SWIFT CSCF v2026 / Control 7.3A

Test once, satisfy many: the SWIFT CSCF v2026 7.3A penetration test as a cross-regime exercise

Cambridge Cyber International / 2026

From the 2026 cycle of the SWIFT Customer Security Programme, Control 7.3A (Penetration Testing) carries community-driven guidance that sets the scope and the testing scenarios expected of a connected institution across a rolling three-year cycle (SWIFT 2025). Read in isolation, this is one more attestation line to satisfy. Read against the wider regulatory landscape, it is evidence of a single direction of travel: supervisors across the European Union, the United States and Canada are converging on intelligence-led, threat-informed testing as the way an institution proves its controls work rather than merely exist. This article argues that an institution preparing for the 7.3A penetration test should design that test once, to a state-of-the-art standard, and harvest the same evidence against the Digital Operational Resilience Act (DORA), the second Network and Information Security Directive (NIS2), the New York State Department of Financial Services cybersecurity regulation (23 NYCRR Part 500), and the Office of the Superintendent of Financial Institutions Guideline B-13, using the United States National Institute of Standards and Technology Cybersecurity Framework version 2.0 (NIST CSF 2.0) as the common spine.

The problem with a checkbox reading of 7.3A

A connected institution that treats each regime as a separate obligation pays a structural penalty. It scopes a SWIFT penetration test narrowly to the secure zone, commissions a separate DORA resilience test, answers a NYDFS questionnaire on annual testing, and prepares evidence for a Canadian supervisor on a fourth timetable. Each engagement repeats the same reconnaissance, the same rules of engagement, the same remediation cycle, and each produces evidence in a shape the next regime does not accept. The cost is not only money. Fragmented testing produces a fragmented picture of risk, because no single exercise sees the institution as a real adversary would: end to end, across the back office, the operator workstations, the messaging interface and the connection to the network.

The argument here is that the convergence now visible across the major regimes makes the fragmented approach obsolete. The 7.3A guidance, DORA's threat-led testing regime, OSFI's intelligence-led expectation, and the NYDFS annual mandate are not four different tests. They are four supervisory expressions of one idea, and an institution that designs to the most demanding of them, and records the result against a shared framework, can satisfy the others as a by-product.

What SWIFT CSCF v2026 Control 7.3A now expects

Control 7.3A sits in the Customer Security Controls Framework as an advisory control whose objective is to validate the operational resilience of the user's SWIFT-related infrastructure by identifying vulnerabilities that could lead to compromise of the secure zone or the back office (SWIFT 2025). The substance of the 2026 change is not a new control number but sharper guidance on how the test should be scoped and what scenarios it should cover. The framework now articulates a set of testing scenarios to be exercised across a three-year cycle, so that an institution cannot satisfy the control with a single narrow external scan repeated annually. The expectation is that, over the cycle, the programme covers application-layer testing of the messaging interface and related components, infrastructure testing of the secure zone and its segmentation, and the human and operator-workstation paths that real intrusions exploit.

Two design consequences follow. First, scope must be defined against the secure zone and its trust boundaries rather than against a convenient network range, because the control's purpose is to prove that an attacker cannot pivot from the back office into the messaging layer. Second, the test must be conducted by a competent and sufficiently independent party, and its findings must feed a tracked

remediation cycle whose closure is itself evidence. The control is advisory rather than mandatory for every architecture type, but for institutions that self-attest against it, the assessor will expect to see scope, method, findings and remediation as a coherent record, not a certificate.

The four neighbouring regimes

DORA and threat-led penetration testing

The Digital Operational Resilience Act requires all in-scope financial entities to test their information and communication technology systems regularly, and requires the subset of significant entities to perform advanced testing by means of threat-led penetration testing (TLPT) at least every three years (European Parliament and Council 2022a). TLPT is intelligence-driven: a controlled red-team simulation against live production systems, modelled on the tactics, techniques and procedures of real threat actors, conducted under a methodology for which the TIBER-EU framework is the European reference (European Central Bank 2018). The institution that prepares a 7.3A test to a threat-led standard, with current threat intelligence shaping its scenarios, is already building the spine of a DORA test, differing mainly in formal scope and in the supervisory governance wrapped around a designated TLPT.

NIS2 and the lex specialis carve-out

The second Network and Information Security Directive raises the baseline for cybersecurity risk management and incident reporting across essential and important entities, and national authorities moved from transposition into active supervision during 2026 (European Parliament and Council 2022b; European Commission 2025). For financial entities the practical point is one of precedence: DORA is lex specialis, and Article 4 of NIS2 yields to it where the financial-sector rules are at least equivalent. An institution should therefore treat DORA as the operative resilience-testing regime, while recognising that group entities outside the financial perimeter, such as a shared technology subsidiary, may remain within NIS2 and benefit from the same testing evidence.

The United States: NYDFS Part 500 and FFIEC expectations

The New York State Department of Financial Services cybersecurity regulation requires each covered entity to conduct penetration testing of its information systems at least annually, from both inside and outside the systems' boundaries, based on the entity's risk assessment (New York State Department of Financial Services 2023). The amended regulation has tightened governance and testing expectations further (Ropes and Gray 2026). At the federal level, the Federal Financial Institutions Examination Council does not impose a fixed rule but treats penetration testing by qualified, independent parties as an examiner expectation and a maturity indicator within its Information Security booklet (Federal Financial Institutions Examination Council 2016). The institution that satisfies 7.3A to a high standard, testing from both inside and outside the boundary on a defined cadence, produces exactly the artefacts a NYDFS examiner and an FFIEC examination expect.

Canada: OSFI Guideline B-13

The Office of the Superintendent of Financial Institutions Guideline B-13, in force since 1 January 2024, requires federally regulated financial institutions to identify vulnerabilities through regular testing, and for institutions with significant technology footprints it expects intelligence-led, threat-led penetration testing and red-team exercises that simulate realistic multi-stage attacks (Office of the Superintendent of Financial Institutions 2022). B-13 is outcome-based and sets no fixed cadence, so the institution evidences compliance through the quality and realism of its testing rather than its frequency. This is the

same intelligence-led standard DORA and the sharpened 7.3A guidance express, which makes B-13 the Canadian member of the same family rather than a separate obligation.

One spine: mapping the regimes onto NIST CSF 2.0

No single financial regulator governs both the United States and Canada, so a cross-border institution needs a neutral reference recognised in both. The NIST Cybersecurity Framework version 2.0 is that reference: voluntary, widely adopted on both sides of the border, and organised around six functions, Govern, Identify, Protect, Detect, Respond and Recover (National Institute of Standards and Technology 2024). Used as a spine, it lets an institution record one penetration-test programme and express the result in the vocabulary every regime understands. The penetration test speaks most directly to Identify, by surfacing vulnerabilities, and to Detect and Respond, by measuring whether the institution's monitoring and response actually catch and contain a realistic intrusion. The Govern function carries the rules of engagement, independence and board reporting that all five regimes require. Table 1 makes the convergence concrete.

Table 1. One penetration-test programme, four regimes, one spine

Dimension	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Nature	Advisory control	Mandatory for significant entities	Mandatory rule	Outcome-based expectation	Voluntary reference
Cadence	3-year scenario cycle	At least every 3 years	At least annual	No fixed cadence	Not prescribed
Method	Scenario-based, secure-zone focus	Intelligence-led red team	Inside and outside, risk-based	Intelligence-led, red team	Functions and outcomes
Independence	Competent, independent party	Accredited providers	Qualified internal or external	Independent assurance	Governance outcome
Primary evidence	Scope, findings, remediation	Threat scenarios, attack narrative, remediation	Test report, remediation cadence	Realism and outcome of test	Mapped outcomes

The reading across each row is the thesis: design the test to the most demanding standard in each column, intelligence-led method, secure-zone-aware scope, inside-and-outside coverage, independent execution, tracked remediation, and the single resulting record satisfies all five.

A risk-led preparation model

The 7.3A guidance invites a compliance reading, in which the institution does the minimum the control names. The more valuable reading, and the one supervisors increasingly reward, is risk-led: the penetration test is the instrument used to surface and retire the institution's most consequential exposures, and compliance is the by-product of doing that well.

Preparation begins with a risk-and-scope baseline. The institution inventories its SWIFT-related estate, the secure zone, the messaging interface, the operator workstations, the connection to the network and the back-office systems that feed it, and ranks the paths by the consequence of compromise rather than by ease of testing. This produces a scope defined by where the money and the trust sit, which is also the scope a real adversary would choose, and which aligns with the consequence-led posture of B-13 and the risk-based posture of NYDFS.

Next comes threat-intelligence framing. Current intelligence on the actors who target financial messaging shapes the scenarios, so that the test rehearses plausible intrusions rather than generic ones. This is the

step that turns a penetration test into a threat-led test, and it is the step that makes the same exercise creditable under DORA and B-13.

Execution then runs the scenarios across the three-year cycle the 7.3A guidance describes, covering application, infrastructure and human paths, from inside and outside the boundary, by an independent party, under documented rules of engagement. The institution measures not only what was found but whether its own detection and response saw the test happen, because that measurement is the evidence the Detect and Respond functions require.

Finally, remediation and evidence close the loop. Findings enter a tracked remediation cycle whose closure is recorded, and the whole record, scope, scenarios, attack narrative, findings, remediation and detection performance, is filed once against the NIST CSF 2.0 spine and tagged to each regime. The institution that completes this loop has not passed one test. It has built a reusable resilience evidence asset.

Our SWIFT CSP assessment service scopes and runs the 7.3A test to this standard, and PenTeva validates and tracks the findings to closure so the evidence holds up under any of the four regimes. Where DORA resilience modelling is in scope, DORA-MAST carries the same evidence into the operational-resilience picture.

Conclusion

The sharpened 7.3A guidance is best understood not as an isolated SWIFT requirement but as one supervisory expression of a global movement toward intelligence-led, threat-informed testing. An institution that designs its 2026 penetration test to that standard, scopes it by consequence, frames it with current threat intelligence, executes it independently across the secure zone, and records the result against a shared framework, can satisfy DORA, NIS2 where it still applies, NYDFS Part 500 and OSFI B-13 from the same exercise. The pen test stops being a recurring compliance cost and becomes the instrument through which the institution finds and retires the risks that matter. Test once, satisfy many.

Acronyms

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