SWIFT CSCF v2026 / Control 7.3A

Einmal testen, viele erfüllen: der SWIFT CSCF v2026 7.3A Penetrationstest als regimeübergreifende Übung

Cambridge Cyber International / 2026

Aus dem Zyklus 2026 des SWIFT Customer Security Programme trägt Control 7.3A (Penetration Testing) von der Gemeinschaft getragene Vorgaben, die den Umfang und die erwarteten Testszenarien einer angebundenen Institution über einen rollierenden Dreijahreszyklus festlegen (SWIFT 2025). Isoliert gelesen ist dies eine weitere Attestierungszeile, die zu erfüllen ist. Gelesen vor dem breiteren regulatorischen Hintergrund ist es der Beweis einer einzigen Marschrichtung: Aufsichtsbehörden in der Europäischen Union, den Vereinigten Staaten und Kanada konvergieren auf nachrichtendienstlich geführtem, bedrohungsinformiertem Testen als dem Weg, auf dem eine Institution nachweist, dass ihre Kontrollen funktionieren statt bloß zu existieren. Dieser Artikel argumentiert, dass eine Institution, die sich auf den 7.3A-Penetrationstest vorbereitet, diesen Test einmal entwerfen sollte, nach einem Standard auf dem Stand der Technik, und denselben Nachweis gegen den Digital Operational Resilience Act (DORA), die zweite Network and Information Security Directive (NIS2), die Cybersicherheitsregulierung des New York State Department of Financial Services (23 NYCRR Part 500) und die Guideline B-13 des Office of the Superintendent of Financial Institutions ernten sollte, wobei das United States National Institute of Standards and Technology Cybersecurity Framework version 2.0 (NIST CSF 2.0) als gemeinsame Wirbelsäule dient.

Das Problem einer Häkchen-Lesart von 7.3A

Eine angebundene Institution, die jedes Regime als gesonderte Pflicht behandelt, zahlt eine strukturelle Strafe. Sie grenzt einen SWIFT-Penetrationstest eng auf die sichere Zone ab, beauftragt einen gesonderten DORA-Resilienztest, beantwortet einen NYDFS-Fragebogen zum jährlichen Testen und bereitet Nachweise für eine kanadische Aufsichtsbehörde nach einem vierten Zeitplan vor. Jeder Auftrag wiederholt dieselbe Aufklärung, dieselben Einsatzregeln, denselben Behebungszyklus, und jeder erzeugt Nachweise in einer Form, die das nächste Regime nicht akzeptiert. Die Kosten sind nicht nur finanzieller Art. Fragmentiertes Testen erzeugt ein fragmentiertes Risikobild, weil keine einzelne Übung die Institution so sieht, wie es ein echter Gegner täte: durchgängig, über das Back-Office, die Bedienerarbeitsplätze, die Messaging-Schnittstelle und die Anbindung an das Netz.

Das Argument hier lautet, dass die nun über die großen Regime hinweg sichtbare Konvergenz den fragmentierten Ansatz obsolet macht. Die 7.3A-Vorgaben, DORAs bedrohungsgeführtes Testregime, OSFIs nachrichtendienstlich geführte Erwartung und das jährliche NYDFS-Mandat sind nicht vier verschiedene Tests. Sie sind vier aufsichtsrechtliche Ausprägungen einer einzigen Idee, und eine Institution, die für die anspruchsvollste von ihnen entwirft und das Ergebnis gegen ein gemeinsames Rahmenwerk erfasst, kann die übrigen als Nebenprodukt erfüllen.

Was das SWIFT CSCF v2026 Control 7.3A nun erwartet

Control 7.3A sitzt im Customer Security Controls Framework als beratende Kontrolle, deren Ziel es ist, die operative Resilienz der SWIFT-bezogenen Infrastruktur des Nutzers zu validieren, indem Schwachstellen identifiziert werden, die zu einer Kompromittierung der sicheren Zone oder des Back-Office führen könnten (SWIFT 2025). Die Substanz der Änderung von 2026 ist keine neue Kontrollnummer, sondern schärfere Vorgaben dazu, wie der Test abzugrenzen ist und welche Szenarien er abdecken soll. Das Rahmenwerk artikuliert nun eine Reihe von Testszenarien, die über einen Dreijahreszyklus auszuüben sind, sodass eine Institution die Kontrolle nicht mit einem einzelnen engen externen Scan erfüllen kann, der jährlich wiederholt wird. Die Erwartung ist, dass das Programm über den Zyklus hinweg das Testen der Messaging-Schnittstelle und zugehöriger Komponenten auf Anwendungsebene, das Infrastrukturtesten der sicheren Zone und ihrer Segmentierung sowie die menschlichen und Bedienerarbeitsplatz-Pfade abdeckt, die echte Eindringlinge ausnutzen.

Zwei Entwurfskonsequenzen folgen. Erstens muss der Umfang gegen die sichere Zone und ihre Vertrauensgrenzen definiert werden statt gegen einen bequemen Netzbereich, denn der Zweck der Kontrolle ist es zu beweisen, dass ein Angreifer nicht vom Back-Office in die Messaging-Schicht pivotieren kann. Zweitens muss der Test von einer kompetenten und hinreichend unabhängigen Partei durchgeführt werden, und seine Befunde müssen einen nachverfolgten Behebungszyklus speisen, dessen Abschluss selbst Nachweis ist. Die Kontrolle ist beratend statt verpflichtend für jeden Architekturtyp, doch für Institutionen, die sich selbst gegen sie attestieren, wird der Prüfer erwarten, Umfang, Methode, Befunde und Behebung als kohärentes Dossier zu sehen, nicht als Zertifikat.

Die vier benachbarten Regime

DORA und der bedrohungsgeführte Penetrationstest

Der Digital Operational Resilience Act verlangt von allen erfassten Finanzunternehmen, ihre Informations- und Kommunikationstechnologiesysteme regelmäßig zu testen, und verlangt von der Teilmenge der bedeutenden Unternehmen, fortgeschrittenes Testen mittels eines bedrohungsgeführten Penetrationstests (TLPT) mindestens alle drei Jahre durchzuführen (European Parliament and Council 2022a). Der TLPT ist nachrichtendienstlich getrieben: eine kontrollierte Red-Team-Simulation gegen Live-Produktionssysteme, modelliert nach den Taktiken, Techniken und Vorgehensweisen echter Bedrohungsakteure, durchgeführt nach einer Methodik, für die das TIBER-EU-Rahmenwerk die europäische Referenz ist (European Central Bank 2018). Die Institution, die einen 7.3A-Test nach einem bedrohungsgeführten Standard vorbereitet, mit aktueller Bedrohungsaufklärung, die ihre Szenarien formt, baut bereits die Wirbelsäule eines DORA-Tests, der sich hauptsächlich im formalen Umfang und in der aufsichtsrechtlichen Governance unterscheidet, die einen ausgewiesenen TLPT umgibt.

NIS2 und die Lex-specialis-Ausnahme

Die zweite Network and Information Security Directive hebt das Grundniveau für das Cybersicherheits-Risikomanagement und die Meldung von Vorfällen über wesentliche und wichtige Einrichtungen hinweg an, und die nationalen Behörden gingen im Laufe von 2026 von der Umsetzung zur aktiven Aufsicht über (European Parliament and Council 2022b ; European Commission 2025). Für Finanzunternehmen ist der praktische Punkt einer des Vorrangs: DORA ist lex specialis, und Artikel 4 von NIS2 weicht ihr, wo die Regeln des Finanzsektors mindestens gleichwertig sind. Eine Institution sollte DORA daher als das maßgebliche Resilienz-Testregime behandeln und zugleich anerkennen, dass Konzerneinheiten außerhalb des Finanzperimeters, etwa eine geteilte Technologietochter, innerhalb von NIS2 bleiben und von demselben Testnachweis profitieren können.

Die Vereinigten Staaten: NYDFS Part 500 und FFIEC-Erwartungen

Die Cybersicherheitsregulierung des New York State Department of Financial Services verlangt von jeder erfassten Einheit, mindestens jährlich einen Penetrationstest ihrer Informationssysteme durchzuführen, sowohl von innerhalb als auch von außerhalb der Systemgrenzen, gestützt auf die Risikobewertung der Einheit (New York State Department of Financial Services 2023). Die geänderte Regulierung hat die Governance- und Testerwartungen weiter verschärft (Ropes and Gray 2026). Auf Bundesebene erlegt das Federal Financial Institutions Examination Council keine feste Regel auf, behandelt aber Penetrationstests durch qualifizierte, unabhängige Parteien als Prüfererwartung und Reifeindikator in seinem Information Security booklet (Federal Financial Institutions Examination Council 2016). Die Institution, die 7.3A auf hohem Standard erfüllt, indem sie von innerhalb wie von außerhalb der Grenze in einer definierten Taktung testet, erzeugt genau die Artefakte, die ein NYDFS-Prüfer und eine FFIEC-Prüfung erwarten.

Kanada: OSFI Guideline B-13

Die Guideline B-13 des Office of the Superintendent of Financial Institutions, in Kraft seit dem 1 January 2024, verlangt von bundesregulierten Finanzinstituten, Schwachstellen durch regelmäßiges Testen zu identifizieren, und für Institute mit erheblichem Technologie-Fußabdruck erwartet sie nachrichtendienstlich geführtes, bedrohungsgeführtes Penetrationstesten und Red-Team-Übungen, die realistische mehrstufige Angriffe simulieren (Office of the Superintendent of Financial Institutions 2022). B-13 ist ergebnisbasiert und setzt keine feste Taktung, sodass die Institution Compliance durch die Qualität und den Realismus ihres Testens statt durch dessen Häufigkeit nachweist. Dies ist derselbe nachrichtendienstlich geführte Standard, den DORA und die geschärften 7.3A-Vorgaben ausdrücken, was B-13 zum kanadischen Mitglied derselben Familie macht statt zu einer gesonderten Pflicht.

Eine Wirbelsäule: die Regime auf NIST CSF 2.0 abbilden

Kein einzelner Finanzregulator beherrscht sowohl die Vereinigten Staaten als auch Kanada, sodass eine grenzüberschreitende Institution eine neutrale, in beiden anerkannte Referenz benötigt. Das NIST Cybersecurity Framework version 2.0 ist diese Referenz: freiwillig, auf beiden Seiten der Grenze breit übernommen und um sechs Funktionen organisiert, Govern, Identify, Protect, Detect, Respond und Recover (National Institute of Standards and Technology 2024). Als Wirbelsäule genutzt, erlaubt es einer Institution, ein Penetrationstest-Programm zu erfassen und das Ergebnis im Vokabular auszudrücken, das jedes Regime versteht. Der Penetrationstest spricht am direktesten zu Identify, indem er Schwachstellen aufdeckt, und zu Detect und Respond, indem er misst, ob die Überwachung und Reaktion der Institution eine realistische Intrusion tatsächlich erfassen und eindämmen. Die Funktion Govern trägt die Einsatzregeln, die Unabhängigkeit und das Berichten an den Vorstand, die alle fünf Regime verlangen. Tabelle 1 macht die Konvergenz greifbar.

Tabelle 1. Ein Penetrationstest-Programm, vier Regime, eine Wirbelsäule

Dimension	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Natur	Beratende Kontrolle	Verpflichtend für bedeutende Unternehmen	Verpflichtende Regel	Ergebnisbasierte Erwartung	Freiwillige Referenz
Taktung	3-Jahres-Szenarien zyklus	Mindestens alle 3 Jahre	Mindestens jährlich	Keine feste Taktung	Nicht vorgeschrieben
Methode	Szenariobasiert, Fokus sichere Zone	Nachrichtendienstlich geführtes Red Team	Innen und außen, risikobasiert	Nachrichtendienstlich geführt, Red Team	Funktionen und Ergebnisse
Unabhängigkeit	Kompetente, unabhängige	Akkreditierte Anbieter	Qualifiziert intern oder extern	Unabhängige Assurance	Governance-Ergebnis
Primärnachweis	Umfang, Befunde, Behebung	Bedrohungsszenarien, Angriffsnarrativ, Behebung	Testbericht, Behebungstaktung	Realismus und Ergebnis des Tests	Abgebildete Ergebnisse

Die Lesart quer durch jede Zeile ist die These: entwerfen Sie den Test nach dem anspruchsvollsten Standard in jeder Spalte, nachrichtendienstlich geführte Methode, auf die sichere Zone bedachter Umfang, Innen- und Außenabdeckung, unabhängige Durchführung, nachverfolgte Behebung, und das eine daraus resultierende Dossier erfüllt alle fünf.

Ein risikogeführtes Vorbereitungsmodell

Die 7.3A-Vorgaben laden zu einer Compliance-Lesart ein, in der die Institution das Minimum tut, das die

Kontrolle benennt. Die wertvollere Lesart, und die, die Aufsichtsbehörden zunehmend belohnen, ist risikogeführt: der Penetrationstest ist das Instrument, mit dem die folgenreichsten Expositionen der Institution aufgedeckt und beseitigt werden, und Compliance ist das Nebenprodukt, wenn dies gut gemacht wird.

Die Vorbereitung beginnt mit einer Risiko- und Umfangs-Grundlinie. Die Institution inventarisiert ihren SWIFT-bezogenen Bestand, die sichere Zone, die Messaging-Schnittstelle, die Bedienerarbeitsplätze, die Anbindung an das Netz und die Back-Office-Systeme, die ihn speisen, und ordnet die Pfade nach der Konsequenz einer Kompromittierung statt nach der Leichtigkeit des Testens. Dies erzeugt einen Umfang, der dadurch definiert ist, wo das Geld und das Vertrauen sitzen, was zugleich der Umfang ist, den ein echter Gegner wählen würde, und der sich an der konsequenzgeführten Haltung von B-13 und der risikobasierten Haltung von NYDFS ausrichtet.

Als Nächstes kommt die Rahmung durch Bedrohungsaufklärung. Aktuelle Aufklärung über die Akteure, die auf Finanz-Messaging zielen, formt die Szenarien, sodass der Test plausible statt generischer Intrusionen probt. Dies ist der Schritt, der einen Penetrationstest in einen bedrohungsgeführten Test verwandelt, und es ist der Schritt, der dieselbe Übung unter DORA und B-13 anrechenbar macht.

Die Durchführung läuft dann die Szenarien über den Dreijahreszyklus, den die 7.3A-Vorgaben beschreiben, ab, wobei Anwendungs-, Infrastruktur- und menschliche Pfade abgedeckt werden, von innen und außen der Grenze, durch eine unabhängige Partei, unter dokumentierten Einsatzregeln. Die Institution misst nicht nur, was gefunden wurde, sondern ob ihre eigene Erkennung und Reaktion den Test geschehen sah, denn diese Messung ist der Nachweis, den die Funktionen Detect und Respond verlangen.

Schließlich schließen Behebung und Nachweis den Kreis. Befunde gehen in einen nachverfolgten Behebungszyklus, dessen Abschluss erfasst wird, und das gesamte Dossier, Umfang, Szenarien, Angriffsnarrativ, Befunde, Behebung und Erkennungsleistung, wird einmal gegen die NIST-CSF-2.0-Wirbelsäule abgelegt und für jedes Regime gekennzeichnet. Die Institution, die diesen Kreis schließt, hat nicht einen Test bestanden. Sie hat ein wiederverwendbares Resilienz-Nachweisaktivum gebaut.

Unser SWIFT-CSP-Bewertungsdienst grenzt den 7.3A-Test ab und führt ihn nach diesem Standard durch, und PenTeva validiert und verfolgt die Befunde bis zum Abschluss, sodass der Nachweis unter jedem der vier Regime standhält. Wo DORA-Resilienzmodellierung im Umfang liegt, trägt DORA-MAST denselben Nachweis in das Bild der operativen Resilienz.

Schluss

Die geschärften 7.3A-Vorgaben werden am besten nicht als isolierte SWIFT-Anforderung verstanden, sondern als eine aufsichtsrechtliche Ausprägung einer globalen Bewegung hin zu nachrichtendienstlich geführtem, bedrohungsinformiertem Testen. Eine Institution, die ihren Penetrationstest 2026 nach diesem Standard entwirft, ihn nach Konsequenz abgrenzt, ihn mit aktueller Bedrohungsaufklärung rahmt, ihn unabhängig über die sichere Zone hinweg durchführt und das Ergebnis gegen ein gemeinsames Rahmenwerk erfasst, kann DORA, NIS2 dort, wo es noch gilt, NYDFS Part 500 und OSFI B-13 aus derselben Übung erfüllen. Der Pentest hört auf, ein wiederkehrender Compliance-Kostenpunkt zu sein, und wird zum Instrument, durch das die Institution die Risiken findet und beseitigt, die zählen. Einmal testen, viele erfüllen.

Akronyme

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 (zweite). 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 (europäisches Rahmenwerk). 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