SWIFT CSCF v2026 / Control 7.3A

اختبِر مرة، تُرضِ الكثيرين: اختبار الاختراق وفق ضابط SWIFT CSCF v2026 رقم 7.3A بوصفه تمرينًا عابرًا للأنظمة

Cambridge Cyber International / 2026

من دورة عام 2026 لبرنامج أمن عملاء SWIFT، يحمل الضابط 7.3A (اختبار الاختراق) توجيهًا مدفوعًا من المجتمع يضع النطاق وسيناريوهات الاختبار المتوقعة من مؤسسة موصولة على مدى دورة متجدّدة من ثلاث سنوات (SWIFT 2025). والمقروء معزولًا، هذا سطر تصديق آخر يجب استيفاؤه. والمقروء في مواجهة المشهد التنظيمي الأوسع، هو دليل على اتجاه سير واحد: المنظّمون عبر الاتحاد الأوروبي والولايات المتحدة وكندا يتقاربون نحو اختبار مقاد بالمعلومات الاستخباراتية ومبني على التهديد بوصفه السبيل الذي تثبت به المؤسسة أن ضوابطها تعمل لا أنها مجرد قائمة. ويحاجج هذا المقال بأن المؤسسة التي تستعدّ لاختبار اختراق 7.3A ينبغي لها أن تصمّم ذلك الاختبار مرة واحدة، إلى مستوى متطوّر، وأن تحصد الأدلة نفسها في مواجهة قانون الصمود التشغيلي الرقمي (DORA)، والتوجيه الثاني لأمن الشبكات والمعلومات (NIS2)، ولائحة الأمن السيبراني لإدارة الخدمات المالية في ولاية نيويورك (23 NYCRR Part 500)، والتوجيه B-13 الصادر عن مكتب مراقب المؤسسات المالية، مستخدمةً إطار الأمن السيبراني للمعهد الوطني الأمريكي للمعايير والتقنية النسخة 2.0 (NIST CSF 2.0) بوصفه العمود الفقري المشترك.

مشكلة قراءة 7.3A بوصفه خانة تأشير

المؤسسة الموصولة التي تعامل كل نظام بوصفه التزامًا منفصلًا تدفع غرامة بنيوية. فهي تحدّد نطاق اختبار اختراق SWIFT ضيّقًا عند المنطقة الآمنة، وتكلّف باختبار صمود منفصل لـ DORA، وتجيب على استبيان NYDFS عن الاختبار السنوي، وتعدّ أدلة لمنظّم كندي على جدول زمني رابع. وكل ارتباط يكرّر الاستطلاع نفسه، وقواعد الاشتباك نفسها، ودورة المعالجة نفسها، وكلٌّ ينتج أدلة في صورة لا يقبلها النظام التالي. والكلفة ليست المال وحده. فالاختبار المجزّأ ينتج صورة مجزّأة للمخاطر، لأن لا تمرين منفرد يرى المؤسسة كما يراها خصم حقيقي: من طرف إلى طرف، عبر المكتب الخلفي، ومحطات عمل المشغّل، وواجهة المراسلة، والاتصال بالشبكة.

والحجة هنا أن التقارب الظاهر الآن عبر الأنظمة الكبرى يجعل النهج المجزّأ متجاوَزًا. فتوجيه 7.3A، ونظام الاختبار المبني على التهديد في DORA، وتوقّع OSFI المقاد بالمعلومات الاستخباراتية، والتفويض السنوي لـ NYDFS، ليست أربعة اختبارات مختلفة. هي أربعة تعبيرات إشرافية عن فكرة واحدة، والمؤسسة التي تصمّم إلى أكثرها تطلّبًا، وتسجّل النتيجة في مواجهة إطار مشترك، تستطيع أن تُرضي الباقي بوصفه منتجًا ثانويًا.

ما الذي يتوقّعه الآن الضابط 7.3A في SWIFT CSCF v2026

يقع الضابط 7.3A في إطار ضوابط أمن العملاء بوصفه ضابطًا إرشاديًا هدفه التحقق من الصمود التشغيلي للبنية المتصلة بـ SWIFT لدى المستخدم عبر تحديد الثغرات التي قد تفضي إلى اختراق المنطقة الآمنة أو المكتب الخلفي (SWIFT 2025). وجوهر تغيير 2026 ليس رقم ضابط جديدًا بل توجيهًا أحدّ حول كيفية تحديد نطاق الاختبار وما السيناريوهات التي ينبغي أن يغطّيها. فالإطار يصوغ الآن مجموعة من سيناريوهات الاختبار التي ينبغي ممارستها عبر دورة من ثلاث سنوات، بحيث لا تستطيع مؤسسة أن تستوفي الضابط بمسح خارجي ضيّق واحد يُكرَّر سنويًا. والتوقّع هو أن يغطّي البرنامج، على مدى الدورة، اختبار طبقة التطبيق لواجهة المراسلة والمكوّنات المتصلة بها، واختبار بنية المنطقة الآمنة وتجزئتها، والمسارات البشرية ومسارات محطات عمل المشغّل التي تستغلّها الاقتحامات الحقيقية.

ويترتّب على ذلك تبعتان تصميميتان. أولًا، يجب تعريف النطاق في مواجهة المنطقة الآمنة وحدود الثقة فيها لا في مواجهة نطاق شبكي مريح، لأن غرض الضابط هو إثبات أن المهاجم لا يستطيع الانتقال من المكتب الخلفي إلى طبقة المراسلة. ثانيًا، يجب أن يُجري الاختبار طرف كفء ومستقل بدرجة كافية، وأن تغذّي نتائجه دورة معالجة متتبَّعة يكون إغلاقها نفسه دليلًا. والضابط إرشادي لا إلزامي لكل نوع بنية، لكن بالنسبة للمؤسسات التي تصدّق ذاتيًا في مواجهته، سينتظر المُقيّم أن يرى النطاق والمنهج والنتائج والمعالجة بوصفها سجلًّا متماسكًا، لا شهادة.

الأنظمة الأربعة المجاورة

واختبار الاختراق المبني على التهديد DORA

يطالب قانون الصمود التشغيلي الرقمي كل الكيانات المالية المشمولة باختبار أنظمتها لتقنية المعلومات والاتصالات بانتظام، ويطالب الفئة الفرعية من الكيانات المهمّة بأداء اختبار متقدّم عبر اختبار الاختراق المبني على التهديد (TLPT) مرة كل ثلاث سنوات على الأقل (European Parliament and Council 2022a). واختبار TLPT مقاد بالمعلومات الاستخباراتية: محاكاة فريق أحمر مضبوطة في مواجهة أنظمة إنتاج حية، مصمَّمة على نمط أساليب المهاجمين الحقيقيين وتقنياتهم وإجراءاتهم، تُجرى وفق منهجية يكون إطار TIBER-EU مرجعها الأوروبي (European Central Bank 2018). والمؤسسة التي تعدّ اختبار 7.3A إلى مستوى

مبني على التهديد، مع تشكيل المعلومات الاستخباراتية الراهنة لسيناريوهاته، تكون قد بنت أصلًا عمود اختبار DORA الفقري، مختلفةً أساسًا في النطاق الرسمي وفي الحوكمة الإشرافية المحيطة باختبار TLPT معيّن.

وإعفاء القانون الخاص NIS2

يرفع التوجيه الثاني لأمن الشبكات والمعلومات خط الأساس لإدارة مخاطر الأمن السيبراني والإبلاغ عن الحوادث عبر الكيانات الأساسية والمهمّة، وانتقلت السلطات الوطنية من النقل إلى الإشراف الفاعل خلال عام 2026 (European Parliament and Council 2022b; European Commission 2025). وبالنسبة للكيانات المالية فالنقطة العملية واحدة من الأسبقية: DORA قانون خاص، والمادة 4 من NIS2 تفسح له المجال حيث تكون قواعد القطاع المالي معادِلة على الأقل. وعليه ينبغي للمؤسسة أن تعامل DORA بوصفه نظام اختبار الصمود الفاعل، مع إدراك أن كيانات المجموعة خارج المحيط المالي، كشركة تقنية تابعة مشتركة، قد تبقى ضمن NIS2 وتستفيد من أدلة الاختبار نفسها.

الولايات المتحدة: NYDFS Part 500 وتوقّعات FFIEC

تطالب لائحة الأمن السيبراني لإدارة الخدمات المالية في ولاية نيويورك كل كيان مشمول بإجراء اختبار اختراق لأنظمة معلوماته مرة سنويًا على الأقل، من داخل حدود الأنظمة ومن خارجها، استنادًا إلى تقييم مخاطر الكيان (New York State Department of Financial Services 2023). وقد شدّدت اللائحة المعدّلة توقّعات الحوكمة والاختبار أكثر (Ropes and Gray 2026). وعلى المستوى الفيدرالي، لا يفرض المجلس الفيدرالي لفحص المؤسسات المالية قاعدة ثابتة لكنه يعامل اختبار الاختراق على يد أطراف مؤهّلة ومستقلة بوصفه توقّع فاحص ومؤشّر نضج ضمن كتيّب أمن المعلومات لديه (Federal Financial Institutions Examination Council 2016). والمؤسسة التي تستوفي 7.3A إلى مستوى رفيع، باختبار من داخل الحدود ومن خارجها على إيقاع معرّف، تنتج بالضبط الوثائق التي يتوقّعها فاحص NYDFS وفحص FFIEC.

كندا: التوجيه B-13 الصادر عن OSFI

يطالب التوجيه B-13 الصادر عن مكتب مراقب المؤسسات المالية، النافذ منذ 1 January 2024، المؤسسات المالية الخاضعة للتنظيم الفيدرالي بتحديد الثغرات عبر اختبار منتظم، وللمؤسسات ذات البصمة التقنية الكبيرة يتوقّع اختبار اختراق مقادًا بالمعلومات الاستخباراتية ومبنيًّا على التهديد وتمارين فريق أحمر تحاكي هجمات واقعية متعدّدة المراحل (Office of the Superintendent of Financial Institutions 2022). والتوجيه B-13 قائم على النتيجة ولا يضع إيقاعًا ثابتًا، فتثبت المؤسسة الامتثال عبر جودة اختبارها وواقعيته لا عبر تواتره. وهذا هو المستوى المقاد بالمعلومات الاستخباراتية نفسه الذي يعبّر عنه DORA وتوجيه 7.3A المشحوذ، وهو ما يجعل B-13 العضو الكندي في العائلة نفسها لا التزامًا منفصلًا.

عمود فقري واحد: تخطيط الأنظمة على NIST CSF 2.0

لا منظّم مالي واحد يحكم كلًّا من الولايات المتحدة وكندا، فالمؤسسة العابرة للحدود تحتاج إلى مرجع محايد معترَف به في كليهما. وإطار الأمن السيبراني للمعهد الوطني للمعايير والتقنية النسخة 2.0 هو ذلك المرجع: طوعي، واسع التبنّي على جانبي الحدود، ومنظَّم حول ست وظائف، الحوكمة والتحديد والحماية والكشف والاستجابة والتعافي (National Institute of Standards and Technology 2024). ومستخدَمًا عمودًا فقريًّا، يتيح للمؤسسة أن تسجّل برنامج اختبار اختراق واحدًا وأن تعبّر عن النتيجة بمفردات يفهمها كل نظام. ويتحدّث اختبار الاختراق على نحو أكثر مباشرة إلى وظيفة التحديد، عبر إظهار الثغرات، وإلى وظيفتي الكشف والاستجابة، عبر قياس ما إن كانت مراقبة المؤسسة واستجابتها تلتقطان فعلًا اقتحامًا واقعيًا وتحتويانه. وتحمل وظيفة الحوكمة قواعد الاشتباك والاستقلال والإبلاغ إلى المجلس التي تطالب بها الأنظمة الخمسة كلها. ويجسّد الجدول 1 التقارب ملموسًا.

الجدول 1. برنامج اختبار اختراق واحد، أربعة أنظمة، عمود فقري واحد

البُعد	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
الطبيعة	ضابط إرشادي	إلزامي للكيانات المهمّة	قاعدة إلزامية	توقّع قائم على النتيجة	مرجع طوعي
الإيقاع	دورة سيناريوهات من 3 سنوات	مرة كل 3 سنوات على الأقل	سنوي على الأقل	لا إيقاع ثابت	غير محدّد
المنهج	قائم على السيناريو، تركيز على المنطقة	فريق أحمر مقاد بالاستخبارات	من الداخل والخارج، قائم على المخاطر	مقاد بالاستخبارات، فريق أحمر	وظائف ونتائج
الاستقلال	طرف كفء ومستقل	مزوّدون معتمدون	مؤهّل داخلي أو خارجي	ضمان مستقل	نتيجة حوكمة
الدليل الأساسي	النطاق والنتائج والمعالجة	سيناريوهات التهديد وسرد الهجوم والمعالجة	تقرير الاختبار وإيقاع المعالجة	واقعية الاختبار ونتيجته	نتائج مخطَّطة

والقراءة عبر كل صفّ هي الأطروحة: صمّم الاختبار إلى أكثر المستويات تطلّبًا في كل عمود، منهج مقاد بالاستخبارات، نطاق واعٍ بالمنطقة الآمنة، تغطية من الداخل والخارج، تنفيذ مستقل، معالجة متتبَّعة، فيرضي السجلّ الناتج الواحد الأنظمة الخمسة كلها.

نموذج إعداد مقاد بالمخاطر

يدعو توجيه 7.3A إلى قراءة امتثالية، تفعل فيها المؤسسة الحدّ الأدنى الذي يسمّيه الضابط. والقراءة الأكثر قيمة، وهي التي يكافئها المنظّمون أكثر فأكثر، مقادة بالمخاطر: اختبار الاختراق هو الأداة المستخدمة لإظهار أكثر مكامن تعرّض المؤسسة عاقبةً وإزالتها، والامتثال هو المنتج الثانوي لفعل ذلك على نحو جيد.

يبدأ الإعداد بخط أساس للمخاطر والنطاق. فالمؤسسة تجرد عقارها المتصل بـ SWIFT، أي المنطقة الآمنة وواجهة المراسلة ومحطات عمل المشغّل والاتصال بالشبكة وأنظمة المكتب الخلفي التي تغذّيه، وترتّب المسارات بحسب عاقبة الاختراق لا بحسب سهولة الاختبار. وهذا ينتج نطاقًا معرّفًا بحيث يقع المال والثقة، وهو أيضًا النطاق الذي سيختاره خصم حقيقي، وهو الذي يتواءم مع الوضعية المقادة بالعاقبة في B-13 والوضعية القائمة على المخاطر في NYDFS.

ويأتي بعد ذلك تأطير المعلومات الاستخباراتية عن التهديدات. فالمعلومات الراهنة عن الفاعلين الذين يستهدفون المراسلة المالية تشكّل السيناريوهات، بحيث يتمرّن الاختبار على اقتحامات معقولة لا عامة. وهذه هي الخطوة التي تحوّل اختبار اختراق إلى اختبار مبني على التهديد، وهي الخطوة التي تجعل التمرين نفسه ذا مصداقية تحت DORA وB-13.

ثم يجري التنفيذ السيناريوهات عبر دورة الثلاث سنوات التي يصفها توجيه 7.3A، مغطّيًا مسارات التطبيق والبنية والإنسان، من الداخل والخارج، على يد طرف مستقل، تحت قواعد اشتباك موثَّقة. وتقيس المؤسسة لا ما عُثر عليه فحسب بل ما إن كان كشفها هي واستجابتها قد رأيا الاختبار يقع، لأن ذلك القياس هو الدليل الذي تطالب به وظيفتا الكشف والاستجابة.

وأخيرًا، تغلق المعالجة والأدلة الحلقة. فالنتائج تدخل دورة معالجة متتبَّعة يُسجَّل إغلاقها، والسجلّ كله، أي النطاق والسيناريوهات وسرد الهجوم والنتائج والمعالجة وأداء الكشف، يُحفَظ مرة واحدة في مواجهة عمود NIST CSF 2.0 الفقري ويُوسَم لكل نظام. والمؤسسة التي تتمّ هذه الحلقة لم تجتَز اختبارًا واحدًا. بل بنت أصل أدلة صمود قابلًا لإعادة الاستخدام.

تتولّى خدمة تقييم SWIFT CSP لدينا تحديد نطاق اختبار 7.3A وإجراءه إلى هذا المستوى، ويتحقّق PenTeva من النتائج ويتتبّعها حتى الإغلاق كي تصمد الأدلة تحت أي من الأنظمة الأربعة. وحيث تكون نمذجة صمود DORA ضمن النطاق، يحمل DORA-MAST الأدلة نفسها إلى صورة الصمود التشغيلي.

الخاتمة

يُفهَم توجيه 7.3A المشحوذ على نحو أفضل لا بوصفه متطلَّب SWIFT معزولًا بل بوصفه تعبيرًا إشرافيًا واحدًا عن حركة عالمية نحو اختبار مقاد بالمعلومات الاستخباراتية ومبني على التهديد. والمؤسسة التي تصمّم اختبار اختراقها لعام 2026 إلى ذلك المستوى، وتحدّد نطاقه بحسب العاقبة، وتؤطّره بالمعلومات الاستخباراتية الراهنة عن التهديدات، وتنفّذه مستقلًّا عبر المنطقة الآمنة، وتسجّل النتيجة في مواجهة إطار مشترك، تستطيع أن تُرضي DORA، وNIS2 حيث لا يزال ينطبق، وNYDFS Part 500، وOSFI B-13 من التمرين نفسه. ويكفّ اختبار الاختراق عن كونه كلفة امتثال متكرّرة ويصير الأداة التي تجد بها المؤسسة المخاطر المهمّة وتزيلها. اختبِر مرة، تُرضِ الكثيرين.

Acronyms

CSCF, إطار ضوابط أمن العملاء (SWIFT). CSP, برنامج أمن العملاء (SWIFT). DORA, قانون الصمود التشغيلي الرقمي. FFIEC, التوجيه الثاني لأمن الشبكات والمعلومات. NIS2, تقنية المعلومات والاتصالات. ICT, المجلس الفيدرالي لفحص المؤسسات المالية. OSFI, إدارة الخدمات المالية في ولاية نيويورك. NYDFS, إطار الأمن السيبراني للمعهد الوطني للمعايير والتقنية NIST CSF, الفريق الأحمر الأخلاقي. TIBER-EU, جمعية الاتصالات المالية العالمية بين البنوك. SWIFT, مكتب مراقب المؤسسات المالية. اختبار الاختراق المبني على التهديد. TLPT, المبني على المعلومات الاستخباراتية عن التهديدات (إطار أوروبي)

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