SWIFT CSCF v2026 / Control 7.3A

한 번 시험하고, 여럿을 충족하다: 법체계를 가로지르는 연습으로서의 SWIFT CSCF v2026 7.3A 침투 시험

Cambridge Cyber International / 2026

SWIFT 고객 보안 프로그램의 2026년 사이클에서, Control 7.3A(침투 시험)는, 연결된 기관에 대해 계속 돌아가는 3년 주기에 걸쳐 기대되는 스코프와 시험 시나리오를 정하는 커뮤니티 주도의 지침을 동반한다(SWIFT 2025년). 고립시켜 읽으면 이것은 충족해야 할 또 하나의 인증 항목에 불과하다. 더 넓은 규제의 지형에 비추어 읽으면, 그것은 단일한 진행 방향의 증거다. 즉 유럽연합, 미국, 캐나다의 감독 당국들은, 기관이 자신의 통제가 단지 존재하는 것이 아니라 작동한다는 것을 증명하는 수단으로서, 인텔리전스 주도의, 위협에 기반한 시험으로 수렴하고 있다. 본고는, 7.3A 침투 시험에 대비하는 기관이 그 시험을 최첨단 수준으로 단 한 번 설계하고, 같은 증거를, 디지털 운영 복원력법(DORA), 제2차 네트워크 및 정보 보안 지침(NIS2), 뉴욕주 금융서비스국의 사이버보안 규정(23 NYCRR Part 500), 그리고 금융감독청 가이드라인 B-13에 대해, 미국 국립표준기술연구소 사이버보안 프레임워크 버전 2.0(NIST CSF 2.0)을 공통의 척추로 삼아 거두어들여야 한다고 논한다.

7.3A를 체크박스로 읽는 것의 문제

각 법체계를 별개의 의무로 다루는 연결된 기관은 구조적 페널티를 치른다. 그것은 SWIFT 침투 시험을 보안 구역으로 좁게 스코핑하고, 별개의 DORA 복원력 시험을 발주하며, 연차 시험에 관한 NYDFS 설문지에 답하고, 네 번째 일정으로 캐나다 감독 당국을 위한 증거를 준비한다. 각 계약은 같은 정찰, 같은 교전 규칙, 같은 시정 사이클을 반복하며, 그 각각은 다음 법체계가 받아들이지 않는 형태의 증거를 만들어낸다. 대가는 돈만이 아니다. 파편화된 시험은 파편화된 위험의 상을 낳는다. 왜냐하면 어떤 단일한 연습도 현실의 적대자가 보듯이 기관을 보지 못하기 때문이다. 즉 백오피스, 운영자 워크스테이션, 메시징 인터페이스, 그리고 네트워크로의 연결을 가로지르는, 끝에서 끝까지의 상이다.

여기서의 논점은, 지금 주요 법체계들을 가로질러 보이게 된 수렴이 파편화된 접근을 시대에 뒤떨어지게 만든다는 것이다. 7.3A 지침, DORA의 위협 주도 시험 체제, OSFI의 인텔리전스 주도 기대, 그리고 NYDFS의 연차 의무는 네 개의 서로 다른 시험이 아니다. 그것들은 하나의 이념의 네 가지 감독적 표현이며, 그중 가장 까다로운 것에 맞추어 설계하고 그 결과를 공통의 프레임워크에 대해 기록하는 기관은 다른 것들을 부산물로 충족할 수 있다.

SWIFT CSCF v2026의 Control 7.3A가 이제 기대하는 것

Control 7.3A는, 고객 보안 통제 프레임워크 안에서, 그 목적이 보안 구역 또는 백오피스의 침해로 이어질 수 있는 취약점을 식별함으로써 이용자의 SWIFT 관련 인프라스트럭처의 운영 복원력을 검증하는 데 있는 권고적 통제로 자리매김되어 있다(SWIFT 2025년). 2026년 변경의 실질은 새로운 통제 번호가 아니라, 시험이 어떻게 스코핑되어야 하고 어떤 시나리오를 망라해야 하는지에 관한 더 날카로운 지침이다. 프레임워크는 이제 3년 주기에 걸쳐 연습되어야 할 일군의 시험 시나리오를 명시하며, 따라서 기관은 연차로 반복되는 단일한 좁은 외부 스캔으로 이 통제를 충족할 수 없다. 기대되는 것은, 그 주기에 걸쳐 프로그램이 메시징 인터페이스와 관련 구성요소의 애플리케이션 계층 시험, 보안 구역과 그 세그먼테이션의 인프라스트럭처 시험, 그리고 실제 침입이 악용하는 인적 및 운영자 워크스테이션 경로를 망라하는 것이다.

두 가지 설계상의 귀결이 따른다. 첫째, 스코프는 편리한 네트워크 범위에 대해서가 아니라 보안 구역과 그 신뢰 경계에 대해 정의되어야 한다. 왜냐하면 이 통제의 목적은 공격자가 백오피스에서 메시징 계층으로 피벗할 수 없음을 증명하는 데 있기 때문이다. 둘째, 시험은 유능하고 충분히 독립적인 당사자에 의해 수행되어야 하며, 그 발견 사항은, 그 종결 자체가 증거가 되는 추적되는 시정 사이클에 공여되어야 한다. 이 통제는 모든 아키텍처 유형에 대해 의무적이 아니라 권고적이지만, 그에 대해 자기 인증하는 기관에 대해서, 평가자는 스코프, 방법, 발견 사항, 시정을 증명서가 아니라 일관된 기록으로 보기를 기대할 것이다.

네 개의 이웃하는 법체계

DORA와 위협 주도 침투 시험

디지털 운영 복원력법은 적용 대상이 되는 모든 금융 주체에 대해 그 정보통신기술 시스템을 정기적으로 시험할 것을 요구하며, 중요한 주체의 부분집합에 대해서는 적어도 3년마다 위협 주도 침투 시험(TLPT)의 수단으로 고도의 시험을 수행할 것을 요구한다(European Parliament and Council 2022a). TLPT는 인텔리전스 주도다. 즉 가동 중인 본번 시스템에 대한 통제된 레드팀 모의 연습이며, 현실의 위협 행위자의 전술, 기법, 절차를 본떠, TIBER-EU 프레임워크가 유럽의 참조 기준이 되는 방법론 아래 수행된다(European Central Bank 2018). 7.3A 시험을, 현재의 위협 인텔리전스가 그 시나리오를 빚는 위협 주도 수준으로 준비하는 기관은 이미 DORA 시험의 척추를 쌓고 있으며, 주로 정식 스코프와, 지정된 TLPT를 감싸는 감독적 거버넌스에서만 다를

뿐이다.

NIS2와 lex specialis 적용 제외

제2차 네트워크 및 정보 보안 지침은 필수 주체와 중요 주체를 가로질러 사이버보안 위험 관리와 사고 보고의 기준선을 끌어올리며, 각국 당국은 2026년 동안 치환에서 능동적 감독으로 이행했다(European Parliament and Council 2022b; European Commission 2025). 금융 주체에게 실무상의 요점은 우선순위의 하나다. 즉 DORA는 lex specialis이며, NIS2의 제4조는 금융 부문 규칙이 적어도 동등한 경우 그에 양보한다. 따라서 기관은 DORA를 실효적인 복원력 시험 체제로 다루어야 하며, 동시에 공유된 기술 자회사 같은 금융 경계 바깥의 그룹 주체가 NIS2 안에 머물면서 같은 시험 증거로부터 편익을 받을 수 있음을 인식해야 한다.

미국: NYDFS Part 500과 FFIEC 기대

뉴욕주 금융서비스국의 사이버보안 규정은 각 대상 주체에 대해 그 정보 시스템의 침투 시험을, 해당 주체의 위험 평가에 기반하여, 시스템 경계의 안쪽과 바깥쪽 양면에서, 적어도 연차로 수행할 것을 요구한다(New York State Department of Financial Services 2023). 개정된 규정은 거버넌스와 시험 기대를 한층 더 조였다(Ropes and Gray 2026). 연방 수준에서, 연방금융기관검사협의회는 고정된 규칙을 부과하지 않지만, 그 정보 보안 안내서 안에서, 자격을 갖춘 독립적 당사자에 의한 침투 시험을 검사관의 기대이자 성숙도 지표로 다룬다(Federal Financial Institutions Examination Council 2016). 7.3A를 높은 수준으로 충족하고, 경계의 안쪽과 바깥쪽 양면에서 정해진 주기로 시험하는 기관은, NYDFS 검사관과 FFIEC 검사가 바로 기대하는 산출물을 만들어낸다.

캐나다: OSFI 가이드라인 B-13

2024년 1월 1일 이래 시행되고 있는 금융감독청 가이드라인 B-13은, 연방 규제 하의 금융기관에 대해 정기적인 시험을 통해 취약점을 식별할 것을 요구하며, 중요한 기술적 발자국을 가진 기관에 대해서는 현실적인 다단계 공격을 모의하는 인텔리전스 주도의, 위협 주도 침투 시험과 레드팀 연습을 기대한다(Office of the Superintendent of Financial Institutions 2022). B-13은 성과에 기반하며 고정된 주기를 두지 않으므로, 기관은 그 빈도가 아니라 시험의 질과 현실성을 통해 준수를 입증한다. 이것은 DORA와 다듬어진 7.3A 지침이 표현하는 것과 같은 인텔리전스 주도 수준이며, 그것이 B-13을 별개의 의무가 아니라 같은 일족의 캐나다 일원이게 한다.

하나의 척추: 각 법체계를 NIST CSF 2.0에 사상하기

미국과 캐나다 양쪽을 통치하는 단일한 금융 규제 당국은 존재하지 않으므로, 국경을 넘나드는 기관은 양쪽에서 인지된 중립적 참조 기준을 필요로 한다. NIST 사이버보안 프레임워크 버전 2.0이 그 참조 기준이다. 즉 임의적이고, 국경의 양쪽에서 널리 채택되며, 여섯 가지 기능을 중심으로 조직되어 있다. 즉 통치, 식별, 방어, 탐지, 대응, 복구다(National Institute of Standards and Technology 2024). 척추로 사용하면, 그것은 기관이 하나의 침투 시험 프로그램을 기록하고 그 결과를 모든 법체계가 이해하는 어휘로 표현하는 것을 가능케 한다. 침투 시험은 취약점을 표면화함으로써 식별에 가장 직접적으로 말을 걸고, 기관의 모니터링과 대응이 현실적인 침입을 실제로 포착하고 봉쇄하는지를 측정함으로써 탐지와 대응에 말을 건다. 통치 기능은 다섯 법체계 모두가 요구하는 교전 규칙, 독립성, 이사회 보고를 담당한다. 표 1이 이 수렴을 구체화한다.

표 1. 하나의 침투 시험 프로그램, 네 법체계, 하나의 척추

차원	SWIFT 7.3A v2026	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
성격	권고적 통제	중요 주체에 의무	의무적 규칙	성과 기반 기대	임의적 참조 기준
주기	3년 시나리오 주기	적어도 3년마다	적어도 연차	고정된 주기 없음	규정되지 않음
방법	시나리오 기반, 보안 구역 중심	인텔리전스 주도 레드팀	안쪽과 바깥쪽, 위험 기반	인텔리전스 주도, 레드팀	기능과 성과
독립성	유능하고 독립적인 당사자	인증된 제공자	자격을 갖춘 내부 또는 외부	독립적 보증	거버넌스 성과
주요 증거	스코프, 발견 사항, 시정	위협 시나리오, 공격 서사, 시정	시험 보고서, 시정 주기	시험의 현실성과 성과	사상된 성과

각 행을 가로질러 읽는 것이 곧 논지다. 즉 각 열에서 가장 까다로운 수준에 시험을 설계하라. 인텔리전스 주도 방법, 보안 구역을

의식한 스코프, 안쪽과 바깥쪽 양면의 망라, 독립적 실행, 추적되는 시정이며, 그렇게 얻어지는 단일한 기록이 다섯 당국 모두를 충족한다.

위험 주도 준비 모델

7.3A 지침은 기관이 통제가 지목하는 최소한을 행하는 컴플라이언스적 읽기를 부른다. 더 가치 있고, 감독 당국이 점점 더 보상하는 읽기는 위험 주도의 것이다. 즉 침투 시험은 기관의 가장 결과가 무거운 노출을 표면화하고 퇴역시키기 위해 사용하는 도구이며, 컴플라이언스는 그것을 잘 행한 것의 부산물이다.

준비는 위험과 스코프의 기준선에서 시작한다. 기관은 자신의 SWIFT 관련 자산, 즉 보안 구역, 메시징 인터페이스, 운영자 워크스테이션, 네트워크로의 연결, 그리고 그에 공급하는 백오피스 시스템을 목록화하고, 시험의 용이함이 아니라 침해의 결과에 따라 각 경로를 순위 매긴다. 이는 돈과 신뢰가 어디에 깃드는지에 따라 정의되는 스코프를 낳으며, 그것은 또한 현실의 적대자가 택할 스코프이기도 하고, B-13의 결과 주도 자세 및 NYDFS의 위험 기반 자세와 정합한다.

다음에 오는 것은 위협 인텔리전스에 의한 틀 잡기다. 금융 메시징을 표적으로 삼는 행위자에 관한 현재의 인텔리전스가 시나리오를 빚어, 그로써 시험이 범용적인 것이 아니라 그럴듯한 침입을 연습하도록 한다. 이것이 침투 시험을 위협 주도 시험으로 바꾸는 단계이며, 그것이 같은 연습을 DORA와 B-13 아래 신뢰할 만하게 하는 단계다.

그런 다음 실행은, 7.3A 지침이 그리는 3년 주기에 걸쳐 각 시나리오를 돌리며, 애플리케이션, 인프라스트럭처, 인적 경로를, 경계의 안쪽과 바깥쪽에서, 독립적 당사자에 의해, 문서화된 교전 규칙 아래 망라한다. 기관은 무엇이 발견되었는지뿐 아니라, 자신의 탐지와 대응이 시험의 발생을 보았는지를 측정한다. 왜냐하면 그 측정이야말로 탐지와 대응 기능이 요구하는 증거이기 때문이다.

마지막으로, 시정과 증거가 고리를 닫는다. 발견 사항은 그 종결이 기록되는 추적되는 시정 사이클로 들어가며, 그 기록의 전체, 즉 스코프, 시나리오, 공격 서사, 발견 사항, 시정, 탐지 성능이 NIST CSF 2.0이라는 척추에 대해 단 한 번 제출되고 각 법체계에 태깅된다. 이 고리를 완수하는 기관은 하나의 시험에 합격한 것이 아니다. 그것은 재사용 가능한 복원력 증거 자산을 쌓은 것이다.

당사의 SWIFT CSP 평가 서비스는 7.3A 시험을 이 수준으로 스코핑하고 돌리며, PenTeva가 발견 사항을 검증하고 종결까지 추적함으로써 그 증거가 네 법체계 어느 것 아래서도 버티도록 한다. DORA 복원력 모델링이 스코프에 들어가는 경우, DORA-MAST가 같은 증거를 운영 복원력의 상으로 운반한다.

결론

다듬어진 7.3A 지침은, 고립된 SWIFT 요건으로서가 아니라, 인텔리전스 주도의, 위협에 기반한 시험으로의 전 지구적 운동의 한 감독적 표현으로 이해하는 것이 가장 좋다. 자신의 2026년 침투 시험을 그 수준으로 설계하고, 결과에 따라 스코핑하며, 현재의 위협 인텔리전스로 틀을 잡고, 보안 구역을 가로질러 독립적으로 실행하며, 그 결과를 공통의 프레임워크에 대해 기록하는 기관은, DORA, 여전히 적용되는 경우의 NIS2, NYDFS Part 500, 그리고 OSFI B-13을, 같은 연습으로부터 충족할 수 있다. 침투 시험은 되풀이되는 컴플라이언스 비용이기를 그치고, 기관이 중요한 위험을 찾아 퇴역시키는 도구가 된다. 한 번 시험하고, 여럿을 충족하라.

두문자어

CSCF, 고객 보안 통제 프레임워크(SWIFT). CSP, 고객 보안 프로그램(SWIFT). DORA, 디지털 운영 복원력법. FFIEC, 연방금융기관검사협의회. ICT, 정보통신기술. NIS2, 네트워크 및 정보 보안 지침(제2차). NIST CSF, 국립표준기술연구소 사이버보안 프레임워크. NYDFS, 뉴욕주 금융서비스국. OSFI, 금융감독청. SWIFT, 국제은행간금융통신협회. TIBER-EU, 위협 인텔리전스 기반 윤리적 레드팀(유럽 프레임워크). TLPT, 위협 주도 침투 시험.

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