Building a better working world

SWIFT Customer Security Programme v2020 – Ist Ihre SWIFT-Umgebung ausreichend gesichert?

EY Angebote für SWIFT-Anwender

Was ist das SWIFT Customer Security Programme?

Die SWIFT-Infrastruktur war das Ziel einer Reihe von Cyber-Angriffen. Zur Verbesserung der Sicherheit globaler Zahlungen hat SWIFT das Customer Security Programme (CSP) eingerichtet, welches SWIFT-Nutzer dazu verpflichtet, den Grad der Umsetzung der Vorgaben aus dem SWIFT CSP zu attestieren. SWIFT aktualisiert dieses regelmäßig und überführt dabei regelmäßig empfohlene in verbindlichen Kontrollen. Zudem wurde im Jahr 2020 ein neues Independent Assessment Framework eingeführt.

Änderungen des SWIFT CSP in 2020

- Umwandlung zwei empfohlener in verbindliche Kontrollen (1.3 Virtualisation Platform Protection & 2.10 Application Hardening)
- Einführung von zwei neuen empfohlenen Kontrollen (1.4A Restriction of Internet Access & 2.11A RMA Business Control)
- Scope-Erweiterung bei 13 Kontrollen (inklusive Middleware/MQ)
- Einführung des Independent Assessment Framework und den verbindlichen Community-Standard Assessments

Für weitere Informationen sowie Fragen hinsichtlich des SWIFT Customer Security Controls Frameworks und des CSP Independent Assessment Framework stehen wir Ihnen gerne jederzeit zur Verfügung.

Customer Security Controls Framework v2020

3 Ziele	8 Prinzipien	31 Kontrollen
Secure your environment	1. Restrict Internet Access 2. Protect critical systems from general IT environment 3. Reduce Attack Surface and Vulnerabilities 4. Physically Secure the Environment	**16 insgesamt** (10 verbindlich, 6 empfohlen)
Know and limit access	5. Prevent Compromise of Credentials 6. Manage Identities and Segregate Privileges	**6 insgesamt** (5 verbindlich, 1 empfohlen)
Detect and respond	7. Detect Anomalous Activity to Systems or Transaction Records 8. Plan for Incident Response and Information Sharing	**9 insgesamt** (6 verbindlich, 3 empfohlen)

Architecture A	31 Kontrollen
A1 – Full stack A2 – Partial stack A3 – Connector	**21 verbindlich** Secure your environment: 10 Know and limit access: 5 Detect and respond: 6
	10 empfohlen Secure your environment: 6 Know and limit access: 1 Detect and respond: 3

Architecture B	22 Kontrollen
B – No local user footprint	**14 verbindlich** Secure your environment: 5 Know and limit access: 5 Detect and respond: 4
	8 empfohlen Secure your environment: 5 Know and limit access: 1 Detect and respond: 2

Das neue SWIFT Independent Assessment Framework

SWIFT veröffentlichte im August 2019 das Independent Assessment Framework, welches Änderungen am CSCF Assessment Prozess enthält. Das Framework skizziert den Assessment Scope, das Assessment Vorgehen, die verfügbaren Ressourcen sowie die Testmethoden und die Berichtsanforderungen.
Die freiwilligen User-initiated Assessments werden ab Mitte des Jahre 2020 durch Community-Standard Assessments abgelöst. Es existieren hauptsächlich 2 Arten von Assessments:

Community-Standard Assessment →

- Verpflichtendes unabhängiges Assessment
- Durchführung durch qualifizierte externe oder interne Parteien (nicht 1st LoD)
- **Ab Mitte des Jahres 2020 sind alle SWIFT-Nutzer dazu verpflichtet, ein Community-Standard Assessment durchführen**

SWIFT-Mandated Assessment

- Verbindlich für durch SWIFT stichprobenhaft ausgewählte SWIFT-Nutzer
- Durchführung erfolgt ausschließlich durch eine unabhängige externe Partei (independent external assurance)
- **Seit dem Jahr 2018 und fortlaufend**

SWIFT verpflichtet seine Nutzer, dass mit Beginn der Attestierungsperiode des Jahres 2020 alle Attestierungen auf Basis des CSCF v2020 über ein unabhängiges **Community-Standard Assessment** zu bewerten sind. Die unterbliebene Durchführung des SWIFT-Mandated Assessment oder des Community-Standard Assessments sowie die fehlende oder mängelbehaftete Selbsteinschätzung wird für andere SWIFT-Nutzer veröffentlicht. Alle Beurteiler müssen angemessen qualifiziert sein und ein unabhängiges Cybersecurity-orientiertes operationales Assessment durchführen. Dies kann erreicht werden durch:

Externes Assessment

Durch eine unabhängige externe Organisation mit
- vorhandenen Erfahrungen im Bereich Cybersecurity Assessment
- individuellen Beurteilern, die über relevante Sicherheitszertifizierungen verfügen

Internes Assessment

Durch die interne 2nd or 3rd LoD-Funktion (bspw. Compliance, Risiko Management oder die Interne Revision)
- Unabhängig von der 1st LoD-Funktion, welche die Self-Attestation einreicht
- Individuelle Beurteiler verfügen über relevante Sicherheitszertifizierungen

Auch im Falle der Auslagerung der lokalen SWIFT-Infrastruktur an einen Servicedienstleister verbleibt die Verantwortung zur Erfüllung der Anforderungen aus dem SWIFT CSFC für alle anwendbaren Kontrollen beim SWIFT-Nutzer und ist durch diesen im Rahmen der Selbsteinschätzung zu bestätigen.

Die jährliche Selbsteinschätzung innerhalb des KYC-SA Tools hat die Ergebnisse des Independent Assessment Reports zu berücksichtigen und darf daher nicht eingereicht werden, bevor das Assessment abgeschlossen ist. Die für das Assessment relevanten Daten (inklusive der Angaben über den Beurteiler, das Datum des Assessments und der berücksichtigten Version des CSCF) sind neben der Selbsteinschätzung ebenfalls zu erfassen.

EY's Kompetenzen zur Unterstützung des Attestation-Prozesses für 2020 und darüber hinaus

1

Pre-Readiness Assessments
Um sicherzustellen, dass Sie auf die kommenden verbindlichen SWIFT CSP Assessments vorbereitet sind, führen unsere erfahrenen Teams Pre-Readiness Assessments durch, die alle erforderlichen Kontrollen abdecken. In diesen Assessments verifizieren wir die Ergebnisse des Jahres 2019, identifizieren Lücken gegenüber den Anforderungen des SWIFT CSCF v2020 und informieren Sie **zeitnah** hinsichtlich Mängeln.

2

Training & Co-Sourcing
Sofern Sie das Assessment eigenständig durch Ihre 2nd or 3rd LoD-Funktion durchführen lassen möchten, Ihnen jedoch die erforderlichen Ressourcen oder Fähigkeiten fehlen, stehen wir Ihnen unterstützend zur Seite: Durch einen Joint-Assessment-Ansatz teilen wir unsere umfangreichen Erfahrungen mit Ihnen. Darüber hinaus schulen wir Ihr Personal, um es auf die zukünftigen Assessments vorzubereiten.

3

Community-Standard Assessments
EY verfügt mit seinem erfahrenen Team über die erforderlichen Fähigkeiten und Qualifikationen, um Community-Standard Assessments in Übereinstimmung mit den durch SWIFT definierten Vorgaben durchzuführen. Da es sich bei den Assessments um eine Zeitpunktbetrachtung handelt, können wir bereits im Vorfeld über ein Readiness Assessment Lücken identifizieren, die wir nach deren Behebung erneut bewerten.

Die Assessments können wir für Sie gerne als "Managed Service" durchführen, so dass sich der Aufwand durch die Kenntnisgewinne hinsichtlich Ihrer Infrastruktur in den Folgejahren erheblich reduziert.

Warum EY?

- Wir verfügen über umfangreiche Kenntnisse und die erforderlichen Qualifikationen zur Durchführung von SWIFT CSP Assessments. Unsere Experten haben bereits zahlreiche Projekte im Bereich Informationssicherheit sowie SWIFT CSP Assessments bei Finanzdienstleistern unterschiedlicher Größenordnungen durchgeführt.
- Basierend auf unseren Erfahrungen aus den SWIFT CSP Assessments haben wir ein Vorgehensmodell entwickelt, das wir an Ihre individuellen Bedürfnisse anpassen können. Unsere Tools, Vorlagen und Accelerators bringen wir dabei gerne mit ein, um Ihr SWIFT Compliance Programm zu unterstützen.

Unser Service-Angebot im Überblick:

- Community-Standard Assessment als unabhängiger Beurteiler
- Pre-Readiness Assessment: Unterstützung bei der Vorbereitung kommender Assessments und der Einstufung der Ergebnisse voriger Assessments
- Training & Co-Sourcing: Training und Unterstützung Ihrer 2nd oder 3rd Line of Defence (LoD) bei der Vorbereitung und Durchführung von Community-Standard Assessments

EY bietet Ihnen umfassende Unterstützung in den Bereichen Cybersecurity, Kontrollsysteme, Aufsichtsrecht und Analytics.

Folgende Fragen sollten Sie sich stellen:

- Verfügen wir über ausreichend qualifiziertes Personal zur Durchführung eines SWIFT CSP Assessments?
- Erfüllen wir bis Ende des Jahres 2020 alle Vorgaben aus den verpflichtenden Kontrollen des SWIFT CSP v2020?
- Besitzen wir genug Personal zur fristgerechten Durchführung des Assessments?
- Kennen wir die aktuellen SWIFT-Anforderungen?
- Sind uns die Konsequenzen bei Mängeln bewusst?

SWIFT Timeline
Die nächsten Termine

Jul 2020 → Zeitraum für die Attestierung des SWIFT CSCF v2020 beginnt - Community-Standard Assessments sind verpflichtend

Dez 2020 → Zeitraum für die Attestierung des SWIFT CSCF v2021 beginnt

Jul 2021 → Erfassung der Ergebnisse der Self-Attestation sowie des Assessment Reports über das SWIFT KYC-SA Tool

Dez 2021 → Erfassung der Ergebnisse der Self-Attestation sowie des Assessment Reports über das SWIFT KYC-SA Tool

EY Team
Cybersecurity Advisory und
SWIFT CSP Assesser

Lars Weimer
+49 160 939 27489
lars.weimer@de.ey.com

Boris Gurewitsch
+49 160 939 19821
boris.gurewitsch@de.ey.com

Matthias Funk
+49 160 939 21191
matthias.funk@de.ey.com

Christoph Capellaro
+49 160 939 23585
christoph.capellaro@de.ey.com

EY | Assurance | Tax | Transactions | Advisory

Die globale EY-Organisation im Überblick
Die globale EY-Organisation ist einer der Marktführer in der Wirtschaftsprüfung, Steuerberatung, Transaktionsberatung und Managementbe ratung. Mit unserer Erfahrung, unserem Wissen und unseren Leistungen stärken wir weltweit das Vertrauen in die Wirtschaft und die Finanzmärkte. Dafür sind wir bestens gerüstet: mit hervorragend ausgebildeten Mitarbeitern, starken Teams, exzellenten Leistungen und einem sprichwörtlichen Kundenservice. Unser Ziel ist es, Dinge voranzubringen und entscheidend besser zu machen – für unsere Mitarbeiter, unsere Mandanten und die Gesellschaft, in der wir leben. Dafür steht unser weltweiter Anspruch *Building a better working world*.

Die globale EY-Organisation besteht aus den Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig und haftet nicht für das Handeln und Unterlassen der jeweils anderen Mitgliedsunternehmen. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Mandanten. Weitere Informationen finden Sie unter ey.com.

In Deutschland ist EY an 20 Standorten präsent. „EY" und „wir" beziehen sich in dieser Publikation auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited.

GSA Agency
SCH 2002-002
ED None

ey.com/de