# SWIFT
# „Customer Security Programme" CSP
## Get Ready to be Prepared

## Das SWIFT Customer Security Programme

In den letzten Jahren hat die Anzahl an schweren Angriffen in der Bankenwelt durch Cyber Attacken drastisch zugenommen. Obwohl jede Bank und jedes Unternehmen für seine eigene Abwehr zuständig ist, hat SWIFT beschlossen die Branche im Kampf gegen Cyberkriminalität zu vereinen und mit der Einführung des „Customer Security Programme" (CSP) in Aktion zu treten.

SWIFT, die Society for Worldwide Interbank Financial Telecommunication, betreibt ein globales, hochverfügbares und sicheres Kommunikationsnetzwerk zum schnellen und sicheren Austausch von Finanznachrichten.[1] SWIFT verarbeitet circa 27,45 Mio. Nachrichten pro Tag und hat über 11.000 Nutzer weltweit.[2]
Das Netzwerk an sich wurde bisher noch nicht Opfer eines Hackerangriffes, allerdings ist aufgrund der wichtigen Rolle, welches das Kommunikationsnetzwerk in der Finanzindustrie einnimmt die Sicherheit innerhalb des Netzwerkes von großer Bedeutung.

Als Teil des „Customer Security Programme", welches in 2016 eingeführt wurde, hat SWIFT eine Übersicht an Cybersicherheit-Standards veröffentlicht, die alle Nutzer in ihre Systemlandschaft implementieren müssen. Dies zielt darauf ab eine grundsätzliche Sicherheit in der Finanzwelt zu erreichen und SWIFT Nutzer gegen Cyberkriminalität zu schützen.

Das Customer Security Controls Regelwerk (CSC Regelwerk) ist seit März 2017 allen Nutzern des SWIFT Netzwerkes zugänglich. Das Regelwerk erklärt und beschreibt alle notwendigen im CSP enthaltenen Sicherheitskontrollen.
Diese Sicherheitskontrollen sind auf die drei allumfassenden Rahmenziele „Secure your Environment", „Know and Limit Access" und „Detect & Respond", und acht Kernprinzipien basiert.
Insgesamt werden 27 Sicherheitsüberprüfungen CSC Regelwerk aufgeführt, 16 davon sind Pflicht, 11 angeraten.

### Daten und Fakten

- Abgabe einer Selbst-Überprüfung für alle Nutzer des SWIFT Netzwerkes
- 27 Sicherheitskontrollen (16 Pflicht, 11 empfohlen)
- Abgabe der ersten Selbst-Überprüfung bis zum 31. Dezember 2017, mindestens jährliche Wiederholung der Abgabe
- Abgabe der Selbst-Überprüfung in das KYC Registry Security Attestation Application

Alle SWIFT Nutzer mit einer 8-stelligen „live" BIC müssen eine Selbst-Überprüfung ihres Compliance-Status auf Basis der Pflicht-Kontrollen im CSC Regelwerkes vornehmen, unabhängig davon ob sie direkt oder über einen Service Provider verbunden sind. Eine jährliche Wiederholung oder eine Durchführung bei dem Eintreten von großen Veränderungen dieser Selbst-Überprüfung ist von SWIFT vorgeschrieben.
Der Compliance-Status jedes Nutzers

[1] Vgl. Gabler Wirtschaftslexikon (URL) http://wirtschaftslexikon.gabler.de/Definition/swift.html
[2] Vgl. SWIFT (URL) https://www.swift.com/about-us/swift-fin-traffic-figures#topic-tabs-menu

muss bis zum 31. Dezember 2017 in die KYC Registry Security Attestation Application[3] eingetragen werden. Grundsätzlich ist hier jedes Unternehmen die oberste Instanz und kann selbst entscheiden, ob der eigene Compliance-Status für andere Nutzer einsehbar ist oder nicht. Allerdings können Unternehmen sich ab sofort weigern mit anderen Nutzern im Netzwerk zu kommunizieren, die einen Nicht-Compliant Status oder einen Nicht-Veröffentlichten Status haben. Dies verbessert die Transparenz und Sicherheit zwischen den Nutzern und hilft Unternehmen risikobasierte Entscheidungen zu treffen, indem der Status des Gegenübers einer Geschäftstransaktion überprüft werden kann.
SWIFT behält sich das Recht vor alle Nutzer, die bis Januar 2018 keine Selbt-Überprüfung abgegeben haben zu melden. Zudem behält sich SWIFT das Recht vor, alle Nutzer die bis Januar 2019 allen verpflichtenden Controls gegenüber compliant sind oder durch einen non-compliant Service-Provider verbunden sind zu melden.

[3] Für Nutzer entwickelte Plattform zur Abgabe ihrer Selbst-Überprüfungsdaten, welche den Complaine Status des Unternehmens gegenüber der SWIFT customer security controls bestätigen.

## Be FIS AG Fakten

- Spezialist in den Bereichen Payment, SWIFT und Info Management
- Consulting, IT-Services und Software
- Zuverlässiger Partner für unsere Kunden seit 1998
- Ansässig in Deutschland
- Member of Be Group
- Umfassendes Know-How und langjährige Projekterfahrung im Bereich SWIFT
- Internationale Player als Kunden
- Integrierter Beratungsansatz

### KONTAKT

Be Shaping the Future -
Financial Industry Soltutions AG
Frühlingstraße 2
D-84034 Landshut
Tel: +49 (0) 871 27 66-0
information@be-stf.de
www.be-stf.de

## Das SWIFT Customer Security Controls Regelwerk (SWIFT CSC Regelwerk)

**3 Kernziele**

| Secure your Environment | Know and Limit Access | Detect and Respond |
|---|---|---|

**8 Kernprinzipien**

| | | |
|---|---|---|
| 1. Internetzugang beschränken<br>2. Kritische Systeme von der generellen IT-Umgebung schützen<br>3. Angriffsfläche und Verwundbarkeit reduzieren<br>4. Umgebung physisch schützen | 5. Kompromittierung von Anmeldeinformationen vermeiden<br>6. Identitäten managen und Berechtigungen trennen | 7. Abnormale Aktivitäten im System oder in den Transaktionsdatensätzen erkennen<br>8. Reaktion auf Vorfälle und Informationsaustausch planen |

**27 Kontrollen (16 Pflicht, 11 empfohlen)**

Quelle: Angepasst von swift.de

## Was die Be FIS AG für Sie tun kann

Die Be FIS AG bietet Ihnen eine breite Auswahl an Services zum Thema „Customer Security Programme" an:

- Überprüfung und Analyse der aktuellen internen und externen Sicherheitsinfrastruktur und der bestehenden Sicherheitskontrollen
- Durchführung einer Eigeninspektion zur Überprüfung des Compliance-Status in Bezug auf die Kontrollen und Ziele des CSP und die Definition möglicher Sicherheitslücken im System
- Durchführung eines SWIFT Compliance Reports
- Implementierung aller notwendigen Kontrollen des SWIFT CSC Regelwerkes
- Implementierung aller empfohlenen Kontrollen des SWIFT CSC Regelwerkes
- Entwicklung und Implementierung aller möglichen zusätzlichen Kontrollen für erhöhte Sicherheit und zukünftige Compliance mit dem SWIFT CSC Regelwerk
- Unterstützung und Training Ihrer Mitarbeiter auf dem Themengebiete SWIFT Compliance
- Unterstützung und Implementierung aller zusätzlich entstandenen Anforderungen an die IT-Infrastruktur nach einer Überprüfung durch SWIFT
- Jährliches Update der bestehenden IT-Sicherheitsinfrastruktur auf Basis des aktuellen SWIFT CSC Regelwerkes

Die Be FIS AG ist ein weltweit etablierter Experte im Bereich SWIFT und dessen Umsystemen und unterstützt Sie bei der Implementierung aller vom „Customer Security Programme" gestellten Anforderungen und der Weiterentwicklung Ihrer Sicherheitsstandards und -kontrollen.

Be SHAPING THE FUTURE

SWIFT Customer Security Programme