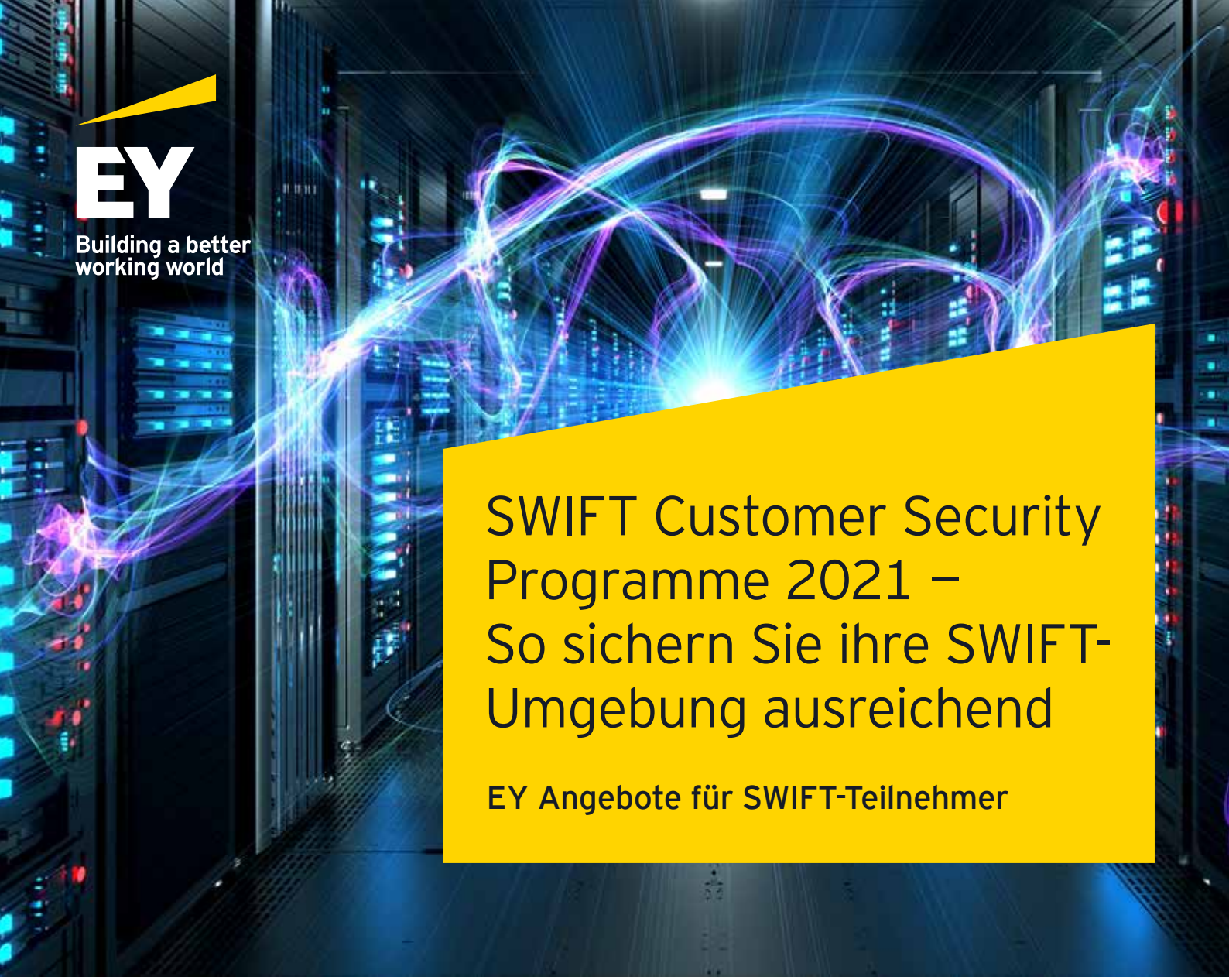

Building a better working world

SWIFT Customer Security Programme 2021 – So sichern Sie ihre SWIFT-Umgebung ausreichend

EY Angebote für SWIFT-Teilnehmer

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) eingeführt, welches SWIFT-Teilnehmer dazuverpflichtet, den Grad der Umsetzung der Vorgaben aus dem SWIFT CSP zu bewerten.

SWIFT aktualisiert dieses regelmäßig und überführt dabei empfohlene in verbindlichen Kontrollen. Zudem wurde im Jahr 2021 die verpflichtende Durchführung einer unabhängigen Beurteilung der Umsetzung der von SWIFT geforderten Kontrollen eingeführt.

Änderungen des SWIFT CSP im Jahr 2021

Für das Jahr 2021 ergaben sich in der neuen Version des SWIFT CSP neben einigen Klarstellungen die folgenden wesentlichen Änderungen im SWIFT Security Controls Framework (CSCF):

- Einführung des neuen Architekturtyps A4 bei Verwendung von eigenen Konnektoren (Middelware oder API)
- Abgrenzung der Kontrolle „1.4 Restriction of Internet Access“ von der Kontrolle „1.1 SWIFT Environment Protection“ und Berücksichtigung als eigene verbindliche Kontrolle

Für weitere Informationen sowie Fragen hinsichtlich SWIFT Customer Security Programme sowie SWIFT Customer Security Controls Framework stehen wir Ihnen gerne jederzeit zur Verfügung.

Das Customer Security Controls Framework v2021

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** (11 verbindlich, 5 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)

Architekturtypen A1–A3 — 31 Kontrollen	Architekturtyp A4 — 24 Kontrollen	Architekturtypen B — 22 Kontrollen
A1 – Full stack A2 – Partial stack A3 – SWIFT Connector	A4 – Other Connector*	B – No local user footprint
22 verbindlich Secure your environment: 11 Know and limit access: 5 Detect and respond: 6	**15 verbindlich** Secure your environment: 8 Know and limit access: 3 Detect and respond: 4	**15 verbindlich** Secure your environment: 6 Know and limit access: 5 Detect and respond: 4
9 empfohlen Secure your environment: 5 Know and limit access: 1 Detect and respond: 3	**9 empfohlen** Secure your environment: 5 Know and limit access: 1 Detect and respond: 3	**7 empfohlen** Secure your environment: 4 Know and limit access: 1 Detect and respond: 2

Das SWIFT Independent Assessment Framework im Überblick

Mit der durch SWIFT für das Jahr 2020 veröffentlichten Version des Independent Assessment Frameworks wurden die freiwilligen User-initiated Assessments durch Community-Standard Assessments abgelöst. Das Framework skizziert den Assessment Scope, das Assessment Vorgehen, die verfügbaren Ressourcen sowie die Testmethoden und die Berichtsanforderungen. Derzeit existieren im wesentlichen die folgenden Ansätzes und Durchführungsmethoden:

Community-Standard Assessment
- Verpflichtendes unabhängiges Assessment
- Durchführung durch qualifizierte externe oder interne Parteien (nicht 1st LoD)
- **Ab Mitte des Jahres 2021 sind alle SWIFT-Teilnehmer dazu verpflichtet, ein Community-Standard Assessment durchführen**

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

SWIFT verpflichtet seine Teilnehmer mit Beginn der Attestierungsperiode des Jahres 2021 dazu, alle Attestierungen auf Basis desCSCF v2021 über ein unabhängiges **Community-Standard Assessment** zu bewerten. Die unterbliebene Durchführung des SWIFT-Mandated Assessment oder des Community-Standard Assessments sowie eine fehlende oder mängelbehaftete Selbsteinschätzung wird für andere SWIFT-Teilnehmer veröffentlicht. Alle Beurteiler müssen angemessen qualifiziert sein, um 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 sowie
- individuellen Beurteilern, die über relevante Zertifizierungen im Bereich der Informationssicherheitverfügen

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 Zertifizierungen im Bereich der Informationssicherheit verfügen

Auch im Falle der Auslagerung der lokalen SWIFT-Infrastruktur an einen Servicedienstleister verbleibt die Verantwortung zur Erfüllung der Anforderungen aus dem SWIFT CSP/CSFC für alle anwendbaren Kontrollen beim SWIFT-Teilnehmer 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 das Jahr 2021 und darüber hinaus

1

Pre-Readiness Assessments
Um sicherzustellen, dass Sie auf die verbindlichen SWIFT CSP Assessments-vorbereitet sind, führen unsere erfahrenen Teams Pre-ReadinessAssessments durch, die alle erforderlichen Kontrollen abdecken. In diesen Assessments verifizieren wir die Ergebnisse des Jahres 2020, identifizieren Lücken gegenüber den Anforderungen des SWIFT CSCF v2021 und informieren Sie zeitnah hinsichtlich Mängeln.

2

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.

3

Training & Co-Sourcing
Sofern Sie das Assessment eigenständig durch Ihre 2nd or 3rd LoD-Funktion durchführen lassen möchten, Ihnen jedoch das Personal oder die Expertisefehlen, 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.

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 Unternehmen unterschiedlicher Größenordnungen und Branchendurchgeführt.

- 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:

- Pre-Readiness Assessment: Unterstützung bei der Vorbereitung kommender Assessments und der Einstufung der Ergebnisse voriger Assessments
- Community-Standard Assessment als unabhängiger Beurteiler
- 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 2021 alle Vorgaben aus den verpflichtenden Kontrollen des SWIFT CSCF v2021?
- 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 2021 → Zeitraum für die Attestierung auf Basis des SWIFT CSCF v2021 beginnt, Community-Standard Assessments sind verpflichtend

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

Jul 2022 → Zeitraum für die Attestierung auf Basis des SWIFT CSCF v2022 beginnt

Dez 2022 → Erfassung der Ergebnisse der Self-Attestation sowie des Assessments über das SWIFT KYC-SA Tool

EY Team
Cybersecurity Advisory und
SWIFT CSP Assessments

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

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

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

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

GSA Agency | KKL 2106-928
ED None

ey.com/de