SWIFT CSCF v2026 / Control 7.3A

Tester une fois, satisfaire plusieurs : le test d'intrusion SWIFT CSCF v2026 7.3A comme exercice trans-régimes

Cambridge Cyber International / 2026

Issu du cycle 2026 du SWIFT Customer Security Programme, le Control 7.3A (Penetration Testing) porte des orientations issues de la communauté qui fixent le périmètre et les scénarios de test attendus d'une institution connectée sur un cycle glissant de trois ans (SWIFT 2025). Lu isolément, c'est une ligne d'attestation de plus à satisfaire. Lu au regard du paysage réglementaire plus large, c'est la preuve d'une seule direction de marche : les superviseurs de l'Union européenne, des États-Unis et du Canada convergent vers un test orienté renseignement et informé par la menace comme moyen pour une institution de prouver que ses contrôles fonctionnent plutôt qu'ils n'existent simplement. Cet article soutient qu'une institution qui prépare le test d'intrusion 7.3A devrait concevoir ce test une seule fois, selon un standard de l'état de l'art, et récolter la même preuve au regard du Digital Operational Resilience Act (DORA), de la deuxième Network and Information Security Directive (NIS2), de la réglementation cybersécurité du New York State Department of Financial Services (23 NYCRR Part 500) et de la Guideline B-13 de l'Office of the Superintendent of Financial Institutions, en utilisant le United States National Institute of Standards and Technology Cybersecurity Framework version 2.0 (NIST CSF 2.0) comme colonne vertébrale commune.

Le problème d'une lecture du 7.3A en case à cocher

Une institution connectée qui traite chaque régime comme une obligation distincte paie une pénalité structurelle. Elle cadre étroitement un test d'intrusion SWIFT sur la zone sécurisée, commande un test de résilience DORA séparé, répond à un questionnaire NYDFS sur le test annuel et prépare des preuves pour un superviseur canadien selon un quatrième calendrier. Chaque mission répète la même reconnaissance, les mêmes règles d'engagement, le même cycle de remédiation, et chacune produit des preuves dans une forme que le régime suivant n'accepte pas. Le coût n'est pas seulement financier. Un test fragmenté produit une image fragmentée du risque, parce qu'aucun exercice unique ne voit l'institution comme le ferait un véritable adversaire : de bout en bout, à travers le back-office, les postes opérateurs, l'interface de messagerie et la connexion au réseau.

L'argument ici est que la convergence désormais visible à travers les grands régimes rend l'approche fragmentée obsolète. Les orientations 7.3A, le régime de test orienté menace de DORA, l'attente orientée renseignement de l'OSFI et le mandat annuel du NYDFS ne sont pas quatre tests différents. Ce sont quatre expressions prudentielles d'une seule idée, et une institution qui conçoit pour la plus exigeante d'entre elles, et enregistre le résultat sur un cadre commun, peut satisfaire les autres comme un produit dérivé.

Ce que le SWIFT CSCF v2026 Control 7.3A attend désormais

Le Control 7.3A se situe dans le Customer Security Controls Framework comme un contrôle consultatif dont l'objectif est de valider la résilience opérationnelle de l'infrastructure liée à SWIFT de l'utilisateur en identifiant les vulnérabilités susceptibles de conduire à une compromission de la zone sécurisée ou du back-office (SWIFT 2025). La substance du changement 2026 n'est pas un nouveau numéro de contrôle mais des orientations plus nettes sur la façon dont le test doit être cadré et sur les scénarios qu'il doit couvrir. Le cadre articule désormais un ensemble de scénarios de test à exercer sur un cycle de trois ans, de sorte qu'une institution ne peut satisfaire le contrôle par un seul scan externe étroit répété chaque année. L'attente est que, sur le cycle, le programme couvre le test au niveau applicatif de l'interface de messagerie et des composants associés, le test d'infrastructure de la zone sécurisée et de sa segmentation, et les chemins humains et de postes opérateurs que les intrusions réelles exploitent.

Deux conséquences de conception en découlent. Premièrement, le périmètre doit être défini par rapport

à la zone sécurisée et à ses frontières de confiance plutôt que par rapport à une plage réseau commode, parce que la finalité du contrôle est de prouver qu'un attaquant ne peut pas pivoter du back-office vers la couche de messagerie. Deuxièmement, le test doit être mené par une partie compétente et suffisamment indépendante, et ses constats doivent alimenter un cycle de remédiation suivi dont la clôture constitue elle-même une preuve. Le contrôle est consultatif plutôt qu'obligatoire pour chaque type d'architecture, mais pour les institutions qui s'auto-attestent à son égard, l'évaluateur s'attendra à voir périmètre, méthode, constats et remédiation comme un dossier cohérent, et non comme un certificat.

Les quatre régimes voisins

DORA et le test d'intrusion orienté menace

Le Digital Operational Resilience Act impose à toutes les entités financières dans son champ de tester régulièrement leurs systèmes de technologies de l'information et de la communication, et impose au sous-ensemble d'entités significatives de réaliser un test avancé au moyen d'un test d'intrusion orienté menace (TLPT) au moins tous les trois ans (European Parliament and Council 2022a). Le TLPT est orienté renseignement : une simulation contrôlée d'équipe rouge contre des systèmes de production en service, modelée sur les tactiques, techniques et procédures d'acteurs de menace réels, conduite selon une méthodologie dont le cadre TIBER-EU est la référence européenne (European Central Bank 2018). L'institution qui prépare un test 7.3A selon un standard orienté menace, avec un renseignement actuel sur les menaces façonnant ses scénarios, bâtit déjà la colonne vertébrale d'un test DORA, ne différant principalement que par le périmètre formel et par la gouvernance prudentielle qui enveloppe un TLPT désigné.

NIS2 et le retrait lex specialis

La deuxième Network and Information Security Directive relève le socle de la gestion du risque cybersécurité et du signalement des incidents pour les entités essentielles et importantes, et les autorités nationales sont passées de la transposition à la supervision active au cours de 2026 (European Parliament and Council 2022b ; European Commission 2025). Pour les entités financières, le point pratique est de priorité : DORA est lex specialis, et l'article 4 de NIS2 lui cède le pas lorsque les règles du secteur financier sont au moins équivalentes. Une institution devrait donc traiter DORA comme le régime opérant de test de résilience, tout en reconnaissant que des entités du groupe hors du périmètre financier, telle une filiale technologique mutualisée, peuvent demeurer dans NIS2 et bénéficier de la même preuve de test.

Les États-Unis : NYDFS Part 500 et attentes du FFIEC

La réglementation cybersécurité du New York State Department of Financial Services impose à chaque entité couverte de mener un test d'intrusion de ses systèmes d'information au moins annuellement, depuis l'intérieur comme depuis l'extérieur des frontières des systèmes, sur la base de l'évaluation des risques de l'entité (New York State Department of Financial Services 2023). La réglementation amendée a resserré davantage les attentes de gouvernance et de test (Ropes and Gray 2026). Au niveau fédéral, le Federal Financial Institutions Examination Council n'impose pas de règle fixe mais traite le test d'intrusion par des parties qualifiées et indépendantes comme une attente d'examinateur et un indicateur de maturité dans son Information Security booklet (Federal Financial Institutions Examination Council 2016). L'institution qui satisfait le 7.3A à un haut standard, en testant depuis l'intérieur comme depuis l'extérieur de la frontière selon une cadence définie, produit exactement les artefacts

qu'attendent un examinateur NYDFS et un examen FFIEC.

Canada : OSFI Guideline B-13

La Guideline B-13 de l'Office of the Superintendent of Financial Institutions, en vigueur depuis le 1 January 2024, impose aux institutions financières sous réglementation fédérale d'identifier les vulnérabilités par un test régulier, et pour les institutions à empreinte technologique significative elle attend un test d'intrusion orienté renseignement et orienté menace ainsi que des exercices d'équipe rouge qui simulent des attaques multi-étapes réalistes (Office of the Superintendent of Financial Institutions 2022). La B-13 est fondée sur les résultats et ne fixe aucune cadence, de sorte que l'institution prouve sa conformité par la qualité et le réalisme de son test plutôt que par sa fréquence. C'est le même standard orienté renseignement que DORA et les orientations 7.3A affinées expriment, ce qui fait de la B-13 le membre canadien de la même famille plutôt qu'une obligation distincte.

Une seule colonne vertébrale : cartographier les régimes sur le NIST CSF 2.0

Aucun régulateur financier unique ne gouverne à la fois les États-Unis et le Canada, de sorte qu'une institution transfrontalière a besoin d'une référence neutre reconnue dans les deux. Le NIST Cybersecurity Framework version 2.0 est cette référence : volontaire, largement adopté des deux côtés de la frontière, et organisé autour de six fonctions, Govern, Identify, Protect, Detect, Respond et Recover (National Institute of Standards and Technology 2024). Utilisé comme colonne vertébrale, il permet à une institution d'enregistrer un seul programme de test d'intrusion et d'exprimer le résultat dans le vocabulaire que chaque régime comprend. Le test d'intrusion parle le plus directement à Identify, en faisant surgir les vulnérabilités, et à Detect et Respond, en mesurant si la surveillance et la réponse de l'institution attrapent et contiennent réellement une intrusion réaliste. La fonction Govern porte les règles d'engagement, l'indépendance et le reporting au conseil que les cinq régimes exigent. Le Tableau 1 rend la convergence concrète.

Tableau 1. Un seul programme de test d'intrusion, quatre régimes, une seule colonne vertébrale

Dimension	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Nature	Contrôle consultatif	Obligatoire pour les entités	Règle obligatoire	Attente fondée sur les résultats	Référence volontaire
Cadence	Cycle de scénarios sur 3 ans	Au moins tous les 3 ans	Au moins annuel	Aucune cadence fixe	Non prescrite
Méthode	Fondée sur scénarios, axée zone sécurisée	Équipe rouge orientée renseignement	Intérieur et extérieur, fondée sur le risque	Orientée renseignement, équipe rouge	Fonctions et résultats
Indépendance	Partie compétente, indépendante	Prestataires accrédités	Interne ou externe qualifié	Assurance indépendante	Résultat de gouvernance
Preuve principale	Périmètre, constats, remédiation	Scénarios de menace, récit d'attaque, remédiation	Rapport de test, cadence de remédiation	Réalisme et résultat du test	Résultats cartographiés

La lecture en travers de chaque ligne est la thèse : concevez le test selon le standard le plus exigeant de chaque colonne, méthode orientée renseignement, périmètre conscient de la zone sécurisée, couverture intérieur et extérieur, exécution indépendante, remédiation suivie, et le dossier unique qui en résulte satisfait les cinq.

Un modèle de préparation orienté risque

Les orientations 7.3A invitent à une lecture conformité, dans laquelle l'institution fait le minimum que le contrôle nomme. La lecture la plus précieuse, et celle que les superviseurs récompensent de plus en plus, est orientée risque : le test d'intrusion est l'instrument utilisé pour faire surgir et retirer les expositions les plus lourdes de conséquences de l'institution, et la conformité est le produit dérivé d'un travail bien fait.

La préparation commence par un référentiel de risque et de périmètre. L'institution inventorie son patrimoine lié à SWIFT, la zone sécurisée, l'interface de messagerie, les postes opérateurs, la connexion au réseau et les systèmes de back-office qui l'alimentent, et classe les chemins par la conséquence d'une compromission plutôt que par la facilité de test. Cela produit un périmètre défini par l'endroit où se trouvent l'argent et la confiance, qui est aussi le périmètre qu'un véritable adversaire choisirait, et qui s'aligne sur la posture orientée conséquence de la B-13 et la posture orientée risque du NYDFS.

Vient ensuite l'encadrement par le renseignement sur les menaces. Le renseignement actuel sur les acteurs qui ciblent la messagerie financière façonne les scénarios, de sorte que le test répète des intrusions plausibles plutôt que génériques. C'est l'étape qui transforme un test d'intrusion en un test orienté menace, et c'est l'étape qui rend le même exercice crédible au titre de DORA et de la B-13.

L'exécution mène ensuite les scénarios sur le cycle de trois ans que les orientations 7.3A décrivent, couvrant les chemins applicatif, d'infrastructure et humain, depuis l'intérieur et l'extérieur de la frontière, par une partie indépendante, sous des règles d'engagement documentées. L'institution mesure non seulement ce qui a été trouvé mais aussi si sa propre détection et réponse ont vu le test se produire, parce que cette mesure est la preuve qu'exigent les fonctions Detect et Respond.

Enfin, la remédiation et la preuve bouclent la boucle. Les constats entrent dans un cycle de remédiation suivi dont la clôture est enregistrée, et l'ensemble du dossier, périmètre, scénarios, récit d'attaque, constats, remédiation et performance de détection, est déposé une seule fois sur la colonne vertébrale NIST CSF 2.0 et étiqueté à chaque régime. L'institution qui boucle cette boucle n'a pas réussi un test. Elle a bâti un actif de preuve de résilience réutilisable.

Notre service d'évaluation SWIFT CSP cadre et mène le test 7.3A selon ce standard, et PenTeva valide et suit les constats jusqu'à la clôture afin que la preuve tienne sous l'un quelconque des quatre régimes. Là où la modélisation de résilience DORA est dans le périmètre, DORA-MAST porte la même preuve dans l'image de résilience opérationnelle.

Conclusion

Les orientations 7.3A affinées se comprennent le mieux non comme une exigence SWIFT isolée mais comme une seule expression prudentielle d'un mouvement mondial vers le test orienté renseignement et informé par la menace. Une institution qui conçoit son test d'intrusion 2026 selon ce standard, le cadre par la conséquence, l'encadre par le renseignement actuel sur les menaces, l'exécute de façon indépendante à travers la zone sécurisée, et enregistre le résultat sur un cadre commun, peut satisfaire DORA, NIS2 là où elle s'applique encore, NYDFS Part 500 et OSFI B-13 à partir du même exercice. Le test d'intrusion cesse d'être un coût de conformité récurrent et devient l'instrument par lequel l'institution trouve et retire les risques qui comptent. Tester une fois, satisfaire plusieurs.

Acronymes

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 (deuxième). 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 (cadre européen). 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