SWIFT CSCF v2026 / Control 7.3A

Testuj raz, zadowól wielu: test penetracyjny SWIFT CSCF v2026 7.3A jako ćwiczenie międzyreżimowe

Cambridge Cyber International / 2026

W cyklu 2026 Programu Bezpieczeństwa Klienta SWIFT Kontrola 7.3A (Testowanie Penetracyjne) niesie wytyczne kształtowane przez społeczność, które ustalają zakres oraz scenariusze testowania oczekiwane od podłączonej instytucji w toczącym się trzyletnim cyklu (SWIFT 2025). Odczytana w izolacji, jest to jeszcze jedna linia atestacji do zadowolenia. Odczytana na tle szerszego krajobrazu regulacyjnego, jest dowodem jednego kierunku marszu: nadzorcy w Unii Europejskiej, Stanach Zjednoczonych i Kanadzie zbiegają się ku testowaniu kierowanemu wywiadem, świadomemu zagrożeń, jako sposobowi, w jaki instytucja dowodzi, że jej kontrole działają, a nie jedynie istnieją. Niniejszy artykuł dowodzi, że instytucja przygotowująca się do testu penetracyjnego 7.3A powinna zaprojektować ten test raz, do standardu na poziomie najnowszej wiedzy, i zebrać te same dowody względem Aktu o Cyfrowej Odporności Operacyjnej (DORA), drugiej Dyrektywy o Bezpieczeństwie Sieci i Informacji (NIS2), regulacji cyberbezpieczeństwa nowojorskiego Departamentu Usług Finansowych (23 NYCRR Part 500) oraz Wytycznej B-13 Urzędu Nadzoru Instytucji Finansowych, posługując się Ramami Cyberbezpieczeństwa amerykańskiego Narodowego Instytutu Norm i Technologii w wersji 2.0 (NIST CSF 2.0) jako wspólnym kręgosłupem.

Problem z odczytem 7.3A jako pola do odhaczenia

Podłączona instytucja, która traktuje każdy reżim jako odrębny obowiązek, płaci karę strukturalną. Zakreśla test penetracyjny SWIFT wąsko do strefy bezpiecznej, zleca odrębny test odporności na potrzeby DORA, odpowiada na kwestionariusz NYDFS o testowaniu rocznym i przygotowuje dowody dla kanadyjskiego nadzorcy na czwartym harmonogramie. Każde zlecenie powtarza to samo rozpoznanie, te same zasady zaangażowania, ten sam cykl remediacji, a każde wytwarza dowody w kształcie, którego nie przyjmuje następny reżim. Kosztem nie są tylko pieniądze. Rozdrobnione testowanie wytwarza rozdrobniony obraz ryzyka, ponieważ żadne pojedyncze ćwiczenie nie widzi instytucji tak, jak ujrzałby ją prawdziwy przeciwnik: od końca do końca, przez zaplecze, stacje robocze operatorów, interfejs komunikatów i połączenie z siecią.

Argument brzmi tu tak, że zbieżność widoczna teraz w głównych reżimach czyni podejście rozdrobnione przestarzałym. Wytyczne 7.3A, reżim testowania kierowanego zagrożeniami DORA, oczekiwanie OSFI co do kierowania wywiadem oraz roczny mandat NYDFS nie są czterema różnymi testami. Są czterema nadzorczymi wyrazami jednej idei, a instytucja, która zaprojektuje wedle najbardziej wymagającego z nich i zapisze wynik względem wspólnych ram, może zadowolić pozostałe jako produkt uboczny.

Czego teraz oczekuje Kontrola 7.3A SWIFT CSCF v2026

Kontrola 7.3A mieści się w Ramach Kontroli Bezpieczeństwa Klienta jako kontrola doradcza, której celem jest zwalidowanie odporności operacyjnej infrastruktury użytkownika związanej ze SWIFT przez zidentyfikowanie podatności, które mogłyby prowadzić do kompromitacji strefy bezpiecznej lub zaplecza (SWIFT 2025). Istotą zmiany 2026 nie jest nowy numer kontroli, lecz ostrzejsze wytyczne co do tego, jak należy zakreślić test oraz jakie scenariusze powinien on objąć. Ramy artykułują teraz zestaw scenariuszy testowych do przećwiczenia w trzyletnim cyklu, tak aby instytucja nie mogła zadowolić kontroli pojedynczym wąskim skanem zewnętrznym powtarzanym corocznie. Oczekiwanie jest takie, że w toku cyklu program obejmuje testowanie na warstwie aplikacji interfejsu komunikatów i powiązanych komponentów, testowanie infrastruktury strefy bezpiecznej i jej segmentacji oraz ścieżki ludzkie i stacji roboczych operatorów, które wykorzystują prawdziwe włamania.

Wynikają stąd dwie konsekwencje projektowe. Po pierwsze, zakres musi być zdefiniowany względem strefy bezpiecznej i jej granic zaufania, a nie względem dogodnego zakresu sieci, ponieważ celem kontroli jest dowiedzenie, że napastnik nie może obrócić się z zaplecza w warstwę komunikatów. Po drugie, test

musi być przeprowadzony przez stronę kompetentną i dostatecznie niezależną, a jego ustalenia muszą zasilać śledzony cykl remediacji, którego domknięcie samo jest dowodem. Kontrola ma charakter doradczy, a nie obowiązkowy dla każdego typu architektury, ale w przypadku instytucji, które same się względem niej atestują, asesor będzie oczekiwał zobaczenia zakresu, metody, ustaleń i remediacji jako spójnego zapisu, a nie certyfikatu.

Cztery sąsiadujące reżimy

DORA i testowanie penetracyjne kierowane zagrożeniami

Akt o Cyfrowej Odporności Operacyjnej wymaga, aby wszystkie objęte zakresem podmioty finansowe regularnie testowały swoje systemy technologii informacyjnych i komunikacyjnych, oraz wymaga od podzbioru podmiotów znaczących wykonywania zaawansowanego testowania za pomocą testowania penetracyjnego kierowanego zagrożeniami (TLPT) co najmniej raz na trzy lata (European Parliament and Council 2022a). TLPT jest kierowane wywiadem: kontrolowana symulacja zespołu czerwonego przeciw żywym systemom produkcyjnym, wzorowana na taktykach, technikach i procedurach prawdziwych aktorów zagrożeń, prowadzona wedle metodyki, dla której europejskim punktem odniesienia są ramy TIBER-EU (European Central Bank 2018). Instytucja, która przygotowuje test 7.3A do standardu kierowanego zagrożeniami, z bieżącym wywiadem o zagrożeniach kształtującym jej scenariusze, buduje już kręgosłup testu DORA, różniąc się głównie formalnym zakresem oraz nadzorczym ładem otaczającym wyznaczony TLPT.

NIS2 i wyłom lex specialis

Druga Dyrektywa o Bezpieczeństwie Sieci i Informacji podnosi poziom bazowy zarządzania ryzykiem cyberbezpieczeństwa oraz zgłaszania incydentów w podmiotach kluczowych i ważnych, a organy krajowe przeszły od transpozycji do czynnego nadzoru w trakcie 2026 (European Parliament and Council 2022b; European Commission 2025). Dla podmiotów finansowych punkt praktyczny dotyczy pierwszeństwa: DORA jest lex specialis, a artykuł 4 NIS2 ustępuje przed nią tam, gdzie zasady sektora finansowego są co najmniej równoważne. Instytucja powinna zatem traktować DORA jako operatywny reżim testowania odporności, jednocześnie uznając, że podmioty grupowe poza perymetrem finansowym, takie jak współdzielona spółka technologiczna, mogą pozostawać w obrębie NIS2 i korzystać z tych samych dowodów testowych.

Stany Zjednoczone: NYDFS Part 500 i oczekiwania FFIEC

Regulacja cyberbezpieczeństwa nowojorskiego Departamentu Usług Finansowych wymaga, aby każdy objęty podmiot prowadził testowanie penetracyjne swoich systemów informacyjnych co najmniej corocznie, zarówno od wewnątrz, jak i z zewnątrz granic systemów, w oparciu o ocenę ryzyka podmiotu (New York State Department of Financial Services 2023). Znowelizowana regulacja dodatkowo zaostrzyła oczekiwania co do ładu i testowania (Ropes and Gray 2026). Na szczeblu federalnym Federalna Rada Egzaminacyjna Instytucji Finansowych nie nakłada stałej reguły, lecz traktuje testowanie penetracyjne przez wykwalifikowane, niezależne strony jako oczekiwanie egzaminatora oraz wskaźnik dojrzałości w swoim podręczniku Bezpieczeństwa Informacji (Federal Financial Institutions Examination Council 2016). Instytucja, która zadowala 7.3A do wysokiego standardu, testując zarówno od wewnątrz, jak i z zewnątrz granicy w określonej kadencji, wytwarza dokładnie te artefakty, których oczekuje egzaminator NYDFS oraz egzaminacja FFIEC.

Kanada: Wytyczna B-13 OSFI

Wytyczna B-13 Urzędu Nadzoru Instytucji Finansowych, obowiązująca od 1 stycznia 2024 roku, wymaga, aby instytucje finansowe regulowane federalnie identyfikowały podatności przez regularne testowanie, a w przypadku instytucji o znaczących odciskach technologicznych oczekuje testowania penetracyjnego kierowanego wywiadem, kierowanego zagrożeniami oraz ćwiczeń zespołu czerwonego, które symulują realistyczne wieloetapowe ataki (Office of the Superintendent of Financial Institutions 2022). B-13 jest oparta na wynikach i nie ustala stałej kadencji, więc instytucja dowodzi zgodności przez jakość i realizm swojego testowania, a nie przez jego częstotliwość. Jest to ten sam standard kierowany wywiadem, który wyrażają DORA i zaostrzone wytyczne 7.3A, co czyni B-13 kanadyjskim członkiem tej samej rodziny, a nie odrębnym obowiązkiem.

Jeden kręgosłup: odwzorowanie reżimów na NIST CSF 2.0

Żaden pojedynczy regulator finansowy nie zarządza zarazem Stanami Zjednoczonymi i Kanadą, więc instytucja transgraniczna potrzebuje neutralnego punktu odniesienia uznanego w obu. Ramy Cyberbezpieczeństwa NIST w wersji 2.0 są tym punktem: dobrowolne, szeroko przyjęte po obu stronach granicy i zorganizowane wokół sześciu funkcji: Zarządzaj, Identyfikuj, Chroń, Wykrywaj, Reaguj i Przywracaj (National Institute of Standards and Technology 2024). Użyte jako kręgosłup, pozwalają instytucji zapisać jeden program testowania penetracyjnego i wyrazić wynik w słownictwie, które rozumie każdy reżim. Test penetracyjny przemawia najbardziej bezpośrednio do funkcji Identyfikuj, wydobywając podatności, oraz do funkcji Wykrywaj i Reaguj, mierząc, czy monitorowanie i reakcja instytucji faktycznie wychwytują i powstrzymują realistyczne włamanie. Funkcja Zarządzaj niesie zasady zaangażowania, niezależność i raportowanie do zarządu, których wymagają wszystkie pięć reżimów. Tabela 1 czyni tę zbieżność konkretną.

Tabela 1. Jeden program testowania penetracyjnego, cztery reżimy, jeden kręgosłup

Wymiar	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Charakter	Kontrola doradcza	Obowiązkowy dla podmiotów	Reguła obowiązkowa	Oczekiwanie oparte na	Dobrowolny punkt odniesienia
Kadencja	3-letni cykl scenariuszy	Co najmniej raz na 3 lata	Co najmniej corocznie	Brak stałej kadencji	Nie przepisana
Metoda	Oparta na scenariuszach, skupiona na strefie	Zespół czerwony kierowany wywiadem	Od wewnątrz i z zewnątrz, oparta na ryzyku	Kierowana wywiadem, zespół czerwony	Funkcje i wyniki
Niezależność	Strona kompetentna, niezależna	Akredytowani dostawcy	Wykwalifikowana wewnętrzna lub zewnętrzna	Niezależne zapewnienie	Wynik ładu
Główny dowód	Zakres, ustalenia, remediacja	Scenariusze zagrożeń, narracja ataku, remediacja	Raport z testu, kadencja remediacji	Realizm i wynik testu	Odwzorowane wyniki

Odczyt w poprzek każdego wiersza jest tezą: zaprojektuj test do najbardziej wymagającego standardu w każdej kolumnie, metoda kierowana wywiadem, zakres świadomy strefy bezpiecznej, pokrycie od wewnątrz i z zewnątrz, niezależne wykonanie, śledzona remediacja, a pojedynczy wynikowy zapis zadowoli wszystkie pięć.

Model przygotowania kierowany ryzykiem

Wytyczne 7.3A zapraszają do odczytu zgodnościowego, w którym instytucja robi minimum nazwane przez kontrolę. Bardziej wartościowy odczyt, i ten, który nadzorcy coraz częściej nagradzają, jest kierowany

ryzykiem: test penetracyjny jest instrumentem używanym do wydobycia i wycofania najbardziej konsekwentnych ekspozycji instytucji, a zgodność jest produktem ubocznym dobrego wykonania tego.

Przygotowanie zaczyna się od podstawy ryzyka i zakresu. Instytucja inwentaryzuje swój majątek związany ze SWIFT, strefę bezpieczną, interfejs komunikatów, stacje robocze operatorów, połączenie z siecią oraz systemy zaplecza, które ją zasilają, i szereguje ścieżki wedle konsekwencji kompromitacji, a nie łatwości testowania. Wytwarza to zakres zdefiniowany przez to, gdzie siedzą pieniądze i zaufanie, który jest też zakresem, jaki wybrałby prawdziwy przeciwnik, i który zestraja się z postawą kierowaną konsekwencją B-13 oraz postawą opartą na ryzyku NYDFS.

Następnie przychodzi kadrowanie wywiadem o zagrożeniach. Bieżący wywiad o aktorach, którzy obierają za cel komunikaty finansowe, kształtuje scenariusze, tak aby test ćwiczył wiarygodne włamania, a nie generyczne. To krok, który zamienia test penetracyjny w test kierowany zagrożeniami, i to krok, który czyni to samo ćwiczenie wiarygodnym pod DORA i B-13.

Wykonanie następnie uruchamia scenariusze w trzyletnim cyklu opisanym przez wytyczne 7.3A, obejmując ścieżki aplikacji, infrastruktury i ludzkie, od wewnątrz i z zewnątrz granicy, przez stronę niezależną, wedle udokumentowanych zasad zaangażowania. Instytucja mierzy nie tylko to, co znaleziono, ale czy jej własna wykrywalność i reakcja zobaczyły, że test się odbywa, ponieważ ten pomiar jest dowodem wymaganym przez funkcje Wykrywaj i Reaguj.

Wreszcie remediacja i dowody domykają pętlę. Ustalenia wchodzą do śledzonego cyklu remediacji, którego domknięcie jest zapisywane, a cały zapis, zakres, scenariusze, narracja ataku, ustalenia, remediacja i wydajność wykrywania, jest składany raz względem kręgosłupa NIST CSF 2.0 i otagowany do każdego reżimu. Instytucja, która domyka tę pętlę, nie zaliczyła jednego testu. Zbudowała aktyw dowodowy odporności wielokrotnego użytku.

Nasza usługa oceny SWIFT CSP zakreśla i prowadzi test 7.3A do tego standardu, a PenTeva waliduje i śledzi ustalenia do domknięcia, tak aby dowody wytrzymały pod którymkolwiek z czterech reżimów. Tam, gdzie modelowanie odporności DORA jest w zakresie, DORA-MAST wnosi te same dowody w obraz odporności operacyjnej.

Wnioski

Zaostrzone wytyczne 7.3A najlepiej rozumieć nie jako odosobniony wymóg SWIFT, lecz jako jeden nadzorczy wyraz globalnego ruchu ku testowaniu kierowanemu wywiadem, świadomemu zagrożeń. Instytucja, która projektuje swój test penetracyjny na rok 2026 do tego standardu, zakreśla go wedle konsekwencji, kadruje bieżącym wywiadem o zagrożeniach, wykonuje niezależnie przez strefę bezpieczną i zapisuje wynik względem wspólnych ram, może zadowolić DORA, NIS2 tam, gdzie wciąż obowiązuje, NYDFS Part 500 oraz OSFI B-13 z tego samego ćwiczenia. Test penetracyjny przestaje być powracającym kosztem zgodności i staje się instrumentem, przez który instytucja znajduje i wycofuje ryzyka, które mają znaczenie. Testuj raz, zadowól wielu.

Akronimy

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 (druga). 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 (ramy europejskie). TLPT, Threat-Led Penetration Testing.

Bibliografia

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