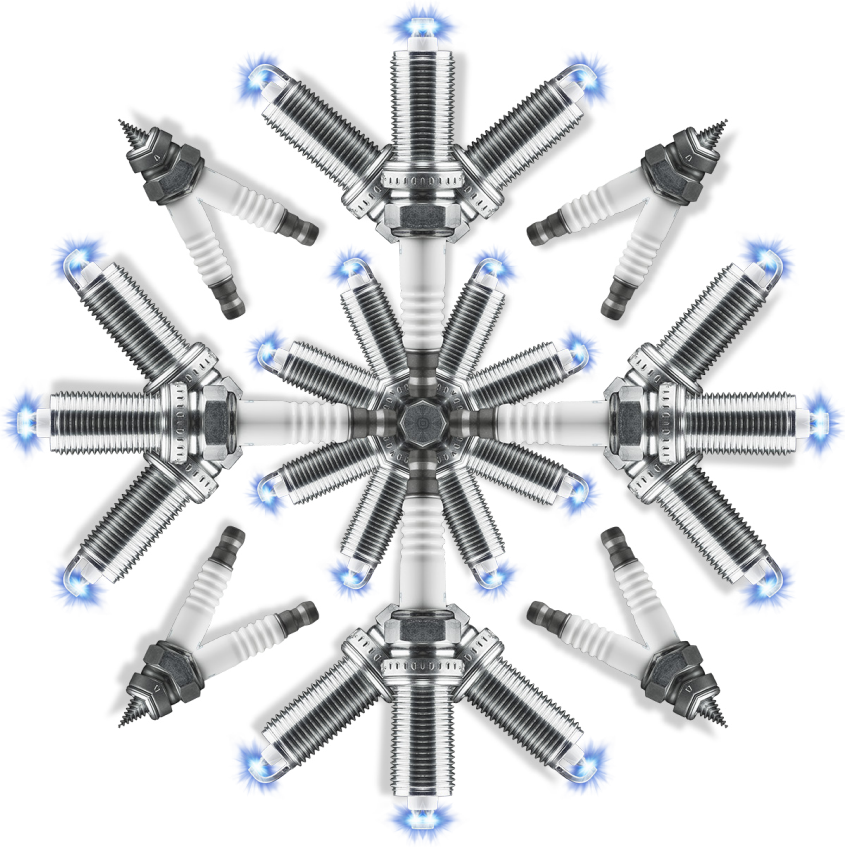
Deloitte.



SWIFT Customer Security Program

Die nächste Cyber-Attacke kommt bestimmt!

Moderne Marktinfrastrukturen und Back-Office Systeme für den Zahlungsverkehr sind zunehmend Ziele ausgefeilter Cyber-Angriffe.

Banken sind deshalb angehalten ihre Sicherheitsmaßnahmen zu verbessern, um auf betrügerische Aktivitäten in Verbindung mit der Ausführung von Zahlungen zu verhindern.

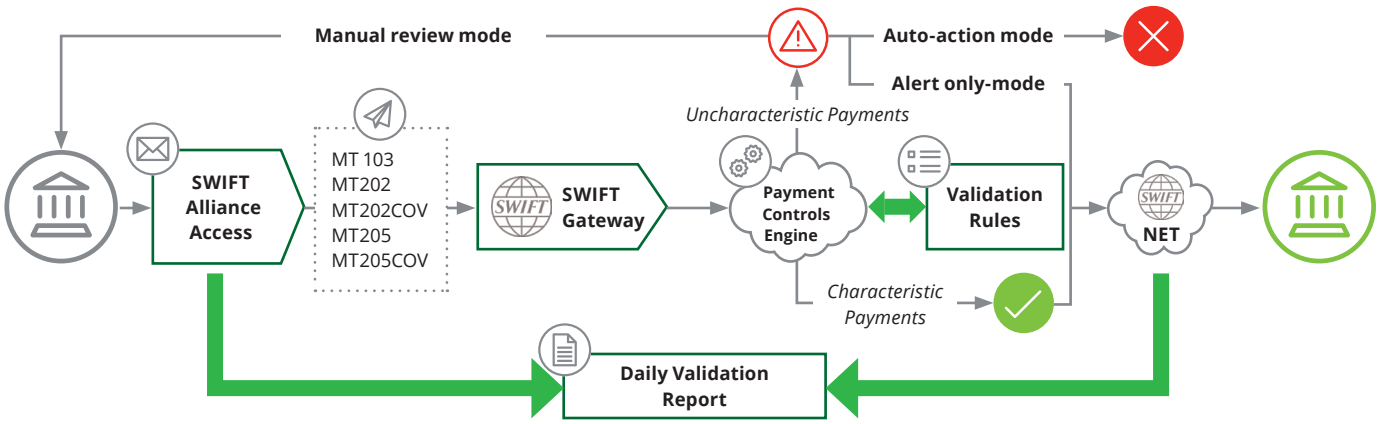
Ferner müssen Banken eine schnelle und einfache Methode zur Überwachung untypischer Zahlungen einführen und sichere und vertrauenswürdige Zahlungen garantieren.

SWIFT hat in diesem Zusammenhang das SWIFT Customer Security Program (CSP) initiiert, welches in den bestehenden Kontrollrahmen für Informationssicherheit integriert werden muss. Hierzu verlangt SWIFT bis zum 31. Dezember 2021 eine Bestätigung über die Einhaltung des SWIFT CSP durch eine unabhängige Instanz. Die Nichteinhaltung des SWIFT CSP kann von SWIFT sanktioniert werden.

Ziele sind dabei die Reduktion der Risiken aus Cyberangriffen, die Gewährleistung der Sicherheit für Ihre Zahlungsverkehrsinfrastruktur und die Sicherung Ihrer Kerngeschäfte und Ihrer Reputation.
Mit der Einführung ihrer Payment Controls im Jahr 2018 bietet SWIFT zusätzlich eine In- Network-Lösung an, die das Betrugsrisiko durch Alerting und Blocking von untypischen Zahlungen minimiert.

Solche Kontrollen ermöglichen die Erstellung von sogenannten Business Rules zur Stärkung der Risiko- und Zahlungsprozesse. Hiermit wiederum soll eine zeitnahe und effiziente Implementierung sowie Absicherung Ihrer Lösung für den Betrieb von SWIFT Payment Controls sowie Stärkung Ihrer Zahlungsverkehrsgovernance und –umgebung erreicht werden.

Typischer Ablauf einer SWIFT-Transaktion



Deloitte Services

Gap Analyse zur Implementierung des SWIFT CSP

- Initiale SWIFT Risikobewertung, Festlegung von Prioritäten und Überprüfung der implementierten Kontrollen und Prozesse
- Strategie- und Roadmap-Entwicklung für die Behebung festgestellter Kontroll- und Prozessschwächen
- Unterstützung bei der Implementierung des SWIFT CSP Customer Security Control Frameworks
- Unterstützung bei der Definition und Einführung einer angemessenen Governance (zzgl. „War Gaming")

SWIFT CSP Health Check

- Reifegradbewertung der implementierten CSP Kontrollen vor internen/ externen Prüfungen
- Identifizierung von Defiziten bezüglich der Einhaltung des CSPs sowie Bereitstellung von Handlungsempfehlungen für die erfolgreiche Vorbereitung auf interne/ externe Prüfungen

Unabhängiges Assessment des SWIFT CSP

- Unabhängige Assessments bezüglich der Angemessenheit und Wirksamkeit der implementierten CSP Kontrollen sowie Unterstützung bei der Erstellung des Abschlussberichts
- Optionale unabhängige Bewertungen zur angemessenen und effektiven Integration weiterer Sicherheitsrahmenwerke mit Bezug zum Zahlungsverkehr (z.B. TARGET2 Selbstzertifizierung).

SWIFT Payment Controls FastTrack

- Ist-Analyse und Auswertung von Zahlungsverkehrsdaten zur Beurteilung der organisatorischen Anforderungen an das Geschäftsmodell, die Risikobereitschaft, die Organisationsstrukturen und -verfahren sowie das implementierte interne Kontrollsystem
- Empfehlung für ein bestmögliches Betriebsmodell sowie für mögliche wesentliche Business Rules einschließlich dem Aufzeigen bestehender Defizite im Vergleich zum Zielzustand
- Unabhängige Überprüfung von implementierten SWIFT Payment Controls auf der Basis von zuvor getätigten Empfehlungen (Minimallösung)

SWIFT Payment Controls CustomTrack

- (Neu-)Definition einer Aufbauorganisation einschließlich der Einrichtung von Stellen und Funktionen entsprechend geltender Vorschriften und Best Practices
- Definition von Prozessen, Richtlinien und organisatorischen Abläufen für das Alerting und Blocking untypischer Zahlungen
- Technische Konfiguration von SWIFT Payment Controls einschließlich der Implementierung spezifischer Business Rules auf der Grundlage von Analysen und in Abstimmung mit Ihrer Organisation sowie Einrichtung von Rollen und Zugriffsrechten im SWIFT Payment Controls Interface
- Durchführung von Schulungen für Mitarbeiter des Zahlungsverkehrs für die Anwendung und Administration von SWIFT Payment Controls (einschließlich der technischen Umsetzung und Pflege der Business Rules)

Ihre Ansprechpersonen

Mag. Alexander Ruzicka
Partner | Risk Advisory
+43 1 537 00-7950
aruzicka@deloitte.at

Mag. Thomas John
Senior Manager | Risk Advisory
+43 1 537 00-3723
tjohn@deloitte.at

www.deloitte.at/risk