編號	260911	金融科技

國際：IOSCO 與 BIS 之 CPMI 共同發布金融市場基礎設施網路韌性工具包（9/8）

■ 國際證券管理機構組織（IOSCO）與國際清算銀行（BIS）之支付與金融市場基礎設施委員會（Committee on Payments and Market Infrastructure, CPMI）共同發布「金融基礎設施（FMIs）實用考量之網路韌性工具包 (Cyber Resilience Toolkit: Practical Considerations for FMIs)」，內容係配合 IOSCO「金融市場基礎設施準則（Principles for Financial Market Infrastructures, PFMI）」[註1]，並參考 2016 年發布之「金融市場基礎設施網路安全指南(Guidance on Cyber Resilience for Financial Market Infrastructures）」[註2]，涵蓋 4 項提升 FMIs 網路安全韌性之考量重點。

- 網路安全風險與韌性管理

  工具包旨在協助 FMIs 加強網路安全韌性架構管理，並對其董事會成員及負責網路安全與韌性之高階管理人員之培訓提出實質建議。此外，提供關於如何管理系統風險，及如何使用風險管理指標和模型來評估和產出有效性與適用性之見解報告。

- 情境識別與設計

  工具包提供實用建議，用於開發網路安全情境，從確定目標及範圍開始，深入瞭解特定 FMIs 對產生威脅情報之環境與情形，其相關情境設計需對極端情境因素及壓力測試提出方法。

- 因應修復及重啟計畫

  基於 FMIs 生態系統可能遭受攻擊風險，擬具計畫應包括應對、回復與重啟 3 項程序，重點包括：

  - ✓ 制定應變計畫(Contingency planning)，在確保目標恢復前提下評估對生態系統之影響與作用；

- ✓ 制定標準程序，在必要時安全地隔離或阻止第三方連結，防止風險擴散至整體生態系統；
- ✓ 建立機制，以便及時通知生態系統相關單位，關於重啟連接之步驟及條件。

➢ 測試與演練

工具包對關鍵風險評估(CRF)測試項目中，各項測試和演練類型，提供如何開發網路彈性測試計畫，以及在各種情境中準備和執行測試與預演之實用建議。

■ IOSCO 對 FMIs 所依賴第三方服務提供商，可能對金融體系之關鍵運作產生風險管理與挑戰之諮詢文件提出，包括：日趨複雜和關連性增加之生態系統、第三方服務提供商過於集中、供應鏈之複雜與不透明性、退出計畫之困難、議價能力之不平衡及監管與審查方面之差異等 6 面向，對外徵詢意見至 12 月 1 日，以作為制定標準及風險管理規畫之參考。

註1：2012 年 4 月由 CPMI 與 IOSCO 共同發布，提供金融市場基礎設施（FMI）營運指導，以提升資訊透明度及金融穩定性。內容涵蓋 24 項準則及 5 項主管機關職責，適用對象包括支付系統(PS)、集中保管機構(CSD)、證券結算系統(SSS)及集中交易對手(CCP)與 FMI 共同完成市場交易之結算與記錄等。詳細內容請參閱 IOSCO 網站，網址：https://www.iosco.org/about/?subSection=cpmi_iosco&subSection1=pfmi。

註2：指南旨在協助 FMI 防範網路攻擊、迅速且有效應對網路攻擊以及在被攻擊後更迅速且安全地執行回復能力。主要包括 5 項關鍵：(1) FMI 之董事會與高階管理層對網路韌性之策略及重視程度至關重要；(2)在遭受網路攻擊後，能否迅速安全地恢復營運；(3) FMI 應使利用高品質的資安威脅情報及嚴格的網路系統測試；(4) 金融機構應致力於培養網路風險意識文化，並在組織內部各層面持續評估和提升網路韌性；(5) 網路韌性並非倚靠單一 FMI 來實現；須由金融體系生態系統共同努力。

資料來源：國際證券管理機構組織 IOSCO