SWIFT CSCF v2026 / Control 7.3A

एक बार परखें, अनेक को संतुष्ट करें: SWIFT CSCF v2026 के नियंत्रण 7.3A का प्रवेश परीक्षण एक अंतर-व्यवस्था अभ्यास के रूप में

Cambridge Cyber International / 2026

SWIFT ग्राहक सुरक्षा कार्यक्रम के 2026 चक्र से, नियंत्रण 7.3A (प्रवेश परीक्षण) समुदाय-संचालित मार्गदर्शन वहन करता है जो किसी जुड़ी हुई संस्था से एक चलायमान तीन वर्षीय चक्र पर अपेक्षित दायरा और परीक्षण परिदृश्य तय करता है (SWIFT 2025). पृथक रूप में पढ़ा जाए तो यह संतुष्ट करने योग्य एक और सत्यापन पंक्ति है. व्यापक नियामक परिदृश्य के विरुद्ध पढ़ा जाए तो यह यात्रा की एक ही दिशा का प्रमाण है: यूरोपीय संघ, संयुक्त राज्य अमेरिका और कनाडा के पर्यवेक्षक आसूचना-नेतृत्व वाले, खतरा-सूचित परीक्षण की ओर अभिसरित हो रहे हैं, इस तरीके के रूप में कि संस्था कैसे सिद्ध करती है कि उसके नियंत्रण केवल मौजूद रहने के बजाय काम करते हैं. यह लेख तर्क देता है कि 7.3A प्रवेश परीक्षण की तैयारी करने वाली संस्था को उस परीक्षण को एक बार, एक अत्याधुनिक मानक तक, रचना चाहिए, और वही प्रमाण डिजिटल परिचालन सहनशीलता अधिनियम (DORA), द्वितीय नेटवर्क एवं सूचना सुरक्षा निर्देश (NIS2), न्यूयॉर्क राज्य वित्तीय सेवा विभाग का साइबर सुरक्षा विनियमन (23 NYCRR Part 500), और वित्तीय संस्थाओं के अधीक्षक कार्यालय का दिशानिर्देश B-13 के विरुद्ध काटना चाहिए, संयुक्त राज्य के राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान के साइबर सुरक्षा ढाँचे के संस्करण 2.0 (NIST CSF 2.0) को साझा रीढ़ के रूप में प्रयोग करते हुए.

7.3A की चेकबॉक्स वाली पठन की समस्या

जो जुड़ी हुई संस्था हर व्यवस्था को अलग बाध्यता के रूप में बरतती है वह एक संरचनात्मक दंड चुकाती है. वह SWIFT प्रवेश परीक्षण का दायरा सुरक्षित ज़ोन तक संकीर्ण रखती है, DORA के लिए अलग सहनशीलता परीक्षण कराती है, वार्षिक परीक्षण पर NYDFS प्रश्नावली का उत्तर देती है, और एक कनाडाई पर्यवेक्षक के लिए चौथी समय-सारणी पर प्रमाण तैयार करती है. हर सहभागिता वही टोह, वही सहभागिता नियम, वही उपचार चक्र दोहराती है, और हर एक ऐसे आकार में प्रमाण उत्पन्न करती है जिसे अगली व्यवस्था स्वीकार नहीं करती. लागत केवल धन नहीं है. खंडित परीक्षण जोखिम का एक खंडित चित्र उत्पन्न करता है, क्योंकि कोई एकल अभ्यास संस्था को वैसे नहीं देखता जैसे कोई वास्तविक प्रतिपक्षी देखता है: सिरे से सिरे तक, बैक ऑफिस, परिचालक कार्यस्थलों, संदेश इंटरफ़ेस और नेटवर्क से जुड़ाव के आर-पार.

यहाँ तर्क यह है कि प्रमुख व्यवस्थाओं में अब दिखाई देने वाला अभिसरण खंडित दृष्टिकोण को अप्रचलित बना देता है. 7.3A मार्गदर्शन, DORA का खतरा-नेतृत्व वाला परीक्षण नियम, OSFI की आसूचना-नेतृत्व वाली अपेक्षा, और NYDFS का वार्षिक अधिदेश चार भिन्न परीक्षण नहीं हैं. ये एक ही विचार की चार पर्यवेक्षी अभिव्यक्तियाँ हैं, और जो संस्था उनमें से सबसे माँग वाले के अनुरूप रचती है, और परिणाम को एक साझा ढाँचे के विरुद्ध दर्ज करती है, बाकी को एक उपोत्पाद के रूप में संतुष्ट कर सकती है.

SWIFT CSCF v2026 का नियंत्रण 7.3A अब क्या अपेक्षा करता है

नियंत्रण 7.3A ग्राहक सुरक्षा नियंत्रण ढाँचे में एक परामर्शी नियंत्रण के रूप में बैठता है जिसका उद्देश्य उपयोक्ता के SWIFT-संबंधी अवसंरचना की परिचालन सहनशीलता को उन कमज़ोरियों की पहचान करके मान्य करना है जो सुरक्षित ज़ोन या बैक ऑफिस के अधिग्रहण की ओर ले जा सकती हैं (SWIFT 2025). 2026 परिवर्तन का सार कोई नया नियंत्रण क्रमांक नहीं बल्कि इस बारे में पैना मार्गदर्शन है कि परीक्षण का दायरा कैसे तय किया जाए और उसे कौन से परिदृश्य आवृत करने चाहिए. ढाँचा अब परीक्षण परिदृश्यों का एक समुच्चय व्यक्त करता है जिसे एक तीन वर्षीय चक्र पर अभ्यास किया जाना है, ताकि कोई संस्था वार्षिक रूप से दोहराए गए एकल संकीर्ण बाहरी स्कैन से नियंत्रण को संतुष्ट न कर सके. अपेक्षा यह है कि चक्र पर, कार्यक्रम संदेश इंटरफ़ेस और संबंधित घटकों का अनुप्रयोग-स्तर परीक्षण, सुरक्षित ज़ोन और उसके विभाजन का अवसंरचना परीक्षण, और उन मानवीय व परिचालक-कार्यस्थल पथों को आवृत करता है जिनका वास्तविक घुसपैठें दोहन करती हैं.

दो डिज़ाइन परिणाम इससे निकलते हैं. पहला, दायरा सुविधाजनक नेटवर्क परास के बजाय सुरक्षित ज़ोन और उसकी विश्वास सीमाओं के विरुद्ध परिभाषित होना चाहिए, क्योंकि नियंत्रण का प्रयोजन यह सिद्ध करना है कि कोई हमलावर बैक ऑफिस से संदेश परत में नहीं पलट सकता. दूसरा, परीक्षण किसी सक्षम और पर्याप्त रूप से स्वतंत्र पक्ष द्वारा संचालित होना चाहिए, और उसके निष्कर्षों को एक अनुगमित उपचार चक्र को आहार देना चाहिए जिसका समापन स्वयं प्रमाण है. नियंत्रण हर वास्तुकला प्रकार के लिए अनिवार्य के बजाय परामर्शी है, परंतु जो संस्थाएँ इसके विरुद्ध स्व-सत्यापन करती हैं, उनके लिए मूल्यांकनकर्ता दायरा, विधि, निष्कर्ष और उपचार को एक सुसंगत अभिलेख के रूप में देखने की अपेक्षा करेगा, न कि एक प्रमाणपत्र.

चार पड़ोसी व्यवस्थाएँ

DORA और खतरा-नेतृत्व वाला प्रवेश परीक्षण

डिजिटल परिचालन सहनशीलता अधिनियम सभी दायरे में आने वाली वित्तीय इकाइयों से अपनी सूचना एवं संचार प्रौद्योगिकी प्रणालियों का नियमित परीक्षण अपेक्षित करता है, और महत्त्वपूर्ण इकाइयों के उपसमुच्चय से कम से कम हर तीन वर्ष में खतरा-नेतृत्व वाले प्रवेश परीक्षण (TLPT) के माध्यम से उन्नत परीक्षण अपेक्षित करता है (European Parliament and Council 2022a). TLPT आसूचना-संचालित है: जीवंत उत्पादन प्रणालियों के विरुद्ध एक नियंत्रित रेड-टीम अनुकरण, वास्तविक खतरा कर्ताओं की रणनीतियों, तकनीकों और प्रक्रियाओं पर प्रतिमानित, एक ऐसी कार्यप्रणाली के अंतर्गत संचालित जिसके लिए TIBER-EU ढाँचा यूरोपीय संदर्भ है (European Central Bank 2018). जो संस्था 7.3A परीक्षण को खतरा-नेतृत्व वाले मानक तक तैयार करती है, वर्तमान खतरा आसूचना के साथ अपने परिदृश्यों को आकार देते हुए, वह पहले ही एक DORA परीक्षण की रीढ़ बना रही है, जो मुख्यतः औपचारिक दायरे में और किसी अभिहित TLPT के इर्द-गिर्द लिपटी पर्यवेक्षी अभिशासन में भिन्न है.

NIS2 और lex specialis अपवर्जन

द्वितीय नेटवर्क एवं सूचना सुरक्षा निर्देश आवश्यक और महत्त्वपूर्ण इकाइयों के आर-पार साइबर सुरक्षा जोखिम प्रबंधन और घटना रिपोर्टिंग का आधार-स्तर ऊँचा करता है, और राष्ट्रीय प्राधिकरण 2026 के दौरान अंतरण से सक्रिय पर्यवेक्षण की ओर बढ़े (European Parliament and Council 2022b; European Commission 2025). वित्तीय इकाइयों के लिए व्यावहारिक बिंदु प्राथमिकता का एक है: DORA lex specialis है, और NIS2 का अनुच्छेद 4 उसके आगे झुकता है जहाँ वित्तीय-क्षेत्र के नियम कम से कम तुल्य हैं. अतः संस्था को DORA को प्रवर्तनीय सहनशीलता-परीक्षण व्यवस्था के रूप में बरतना चाहिए, यह पहचानते हुए कि वित्तीय परिमिति के बाहर समूह इकाइयाँ, जैसे एक साझा प्रौद्योगिकी सहायक कंपनी, NIS2 के भीतर बनी रह सकती हैं और उसी परीक्षण प्रमाण से लाभान्वित हो सकती हैं.

संयुक्त राज्य: NYDFS Part 500 और FFIEC अपेक्षाएँ

न्यूयॉर्क राज्य वित्तीय सेवा विभाग का साइबर सुरक्षा विनियमन प्रत्येक आवृत इकाई से अपेक्षित करता है कि वह अपनी सूचना प्रणालियों का प्रवेश परीक्षण कम से कम वार्षिक रूप से, प्रणालियों की सीमाओं के भीतर और बाहर दोनों से, इकाई के जोखिम मूल्यांकन के आधार पर संचालित करे (New York State Department of Financial Services 2023). संशोधित विनियमन ने अभिशासन और परीक्षण अपेक्षाओं को और कस दिया है (Ropes and Gray 2026). संघीय स्तर पर, संघीय वित्तीय संस्था परीक्षा परिषद कोई निश्चित नियम नहीं थोपती परंतु योग्य, स्वतंत्र पक्षों द्वारा प्रवेश परीक्षण को अपनी सूचना सुरक्षा पुस्तिका के भीतर एक परीक्षक अपेक्षा और परिपक्वता संकेतक के रूप में बरतती है (Federal Financial Institutions Examination Council 2016). जो संस्था 7.3A को उच्च मानक तक संतुष्ट करती है, एक परिभाषित ताल पर सीमा के भीतर और बाहर दोनों से परीक्षण करते हुए, वह ठीक वही कलाकृतियाँ उत्पन्न करती है जिनकी NYDFS परीक्षक और FFIEC परीक्षा अपेक्षा करती है.

कनाडा: OSFI दिशानिर्देश B-13

वित्तीय संस्थाओं के अधीक्षक कार्यालय का दिशानिर्देश B-13, जो 1 January 2024 से प्रभावी है, संघीय रूप से विनियमित वित्तीय संस्थाओं से नियमित परीक्षण के माध्यम से कमज़ोरियों की पहचान अपेक्षित करता है, और महत्त्वपूर्ण प्रौद्योगिकी पदचिह्न वाली संस्थाओं के लिए वह आसूचना-नेतृत्व वाले, खतरा-नेतृत्व वाले प्रवेश परीक्षण और रेड-टीम अभ्यासों की अपेक्षा करता है जो यथार्थवादी बहु-चरणीय हमलों का अनुकरण करते हैं (Office of the Superintendent of Financial Institutions 2022). B-13 परिणाम-आधारित है और कोई निश्चित ताल तय नहीं करता, अतः संस्था अनुपालन को अपने परीक्षण की आवृत्ति के बजाय उसकी गुणवत्ता और यथार्थपरकता के माध्यम से प्रमाणित करती है. यह वही आसूचना-नेतृत्व वाला मानक है जिसे DORA और पैना 7.3A मार्गदर्शन व्यक्त करते हैं, जो B-13 को एक अलग बाध्यता के बजाय उसी परिवार का कनाडाई सदस्य बनाता है.

एक रीढ़: व्यवस्थाओं को NIST CSF 2.0 पर मानचित्रित करना

कोई एकल वित्तीय नियामक संयुक्त राज्य और कनाडा दोनों पर शासन नहीं करता, अतः किसी सीमा-पार संस्था को दोनों में मान्य एक तटस्थ संदर्भ चाहिए. राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान का साइबर सुरक्षा ढाँचा संस्करण 2.0 वह संदर्भ है: स्वैच्छिक, सीमा के दोनों ओर व्यापक रूप से अपनाया गया, और छह कार्यों के इर्द-गिर्द संगठित, अभिशासन, पहचान, सुरक्षा, पहचान-पता, प्रतिक्रिया और पुनर्प्राप्ति (National Institute of Standards and Technology 2024). रीढ़ के रूप में प्रयुक्त, यह किसी संस्था को एक प्रवेश-परीक्षण कार्यक्रम दर्ज करने और परिणाम को हर व्यवस्था की समझ में आने वाली शब्दावली में व्यक्त करने देता है. प्रवेश परीक्षण सबसे सीधे पहचान से बात करता है, कमज़ोरियाँ सतह पर लाकर, और पहचान-पता व प्रतिक्रिया से, यह मापकर कि संस्था की निगरानी और प्रतिक्रिया वास्तव में किसी यथार्थवादी घुसपैठ को पकड़ती और रोकती है या नहीं.

अभिशासन कार्य वे सहभागिता नियम, स्वतंत्रता और बोर्ड रिपोर्टिंग वहन करता है जिनकी पाँचों व्यवस्थाएँ अपेक्षा करती हैं. तालिका 1 अभिसरण को मूर्त बनाती है.

तालिका 1. एक प्रवेश-परीक्षण कार्यक्रम, चार व्यवस्थाएँ, एक रीढ़

आयाम	SWIFT 7.3A v2026	DORA TLPT	NYDFS Part 500	OSFI B-13	NIST CSF 2.0
प्रकृति	परामर्शी नियंत्रण	महत्त्वपूर्ण इकाइयों के लिए अनिवार्य	अनिवार्य नियम	परिणाम-आधारित अपेक्षा	स्वैच्छिक संदर्भ
ताल	3-वर्षीय परिदृश्य	कम से कम हर 3 वर्ष	कम से कम वार्षिक	कोई निश्चित ताल	निर्धारित नहीं
विधि	परिदृश्य-आधारित, सुरक्षित-ज़ोन केंद्रित	आसूचना-नेतृत्व रेड टीम	भीतर और बाहर, जोखिम-आधारित	आसूचना-नेतृत्व, रेड टीम	कार्य और परिणाम
स्वतंत्रता	सक्षम, स्वतंत्र पक्ष	प्रत्यायित प्रदाता	योग्य आंतरिक या	स्वतंत्र आश्वासन	अभिशासन परिणाम
प्राथमिक प्रमाण	दायरा, निष्कर्ष, उपचार	खतरा परिदृश्य, हमला आख्यान, उपचार	परीक्षण रिपोर्ट, उपचार ताल	परीक्षण की यथार्थपरकता और परिणाम	मानचित्रित परिणाम

हर पंक्ति के आर-पार पठन ही प्रबंध है: परीक्षण को हर स्तंभ में सबसे माँग वाले मानक तक रचें, आसूचना-नेतृत्व विधि, सुरक्षित-ज़ोन-सचेत दायरा, भीतर-और-बाहर कवरेज, स्वतंत्र निष्पादन, अनुगमित उपचार, और एकल परिणामी अभिलेख पाँचों को संतुष्ट करता है.

एक जोखिम-नेतृत्व वाला तैयारी प्रतिमान

7.3A मार्गदर्शन एक अनुपालन पठन को आमंत्रित करता है, जिसमें संस्था वह न्यूनतम करती है जिसका नियंत्रण नाम लेता है. अधिक मूल्यवान पठन, और वह जिसे पर्यवेक्षक उत्तरोत्तर पुरस्कृत करते हैं, जोखिम-नेतृत्व वाला है: प्रवेश परीक्षण वह उपकरण है जिसका प्रयोग संस्था के सर्वाधिक परिणामकारी अनावरणों को सतह पर लाने और सेवानिवृत्त करने के लिए होता है, और अनुपालन उसे भली-भाँति करने का उपोत्पाद है.

तैयारी एक जोखिम-और-दायरा आधार-रेखा से आरंभ होती है. संस्था अपनी SWIFT-संबंधी संपदा की सूची बनाती है, सुरक्षित ज़ोन, संदेश इंटरफ़ेस, परिचालक कार्यस्थल, नेटवर्क से जुड़ाव और उसे आहार देने वाली बैक-ऑफिस प्रणालियाँ, और पथों को परीक्षण की सुगमता के बजाय अधिग्रहण के परिणाम के अनुसार क्रमबद्ध करती है. यह एक ऐसा दायरा उत्पन्न करता है जो वहाँ परिभाषित है जहाँ धन और विश्वास बैठते हैं, जो वही दायरा भी है जिसे कोई वास्तविक प्रतिपक्षी चुनता, और जो B-13 की परिणाम-नेतृत्व मुद्रा और NYDFS की जोखिम-आधारित मुद्रा से संरेखित होता है.

इसके बाद खतरा-आसूचना रूपरेखा आती है. वित्तीय संदेशन को लक्ष्य बनाने वाले कर्ताओं पर वर्तमान आसूचना परिदृश्यों को आकार देती है, ताकि परीक्षण सामान्य के बजाय प्रशंसनीय घुसपैठों का पूर्वाभ्यास करे. यह वह चरण है जो किसी प्रवेश परीक्षण को एक खतरा-नेतृत्व वाला परीक्षण बनाता है, और यह वह चरण है जो उसी अभ्यास को DORA और B-13 के अंतर्गत साख-योग्य बनाता है.

फिर निष्पादन परिदृश्यों को उस तीन वर्षीय चक्र के आर-पार चलाता है जिसका 7.3A मार्गदर्शन वर्णन करता है, अनुप्रयोग, अवसंरचना और मानवीय पथों को आवृत करते हुए, सीमा के भीतर और बाहर से, एक स्वतंत्र पक्ष द्वारा, प्रलेखित सहभागिता नियमों के अंतर्गत. संस्था केवल यह नहीं मापती कि क्या मिला बल्कि यह भी कि उसकी अपनी पहचान और प्रतिक्रिया ने परीक्षण को घटित होते देखा या नहीं, क्योंकि वह माप वह प्रमाण है जिसकी पहचान-पता और प्रतिक्रिया कार्य अपेक्षा करते हैं.

अंततः, उपचार और प्रमाण घेरा बंद करते हैं. निष्कर्ष एक अनुगमित उपचार चक्र में प्रवेश करते हैं जिसका समापन दर्ज होता है, और पूरा अभिलेख, अर्थात दायरा, परिदृश्य, हमला आख्यान, निष्कर्ष, उपचार और पहचान निष्पादन, NIST CSF 2.0 रीढ़ के विरुद्ध एक बार दाखिल होता है और हर व्यवस्था के लिए चिह्नित होता है. जो संस्था इस घेरे को पूरा करती है उसने एक परीक्षण उत्तीर्ण नहीं किया है. उसने एक पुनः प्रयोज्य सहनशीलता प्रमाण परिसंपत्ति बनाई है.

हमारी SWIFT CSP मूल्यांकन सेवा 7.3A परीक्षण का दायरा तय करती है और उसे इस मानक तक चलाती है, और PenTeva निष्कर्षों को मान्य करता और समापन तक अनुगमित करता है ताकि प्रमाण चारों व्यवस्थाओं में से किसी के भी अंतर्गत टिके. जहाँ DORA सहनशीलता प्रतिरूपण दायरे में है, वहाँ DORA-MAST उसी प्रमाण को परिचालन-सहनशीलता चित्र में ले जाता है.

निष्कर्ष

पैना 7.3A मार्गदर्शन सर्वोत्तम रूप से एक पृथक SWIFT आवश्यकता के बजाय आसूचना-नेतृत्व वाले, खतरा-सूचित परीक्षण की ओर एक वैश्विक आंदोलन की एक पर्यवेक्षी अभिव्यक्ति के रूप में समझा जाता है. जो संस्था अपने 2026 प्रवेश परीक्षण को उस मानक तक रचती है, उसका दायरा परिणाम के अनुसार तय करती है, उसे वर्तमान खतरा आसूचना से रूपरेखित करती है, उसे सुरक्षित ज़ोन के आर-पार स्वतंत्र रूप से निष्पादित करती है, और परिणाम को एक साझा ढाँचे के विरुद्ध दर्ज करती है, वह उसी अभ्यास से DORA, NIS2 जहाँ वह अब भी लागू है, NYDFS Part 500 और OSFI B-13 को संतुष्ट कर सकती है. प्रवेश परीक्षण एक आवर्ती अनुपालन लागत होना बंद कर देता है और वह उपकरण बन जाता है जिसके माध्यम से संस्था उन जोखिमों को पाती और सेवानिवृत्त करती है जो मायने रखते हैं. एक बार परखें, अनेक को संतुष्ट करें.

Acronyms

CSCF, ग्राहक सुरक्षा नियंत्रण ढाँचा (SWIFT). CSP, ग्राहक सुरक्षा कार्यक्रम (SWIFT). DORA, डिजिटल परिचालन सहनशीलता अधिनियम. FFIEC, संघीय वित्तीय संस्था परीक्षा परिषद. ICT, सूचना एवं संचार प्रौद्योगिकी. NIS2, नेटवर्क एवं सूचना सुरक्षा निर्देश (द्वितीय). NIST CSF, राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान साइबर सुरक्षा ढाँचा. NYDFS, न्यूयॉर्क राज्य वित्तीय सेवा विभाग. OSFI, वित्तीय संस्थाओं के अधीक्षक का कार्यालय. SWIFT, वर्ल्डवाइड इंटरबैंक फाइनेंशियल टेलीकम्युनिकेशन के लिए सोसाइटी. TIBER-EU, खतरा आसूचना-आधारित नैतिक रेड टीमिंग (यूरोपीय ढाँचा). TLPT, खतरा-नेतृत्व वाला प्रवेश परीक्षण.

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