SWIFT CSCF v2026 / Control 7.3A

Eenmaal testen, velen tevredenstellen: de penetratietest van SWIFT CSCF v2026 Controle 7.3A als regime-overstijgende oefening

Cambridge Cyber International / 2026

Uit de cyclus van 2026 van het SWIFT Customer Security Programme draagt Controle 7.3A (Penetratietesten) door de gemeenschap aangestuurde richtlijnen die de scope en de testscenario's vastleggen die van een verbonden instelling worden verwacht over een doorlopende cyclus van drie jaar (SWIFT 2025). Op zichzelf gelezen is dit nog een attestatieregel om aan te voldoen. Gelezen tegen het bredere regelgevende landschap is het bewijs van een enkele reisrichting: toezichthouders in de Europese Unie, de Verenigde Staten en Canada convergeren naar inlichtingengestuurd, dreigingsgeinformeerd testen als de manier waarop een instelling bewijst dat haar controles werken in plaats van enkel bestaan. Dit artikel betoogt dat een instelling die zich voorbereidt op de 7.3A-penetratietest die test eenmaal moet ontwerpen, naar een toonaangevende standaard, en hetzelfde bewijs moet oogsten tegen de Digital Operational Resilience Act (DORA), de tweede richtlijn inzake netwerk- en informatiebeveiliging (NIS2), de cyberbeveiligingsverordening van het New York State Department of Financial Services (23 NYCRR Part 500) en Richtlijn B-13 van het Office of the Superintendent of Financial Institutions, met versie 2.0 van het Cybersecurity Framework van het National Institute of Standards and Technology van de Verenigde Staten (NIST CSF 2.0) als gemeenschappelijke ruggengraat.

Het probleem met een afvinkvakjeslezing van 7.3A

Een verbonden instelling die elk regime als een afzonderlijke verplichting behandelt, betaalt een structurele boete. Zij bepaalt de scope van een SWIFT-penetratietest smal tot de beveiligde zone, geeft opdracht voor een afzonderlijke DORA-veerkrachttest, beantwoordt een NYDFS-vragenlijst over jaarlijks testen en bereidt bewijs voor een Canadese toezichthouder voor op een vierde tijdschema. Elke opdracht herhaalt dezelfde verkenning, dezelfde regels van betrokkenheid, dezelfde herstelcyclus, en elk levert bewijs op in een vorm die het volgende regime niet aanvaardt. De kosten zijn niet alleen geld. Gefragmenteerd testen levert een gefragmenteerd beeld van het risico op, omdat geen enkele oefening de instelling ziet zoals een echte tegenstander dat zou doen: van begin tot eind, over de backoffice, de operatorwerkstations, de berichteninterface en de verbinding met het netwerk.

Het argument hier is dat de convergentie die nu zichtbaar is over de grote regimes heen de gefragmenteerde aanpak achterhaald maakt. De 7.3A-richtlijn, het dreigingsgestuurde testregime van DORA, de inlichtingengestuurde verwachting van OSFI en het jaarlijkse mandaat van NYDFS zijn geen vier verschillende tests. Het zijn vier toezichthoudende uitdrukkingen van een idee, en een instelling die ontwerpt naar de veeleisendste daarvan, en het resultaat registreert tegen een gedeeld kader, kan aan de overige voldoen als bijproduct.

Wat SWIFT CSCF v2026 Controle 7.3A nu verwacht

Controle 7.3A bevindt zich in het Customer Security Controls Framework als een adviserende controle waarvan het doel is de operationele veerkracht van de aan SWIFT gerelateerde infrastructuur van de gebruiker te valideren door kwetsbaarheden te identificeren die zouden kunnen leiden tot compromittering van de beveiligde zone of de backoffice (SWIFT 2025). De kern van de wijziging van 2026 is geen nieuw controlenummer, maar scherpere richtlijnen over hoe de test moet worden gescopet en welke scenario's hij moet bestrijken. Het kader formuleert nu een reeks testscenario's die over een cyclus van drie jaar moeten worden uitgevoerd, zodat een instelling de controle niet kan vervullen met een enkele smalle externe scan die jaarlijks wordt herhaald. De verwachting is dat het programma over de cyclus heen het testen op applicatieniveau van de berichteninterface en verwante componenten bestrijkt, het infrastructuurtesten van de beveiligde zone en haar segmentatie, en de menselijke en operatorwerkstationpaden die echte inbraken uitbuiten.

Hieruit volgen twee ontwerpconsequenties. Ten eerste moet de scope worden bepaald tegen de beveiligde zone en haar vertrouwensgrenzen, en niet tegen een handig netwerkbereik, omdat het doel van de controle is te bewijzen dat een aanvaller niet vanuit de backoffice naar de berichtenlaag kan pivoteren. Ten tweede moet de test worden uitgevoerd door een bekwame en voldoende onafhankelijke partij, en haar bevindingen moeten een gevolgde herstelcyclus voeden waarvan de afsluiting zelf bewijs is. De controle is adviserend in plaats van verplicht voor elk architectuurtype, maar voor instellingen die zich daartegen zelf attesteren, zal de beoordelaar scope, methode, bevindingen en herstel verwachten te zien als een samenhangend dossier, niet als een certificaat.

De vier naburige regimes

DORA en dreigingsgestuurd penetratietesten

De Digital Operational Resilience Act vereist dat alle in scope vallende financiele entiteiten hun informatie- en communicatietechnologiesystemen regelmatig testen, en vereist dat de deelverzameling van significante entiteiten geavanceerd testen uitvoert door middel van dreigingsgestuurd penetratietesten (TLPT) ten minste om de drie jaar (European Parliament and Council 2022a). TLPT is inlichtingengestuurd: een gecontroleerde red-teamsimulatie tegen live productiesystemen, gemodelleerd naar de tactieken, technieken en procedures van echte dreigingsactoren, uitgevoerd volgens een methodologie waarvoor het TIBER-EU-kader de Europese referentie is (European Central Bank 2018). De instelling die een 7.3A-test voorbereidt naar een dreigingsgestuurde standaard, met actuele dreigingsinformatie die haar scenario's vormgeeft, bouwt al de ruggengraat van een DORA-test, die voornamelijk verschilt in formele scope en in het toezichthoudende bestuur dat om een aangewezen TLPT is gewikkeld.

NIS2 en de lex specialis-uitzondering

De tweede richtlijn inzake netwerk- en informatiebeveiliging verhoogt de basislijn voor het beheer van cyberbeveiligingsrisico's en de melding van incidenten over essentiele en belangrijke entiteiten heen, en nationale autoriteiten gingen tijdens 2026 over van omzetting naar actief toezicht (European Parliament and Council 2022b; European Commission 2025). Voor financiele entiteiten is het praktische punt er een van voorrang: DORA is lex specialis, en artikel 4 van NIS2 wijkt ervoor waar de regels van de financiele sector ten minste gelijkwaardig zijn. Een instelling moet DORA daarom behandelen als het werkzame regime voor veerkrachttesten, terwijl zij erkent dat groepsentiteiten buiten de financiele perimeter, zoals een gedeelde technologiedochter, binnen NIS2 kunnen blijven en kunnen profiteren van hetzelfde testbewijs.

De Verenigde Staten: NYDFS Part 500 en FFIEC-verwachtingen

De cyberbeveiligingsverordening van het New York State Department of Financial Services vereist dat elke gedekte entiteit ten minste jaarlijks penetratietesten van haar informatiesystemen uitvoert, zowel van binnen als van buiten de grenzen van de systemen, op basis van de risicobeoordeling van de entiteit (New York State Department of Financial Services 2023). De gewijzigde verordening heeft de verwachtingen inzake bestuur en testen verder aangescherpt (Ropes and Gray 2026). Op federaal niveau legt de Federal Financial Institutions Examination Council geen vaste regel op, maar behandelt penetratietesten door gekwalificeerde, onafhankelijke partijen als een verwachting van de onderzoeker en een volwassenheidsindicator binnen haar Information Security-boekje (Federal Financial Institutions Examination Council 2016). De instelling die 7.3A naar een hoge standaard vervult, en zowel van binnen als van buiten de grens test op een gedefinieerde cadans, levert precies de artefacten op die een

NYDFS-onderzoeker en een FFIEC-onderzoek verwachten.

Canada: OSFI Richtlijn B-13

Richtlijn B-13 van het Office of the Superintendent of Financial Institutions, van kracht sinds 1 januari 2024, vereist dat federaal gereguleerde financiele instellingen kwetsbaarheden identificeren door middel van regelmatig testen, en voor instellingen met aanzienlijke technologische voetafdrukken verwacht zij inlichtingengestuurd, dreigingsgestuurd penetratietesten en red-teamoefeningen die realistische meerfasige aanvallen simuleren (Office of the Superintendent of Financial Institutions 2022). B-13 is uitkomstgericht en stelt geen vaste cadans, dus de instelling bewijst naleving door de kwaliteit en het realisme van haar testen, en niet door de frequentie. Dit is dezelfde inlichtingengestuurde standaard die DORA en de aangescherpte 7.3A-richtlijn uitdrukken, wat B-13 het Canadese lid van dezelfde familie maakt, en niet een afzonderlijke verplichting.

Een ruggengraat: de regimes in kaart brengen op NIST CSF 2.0

Geen enkele financiele toezichthouder bestuurt zowel de Verenigde Staten als Canada, dus een grensoverschrijdende instelling heeft een neutrale referentie nodig die in beide wordt erkend. Versie 2.0 van het Cybersecurity Framework van NIST is die referentie: vrijwillig, breed toegepast aan beide zijden van de grens, en georganiseerd rond zes functies, Besturen, Identificeren, Beschermen, Detecteren, Reageren en Herstellen (National Institute of Standards and Technology 2024). Gebruikt als ruggengraat stelt het een instelling in staat een penetratietestprogramma te registreren en het resultaat uit te drukken in het vocabulaire dat elk regime begrijpt. De penetratietest spreekt het meest rechtstreeks tot Identificeren, door kwetsbaarheden aan het licht te brengen, en tot Detecteren en Reageren, door te meten of de monitoring en respons van de instelling een realistische inbraak daadwerkelijk opvangen en indammen. De functie Besturen draagt de regels van betrokkenheid, de onafhankelijkheid en de rapportage aan het bestuur die alle vijf regimes vereisen. Tabel 1 maakt de convergentie concreet.

Tabel 1. Een penetratietestprogramma, vier regimes, een ruggengraat

Dimensie	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Aard	Adviserende controle	Verplicht voor significante	Verplichte regel	Uitkomstgerichte verwachting	Vrijwillige referentie
Cadans	Scenariocyclus van 3 jaar	Ten minste om de 3 jaar	Ten minste jaarlijks	Geen vaste cadans	Niet voorgeschreven
Methode	Scenariogebaseerd, focus op beveiligde zone	Inlichtingengestuurd red team	Van binnen en buiten, risicogebaseerd	Inlichtingengestuurd, red team	Functies en uitkomsten
Onafhankelijkheid	Bekwame, onafhankelijke	Geaccrediteerde aanbieders	Gekwalificeerd intern of extern	Onafhankelijke zekerheid	Bestuursuitkomst
Primair bewijs	Scope, bevindingen, herstel	Dreigingsscenario's, aanvalsverhaal, herstel	Testverslag, herstelcadans	Realisme en uitkomst van test	In kaart gebrachte uitkomsten

De lezing over elke rij heen is de stelling: ontwerp de test naar de veeleisendste standaard in elke kolom, inlichtingengestuurde methode, scope die zich bewust is van de beveiligde zone, dekking van binnen en buiten, onafhankelijke uitvoering, gevolgd herstel, en het enkele resulterende dossier voldoet aan alle vijf.

Een risicogestuurd voorbereidingsmodel

De 7.3A-richtlijn nodigt uit tot een nalevingslezing, waarin de instelling het minimum doet dat de controle noemt. De waardevollere lezing, en die welke toezichthouders steeds meer belonen, is risicogestuurd: de penetratietest is het instrument dat wordt gebruikt om de meest ingrijpende blootstellingen van de instelling aan het licht te brengen en weg te nemen, en naleving is het bijproduct van het goed doen daarvan.

De voorbereiding begint met een risico- en scopebasislijn. De instelling inventariseert haar aan SWIFT gerelateerde landschap, de beveiligde zone, de berichteninterface, de operatorwerkstations, de verbinding met het netwerk en de backofficesystemen die haar voeden, en rangschikt de paden naar het gevolg van compromittering, en niet naar het gemak van testen. Dit levert een scope op die wordt bepaald door waar het geld en het vertrouwen zitten, wat ook de scope is die een echte tegenstander zou kiezen, en die aansluit bij de gevolggestuurde houding van B-13 en de risicogebaseerde houding van NYDFS.

Vervolgens komt de kadering met dreigingsinformatie. Actuele inlichtingen over de actoren die financiele berichtgeving viseren, vormen de scenario's, zodat de test plausibele inbraken oefent in plaats van generieke. Dit is de stap die een penetratietest verandert in een dreigingsgestuurde test, en het is de stap die dezelfde oefening geloofwaardig maakt onder DORA en B-13.

De uitvoering voert dan de scenario's uit over de cyclus van drie jaar die de 7.3A-richtlijn beschrijft, en bestrijkt applicatie-, infrastructuur- en menselijke paden, van binnen en buiten de grens, door een onafhankelijke partij, onder gedocumenteerde regels van betrokkenheid. De instelling meet niet alleen wat werd gevonden, maar of haar eigen detectie en respons de test zagen gebeuren, omdat die meting het bewijs is dat de functies Detecteren en Reageren vereisen.

Ten slotte sluiten herstel en bewijs de lus. Bevindingen gaan een gevolgde herstelcyclus in waarvan de afsluiting wordt geregistreerd, en het hele dossier, scope, scenario's, aanvalsverhaal, bevindingen, herstel en detectieprestaties, wordt eenmaal ingediend tegen de NIST CSF 2.0-ruggengraat en aan elk regime gekoppeld. De instelling die deze lus voltooit, heeft niet een test doorstaan. Zij heeft een herbruikbaar veerkrachtbewijsactief gebouwd.

Onze SWIFT CSP-beoordelingsdienst bepaalt de scope en voert de 7.3A-test uit naar deze standaard, en PenTeva valideert en volgt de bevindingen tot afsluiting, zodat het bewijs standhoudt onder elk van de vier regimes. Waar DORA-veerkrachtmodellering in scope is, draagt DORA-MAST hetzelfde bewijs over naar het beeld van de operationele veerkracht.

Conclusie

De aangescherpte 7.3A-richtlijn wordt het best begrepen niet als een geisoleerde SWIFT-vereiste, maar als een toezichthoudende uitdrukking van een wereldwijde beweging naar inlichtingengestuurd, dreigingsgeinformeerd testen. Een instelling die haar penetratietest van 2026 ontwerpt naar die standaard, de scope ervan bepaalt op gevolg, haar kadert met actuele dreigingsinformatie, haar onafhankelijk uitvoert over de beveiligde zone heen en het resultaat registreert tegen een gedeeld kader, kan voldoen aan DORA, NIS2 waar het nog van toepassing is, NYDFS Part 500 en OSFI B-13 vanuit dezelfde oefening. De penetratietest houdt op een terugkerende nalevingskost te zijn en wordt het instrument waarmee de instelling de risico's vindt en wegneemt die ertoe doen. Eenmaal testen, velen tevredenstellen.

Acroniemen

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 (tweede). 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 (Europees kader). TLPT, Threat-Led Penetration Testing.

Referenties

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