SWIFT CSCF v2026 / Control 7.3A

一次測試，多方滿足：將 SWIFT CSCF v2026 7.3A 滲透測試作為跨法制演練

Cambridge Cyber International / 2026

在 SWIFT 客戶安全計劃的 2026 年週期中，Control 7.3A（滲透測試）載有社群驅動的指引，為一家連線機構在滾動式三年週期內所應達到的測試範圍與測試情境設定了標準（SWIFT 2025）。孤立地讀，這只是又一條待滿足的聲明項目。但對照更廣的監管景觀來讀，它便是單一行進方向的證據：歐洲聯盟、美國與加拿大的監管機關正趨同於情報導向、威脅知情的測試，視其為一家機構證明其控制確實有效（而非僅僅存在）的方式。本文主張，一家為 7.3A 滲透測試做準備的機構，應將該測試一次設計到位、達到當前最高水準，並就同一份證據同時收穫對數位營運韌性法（DORA）、第二號網路與資訊安全指令（NIS2）、紐約州金融服務署網路安全規則（23 NYCRR Part 500）以及金融機構監理署 B-13 指引的滿足，並以美國國家標準暨技術研究院網路安全框架 2.0 版（NIST CSF 2.0）作為共同主幹。

以勾選框心態讀 7.3A 的問題

一家將每套法制視為各自獨立義務的連線機構，會付出結構性的代價。它將 SWIFT 滲透測試的範圍窄化至安全區域，另行委託一次 DORA 韌性測試，回答一份關於年度測試的 NYDFS 問卷，再按第四套時程為加拿大監管機關準備證據。每一次委託都重複同樣的偵察、同樣的交戰規則、同樣的補救週期，而每一次所產出的證據，其形態都不為下一套法制所接受。代價不僅是金錢。零碎的測試產出零碎的風險圖像，因為沒有任何單一演練能像真實對手那樣看待這家機構：端到端，橫跨後台、操作員工作站、訊息傳遞介面，以及通往網路的連線。

此處的主張是，如今橫跨各主要法制可見的趨同，已使零碎的做法過時。7.3A 指引、DORA 的威脅導向測試體制、OSFI 的情報導向期待，以及 NYDFS 的年度強制要求，並非四種不同的測試。它們是同一理念的四種監管表述，而一家依其中最嚴苛者進行設計、並就共享框架記錄結果的機構，便能將其餘者的滿足作為附帶產物獲得。

SWIFT CSCF v2026 Control 7.3A 如今的期待

Control 7.3A 在客戶安全控制框架中屬於建議性控制，其目標是透過辨識可能導致安全區域或後台遭入侵的弱點，來驗證使用者 SWIFT 相關基礎設施的營運韌性（SWIFT 2025）。2026 年變動的實質並非一個新的控制編號，而是對測試應如何界定範圍、應涵蓋哪些情境的更銳利指引。框架如今闡明了一組應在三年週期內演練的測試情境，使一家機構無法以每年重複一次窄範圍的外部掃描來滿足該控制。其期待是，在整個週期內，該計劃涵蓋訊息傳遞介面及相關元件的應用層測試、安全區域及其分段的基礎設施測試，以及真實入侵所利用的人員與操作員工作站路徑。

由此引出兩項設計後果。第一，範圍必須對照安全區域及其信任邊界來界定，而非對照一個方便的網路範圍，因為該控制的目的是要證明攻擊者無法從後台樞轉進入訊息傳遞層。第二，測試必須由有能力且具備充分獨立性的一方進行，且其發現必須饋入一個受追蹤的補救週期，而該週期的結案本身即為證據。對某些架構類型而言，該控制屬建議性而非強制性，但對自我聲明遵循的機構，評估者會期待看見範圍、方法、發現與補救構成一份連貫的紀錄，而非一紙證書。

四套毗鄰的法制

DORA 與威脅導向滲透測試

數位營運韌性法要求所有在範圍內的金融實體定期測試其資訊與通訊科技系統，並要求其中屬重要實體的子集至少每三年以威脅導向滲透測試（TLPT）方式進行進階測試（European Parliament and Council 2022a）。TLPT 是情報驅動的：一場針對線上生產系統、以真實威脅行為者的戰術、技術與程序為藍本、在某一方法論下進行的受控紅隊模擬，而 TIBER-EU 框架是該方法論的歐洲參照（European Central Bank 2018）。一家以威脅導向標準準備 7.3A 測試、並以當前威脅情報構築其情境的機構，已在建構一次 DORA

測試的主幹，主要差別在於正式範圍，以及環繞著一次指定 TLPT 的監管治理。

NIS2 與特別法的劃出

第二號網路與資訊安全指令提高了基本與重要實體在網路安全風險管理與事件通報上的基準線，而各國主管機關在 2026 年間從轉置邁入了積極監督（European Parliament and Council 2022b；European Commission 2025）。對金融實體而言，實務要點在於優先順序：DORA 為特別法，而 NIS2 第 4 條在金融部門規則至少同等時讓位於它。因此一家機構應將 DORA 視為運作中的韌性測試法制，同時認知到金融邊界之外的集團實體（例如一家共用的科技子公司）可能仍處於 NIS2 之內，並能受益於同一份測試證據。

美國：NYDFS Part 500 與 FFIEC 期待

紐約州金融服務署網路安全規則要求每一家受涵蓋實體，依該實體的風險評估，至少每年從系統邊界的內外兩側對其資訊系統進行滲透測試（New York State Department of Financial Services 2023）。修訂後的規則進一步收緊了治理與測試期待（Ropes and Gray 2026）。在聯邦層級，聯邦金融機構檢查委員會並未課以固定規則，而是在其資訊安全手冊中，將由合格、獨立各方進行的滲透測試視為一項檢查者期待與一個成熟度指標（Federal Financial Institutions Examination Council 2016）。一家以高標準滿足 7.3A、按既定節奏從邊界內外兩側進行測試的機構，所產出的正是 NYDFS 檢查者與一次 FFIEC 檢查所期待的產物。

加拿大：OSFI B-13 指引

金融機構監理署 B-13 指引自 2024 年 1 月 1 日起生效，要求受聯邦監理的金融機構透過定期測試辨識弱點，而對科技足跡龐大的機構，它期待情報導向、威脅導向的滲透測試與模擬真實多階段攻擊的紅隊演練（Office of the Superintendent of Financial Institutions 2022）。B-13 以成果為本且未設固定節奏，因此機構是透過其測試的品質與真實性、而非其頻率來證明遵循。這與 DORA 及銳化後的 7.3A 指引所表述的，是同一套情報導向標準，這使 B-13 成為同一家族的加拿大成員，而非一項獨立義務。

一條主幹：將各法制對應至 NIST CSF 2.0

沒有任何單一金融監管機關同時治理美國與加拿大，因此一家跨境機構需要一個在兩地皆受認可的中立參照。NIST 網路安全框架 2.0 版正是該參照：自願性、在邊界兩側皆獲廣泛採用，並圍繞六項職能組織起來，即治理（Govern）、辨識（Identify）、保護（Protect）、偵測（Detect）、應變（Respond）與復原（Recover）（National Institute of Standards and Technology 2024）。用作主幹，它讓一家機構得以記錄一套滲透測試計劃，並以每套法制都能理解的詞彙表述結果。滲透測試最直接地對應到辨識（透過浮現弱點），以及偵測與應變（透過衡量機構的監控與應變是否真能捕捉並遏制一次真實入侵）。治理職能承載著五套法制皆要求的交戰規則、獨立性與董事會報告。表 1 將這份趨同具體化。

表 1. 一套滲透測試計劃，四套法制，一條主幹

面向	SWIFT 7.3A v2026	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
性質	建議性控制	對重要實體為強制	強制規則	以成果為本的期待	自願性參照
節奏	3 年情境週期	至少每 3 年	至少每年	無固定節奏	未予規定
方法	情境導向，聚焦安全區域	情報導向紅隊	內外兼顧，以風險為本	情報導向，紅隊	職能與成果
獨立性	有能力的獨立一方	經認可的供應商	合格的內部或外部	獨立保證	治理成果
主要證據	範圍、發現、補救	威脅情境、攻擊敘事、補救	測試報告、補救節奏	測試的真實性與成果	已對應的成果

逐列橫讀，便是本文的論點：將測試設計到每一欄中最嚴苛的標準，即情報導向的方法、知曉安全區域的範圍、內外兼顧

的涵蓋、獨立的執行、受追蹤的補救，而由此產生的單一紀錄，便滿足全部五者。

一套風險導向的準備模型

7.3A
指引邀請一種合規式的讀法，亦即機構只做該控制所點名的最低限度。更有價值、也是監管機關日益獎賞的讀法，是風險導向的：滲透測試是用以浮現並退役機構最具後果之暴險的工具，而合規是把這件事做好後的附帶產物。

準備始於一條風險與範圍的基準線。機構盤點其 SWIFT
相關資產，即安全區域、訊息傳遞介面、操作員工作站、通往網路的連線，以及饋入其中的後台系統，並依遭入侵的後果而非依測試的難易來為各路徑排序。這產出一個由金錢與信任所在之處所界定的範圍，這也是真實對手會選擇的範圍，並與 B-13 以後果為本的姿態及 NYDFS 以風險為本的姿態一致。

接著是威脅情報的構築。關於鎖定金融訊息傳遞之行為者的當前情報塑造了情境，使測試演練的是合理的入侵而非通用的入侵。這是把滲透測試轉化為威脅導向測試的一步，也是使同一演練在 DORA 與 B-13 之下可採信的一步。

執行則在 7.3A
指引所描述的三年週期內跑完各情境，涵蓋應用、基礎設施與人員路徑，從邊界內外兩側，由一個獨立的一方，在有文件依據的交戰規則下進行。機構不僅衡量找到了什麼，更衡量其自身的偵測與應變是否看見了測試的發生，因為那份衡量正是偵測與應變職能所要求的證據。

最後，補救與證據閉合迴圈。發現進入一個受追蹤的補救週期，其結案被記錄下來，而整份紀錄，即範圍、情境、攻擊敘事、發現、補救與偵測表現，一次性歸檔於 NIST CSF 2.0
主幹之上，並標記至每一套法制。完成此迴圈的機構並非通過了一次測試，而是建立了一項可重複使用的韌性證據資產。

本公司的 SWIFT CSP 評估服務會依此標準界定範圍並執行 7.3A 測試，而 PenTeva
則驗證並追蹤發現直至結案，使證據在四套法制中任一者之下都站得住腳。在 DORA
韌性建模處於範圍內時，DORA-MAST 會將同一份證據帶入營運韌性的圖像之中。

結論

銳化後的 7.3A 指引，最好不要理解為一項孤立的 SWIFT
要求，而要理解為一場邁向情報導向、威脅知情測試之全球運動的單一監管表述。一家將其 2026
年滲透測試設計到該標準、依後果界定範圍、以當前威脅情報構築框架、橫跨安全區域獨立執行、並就共享框架記錄結果的機構，便能以同一次演練滿足 DORA、仍適用之處的 NIS2、NYDFS Part 500 與 OSFI
B-13。滲透測試不再是一項反覆出現的合規成本，而成為機構藉以找出並退役要緊風險的工具。一次測試，多方滿足。

縮寫

CSCF，客戶安全控制框架（SWIFT）。CSP，客戶安全計劃（SWIFT）。DORA，數位營運韌性法。FFIEC，聯邦金融機構檢查委員會。ICT，資訊與通訊科技。NIS2，網路與資訊安全指令（第二號）。NIST
CSF，國家標準暨技術研究院網路安全框架。NYDFS，紐約州金融服務署。OSFI，金融機構監理署。SWIFT，環球銀行金融電信協會。TIBER-EU，威脅情報導向的道德紅隊演練（歐洲框架）。TLPT，威脅導向滲透測試。

參考文獻

European Central Bank (2018). TIBER-EU Framework.
https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

European Commission (2025). NIS2 Directive: transposition in EU countries.

https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

European Parliament and Council (2022a). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj

European Parliament and Council (2022b). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Federal Financial Institutions Examination Council (2016). Information Technology Examination Handbook: Information Security. https://ithandbook.ffiec.gov/it-booklets/information-security/

National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

New York State Department of Financial Services (2023). Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Part 500 (as amended). https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

Office of the Superintendent of Financial Institutions (2022). Guideline B-13: Technology and Cyber Risk Management. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management

Ropes and Gray (2026). NYDFS-regulated entities face stronger cybersecurity regulations. https://www.ropesgray.com/en/insights/alerts/2026/01/nydfs-regulated-entities-face-stronger-cybersecurity-regulations

SWIFT (2025). Customer Security Controls Framework v2026, Customer Security Programme. https://www.swift.com/myswift/customer-security-programme-csp