥為記錄及作出備份（包括各個舊有及變更後的程式版本和數據），以備有需要時可復原舊有的程式版本和數據檔案。應急變更必須經由獨立人員審核。該等人員從職能分隔的角度而言，應獨立於實際變更過程，以確保有關變更屬恰當，以及不會對生產環境造成不利影響。系統營運者應在作出應急變更後，隨即透過正式的驗收測試及變更管理程序，以適當的修補取代所作出的應急變更。

<u>培訓</u>

29. 由於確保積金易平台運作的可靠性及健全度十分重要，因此應安排足夠數目、曾接受充分培訓且具有足夠能力的人員參與運作。有關人員應具備適當程度的知識及經驗，以履行其獲指派的職務。鑑於科技發展一日千里，系統營運者必須確保負責科技發展職能、風險管理職能以及合規職能的職員，以及內部審核人員，均持續具備足夠能力並能達到所需程度的專業知識及經驗。系統營運者應確保人手編制的水平足以應付現時及預期的工作需求，並因應員工流失率預留合理水平的人手。

30. 為確保制訂完善周全的人員培訓計劃，系統營運者必須制訂程序，以識別負責積金易平台關鍵運作的職員是否存在重大的技術差距。系統營運者可鼓勵及在適當情況下利便職員（例如負責保安管理及風險管理職能的職員）考取相關專業資格，以及應促使承辦商及其次承辦商鼓勵及在適當情況下利便負責該等職務的職員考取相關專業資格。

ii. 對接觸系統的管制

31. 系統營運者應透過管制對積金易平台運作的接觸，確保積金易平台的安全。系統營運者應以完善周全的認證機制輔以接觸管制規則，對接觸

積金易平台施以限制。接觸管制規則訂明用戶的權限以及可以接觸的功能、系統資源及資料。系統營運者應定期檢討用戶的接觸權限，以盡量減低在未獲授權的情況下接觸平台的風險。

32. 系統營運者應實施有效的密碼管控措施，確保防止使用強度低或易於猜測的密碼，以及確保定期更改密碼。應就較高風險的交易（例如繳付款項）採取較高強度的認證管控措施（例如多重認證）以確保交易的完整性。

33. 系統營運者應妥善管制特權帳戶的使用和接觸，包括（但不限於）須獲適當的管理人員正式核准、監察帳戶活動、加強密碼管控，以及定期檢討已授予的接觸權限。

34. 當使用應用程式介面以利便其他各方連接並接觸積金易平台時，系統營運者應採取適當的接觸管制配置及措施，以防止在未獲授權的情況下接觸平台。系統營運者應適當監察、識別、評估及減少關乎使用和接觸應用程式介面的欺詐活動。

35. 另一方面，採取實體的接觸管制措施對保障電腦設施及設備免受破壞及未獲授權的接觸是十分重要的。應制訂全面的實體保安政策以保護積金易平台，該等政策須能有效輔助系統營運者識別、評估和減少放置積金易平台及與其有關聯的基礎設施的實體場所的保安威脅和漏洞。有關場所應設有妥善的保安屏障和進出管制作為防禦措施，並只向獲授權人士發出進出權限。系統營運者應定期檢討進出權限，以減少在未獲授權的情況下進出有關場所的風險。此外，應使用適當的監察工具（例如監控鏡頭）輔助執行實體保安工作。

iii. 在系統內持有的資料的完整性，以及對接觸該等資料的管制

36. 資料完整性指資料的準確性、全面性及一致性，以確保其適合使用。系統營運者應採取適當的措施和有效的管制，以確保資料的完整性和保密性。這些措施和管制包括（但不限於）：

(a) 為積金易平台內的所有數據及資料備存足夠備份，以及定期進行備份復原測試；

(b) 妥善管制對重要備份紀錄的接觸；

(c) 第31至35段所載有關對系統接觸的管制；

(d) 第37至40段所載有關資料保護及安全的措施；及

(e) 設立妥善的內部控制機制以確保資料的完整性。

iv. 資料保護及安全

37. 系統營運者應制訂管控程序以保護應用程式、運作系統、系統軟件及資料庫。具體而言，系統營運者應考慮《條例》下所有適用的保密規定（例如《條例》第41、41A及41B條），制訂穩健而健全的資料安全政策和程序，以保障系統內的資料，當中應涵蓋以下各個範疇：

(a) 在資料保護方面的角色和責任；

(b) 管理保安威脅和漏洞，包括進行識別、評估及補救工作；

(c) 安全的受監控環境以儲存資料；

(d) 邏輯及實體接觸管制；

(e) 資料傳送，包括偵測及防止資料外洩；及

(f) 管理承辦商所使用的資料。

38. 如涉及個人資料，相關的政策和程序（包括承辦商須遵從的政策和程序）亦應符合資料保障法例。系統營運者應根據既定政策和程序，實施足夠的保安管制。

39. 系統營運者應以書面形式載列確保資料安全的政策和程序，並要求所有職員，以及促使承辦商及其次承辦商確保其所有職員，遵從該等政策和程序，以及確保他們知悉如何取覽該等政策和程序。系統營運者應在確保資料安全的政策和程序出現任何變更時通知所有職員、承辦商和其次承辦商，並確保所有職員能夠取覽已更新的政策和程序。

40. 為保障資料的機密性，系統營運者應確保職員對保護資料具備高度意識。系統營運者應就提高資料安全意識制訂有效的加強意識計劃，以定期提醒職員、承辦商及其次承辦商必須遵守各項確保資料安全的政策和程序，盡快報告任何潛在的資料（例如僱主或計劃成員的資料）外洩或遺失的事故，以及違反該等政策和程序可能遭受的紀律處分。有關資料安全的政策和程序應定期予以檢討。

v. 備存紀錄

41. 系統營運者應訂立一套備存紀錄的政策及程序。該等政策的目標，應為建立及管理真確、可靠、準確、完整及可用的紀錄，足以支援系統營運者提供計劃管理服務及進行其他業務。為達致這個目標，系統營運者應制訂穩健的機制和作出適當的控制，以在資料壽命周期的不同階段（一般包括資料收集、處理、保留及處置等階段）管理資料。

42. 系統營運者應準確、完整和及時地收集與計劃管理有關的交易及資料（包括但不限於成員登記、供款處理、權益轉移、基金轉換及權益提取），並應在工作流程中建立確認機制，以盡量減低人為錯誤的風險，以及從外部來源（例如核准受託人）自動輸入資料，以便能迅速識別錯誤資料。

43. 系統營運者應在每個工作日把各名計劃成員及參與僱主單位的權益總和，與該註冊計劃持有的資產總額核對，除非在該日電子強積金系統根據《條例》第19J或19L(1)(a)或19L(1)(b)條暫停運作或供人使用，而暫停對進行該項核對有所影響。

44. 系統營運者應按照既定政策及程序，妥善儲存紀錄及施以適當管制。具體而言，系統營運者應制訂有效程序，以解釋計劃資產的調撥及保存足夠審核線索。系統營運者應定期為有關紀錄備份，以及定期檢討備存紀錄的政策和程序，以確保其與業務需要相稱。

45. 系統營運者應制訂保存及處置紀錄的時間表，在確保已遵從規定把紀錄保存一段指定時間後，能有系統地計劃及有序地處置紀錄。系統營運者應遵守資料保障法例以及《強積金（一般）規例》第93條有關備存紀錄的規定。該條文規定，須確保任何就註冊計劃而須備存的會計或其他紀錄，在作出該紀錄時的財政期終結後備存至少七年；或如該紀錄關乎某人在該計劃中的成員身分，則在該人不再是計劃成員後備存至少七年。該等紀錄可以電子形式備存（如適用），但應可讓管理局隨時查閱以進行監督和檢查。

46. 系統營運者應確保遵從既定的政策和程序處置紀錄，以及在進行處置前事先獲得充分相關的高級職員妥為批准，以防止過早處置紀錄或銷毀具存檔價值的紀錄。

47. 系統營運者應設立並維持適當而有效的交易審查程序，以防止或查辨錯誤、詐騙及其他不當活動。系統營運者應時刻瞭解在法律及規管領域（包括但不限於《條例》和其附屬法例以及資料保障法例）內會影響其紀錄備存安排的最新發展。

48. 當系統營運者從其紀錄中擬備資料並將該等資料提交予管理局時，應採取適當的管制措施，以確保該等資料準確、可靠。系統營運者應制訂適當的資料編製程序，以確保擬備的資料完整、準確、及時。系統營運者應確保清楚記錄該等程序，以及向負責擬備及核對資料的職員清楚傳達並確保他們清楚瞭解該等程序。

49. 系統營運者應實施品質保證計劃，以確保按照既定的政策和程序妥善收集和備存紀錄，並改進所識別的須予改善的範疇。

vi. 系統運作風險管理及管控程序

50. 系統營運者應就積金易平台的運作制訂有效的風險管理及管控程序。系統營運者的高層管理人員應清楚訂明，由哪個內部部門負責實施及管理風險管理程序。系統營運者應採取適當的政策、程序和控制措施，以識別、追蹤和減低相關風險，包括但不限於與運作及科技有關的風險，並定期檢討風險管理程序。

51. 既有的風險管理部門不僅負責實施及管理風險管理程序，亦應協助各業務部門和資訊科技部門執行風險管理程序，以識別、衡量、監察及管理與運作和科技有關的風險。風險管理部門亦應協助識別、衡量、監察及管理相關各方（例如使用或將會連接積金易平台的各方）可能對積金易平台的運作構成的風險。同樣，風險管理部門也應協助識別、衡量、監察及管理平台運作可能對其他相關各方構成的風險。

52. 系統營運者應制訂有效的管控措施，以確保積金易平台正常運作。風險管理部門應協助確保相關職員知悉及遵循系統營運者的管控政策、運作守則、服務協議，以及上文第11(f)段所述管理局給予的指示或指令；以及支援對欺詐和事故、可能違反法律和法定規定及／或規管規定的情況而進行的調查工作。風險管理部門應能自由溝通，以有效履行職務。此外，第三道防線應定期進行風險為本的獨立審計，以確保積金易平台的安全和效率。

53. 系統營運者應建立足夠及全面的匯報及溝通途徑，以便把內部管控的缺失或未能有效控制的風險向適當層級的管理人員匯報，並就此進行溝通。

vii. 系統的穩健程度

54. 系統營運者應建立穩健及健全的保安框架，以識別、應對和監察與積金易平台的管理和運作有關的保安風險，包括潛在的保安漏洞和威脅。保安框架應以積金易平台的定期保安風險分析為基礎，並須符合相關標準（例如資科辦制定的標準）。系統營運者應持續監察保安程序及遵循保安框架的規定。

55. 鑑於網絡風險不斷變化，系統營運者應把有效及全面應對網絡風險的框架納入保安框架，作為保安框架的一部分。系統營運者應根據其業務運作的類型、規模、價值和複雜性，識別其可能面對的網絡風險，並利用風險為本的方式決定相關風險的緩急優次，從而找出關乎積金易平台運作的威脅所在。為防範網絡攻擊，應制訂有效的管控程序，包括偵測、保護、復原和應對網絡威脅的程序。因此，系統營運者應定期評估管控程序及進行漏洞測試，以確保保安框架有能力應對相關的網絡風險。

56. 鑑於網絡防衛十分重要，系統營運者應定期進行模擬演習，透過模擬不同的攻擊情景，改進現有應對網絡風險的管控措施。系統營運者應監察網絡威脅的趨勢，實施足夠措施應對不同的網絡攻擊情景，以及定期進行滲透測試和保安評估。

viii. 由與系統有關聯的基礎設施提供予系統的服務

57. 積金易平台運作的可靠性及健全度，或取決於與積金易平台有關聯的基礎設施提供的服務的延續性，而有關聯的基礎設施應放置在數據中心。系統營運者應識別、量度、監察及管理因使用有關聯的基礎設施提供的服務而產生的風險。

58. 考慮到通訊網絡的功能是傳送資料以及作為接觸積金易平台的媒介，系統營運者應遵行妥善的網絡保安措施，包括健全的網絡設計、明確界定的網絡服務以及良好的紀律。為防止不安全連接至系統營運者的網絡，系統營運者應制訂使用網絡及網絡服務的程序，當中應包括授權程序、保護網絡接觸的管控措施和程序，以及定期檢討與網絡相關的設備的參數配置。

59. 鑑於與積金易平台有關聯的基礎設施十分重要，系統營運者應審慎考慮可能對有關聯的基礎設施的運作產生不利影響的環境風險（例如火、煙霧、溫度、水、濕度及灰塵）。系統營運者應制訂一套有效的環境控制措施，以助監察及保護有關聯的基礎設施。有關聯的基礎設施亦應裝設不間斷電源供應器，以免受到停電及供電干擾影響。

60. 有關聯的基礎設施亦應設有足夠的接觸管制，以防止在未獲授權的情況下接觸有關設施。此外，系統營運者應定期進行檢查，確保對有關聯的基礎設施實施的接觸管制和環境控制均有效運作。

ix. 系統按照運作守則管理和運作

61. 系統營運者應設立有效的管控機制，以確保積金易平台的管理和運作符合運作守則的要求。請參閱第IV.4部第ii節「監察運作守則的遵守情況」瞭解詳情。

IV.3 效率

i. 系統在提供計劃管理服務方面的速度及效率

62. 根據《條例》第19K(4)(a)條，在斷定積金易平台是否以有效率的方式管理和運作時，須尤其顧及積金易平台在提供計劃管理服務方面的速度及效率，特別是應符合以下要求：

(a) 系統營運者應確保積金易平台可按照規定的速度（包括在高峰時間或高峰日子），處理與計劃管理服務有關的交易。系統營運者

應確保積金易平台的技術安排能靈活應對不斷變化的需求和新科技。此外，系統營運者應盡最大努力評估平台因應交易量或業務模式變化而須提升效能的幅度，以維持所需的速度；

(b) 應訂明各項表現指標（如回應時間、交易處理量、系統可用性和穩定性），以評估積金易平台所提供的計劃管理服務的效率。系統營運者應參照各項預設指標，定期測試及監察計劃管理服務的表現，以確保其服務具有效率，包括在成本和費用方面的考慮。系統營運者亦應定期檢討各項訂明的表現指標；

(c) 系統營運者應訂明各項服務水平，以評估其在管理和營運積金易平台方面的表現。服務表現的量度準則，應包括系統營運者所提供的計劃管理服務在時間及質素上須達到的水平。系統營運者應能客觀及可靠地量度每一個服務水平，並定期監察、量度及向管理局匯報其所達到的服務水平以供查核。此外，系統營運者應定期檢討上述各項服務水平；及

(d) 系統營運者應定期測試相關的內部管控程序的運作情況，以識別可提升效率之處，從而確保運作具備效率。

ii. 維持和營運系統的整體成本

63. 根據《條例》第19K(4)(b)條，在斷定積金易平台是否以有效率的方式管理和運作時，須尤其顧及維持和營運積金易平台的整體成本。一般而言，整體成本包括以下組成部分：

(a) 系統維護開支—包括修正程式錯誤、改善系統性能、提升功能，或任何為確保積金易平台按預期方式運作而進行的工作；及

(b) 系統營運成本—與積金易平台日常管理及運作有關的成本，包括系統營運者使用的資源成本。

64. 系統營運者應定期監察維持和營運積金易平台的整體成本，透過有效運用資源確保符合成本效益，從而實踐營運目標。

IV.4 運作守則

65. 根據《條例》第19K(2)(a)條，系統營運者須制訂及備有經管理局審批的、規管積金易平台的管理及運作，以及暫停該平台運作或供人使用的守則（即運作守則）。運作守則會訂定核准受託人及系統營運者在營運積金易平台時所須依循的規則，以及訂明以下事宜的規則：(i)系統營運者管理及運作積金易平台，以及暫停該平台運作或供人使用；(ii)由系統營運者提供計劃管理服務；以及(iii)核准受託人使用積金易平台及計劃管理服務，以執行註冊計劃的計劃管理職能。

i. 守則的設計

66. 運作守則應清晰、全面及切合現況。運作守則應與《條例》及其他適用的法定及監管規定一致，並應概述就積金易平台的管理、運作及暫停該平台運作或供人使用而進行的活動。運作守則應清楚列明核准受託人及系統營運者在主要計劃管理程序中的角色和責任。系統營運者應根據運作守則所載的機制，通知核准受託人已獲管理局核准的對運作守則所作的任何修訂，以及就該等修訂的實施給予核准受託人合理的通知。

ii. 監察運作守則的遵守情況

67. 根據《條例》第19K(2)(c)條，系統營運者須確保設有充分安排，以監察運作守則的遵守情況和確保運作守則得以遵守，包括關於可供系統營運者運用的資源的安排。

68. 系統營運者尤須設立有效的監察和匯報機制，以便持續監察運作守則的遵守情況，以及持續遵守運作守則。如出現可能導致違反運作守則的情況，有關機制應能預先給予系統營運者警示，以便有充裕時間採取適當的補救行動。

69. 如營運積金易平台的特定範疇根據運作守則訂立了詳細的程序及手冊，系統營運者應設立有效的控制措施，確保有關程序及手冊與運作守則的規定時刻保持一致。

70. 如系統營運者或任何核准受託人沒有遵守運作守則，因而可能對積金易平台的管理及運作構成風險，系統營運者應迅速通知管理局。

iii. 處理新增、終止或重組註冊計劃及成分基金的安排

71. 當系統營運者收到任何關於新增、終止或重組註冊計劃或成分基金建議的通知，系統營運者應制訂適當計劃，以應對和有序處理有關情況，確保運作保持穩健。

iv. 修訂運作守則

72. 系統營運者有責任在顧及管理局根據《條例》第6H條發出的相關指引的情況下，確保運作守則及任何根據運作守則制訂的程序或手冊均符合《條例》、附屬法例及其他適用法定及監管規定。

73. 系統營運者或會不時建議對運作守則作出其認為必要或適宜的修訂，而在對運作守則作任何修訂前，均應事先獲管理局核准。系統營運者應向管理局提交以下資料及管理局認為必要的任何其他相關資料，以便管理局就有關運作守則的建議修訂作出考慮：

(a) 修訂的範圍、詳情及原因；

(b) 修訂的建議生效日期；

(c) 就修訂引致的風險進行的評估及相關的風險緩解措施；及

(d) 對計劃、計劃參與者及核准受託人的影響。

74. 如對運作守則作出任何修訂，應按運作守則所載方式通知核准受託人。

75. 此外，管理局可給予系統營運者指示及指令以修訂運作守則，確保積金易平台以安全及有效率的方式管理和運作。

v. 暫停積金易平台運作或供人使用

76. 在以下情況下，系統營運者可暫停積金易平台的全部或其任何部分的運作或供人使用：

(a) 按管理局指示（《條例》第19J條）；

(b) 為進行經排期維修（《條例》第19L(1)(a)條）；或

(c) 因為未有預見的情況（《條例》第19L(1)(b)條）。

77. 如有必要暫停積金易平台運作或供人使用，系統營運者應在切實可行的範圍內盡快通知管理局。經排期的維修應安排在非繁忙時間（如適用）進行。

78. 系統營運者如根據上文第76(a)段暫停積金易平台（或其任何部分）運作或供人使用，將以管理局認為適當的方式發布關於該項暫停的資料。

79. 系統營運者在根據上文第76(b)段暫停積金易平台（或其任何部分）運作或供人使用前，須遵照《條例》第19L(2)條的規定，按照運作守則發布關於該項暫停的資料。

80. 系統營運者如根據上文第76(c)段暫停積金易平台（或其任何部分）運作或供人使用，須遵照《條例》第19L(3)條的規定，按照運作守則發

布關於引致有需要暫停積金易平台（或其任何部分）運作或供人使用的情況的資料。

81. 應發布的資料載列如下：

(a) 暫停運作或供人使用的範圍、詳情及原因；

(b) 建議暫停運作或供人使用的期間；

(c) 暫停運作或供人使用的影響；及

(d) 補救措施（如有）。

82. 系統營運者應制訂穩妥的持續業務運作計劃，確保如積金易平台暫停運作或供人使用，平台的全部或其任何部分的運作能夠及時恢復。系統營運者應定期更新持續業務運作計劃，並定期向管理局提交最新計劃以供審閱。

V. 監督方法

83. 管理局已制定監督方法，以持續監察及評估系統營運者遵守《條例》及附屬法例所施加責任的情況。管理局尤其會監察系統營運者遵守運作守則及管理局為保障積金易平台的完整及穩定而發出的指示及指令的情況。系統營運者須確保積金易平台以安全及有效率的方式管理和運作。按照風險為本的模式，監督工作涉及持續監察系統營運者在符合第IV部（監督標準）所載規定方面的表現和成效，重點涵蓋可能會對積金易平台的管理及運作存在重大潛在影響的高風險範疇，以期盡早識別問題所在和作出補救。若系統營運者把計劃管理服務外判予承辦商，系統營運者須訂立充足及有效的安排，以便管理局履行其監督角色，就外判業務或職能對承辦商的運作、程序及管控措施作出審查或檢討。

84. 雖然管理局對系統營運者負有監督責任，但系統營運者的日常運作主要是由系統營運者自行負責。管理局不會參與系統營運者的日常運作。

85. 管理局會透過以下方式監督系統營運者：

(a) 實地巡查；

(b) 非實地監察，包括與系統營運者的高級管理人員聯繫；

(c) 匯報重大事件／事故；及

(d) 第三方保證報告。

V.1 <u>實地巡查</u>

86. 實地巡查有助管理局瞭解系統營運者的運作、風險管理及內部控制，並有助確保系統營運者遵守法定及監管規定，以及監督標準下的規定。巡查會基於管理局的決定進行，而有關決定會訂明每次巡查的主題和目的。儘管巡查通常是事先計劃的，但如發生須即時採取行動的事件或事故，管理局亦可為此進行巡查。

87. 一般而言，實地巡查會採用風險為本的模式進行，而在系統營運者管轄下屬風險較高或管控水平較低的範疇，會優先安排進行巡查。風險較高的範疇，實地巡查的次數一般會較為頻密。實地巡查的範圍可包括（但不限於）機構管治、運作及科技風險管理、業務及持續業務運作計劃，以及外判安排。巡查方法可包括會面、查訪處所，以及查閱相關資料及文件。收集所得的證據會作為在巡查期間所發現不足之處的審查線索。

88. 管理局會擬備巡查報告，載述巡查結果。在報告定稿前，管理局會與系統營運者討論巡查期間的發現，以取得系統營運者的回應以作考慮。其後報告會概述巡查結果或關注事項，並會就補救措施提出建議。系統營運者須在管理局指明的時限內，糾正在巡查中發現的不合規事宜，以及內部控制的不足之處。

V.2 非實地監察

89. 非實地監察是監督系統營運者的方法之一，屬管理局監督方法的核心。根據《條例》第19A條，管理局有權要求系統營運者在管理局發出的書面通知指明的期限內，出示任何根據《條例》須予備存的紀錄或任何由系統營運者管有或控制的紀錄，以供查閱。

90. 管理局會透過非實地監察定期向系統營運者收集有關積金易平台的資料，包括（但不限於）業務計劃、控制／風險管理政策、資源安排、系統表現統計數字、交易量、系統變更、持續業務運作計劃、投訴及相關統計數字、服務達標水平。

91. 管理局亦可要求系統營運者適時提供補充資料，以配合非實地監察及其他分析。有關資料可包括系統營運者的財務數據、調查、積金易平台的質素保證／合規安排檢討、風險管理報告、內部或外聘核數師報告及管理局要求提供與系統營運者表現有關的自我評估。

92. 另外，管理局會與系統營運者的高級管理人員定期聯繫（例如會面），瞭解其運作模式、最新計劃及業務方案、事故、科技發展，以及上述活動引致的風險，以適時識別和評估該等活動涉及的風險。

93. 系統營運者迅速及準確匯報上述監督資料，有助提升管理局規管監督框架的效能。就此而言，管理局能更有效地根據監督標準下的安全及效率規定，全面審視系統營運者的表現。如出現任何不符合資料要求的情況，管理局均會作出密切調查及跟進。

94. 如管理局得悉有任何缺失、錯誤、內部控制措施失效、不合規事宜等，管理局可向系統營運者發出書面通知，指示系統營運者在指明時限內糾正有關事宜，並達致管理局滿意的程度。

V.3 匯報重大事件／事故

95. 按照一般指導，系統營運者應向管理局匯報(i)系統營運者合理地相信會導致核准受託人違反《條例》或其註冊計劃的管限規則的任何事件，惟所須匯報的事件，只限於涉及系統營運者作為其根據《條例》第19K(1)(b)條所提供計劃管理服務的一部分而管理的註冊計劃；或(ii)系統營運者在因應管理局行使《條例》第6E(1)(ec)條下的職能或遵照管理局根據《條例》第6H條發出的任何指引而提供計劃管理服務時得悉，《條例》第19I(1)條提述的電子強積金系統出現任何系統故障，而系統營運者合理地相信有關故障會影響核准受託人履行其職責。

96. 除第95段所述系統營運者的匯報責任外，系統營運者應匯報以下各類與計劃管理服務有關的事件／事故：

(a) 由系統營運者或核准受託人引起的事件，導致違反運作守則或服務協議，並可能會對計劃成員的利益造成重大不利影響（例如財政影響），或對積金易平台的管理及運作構成風險。

(b) 違反不屬於第95段所述的其他法定及監管規定，例如資料保障法例及《打擊洗錢及恐怖分子資金籌集條例》（第615章）。

(c) 涉及下列情況的運作事故（但不屬於第95段所述的事故）：

(i) 對參與僱主或計劃成員造成不利財政影響；

(ii) 可能引起傳媒或社交媒體關注的事故；

(iii) 欺詐及疏忽，包括職員的欺詐／不當行為；

(iv) 對某個組別的參與僱主或計劃成員造成影響；

(v) 資料遺失或洩漏，而事件性質可能會導致系統營運者、核准受託人及／或管理局蒙受重大信譽風險；

(vi) 懷疑或已確認的網絡攻擊，並可能導致系統營運者或積金易平台使用者的敏感資料（包括但不限於個人資料）遺失或洩漏；或

(vii) 違反管理局根據《條例》第6H條發出的指引，或違反管理局根據《條例》第6E(1)(ec)(ii)條發出的指示或指令。

97. 系統營運者應在得悉事件或事故後的三個指明工作日內，向管理局匯報事件或事故。有關報告應以書面擬備，概述所匯報事件或事故的關鍵事實、原因及影響，以及系統營運者在處理該事件或事故時已經或將會採取的措施。

V.4 第三方保證報告

98. 除以實地巡查及非實地監察的方式進行監督外，管理局可要求系統營運者提交管理局為履行或行使其在《條例》或附屬法例下的職能、職責及權力而可能需要的第三方保證報告。

99. 系統營運者或透過其承辦商須就內部控制定期提交一份與控制目標（在《強積金（一般）規例》第39條訂明）有關的獨立核數師評估報告，而

此項規定適用於由系統營運者提供計劃管理服務的情況。管理局亦可要求系統營運者就本規管監督框架第IV.2及IV.3部所載的規定提交獨立核數師評估報告。評估報告將利便管理局評核系統營運者或承辦商有否實施有效的內部控制，以履行其提供計劃管理服務的職責，以及符合本規管監督框架第IV.2及IV.3部所載的規定。

100. 為配合系統營運者的監督工作，管理局亦可要求系統營運者就任何會對積金易平台的管理及運作構成風險的事件或事故提交第三方保證報告。

101. 如有需要，管理局可聯同系統營運者的高級管理人員，與核數師或提供第三方保證報告的有關各方會面，討論因審計或第三方保證報告所引起的事宜。

V.5 管理局的跟進行動

102. 根據《條例》第6E(1)(ec)條，管理局獲賦權監督電子強積金系統的運作，包括向系統營運者及核准受託人，發出管理局認為對保障該系統的完整及穩定屬適當的指示或指令。基於這項規定，管理局可向系統營運者提出建議，以便系統營運者符合規管監督框架下的規定（如適用）。系統營運者應在切實可行的範圍內盡快依循建議行事，而管理局會密切監察系統營運者執行建議的情況。

103. 如系統營運者拒絕或沒有在管理局指明的時限內執行其提出的任何建議，管理局可考慮根據《條例》第6E(1)(ec)條發出指示，指明系統營運者在指明期限內所須採取的行動。若管理局認為會出現對積金易平台的管理及運作構成風險的情況（例如系統營運者沒有遵守管理局發出的指示），管理局可考慮對系統營運者採取其他行動（例如把有關事宜提升至系統營運者董事局的層面處理）。