SWIFT CSCF v2026 • Control 7.3A

SWIFT CSCF v2026 Control 7.3A 滲透測試準備檢查清單

1. 依後果界定範圍

- ☐ 已完成 SWIFT 環境的資產盤點 (安全區、訊息介面、操作員工作站、與網路的連線，以及供應這些系統的後台系統)。
- ☐ 攻擊路徑是依遭入侵後的後果排序，而非依測試的難易程度排序。
- ☐ 範圍是以安全區及其信任邊界來界定，使測試能證明攻擊者無法從後台橫向移動進入訊息層。
- ☐ 測試已依三年情境週期規劃，涵蓋應用程式、基礎設施與人員路徑。

2. 以威脅情資建構

- ☐ 針對鎖定金融訊息之攻擊者的最新情資，已納入測試情境。
- ☐ 情境演練的是合理且有具體命名的入侵路徑，而非籠統的弱點類別。
- ☐ 情資依據已記錄在案，使該測試符合 DORA 與 OSFI B-13 所稱的威脅導向測試。

3. 以最嚴格的標準執行

- ☐ 測試同時從系統邊界的內部與外部執行，符合 NYDFS Part 500 的期望。
- ☐ 測試由具備能力且足夠獨立的一方執行。
- ☐ 針對測試運行中系統的交戰規則、授權與安全控制，皆已記錄並核准。
- ☐ 已設定並記錄明確的執行頻率，同時滿足 NYDFS 的年度最低要求與 SWIFT 週期。

4. 衡量自身的防禦能力

- ☐ 此演練不僅衡量發現了什麼，也衡量監控是否偵測到模擬入侵。
- ☐ 回應與圍堵的表現，是對照偵測與回應職能來記錄。
- ☐ 偵測缺口本身即列為獨立的發現事項。

5. 收尾並留存證據

- ☐ 發現事項進入有負責人與期限的可追蹤修補週期。
- ☐ 修補完成是以證據佐證，而非僅憑聲稱。
- ☐ 完整紀錄 (範圍、情境、攻擊敘事、發現事項、修補、偵測表現) 以 NIST CSF 2.0 為主軸，僅歸檔一次。
- ☐ 該單一紀錄分別標註至各法規 (SWIFT 7.3A、DORA、NYDFS Part 500、OSFI B-13)。

想為您的機構取得評分嗎。Cambridge Cyber International 依此標準執行 SWIFT CSP 評核與 7.3A 滲透測試，並將發現事項驗證至完成。請在您的認證申報期開始前，預約一次範圍界定的洽談。

contact@cambridgecyberinternational.com • cambridgecyberinternational.com/zh-tw/contact/