SWIFT CSCF v2026 / Control 7.3A

Bir kez test et, çoğunu karşıla: SWIFT CSCF v2026 7.3A sızma testi bir rejimler arası tatbikat olarak

Cambridge Cyber International / 2026

SWIFT Müşteri Güvenliği Programı'nın 2026 döngüsünden, Control 7.3A (Sızma Testi), bağlı bir kurumun döner üç yıllık bir döngü boyunca ulaşması beklenen kapsamı ve test senaryolarını belirleyen, topluluk öncülüklü bir rehberlik taşır (SWIFT 2025). Tek başına okunduğunda bu, karşılanacak bir başka beyan satırıdır. Daha geniş düzenleyici manzaraya karşı okunduğunda ise tek bir gidiş yönünün kanıtıdır: Avrupa Birliği, Amerika Birleşik Devletleri ve Kanada'daki denetçiler, bir kurumun kontrollerinin yalnızca var olmaktan ziyade işlediğini kanıtlamasının yolu olarak istihbarat öncülüklü, tehdit bilgili teste yakınsamaktadır. Bu makale, 7.3A sızma testine hazırlanan bir kurumun o testi bir kez, en ileri standartta tasarlaması ve aynı kanıtı Dijital Operasyonel Dayanıklılık Yasası'na (DORA), İkinci Ağ ve Bilgi Güvenliği Direktifi'ne (NIS2), New York Eyaleti Finansal Hizmetler Departmanı siber güvenlik düzenlemesine (23 NYCRR Part 500) ve Finansal Kurumlar Denetleme Ofisi B-13 Kılavuzu'na karşı, Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü Siber Güvenlik Çerçevesi sürüm 2.0'ı (NIST CSF 2.0) ortak omurga olarak kullanarak hasat etmesi gerektiğini savunur.

7.3A'nın onay kutusu okumasının sorunu

Her rejimi ayrı bir yükümlülük olarak ele alan bağlı bir kurum, yapısal bir bedel öder. Bir SWIFT sızma testini güvenli bölgeye dar bir biçimde kapsamlandırır, ayrı bir DORA dayanıklılık testi sipariş eder, yıllık test üzerine bir NYDFS anketini yanıtlar ve dördüncü bir takvimde bir Kanada denetçisi için kanıt hazırlar. Her görevlendirme aynı keşfi, aynı angajman kurallarını, aynı iyileştirme döngüsünü tekrarlar ve her biri bir sonraki rejimin kabul etmediği bir biçimde kanıt üretir. Maliyet yalnızca para değildir. Parçalı test, parçalı bir risk resmi üretir, çünkü hiçbir tek tatbikat kurumu gerçek bir hasmın göreceği gibi görmez: uçtan uca, arka ofis, operatör iş istasyonları, mesajlaşma arayüzü ve ağa bağlantı boyunca.

Buradaki sav, başlıca rejimler genelinde artık görünür olan yakınsamanın parçalı yaklaşımı çağdışı kıldığıdır. 7.3A rehberliği, DORA'nın tehdit öncülüklü test rejimi, OSFI'nin istihbarat öncülüklü beklentisi ve NYDFS yıllık zorunluluğu dört farklı test değildir. Bunlar tek bir fikrin dört denetsel ifadesidir ve bunların en zorlayıcısına tasarlayan, sonucu paylaşılan bir çerçeveye karşı kaydeden bir kurum, diğerlerini bir yan ürün olarak karşılayabilir.

SWIFT CSCF v2026 Control 7.3A artık neyi bekliyor

Control 7.3A, Müşteri Güvenliği Kontrolleri Çerçevesi'nde, amacı güvenli bölgenin veya arka ofisin tehlikeye girmesine yol açabilecek güvenlik açıklarını saptayarak kullanıcının SWIFT ile ilgili altyapısının operasyonel dayanıklılığını doğrulamak olan tavsiye niteliğinde bir kontrol olarak yer alır (SWIFT 2025). 2026 değişikliğinin özü yeni bir kontrol numarası değil, testin nasıl kapsamlandırılması gerektiği ve hangi senaryoları kapsaması gerektiği konusunda daha keskin bir rehberliktir. Çerçeve artık üç yıllık bir döngü boyunca uygulanacak bir test senaryoları kümesini ifade eder, böylece bir kurum kontrolü yıllık olarak tekrarlanan tek bir dar dış taramayla karşılayamaz. Beklenti, döngü boyunca programın mesajlaşma arayüzü ve ilgili bileşenlerin uygulama katmanı testini, güvenli bölge ve bölümlemesinin altyapı testini ve gerçek izinsiz girişlerin sömürdüğü insan ve operatör iş istasyonu yollarını kapsamasıdır.

İki tasarım sonucu çıkar. Birincisi, kapsam, uygun bir ağ aralığına karşı değil, güvenli bölgeye ve güven sınırlarına karşı tanımlanmalıdır, çünkü kontrolün amacı bir saldırganın arka ofisten mesajlaşma katmanına geçemeyeceğini kanıtlamaktır. İkincisi, test yetkin ve yeterince bağımsız bir tarafça yürütülmelidir ve bulguları, kapanışı kendisi kanıt olan izlenen bir iyileştirme döngüsünü beslemelidir. Kontrol her mimari türü için zorunlu değil tavsiye niteliğindedir, ancak ona karşı öz beyanda bulunan kurumlar için değerlendirici, bir sertifika değil, tutarlı bir kayıt olarak kapsam, yöntem, bulgular ve iyileştirmeyi görmeyi bekler.

Dört komşu rejim

DORA ve tehdit öncülüklü sızma testi

Dijital Operasyonel Dayanıklılık Yasası, kapsamdaki tüm finansal kuruluşların bilgi ve iletişim teknolojisi sistemlerini düzenli olarak test etmesini gerektirir ve önemli kuruluşlardan oluşan alt kümenin en az her üç yılda bir tehdit öncülüklü sızma testi (TLPT) yoluyla ileri düzey test yapmasını gerektirir (European Parliament and Council 2022a). TLPT istihbarat öncülüklüdür: gerçek tehdit aktörlerinin taktik, teknik ve prosedürleri model alınarak, TIBER-EU çerçevesinin Avrupa referansı olduğu bir metodoloji altında, canlı üretim sistemlerine karşı kontrollü bir kırmızı takım simülasyonu (European Central Bank 2018). Senaryolarını güncel tehdit istihbaratıyla biçimlendirerek 7.3A testini tehdit öncülüklü bir standartta hazırlayan kurum, bir DORA testinin omurgasını zaten inşa eder; başlıca farkı resmi kapsam ve belirlenmiş bir TLPT'yi saran denetsel yönetişimdedir.

NIS2 ve özel kanun istisnası

İkinci Ağ ve Bilgi Güvenliği Direktifi, temel ve önemli kuruluşlar genelinde siber güvenlik risk yönetimi ile olay raporlaması için taban çizgisini yükseltir ve ulusal otoriteler 2026 boyunca aktarımdan etkin denetime geçti (European Parliament and Council 2022b; European Commission 2025). Finansal kuruluşlar için pratik nokta önceliktir: DORA özel kanundur ve NIS2'nin 4. Maddesi, finansal sektör kuralları en azından eşdeğer olduğunda ona yol verir. Bir kurum bu nedenle DORA'yı işlevdeki dayanıklılık testi rejimi olarak ele almalı, aynı zamanda finansal çevrenin dışındaki grup kuruluşlarının (örneğin paylaşılan bir teknoloji yan kuruluşunun) NIS2 içinde kalabileceğini ve aynı test kanıtından yararlanabileceğini tanımalıdır.

Amerika Birleşik Devletleri: NYDFS Part 500 ve FFIEC beklentileri

New York Eyaleti Finansal Hizmetler Departmanı siber güvenlik düzenlemesi, her kapsanan kuruluşun, kuruluşun risk değerlendirmesine dayanarak, bilgi sistemlerine hem sistem sınırlarının içinden hem de dışından en az yılda bir sızma testi yapmasını gerektirir (New York State Department of Financial Services 2023). Değiştirilen düzenleme yönetişim ve test beklentilerini daha da sıkılaştırmıştır (Ropes and Gray 2026). Federal düzeyde, Federal Finansal Kurumlar Sınav Konseyi sabit bir kural dayatmaz ancak Bilgi Güvenliği kitapçığında, nitelikli, bağımsız taraflarca yapılan sızma testini bir sınav uzmanı beklentisi ve bir olgunluk göstergesi olarak ele alır (Federal Financial Institutions Examination Council 2016). 7.3A'yı yüksek bir standartta karşılayan, tanımlı bir kadansta sınırın hem içinden hem dışından test eden kurum, bir NYDFS sınav uzmanının ve bir FFIEC sınavının beklediği tam da o eserleri üretir.

Kanada: OSFI B-13 Kılavuzu

1 Ocak 2024'ten beri yürürlükte olan Finansal Kurumlar Denetleme Ofisi B-13 Kılavuzu, federal düzeyde düzenlenen finansal kurumların güvenlik açıklarını düzenli test yoluyla saptamasını gerektirir ve önemli teknoloji ayak izlerine sahip kurumlar için gerçekçi çok aşamalı saldırıları simüle eden istihbarat öncülüklü, tehdit öncülüklü sızma testi ve kırmızı takım tatbikatları bekler (Office of the Superintendent of Financial Institutions 2022). B-13 sonuç temellidir ve sabit bir kadans belirlemez, dolayısıyla kurum uyumu sıklığından ziyade testinin kalitesi ve gerçekçiliği yoluyla kanıtlar. Bu, DORA ve keskinleştirilmiş 7.3A rehberliğinin ifade ettiği aynı istihbarat öncülüklü standarttır, bu da B-13'ü ayrı bir yükümlülükten ziyade aynı ailenin Kanadalı üyesi yapar.

Tek omurga: rejimleri NIST CSF 2.0'a eşlemek

Tek bir finansal düzenleyici hem Amerika Birleşik Devletleri'ni hem de Kanada'yı yönetmediğinden, sınır ötesi bir kurumun her ikisinde de tanınan tarafsız bir referansa ihtiyacı vardır. NIST Siber Güvenlik Çerçevesi sürüm 2.0 o referanstır: gönüllü, sınırın her iki yanında geniş biçimde benimsenmiş ve altı işlev etrafında düzenlenmiş, yani Yönet (Govern), Tanımla (Identify), Koru (Protect), Tespit Et (Detect), Müdahale Et (Respond) ve Kurtar (Recover) (National Institute of Standards and Technology 2024). Bir omurga olarak kullanıldığında, bir kurumun tek bir sızma testi programını kaydetmesine ve sonucu her rejimin anladığı söz dağarcığıyla ifade etmesine olanak tanır. Sızma testi en doğrudan Tanımla'ya, güvenlik açıklarını yüzeye çıkararak, ve Tespit Et ile Müdahale Et'e, kurumun izleme ve müdahalesinin gerçekçi bir izinsiz girişi gerçekten yakalayıp yakalamadığını ve kontrol altına alıp almadığını ölçerek konuşur. Yönet işlevi, beş rejimin de gerektirdiği angajman kurallarını, bağımsızlığı ve yönetim kurulu raporlamasını taşır. Tablo 1 yakınsamayı somutlaştırır.

Tablo 1. Tek bir sızma testi programı, dört rejim, tek bir omurga

Boyut	SWIFT 7.3A	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
Nitelik	Tavsiye kontrolü	Önemli kuruluşlar için zorunlu	Zorunlu kural	Sonuç temelli beklenti	Gönüllü referans
Kadans	3 yıllık senaryo döngüsü	En az her 3 yılda bir	En az yıllık	Sabit kadans yok	Belirlenmemiş
Yöntem	Senaryo temelli, güvenli bölge	İstihbarat öncülüklü kırmızı	İçeriden ve dışarıdan, risk	İstihbarat öncülüklü, kırmızı	İşlevler ve sonuçlar
Bağımsızlık	Yetkin, bağımsız taraf	Akredite sağlayıcılar	Nitelikli iç veya dış	Bağımsız güvence	Yönetişim sonucu
Birincil kanıt	Kapsam, bulgular, iyileştirme	Tehdit senaryoları, saldırı anlatısı, iyileştirme	Test raporu, iyileştirme kadansı	Testin gerçekçiliği ve sonucu	Eşlenen sonuçlar

Her satırı yatay okumak tezdir: testi her sütundaki en zorlayıcı standarda, yani istihbarat öncülüklü yönteme, güvenli bölge bilinçli kapsama, içeriden ve dışarıdan kapsamaya, bağımsız yürütmeye, izlenen iyileştirmeye tasarlayın ve ortaya çıkan tek kayıt beşini de karşılar.

Risk öncülüklü bir hazırlık modeli

7.3A rehberliği, kurumun kontrolün adlandırdığı asgariyi yaptığı bir uyum okumasına davet eder. Daha değerli olan ve denetçilerin giderek ödüllendirdiği okuma risk öncülüklüdür: sızma testi, kurumun en sonuç doğuran maruziyetlerini yüzeye çıkarmak ve emekliye ayırmak için kullanılan araçtır ve uyum, bunu iyi yapmanın yan ürünüdür.

Hazırlık bir risk ve kapsam taban çizgisiyle başlar. Kurum SWIFT ile ilgili mülkünü, yani güvenli bölgeyi, mesajlaşma arayüzünü, operatör iş istasyonlarını, ağa bağlantıyı ve onu besleyen arka ofis sistemlerini envanterler ve yolları test kolaylığına göre değil, tehlikeye girmenin sonucuna göre sıralar. Bu, paranın ve güvenin bulunduğu yere göre tanımlanmış bir kapsam üretir; bu aynı zamanda gerçek bir hasmın seçeceği kapsamdır ve B-13'ün sonuç öncülüklü duruşuyla ve NYDFS'nin risk temelli duruşuyla hizalanır.

Ardından tehdit istihbaratı çerçevelemesi gelir. Finansal mesajlaşmayı hedef alan aktörler hakkındaki güncel istihbarat senaryoları biçimlendirir, böylece test genel değil makul izinsiz girişleri prova eder. Bu, bir sızma testini tehdit öncülüklü bir teste dönüştüren adımdır ve aynı tatbikatı DORA ve B-13 altında güvenilir kılan adımdır.

Yürütme daha sonra senaryoları 7.3A rehberliğinin tanımladığı üç yıllık döngü boyunca, uygulama, altyapı ve insan yollarını kapsayarak, sınırın hem içinden hem dışından, bağımsız bir tarafça, belgelenmiş angajman kuralları altında yürütür. Kurum yalnızca neyin bulunduğunu değil, kendi tespit ve

müdahalesinin testin gerçekleştiğini görüp görmediğini de ölçer, çünkü o ölçüm Tespit Et ve Müdahale Et işlevlerinin gerektirdiği kanıttır.

Son olarak, iyileştirme ve kanıt döngüyü kapatır. Bulgular kapanışı kaydedilen, izlenen bir iyileştirme döngüsüne girer ve kapsamı, senaryoları, saldırı anlatısını, bulguları, iyileştirmeyi ve tespit performansını içeren tüm kayıt, NIST CSF 2.0 omurgasına karşı bir kez dosyalanır ve her rejime etiketlenir. Bu döngüyü tamamlayan kurum tek bir testi geçmemiştir. Yeniden kullanılabilir bir dayanıklılık kanıt varlığı inşa etmiştir.

SWIFT CSP değerlendirme hizmetimiz 7.3A testini bu standarda kapsamlandırıp yürütür ve PenTeva bulguları doğrulayıp kapanışa kadar izler, böylece kanıt dört rejimden herhangi biri altında ayakta durur. DORA dayanıklılık modellemesi kapsamda olduğunda, DORA-MAST aynı kanıtı operasyonel dayanıklılık resmine taşır.

Sonuç

Keskinleştirilmiş 7.3A rehberliği en iyi, izole bir SWIFT gerekliliği olarak değil, istihbarat öncülüklü, tehdit bilgili teste yönelik küresel bir hareketin tek bir denetsel ifadesi olarak anlaşılır. 2026 sızma testini o standarda tasarlayan, onu sonuca göre kapsamlandıran, güncel tehdit istihbaratıyla çerçeveleyen, güvenli bölge boyunca bağımsızca yürüten ve sonucu paylaşılan bir çerçeveye karşı kaydeden bir kurum, DORA'yı, hâlâ uygulandığı yerde NIS2'yi, NYDFS Part 500'ü ve OSFI B-13'ü aynı tatbikattan karşılayabilir. Sızma testi tekrarlayan bir uyum maliyeti olmaktan çıkar ve kurumun önemli olan riskleri bulduğu ve emekliye ayırdığı araç haline gelir. Bir kez test et, çoğunu karşıla.

Kısaltmalar

CSCF, Müşteri Güvenliği Kontrolleri Çerçevesi (SWIFT). CSP, Müşteri Güvenliği Programı (SWIFT). DORA, Dijital Operasyonel Dayanıklılık Yasası. FFIEC, Federal Finansal Kurumlar Sınav Konseyi. ICT, Bilgi ve İletişim Teknolojisi. NIS2, Ağ ve Bilgi Güvenliği Direktifi (ikinci). NIST CSF, Ulusal Standartlar ve Teknoloji Enstitüsü Siber Güvenlik Çerçevesi. NYDFS, New York Eyaleti Finansal Hizmetler Departmanı. OSFI, Finansal Kurumlar Denetleme Ofisi. SWIFT, Dünya Çapında Bankalararası Finansal Telekomünikasyon Topluluğu. TIBER-EU, Tehdit İstihbaratı Temelli Etik Kırmızı Takım (Avrupa çerçevesi). TLPT, Tehdit Öncülüklü Sızma Testi.

Kaynakça

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