SWIFT CSCF v2026 / Control 7.3A

Testa una volta, soddisfa molti: il penetration test SWIFT CSCF v2026 7.3A come esercizio trasversale ai regimi

Cambridge Cyber International / 2026

Dal ciclo 2026 dello SWIFT Customer Security Programme, il Controllo 7.3A (Penetration Testing) porta con sé una guida elaborata dalla comunità che stabilisce il perimetro e gli scenari di test attesi da un'istituzione connessa nell'arco di un ciclo triennale continuo (SWIFT 2025). Letto in isolamento, è una riga di attestazione in più da soddisfare. Letto a fronte del più ampio panorama regolatorio, è la prova di un'unica direzione di marcia: le autorità di vigilanza dell'Unione europea, degli Stati Uniti e del Canada stanno convergendo sul testing guidato dall'intelligence e informato dalle minacce come modo in cui un'istituzione prova che i suoi controlli funzionano anziché limitarsi a esistere. Questo articolo sostiene che un'istituzione che si prepara al penetration test 7.3A dovrebbe progettare quel test una volta sola, secondo uno standard allo stato dell'arte, e raccogliere le stesse prove a fronte del Digital Operational Resilience Act (DORA), della seconda direttiva sulla sicurezza delle reti e dell'informazione (NIS2), della regolamentazione sulla cybersicurezza del New York State Department of Financial Services (23 NYCRR Part 500) e della Guideline B-13 dell'Office of the Superintendent of Financial Institutions, usando il Cybersecurity Framework versione 2.0 del National Institute of Standards and Technology degli Stati Uniti (NIST CSF 2.0) come colonna vertebrale comune.

Il problema di una lettura del 7.3A come casella da spuntare

Un'istituzione connessa che tratta ogni regime come un obbligo separato paga una penalità strutturale. Definisce il perimetro di un penetration test SWIFT in modo ristretto alla zona sicura, commissiona un separato test di resilienza DORA, risponde a un questionario NYDFS sul testing annuale e prepara prove per un'autorità di vigilanza canadese secondo un quarto calendario. Ogni ingaggio ripete la stessa ricognizione, le stesse regole di ingaggio, lo stesso ciclo di rimedio, e ciascuno produce prove in una forma che il regime successivo non accetta. Il costo non è solo economico. Un testing frammentato produce un quadro frammentato del rischio, perché nessun singolo esercizio vede l'istituzione come la vedrebbe un vero avversario: da un capo all'altro, attraverso il back office, le postazioni di lavoro degli operatori, l'interfaccia di messaggistica e la connessione alla rete.

L'argomento qui è che la convergenza ora visibile tra i principali regimi rende obsoleto l'approccio frammentato. La guida 7.3A, il regime di testing guidato dalle minacce di DORA, l'aspettativa guidata dall'intelligence di OSFI e il mandato annuale di NYDFS non sono quattro test diversi. Sono quattro espressioni di vigilanza di un'unica idea, e un'istituzione che progetta secondo il più esigente di essi, e registra il risultato a fronte di un framework condiviso, può soddisfare gli altri come sottoprodotto.

Cosa attende ora il Controllo 7.3A di SWIFT CSCF v2026

Il Controllo 7.3A si colloca nel Customer Security Controls Framework come controllo consultivo il cui obiettivo è convalidare la resilienza operativa dell'infrastruttura legata a SWIFT dell'utente, individuando le vulnerabilità che potrebbero condurre a una compromissione della zona sicura o del back office (SWIFT 2025). La sostanza del cambiamento del 2026 non è un nuovo numero di controllo, ma una guida più netta su come il test dovrebbe essere perimetrato e quali scenari dovrebbe coprire. Il framework ora articola un insieme di scenari di test da esercitare nell'arco di un ciclo triennale, così che un'istituzione non possa soddisfare il controllo con una singola scansione esterna ristretta ripetuta annualmente. L'aspettativa è che, nell'arco del ciclo, il programma copra il testing a livello applicativo dell'interfaccia di messaggistica e dei componenti correlati, il testing infrastrutturale della zona sicura e della sua segmentazione, e i percorsi umani e delle postazioni di lavoro degli operatori che le vere intrusioni sfruttano.

Ne derivano due conseguenze di progettazione. Primo, il perimetro deve essere definito a fronte della

zona sicura e dei suoi confini di fiducia anziché a fronte di un comodo intervallo di rete, perché lo scopo del controllo è provare che un attaccante non possa spostarsi dal back office allo strato di messaggistica. Secondo, il test deve essere condotto da una parte competente e sufficientemente indipendente, e le sue risultanze devono alimentare un ciclo di rimedio tracciato la cui chiusura è essa stessa una prova. Il controllo è consultivo anziché obbligatorio per ogni tipo di architettura, ma per le istituzioni che si autoattestano a fronte di esso, il valutatore si aspetterà di vedere perimetro, metodo, risultanze e rimedio come un record coerente, non come un certificato.

I quattro regimi vicini

DORA e il penetration testing guidato dalle minacce

Il Digital Operational Resilience Act richiede a tutte le entità finanziarie in ambito di testare regolarmente i propri sistemi di tecnologia dell'informazione e della comunicazione, e richiede al sottoinsieme delle entità significative di eseguire un testing avanzato per mezzo del threat-led penetration testing (TLPT) almeno ogni tre anni (European Parliament and Council 2022a). Il TLPT è guidato dall'intelligence: una simulazione controllata di red team contro sistemi di produzione attivi, modellata sulle tattiche, tecniche e procedure di veri attori delle minacce, condotta secondo una metodologia per la quale il framework TIBER-EU è il riferimento europeo (European Central Bank 2018). L'istituzione che prepara un test 7.3A secondo uno standard guidato dalle minacce, con l'intelligence sulle minacce attuali a plasmare i suoi scenari, sta già costruendo la colonna vertebrale di un test DORA, differendo principalmente nel perimetro formale e nella governance di vigilanza che avvolge un TLPT designato.

NIS2 e l'esclusione di tipo lex specialis

La seconda direttiva sulla sicurezza delle reti e dell'informazione alza la soglia di base per la gestione del rischio di cybersicurezza e la segnalazione degli incidenti tra le entità essenziali e importanti, e le autorità nazionali sono passate dal recepimento alla vigilanza attiva nel corso del 2026 (European Parliament and Council 2022b; European Commission 2025). Per le entità finanziarie il punto pratico è di precedenza: DORA è lex specialis, e l'articolo 4 della NIS2 le cede il passo laddove le regole del settore finanziario siano almeno equivalenti. Un'istituzione dovrebbe quindi trattare DORA come il regime operativo di testing della resilienza, pur riconoscendo che le entità del gruppo al di fuori del perimetro finanziario, come una controllata tecnologica condivisa, possono restare all'interno della NIS2 e beneficiare delle stesse prove di testing.

Stati Uniti: NYDFS Part 500 e aspettative FFIEC

La regolamentazione sulla cybersicurezza del New York State Department of Financial Services richiede a ciascuna entità coperta di condurre penetration testing dei propri sistemi informativi almeno annualmente, sia dall'interno sia dall'esterno dei confini dei sistemi, sulla base della valutazione del rischio dell'entità (New York State Department of Financial Services 2023). La regolamentazione emendata ha ulteriormente irrigidito le aspettative in materia di governance e di testing (Ropes and Gray 2026). A livello federale, il Federal Financial Institutions Examination Council non impone una regola fissa ma tratta il penetration testing da parte di soggetti qualificati e indipendenti come un'aspettativa dell'esaminatore e un indicatore di maturità all'interno del suo Information Security booklet (Federal Financial Institutions Examination Council 2016). L'istituzione che soddisfa il 7.3A secondo uno standard elevato, testando sia dall'interno sia dall'esterno del confine con una cadenza definita, produce esattamente gli artefatti che un esaminatore NYDFS e un esame FFIEC si aspettano.

Canada: OSFI Guideline B-13

La Guideline B-13 dell'Office of the Superintendent of Financial Institutions, in vigore dal 1 gennaio 2024, richiede alle istituzioni finanziarie regolate a livello federale di individuare le vulnerabilità tramite test regolari, e per le istituzioni con impronte tecnologiche significative si attende penetration testing guidato dall'intelligence e dalle minacce ed esercizi di red team che simulano attacchi realistici a più fasi (Office of the Superintendent of Financial Institutions 2022). La B-13 è basata sui risultati e non fissa alcuna cadenza prestabilita, quindi l'istituzione comprova la conformità attraverso la qualità e il realismo del proprio testing anziché la sua frequenza. È lo stesso standard guidato dall'intelligence che DORA e la guida affinata del 7.3A esprimono, il che rende la B-13 il membro canadese della stessa famiglia anziché un obbligo separato.

Una colonna vertebrale: mappare i regimi su NIST CSF 2.0

Nessun singolo regolatore finanziario governa sia gli Stati Uniti sia il Canada, quindi un'istituzione transfrontaliera ha bisogno di un riferimento neutrale riconosciuto in entrambi. Il NIST Cybersecurity Framework versione 2.0 è quel riferimento: volontario, ampiamente adottato su entrambi i lati del confine e organizzato attorno a sei funzioni, Govern, Identify, Protect, Detect, Respond e Recover (National Institute of Standards and Technology 2024). Usato come colonna vertebrale, consente a un'istituzione di registrare un solo programma di penetration test ed esprimere il risultato nel vocabolario che ogni regime comprende. Il penetration test parla in modo più diretto a Identify, facendo emergere le vulnerabilità, e a Detect e Respond, misurando se il monitoraggio e la risposta dell'istituzione effettivamente colgono e contengono un'intrusione realistica. La funzione Govern porta le regole di ingaggio, l'indipendenza e la rendicontazione al consiglio che tutti e cinque i regimi richiedono. La Tabella 1 rende concreta la convergenza.

Tabella 1. Un programma di penetration test, quattro regimi, una colonna vertebrale

Dimensione	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Natura	Controllo consultivo	Obbligatorio per entità significative	Regola obbligatoria	Aspettativa basata sui risultati	Riferimento volontario
Cadenza	Ciclo di scenari triennale	Almeno ogni 3 anni	Almeno annuale	Nessuna cadenza fissa	Non prescritta
Metodo	Basato su scenari, focus sulla zona	Red team guidato dall'intelligence	Interno ed esterno, basato sul rischio	Guidato dall'intelligence,	Funzioni e risultati
Indipendenza	Parte competente e indipendente	Fornitori accreditati	Interno o esterno qualificato	Assurance indipendente	Risultato di governance
Prova principale	Perimetro, risultanze, rimedio	Scenari di minaccia, narrazione dell'attacco, rimedio	Rapporto di test, cadenza di rimedio	Realismo ed esito del test	Risultati mappati

La lettura lungo ciascuna riga è la tesi: progetta il test secondo lo standard più esigente in ciascuna colonna, metodo guidato dall'intelligence, perimetro consapevole della zona sicura, copertura interna ed esterna, esecuzione indipendente, rimedio tracciato, e il singolo record risultante soddisfa tutti e cinque.

Un modello di preparazione guidato dal rischio

La guida 7.3A invita a una lettura di conformità, in cui l'istituzione fa il minimo che il controllo nomina. La lettura più preziosa, e quella che le autorità di vigilanza premiano sempre più, è guidata dal rischio: il penetration test è lo strumento usato per far emergere e ritirare le esposizioni più consequenziali

dell'istituzione, e la conformità è il sottoprodotto del farlo bene.

La preparazione comincia con una linea di base di rischio e perimetro. L'istituzione inventaria il proprio patrimonio legato a SWIFT, la zona sicura, l'interfaccia di messaggistica, le postazioni di lavoro degli operatori, la connessione alla rete e i sistemi di back office che la alimentano, e classifica i percorsi in base alla conseguenza di una compromissione anziché alla facilità di testarli. Questo produce un perimetro definito da dove risiedono il denaro e la fiducia, che è anche il perimetro che un vero avversario sceglierebbe, e che si allinea con la postura guidata dalle conseguenze della B-13 e con la postura basata sul rischio di NYDFS.

Segue l'inquadramento dell'intelligence sulle minacce. L'intelligence attuale sugli attori che prendono di mira la messaggistica finanziaria plasma gli scenari, così che il test provi intrusioni plausibili anziché generiche. Questo è il passaggio che trasforma un penetration test in un test guidato dalle minacce, ed è il passaggio che rende lo stesso esercizio credibile sotto DORA e B-13.

L'esecuzione poi svolge gli scenari nell'arco del ciclo triennale che la guida 7.3A descrive, coprendo i percorsi applicativi, infrastrutturali e umani, dall'interno e dall'esterno del confine, a opera di una parte indipendente, secondo regole di ingaggio documentate. L'istituzione misura non solo cosa è stato trovato ma se il proprio rilevamento e la propria risposta hanno visto avvenire il test, perché quella misurazione è la prova che le funzioni Detect e Respond richiedono.

Infine, rimedio e prove chiudono il cerchio. Le risultanze entrano in un ciclo di rimedio tracciato la cui chiusura è registrata, e l'intero record, perimetro, scenari, narrazione dell'attacco, risultanze, rimedio e prestazioni di rilevamento, viene archiviato una sola volta a fronte della colonna vertebrale NIST CSF 2.0 e contrassegnato per ciascun regime. L'istituzione che completa questo cerchio non ha superato un test. Ha costruito un riutilizzabile bene probatorio di resilienza.

Il nostro servizio di valutazione SWIFT CSP perimetra ed esegue il test 7.3A secondo questo standard, e PenTeva convalida e traccia le risultanze fino alla chiusura, così che le prove reggano sotto uno qualsiasi dei quattro regimi. Laddove la modellazione della resilienza DORA sia in ambito, DORA-MAST porta le stesse prove nel quadro della resilienza operativa.

Conclusione

La guida affinata del 7.3A si comprende meglio non come un requisito SWIFT isolato ma come un'unica espressione di vigilanza di un movimento globale verso il testing guidato dall'intelligence e informato dalle minacce. Un'istituzione che progetta il suo penetration test 2026 secondo quello standard, ne perimetra l'ambito in base alle conseguenze, lo inquadra con l'intelligence sulle minacce attuali, lo esegue in modo indipendente attraverso la zona sicura e registra il risultato a fronte di un framework condiviso, può soddisfare DORA, la NIS2 dove ancora si applica, NYDFS Part 500 e OSFI B-13 dallo stesso esercizio. Il pen test smette di essere un costo di conformità ricorrente e diventa lo strumento attraverso cui l'istituzione trova e ritira i rischi che contano. Testa una volta, soddisfa molti.

Acronimi

CSCF, Customer Security Controls Framework (SWIFT). CSP, Customer Security Programme (SWIFT). DORA, Digital Operational Resilience Act. FFIEC, Federal Financial Institutions Examination Council. ICT, Information and Communication Technology. NIS2, Network and Information Security Directive (second). NIST CSF, National Institute of Standards and Technology Cybersecurity Framework. NYDFS, New York State Department of Financial Services. OSFI, Office of the Superintendent of Financial Institutions.

SWIFT, Society for Worldwide Interbank Financial Telecommunication. TIBER-EU, Threat Intelligence-Based Ethical Red Teaming (European framework). TLPT, Threat-Led Penetration Testing.

References

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