Deloitte.

SWIFT Customer Security Programme (CSP)

Neuerungen im SWIFT Customer Security Controls Framework v2022 (CSCF v2022) und im Independent Assessment Framework (IAF) 2022

MAKING AN IMPACT THAT MATTERS since 1845


B
B
A
A

Anpassungen des SWIFT CSCF v2022

Mit der Veröffentlichung des SWIFT Customer Security Controls Framework v2022 (SWIFT CSCF v2022; Stand: Juli 2021) hat SWIFT Konkretisierungen der Kontrollanforderungen sowie im Anwendungsbereich des SWIFT CSCF v2022 der einzubeziehenden Komponenten vorgenommen. Des Weiteren wird Kontrolle 2.9 Transaction Business Controls von einer empfohlenen in eine verpflichtend umzusetzende Kontrolle überführt. Darüber hinaus wurde die empfohlene Umsetzung von Kontrollen für die Architekturtypen A4 und B erweitert. Das SWIFT Customer Security Controls Framework umfasst ab dem Attestierungszeitraum 2022 somit insgesamt 23 verpflichtende und neun empfohlene Kontrollen.

Änderungen in Bezug auf den Customer Connector

Mit Einführung des Architekturtyps A4 „Customer Connector" im SWIFT CSCF v2021 wurde durch SWIFT der Absicherung des Austauschs von Zahlungsverkehrsdateien über einen Middleware Server (Customer Conenctor) gegen Cyber-Angriffe eine größere Bedeutung zugemessen, als dies durch die bisherige Einstufung als Architekturtyp B der Fall war. Mit dem SWIFT CSCF v2022 rückt die Absicherung des Customer Connector gegen Cyber-Angriffe weiter in den Fokus, indem der Customer Connector jetzt als verpflichtende Komponente in das SWIFT CSCF v2022 aufgenommen wird.

Des Weiteren wird mit der Einführung der empfohlenen Kontrolle **1.5A Customer Protection Environment** ein Äquivalent zur Kontrolle **1.1 SWIFT Environment Protection** geschaffen. Beide Kontrollen haben das Ziel, die SWIFT-relevante Infrastruktur bzw. den Customer Connector vor Kompromittierung zu schützen.

Die Aufnahme des Customer Connector als verpflichtende Komponente im SWIFT CSCF v2022 hat Auswirkungen auf SWIFT-Teilnehmer, die ihre entsprechende lokale SWIFT-Infrastruktur an ein SWIFT Service Bureau ausgelagert haben oder über einen Lite2 Business Application Provider mittels Customer Connector an das SWIFT-Netzwerk angeschlossen sind.

Überführung bisher empfohlener in verpflichtende Kontrolle

Mit dem SWIFT CSCF v2022 wird die bisherige Kontrolle **2.9 Transaction Business Controls** von einer empfohlenen in eine verpflichtende Kontrolle überführt und ist somit unabhängig vom Architekturtyp durch die SWIFT-Teilnehmer umzusetzen.

Zudem wird Kontrolle **2.9 Transaction Business Controls** weiter präzisiert und um den Implementierungshinweis zur Begrenzung des Zahlungsverkehrs auf Grundlage von bzw. durch den SWIFT-Teilnehmer definierten Betragsgrenzen ergänzt. Letztere können hierbei global, regional und/oder auf Korrespondenzbankebene gesetzt werden.

Präzisierung der Terminologie

- **Secure Zone**
  Das SWIFT CSCF v2022 wird um eine Definition für SWIFT-spezifische Systeme und Komponenten ergänzt, welche zusammengenommen die Secure Zone bilden. Insbesondere der Customer Connector wird in die Definition der SWIFT-spezifischen Komponenten aufgenommen und bildet somit die Customer Secure Zone, deren Absicherung ab dem Attestierungszeitraum 2022 entsprechend der empfohlenen Kontrolle **1.5A Customer Environment Protection** vorzunehmen ist.

- **Testsysteme**
  Auch wenn unter Berücksichtigung gängiger Standards typischerweise bereits eine vollständige Trennung von Test- und Produktionsumgebung umgesetzt ist, befinden sich Testsysteme im Anwendungsbereich des SWIFT CSCF v2022, wenn (i) das Testsystem nicht vollständig von der Produktionsumgebung getrennt ist und (ii) die Konfiguration den Versand von Zahlungsverkehrsnachrichten zulässt. In diesem Fall sind für Testsysteme die Kontrollen **1.1 SWIFT Environment Protection** bzw. **1.5A Customer Environment Protection** zu implementieren.

Erweiterung des Anwendungsbereichs von Kontrollen des SWIFT CSCF

- **1.2 Operating System Privileged Account Control**
  SWIFT hat Kontrolle **1.2 Operating System Privileged Account Control** dahingehend präzisiert, dass die zu betrachtenden Komponenten nun dediziert aufgeführt werden und somit die Konsistenz zum Umsetzungsleitfaden geschaffen wurde. Des Weiteren werden explizit Netzwerkkomponenten, die die Secure Zone schützen, als zu betrachtende Komponenten aufgeführt.

  Darüber hinaus wird als empfohlene Komponente der General Purpose Operator PC (Endanwender-PC) aufgenommen. Hierdurch erweitert sich der Anwendungsbereich der Kontrolle auf den Architekturtyp B.

  Die Erweiterung der betrachteten Komponenten ist insoweit nachvollziehbar, dass über hochprivilegierte Berechtigungen auf Netzwerkkomponenten sowie auf Endanwender-PCs Sicherheitseinstellungen sowie zugelassene Verbindungen zu vor- und nachgelagerten Systemen als auch auf Anwendungen geändert werden können. Bei unsachgemäßer Handhabung kann dies einen Angriffsvektor für Cyber-Angriffe darstellen.

- **4.2 Multi-Factor Authentication**
  Mit der verpflichtenden Berücksichtigung des Customer Connector wird durch SWIFT der Anwendungsbereich der Multi-Faktor-Authentifizierung auf den Customer Connector ausgeweitet. Somit ist ab dem Attestierungszeitraum 2022 für den Zugriff auf den Customer Connector sowie auf das dem Customer Connector zugrundeliegende (Betriebs-) System eine Multi-Faktor-Authentifizierung verpflichtend umzusetzen.

  Des Weiteren werden zeitlich begrenzte Einmalpasswörter („time-based one time passwords“) sowie Softtokens als mögliche Ausprägungen der Multi-Faktor-Authentifizierung aufgenommen, um den technischen Entwicklungen im Bereich der Authentifizierung gerecht zu werden.

- **5.1 Logical Access Control**
  SWIFT hat die verpflichtend zu betrachtenden Komponenten präzisiert und explizit den Customer Connector sowie die Netzwerkkomponenten aufgenommen. Dies ist unter Berücksichtigung der Erweiterung des Anwendungsbereichs in Kontrolle **1.2 Operator System Privileged Account Control** naheliegend, da Benutzerberechtigungskonzepte die Grundlage für die Zuordnung und Überwachung (hoch) privilegierter Benutzerberechtigungen darstellen.

  Darüber hinaus wird der Umsetzungsleitfaden in Bezug auf die Rezertifizierung präzisiert. Zukünftig sind auch an Dienstleister vergebene Zugriffsberechtigungen im Rahmen der Rezertifizierung zu berücksichtigen sowie die Zugriffsberechtigungen eindeutig einer Person zuzuordnen und hierdurch die Nachvollziehbarkeit deren Aktivitäten sicherzustellen.

- **6.2 Software Integrity**
  Der Software-Integritätscheck wird für den Customer Connector neu aufgenommen; jedoch lediglich als empfohlene Kontrolle.

  Eine Kontrolle der Integrität von durch den Hersteller über das Internet bereitgestellter Software vor Einsatz in Produktivsystemen ist dennoch zu befürworten, um auszuschließen, dass manipulierte Software in den produktiven Betrieb überführt wird. Dies ist auch konsistent zu Kontrolle **2.2 Security Updates**, die ebenfalls eine Herkunfts- und Integritätsprüfung von Software-Updates und -Patches vorsieht.

  Darüber hinaus sollte auch der Customer Connector wie u.a. das Messaging und Communication Interface einem täglichen Integritätscheck, z.B. mittels automatisiertem Code Check, unterzogen werden, um Änderungen an der Software identifizieren und bewerten zu können.

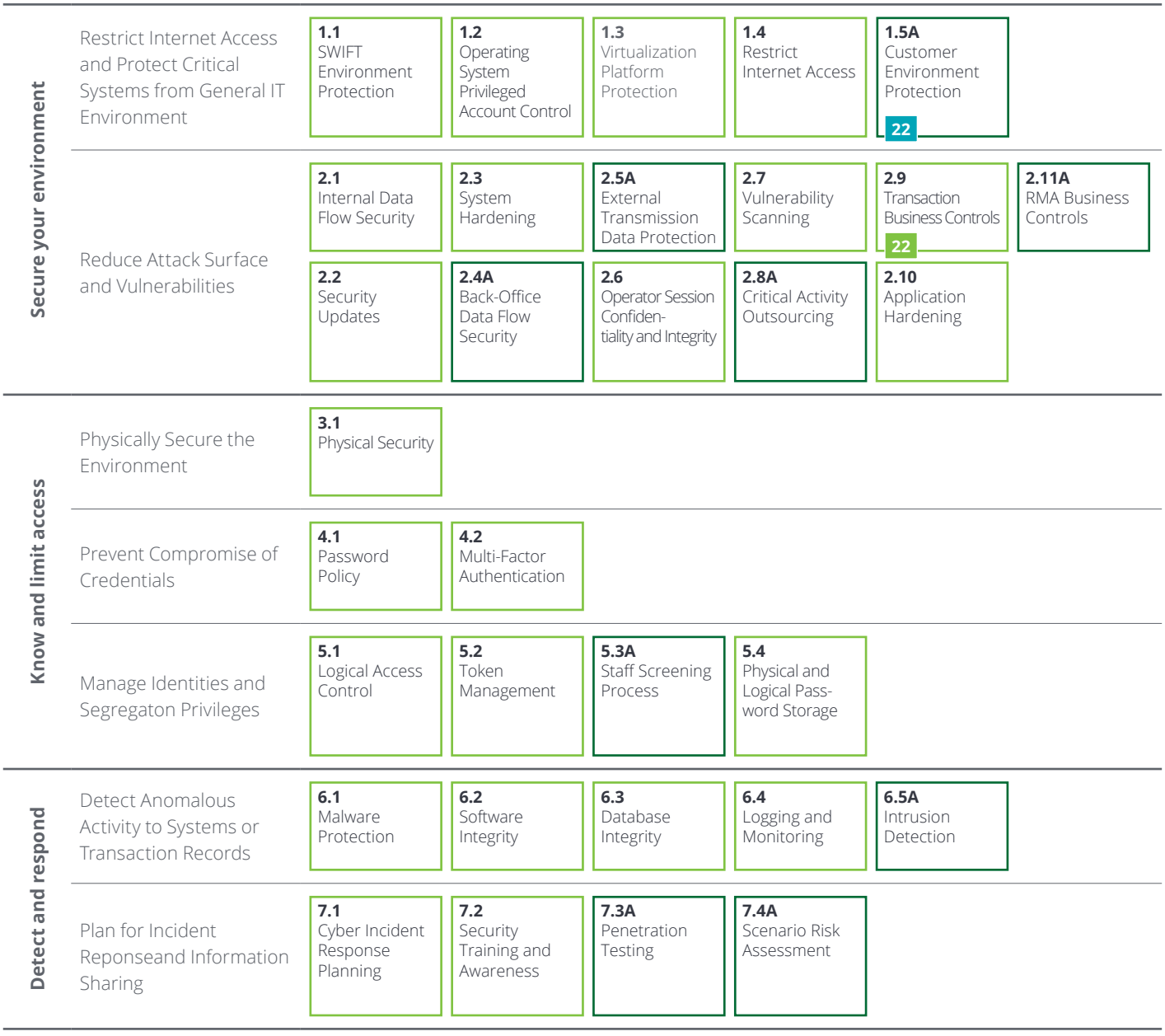
- **6.3 Database Integrity**
  Der Anwendungsbereich der Kontrolle **6.3 Database Integrity** wird ebenfalls auf den Customer Connector ausgeweitet, wenn diesem eine Datenbank zugrunde liegt, welche Zahlungsverkehrsnachrichten für das Messaging Interface speichert. Dies stellt sicher, dass vor Versand an das Messaging Interface keine Änderungen an Zahlungsverkehrsnachrichten aufgrund manueller Eingriffe oder technischer Störungen vorgenommen werden. Werden Änderungen erkannt, sind diese zu bewerten und entsprechende Maßnahmen zu ergreifen.

  Des Weiteren wird präzisiert, in welchen Architekturausprägungen die Kontrolle **6.3 Database Integrity** nicht anwendbar ist. Dies ist bspw. für den Architekturtyp A1 der Fall, wenn die lokale SWIFT-Infrastruktur kein Messaging Interface umfasst.

Der Customer Connector ist ab 2022 eine verpflichtend zu betrachtende Komponente im SWIFT CSP Independent Assessment.

Übersicht der Advisory und Mandatory Controls des SWIFT CSCF v2022

Abb. 1 – Übersicht der Änderungen in den Kontrollen des SWIFT CSCF v2022



Weiterentwicklung der Assessment-Methodik

SWIFT hat die Anforderungen an das verpflichtende Community Standard Assessment weiter präzisiert und die Assessment-Optionen (i) vollständige Verwertung der Ergebnisse des Independent Assessment aus dem Vorjahr, (ii) Delta-Assessment und (iii) Re-Assessment explizit aufgenommen sowie die Bedingungen, unter denen eine der drei Assessment-Optionen zum Tragen kommt, zugeordnet.

Mit dem Attestierungszeitraum 2021 war erstmalig verpflichtend das Community Standard Assessment umzusetzen. Das zugrundeliegende Independent Assessment Framework (IAF) konkretisiert hierbei Anforderungen an die Durchführung des SWIFT CSP Independent Assessment und regelt Umfang und Arten des Assessment, Verantwortlichkeiten sowie den Umgang mit den Ergebnissen aus der Durchführung vorheriger SWIFT CSP Independent Assessments.

Die aktuell gültige Version des IAF (Stand: Juli 2021) definiert drei Optionen für die Durchführung des Independent Assessment: (i) vollständige Verwertung der Ergebnisse des Independent Assessment aus dem Vorjahr, (ii) Delta-Assessment und (iii) Re-Assessment.

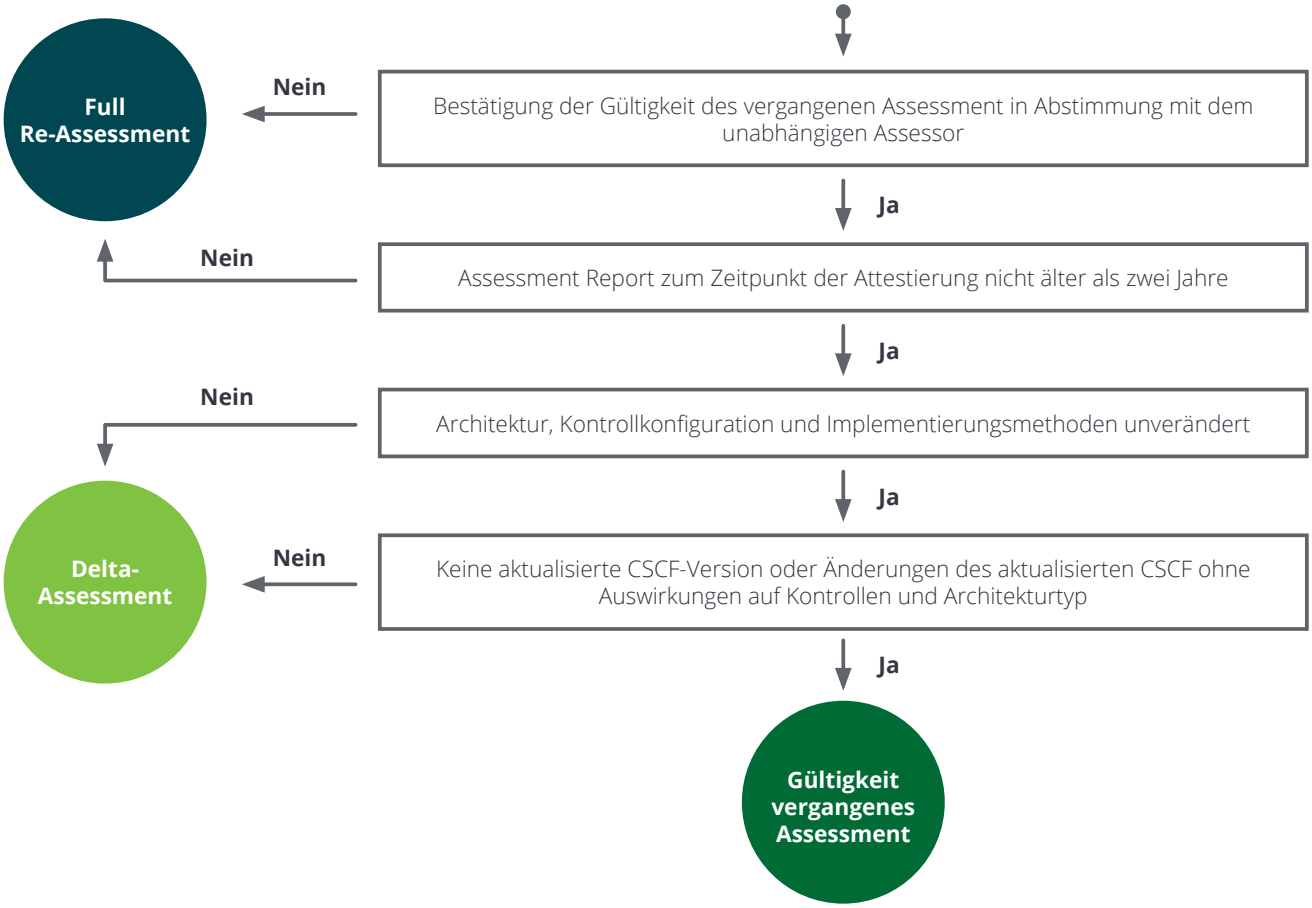
Vollständige Verwertung der Ergebnisse des Independent Assessment des Vorjahres

Es ist möglich, dass SWIFT-Teilnehmer die Ergebnisse des Vorjahres-Assessment wiederverwerten können, wenn nachfolgende Bedingungen kumulativ erfüllt werden:

- Der SWIFT-Teilnehmer muss zusammen mit dem unabhängigen Assessor bestätigen, dass die Ergebnisse aus dem vorangegangenen SWIFT CSP Independent Assessment weiterhin gelten.
- Architektur, Kontrollkonfiguration und Implementierungsmethoden des SWIFT-Teilnehmers haben sich seit dem vorherigen Independent Assessment nicht geändert.
- Es wurde keine aktualisierte Version des SWIFT CSCF veröffentlicht, oder die aktualisierte Version des SWIFT CSCF hat keine Auswirkungen auf die durch den SWIFT-Teilnehmer umzusetzenden Kontrollanforderungen und seinen Architekturtypen.
- Das zuletzt durchgeführte Independent Assessment ist nicht älter als zwei Jahre.

Mögliche Gründe, die gegen eine vollständige Verwertung der Ergebnisse des Independent Assessment des Vorjahres sprechen, sind u.a. (i) vertraglich geschlossene Vereinbarungen mit dem externen unabhängigen Assessor, (ii) ein Wechsel des unabhängigen Assessors im aktuellen Attestierungszeitraum oder (iii) interne Richtlinien erlauben es dem internen unabhängigen Assessor (Interne Revision) nicht, die Ergebnisse des vorherigen Independent Assessment vollständig wiederzuverwerten.

Abb. 2 – Bedingungen für die Wahl des unabhängigen Assessment-Ansatzes



Delta-Assessment

SWIFT-Teilnehmer haben die Möglichkeit, mit ihrem unabhängigen Assessor ein Delta-Assessment durchzuführen, wenn eine oder beide der folgenden Bedingungen erfüllt ist/sind:

- Architektur, Kontrollkonfiguration und Implementierungsmethoden des SWIFT-Teilnehmers haben sich seit dem vorherigen Independent Assessment geändert.

- Es wurde eine aktualisierte Version des SWIFT CSCF veröffentlicht, oder die aktualisierte Version des SWIFT CSCF hat Auswirkungen auf die durch den SWIFT-Teilnehmer umzusetzenden Kontrollanforderungen und seinen Architekturtypen.

Re-Assessment

Ein vollständiges Re-Assessment ist erforderlich, wenn:

- über das zuletzt durchgeführte unabhängige Assessment vor mehr als zwei Jahren berichtet wurde und/oder

- der SWIFT-Teilnehmer zusammen mit seinem unabhängigen Assessor nicht bestätigen kann, dass sich auf die Ergebnisse aus dem vorangegangenen SWIFT CSP Independent Assessment weiterhin verlassen werden kann.

Herausforderungen im Rahmen des SWIFT CSP 2022

Implikationen durch die Aktualisierung des SWIFT CSCF

Im folgenden Abschnitt stellen wir die wesentlichen Herausforderungen vor, denen alle SWIFT-Teilnehmer bei der SWIFT CSP-Attestierung im Attestierungszeitraum 2022 gegenüberstehen.

Unabhängig vom Architekturtyp müssen SWIFT-Teilnehmer ab dem Attestierungszeitraum 2022 die Kontrolle **2.9 Transaction Business Controls** verpflichtend implementieren. Soweit dies bisher noch nicht erfolgt ist, sind entsprechende Kontrollen zur Erkennung, Validierung und ggf. Verhinderung der Ausführung von Transaktionen mit dem Ziel, betrügerische SWIFT-Transaktionen oder ungewöhnliche Zahlungen z.B. außerhalb der normalen Geschäftszeiten erkennen und verhindern zu können, einzuführen. Insbesondere Kontrollen für die mindestens täglich durchzuführende Abstimmung von versendeten Zahlungsverkehrsnachrichten sowie die Erkennung ungewöhnlicher Zahlungen erfordern in der Regel eine technische Lösung, um die Masse an Zahlungsverkehrsnachrichten verarbeiten zu können, Kontobewegungen und Kontostände zeitnah und effizient miteinander abzugleichen und identifizierte Mismatches zu untersuchen oder ungewöhnliche Zahlungen (der Höhe, dem Empfänger oder der Währung nach) zu erkennen und zu plausibilisieren.

In der aktuellen Version des SWIFT CSCF wird bei mehreren Kontrollen der Anwendungsbereich um verpflichtende Komponenten erweitert, wie bspw. bei Kontrolle **1.2 Operating System Privileged Account Control** um Netzwerkkomponenten. Zusätzliche Aufwände für die Implementierung der Änderungen und die Bereitstellung geeigneter Nachweise in Vorbereitung auf das unabhängige Assessment sollten von den SWIFT-Teilnehmern frühzeitig eingeplant werden.

Die Kontrollen **1.1 SWIFT Environment Protection** und **1.5A Customer Environment Protection** sind, soweit eine vollständige Trennung zwischen Test- und Produktionsumgebung nicht besteht, für Testsystemumgebungen umzusetzen. Hier sind ebenfalls zusätzliche Nachweise einzuholen, bspw. Systemkonfigurationen, welche die Durchgängigkeit der Systemtrennung belegen.

Herausforderungen für Nutzer eines Customer Connector

Die Aktualisierung des SWIFT CSCF v2022 stellt insbesondere SWIFT-Teilnehmer, die einen Customer Connector im Einsatz haben, vor neue Herausforderungen in den Vorbereitungen des SWIFT CSP Independent Assessment für den Attestierungszeitraum 2022.

Mit der Überführung des Customer Connector in eine verpflichtend zu betrachtende Komponente ist für den Attestierungszeitraum 2022 mindestens ein Delta-Assessment für Kontrollen, die den Customer Connector als verpflichtende Komponente umfassen, durchzuführen, sofern dieser im Independent Assessment für den Attestierungszeitraum 2021 nicht bereits berücksichtigt wurde.

Des Weiteren haben SWIFT-Teilnehmer mit einem Customer Connector den Zugriff auf diesen mittels Multi-Faktor-Authentifizierung abzusichern, sodass ein ausschließlicher Zugriff mittels Benutzerkennung in Kombination mit einem individuellen Passwort nicht mehr möglich ist. Dies hat zur Folge, dass insbesondere SWIFT-Teilnehmer mit dem Architekturtyp A4 eine Multi-Faktor-Authentifizierungslösung für den Zugriff auf den Customer Connector implementieren müssen.

Darüber hinaus haben SWIFT-Teilnehmer mit einem Customer Connector die Kontrollen **6.2 Software Integrity und 6.3 Database Integrity** optional umzusetzen. Sofern der Customer Connector nicht über eine integrierte Software-Integritätsprüfung verfügt, ist die Software in einen automatischen Code-Review bzw. eine File-Integritätsüberwachung einzubinden, um Änderungen an der Software zu erkennen.

Des Weiteren ist eine Durchführung von Prüfsummenabgleichen für über das Internet bezogene Software vor Produktivsetzung vorzunehmen und entsprechend zu dokumentieren. Sofern Kontrolle **6.3 Database Integrity** für den Customer Connector zu berücksichtigen ist, sind hierzu ebenfalls Maßnahmen für die Erkennung und Nachverfolgung von gelöschten oder geänderten Datenbankeinträgen im Zusammenhang mit Zahlungsverkehrsnachrichten zu implementieren.

In Bezug auf die neu eingeführte empfohlene Kontrolle **1.5A Customer Secure Zone** ist davon auszugehen, dass diese

mittelfristig in eine verpflichtende Kontrolle überführt wird. Dementsprechend sollte bereits im Rahmen des Independent Assessment für den Attestierungszeitraum 2022 eine Gap-Analyse durchgeführt und eine entsprechende Mitigation Roadmap zur Schließung eventuell identifizierter Gaps erstellt werden.

Herausforderungen im Rahmen der Durchführung des Independent Assessment

Neben den Änderungen im SWIFT CSCF v2022 führen auch die unterschiedlichen Optionen der Durchführung des SWIFT CSP Independent Assessment zu zusätzlichen Herausforderungen.

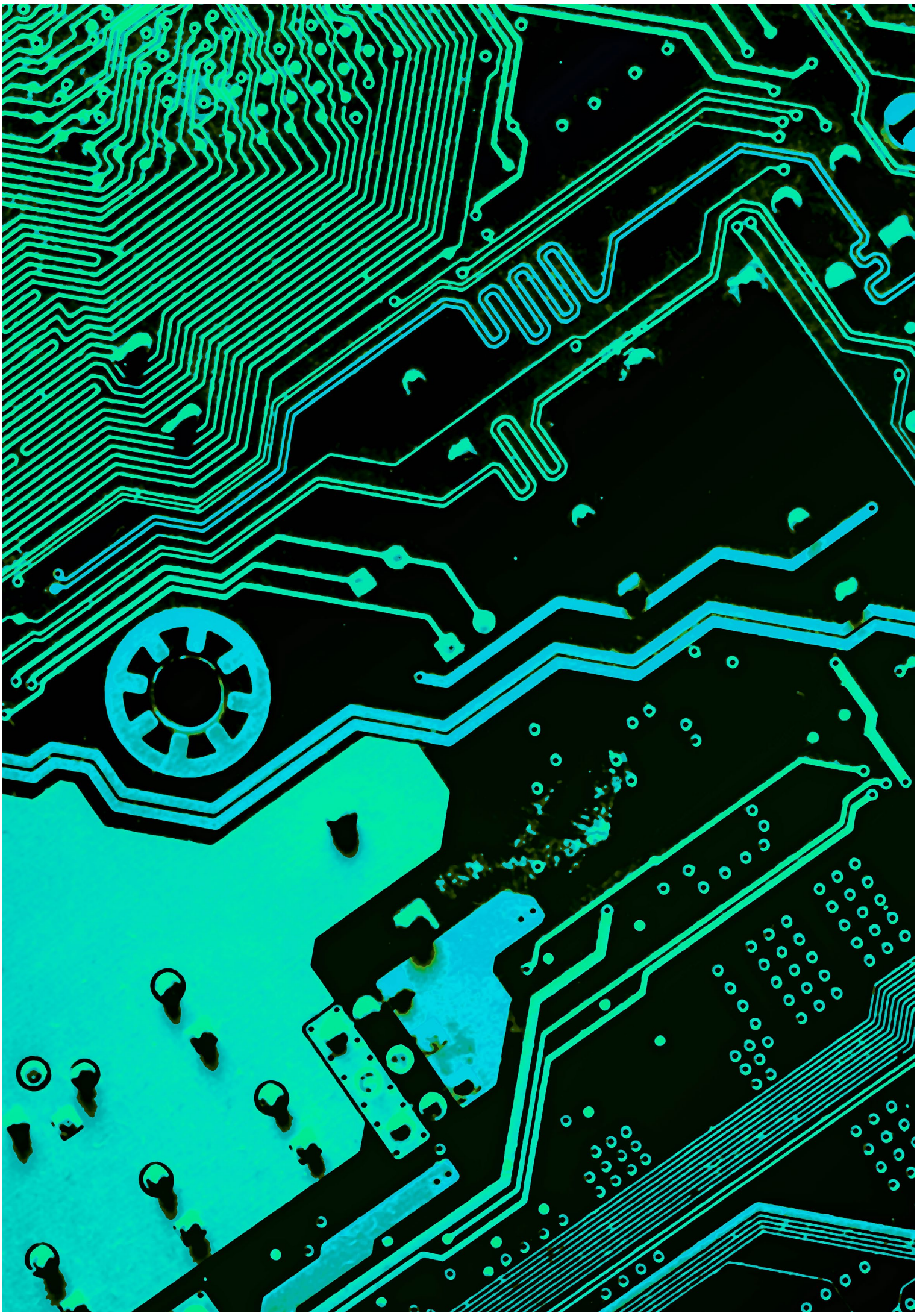
Während bei der Option des Re-Assessment wie bisher die verpflichtenden und optional die empfohlenen Kontrollen für die in den Anwendungsbereich des SWIFT CSCF v2022 fallenden Komponenten in Abhängigkeit vom Architekturtyp vollständig zu bewerten sind, unterscheidet sich bei der Option des Delta-Assessment dessen Umfang. Dieser bestimmt sich durch die Änderungen des SWIFT CSCF v2022 gegenüber der Vorjahresversion und/oder durch Infrastrukturänderungen des SWIFT-Teilnehmers seit dem zuletzt durchgeführten Assessment. Hierbei sind durch den unabhängigen Assessor neben den Auswirkungen der aktualisierten Version des SWIFT CSCF auf die bereits implementierten Kontrollen ebenso die Änderungen in der Architektur des SWIFT-Teilnehmers, Änderungen in den Kontrollen und Implementierungsmethoden sowie die geänderten Komponenten zu beurteilen.

Bei der vollständigen Wiederverwertung der Ergebnisse des Vorjahres-Assessment steht allen voran die Fragestellung, wie SWIFT-Teilnehmer und ihr unabhängiger Assessor gemeinsam zum Ergebnis kommen, dass die Ergebnisse des Vorjahres-Assessment weiterhin Gültigkeit besitzen. Diese Option könnte perspektivisch zunehmend an Bedeutung gewinnen, sollte SWIFT von einem jährlichen Veröffentlichungsturnus abweichen oder sollten zukünftige Versionen des SWIFT CSCF nur marginale Änderungen beinhalten.

Damit der SWIFT-Teilnehmer und der unabhängige Assessor zu einer validen Aussage bzgl. der Gültigkeit des Vorjahres-Assessment kommen, sind neben Interviews zumindest zentrale Kontrollen, die Hochrisikobereiche adressieren, zu revalidieren, sodass auch bei der vollständigen Verwertung der Ergebnisse des Independent Assessment des Vorjahres Aufwände entstehen.

SWIFT-Teilnehmer sollten daher die Optionen und deren Voraussetzungen frühzeitig mit ihrem unabhängigen Assessor evaluieren.

Eine weitere Herausforderung betrifft die im November 2022 anstehende ISO-20022-Migration des Eurosystems. SWIFT-Teilnehmer sollten sich frühzeitig über den geplanten Zeitraum für die Durchführung des Independent Assessment auseinandersetzen, da erfolgskritische Ressourcen möglicherweise sowohl im Rahmen des SWIFT CSP Independent Assessment als auch in der ISO-20022-Migration des Eurosystems eingebunden sind. Potenzielle Ressourcenkonflikte sollten daher frühzeitig identifiziert und die Verfügbarkeit durch eine angemessene Ressourcenplanung sichergestellt werden.



Unsere Services

Deloitte unterstützt Sie mit individuell auf Sie zugeschnittenen Lösungen zur Umsetzung der Herausforderungen rund um das SWIFT CSP. Wir bieten Expertise bei der Implementierung der Sicherheitskontrollen, der Durchführung eines SWIFT CSP Readiness Assessment sowie der Durchführung unabhängiger Assessments entsprechend Ihren Bedürfnissen. Darüber hinaus offerieren wir Ihnen integrierte Assessments in Bezug auf Anforderungen anderer Marktinfrastrukturen, wie beispielsweise TARGET2-Selbstzertifizierung oder PCI-DSS sowie allgemeiner Standards im Umfeld der Informationssicherheit.

Unterstützung bei der Implementierung

- Durchführung eines Soll-Ist-Abgleichs der Änderungen des SWIFT CSCF v2022, Analyse des Architekturtyps, der SWIFT-Infrastruktur und der in den Anwendungsbereich fallenden Komponenten
- Entwicklung einer Roadmap zur Implementierung der geänderten und neuen Anforderungen aus dem SWIFT CSCF v2022 unter Berücksichtigung bestehender SWIFT-Release-Wechsel sowie ggf. weiterer interner Projekte
- Unterstützung der Implementierung der geänderten und neuen Anforderungen aus dem SWIFT CSCF v2022 sowie sonstiger Gaps unter Berücksichtigung der entwickelten Roadmap

SWIFT CSP Readiness Assessment

- Bewertung des Reifegrades der implementierten Sicherheitskontrollen vor dem unabhängigen Assessment
- Identifizierung von Schwachstellen und Optimierungsbedarfen in Bezug auf die Angemessenheit und Wirksamkeit der Kontrollen
- Ableitung von Handlungsempfehlungen zur Behebung identifizierter Schwachstellen, zur Sicherstellung der Compliance sowie zur Realisierung identifizierter Optimierungsbedarfe
- Unterstützung bei der Umsetzung identifizierter Handlungsbedarfe und Optimierungspotenziale vor Durchführung des unabhängigen Assessment
- Unterstützung bei der Bereitstellung geeigneter Nachweise, Vorbereitung des Personals auf das unabhängige interne oder externe Assessment und Erfahrungsaustausch hinsichtlich Good Practices

Unabhängiges SWIFT CSP Assessment

- Durchführung eines unabhängigen externen Assessment hinsichtlich der Angemessenheit und Wirksamkeit der implementierten Sicherheitskontrollen gemäß dem SWIFT CSCF sowie Berichterstellung
- Alternativ: Durchführung eines integrierten unabhängigen internen und externen Assessment in Kooperation mit Ihrer 2nd oder 3rd Line of Defense oder bei Anwendbarkeit Durchführung eines Delta-Assessment auf Basis des letzten unabhängigen Assessment
- In allen Fällen unterstützen wir Sie bei der Darstellung von Handlungs- und Optimierungsbedarfen inkl. Unterstützung bei der Umsetzung kurzfristiger Maßnahmen zur Sicherstellung der Angemessenheit und Wirksamkeit verpflichtend sowie zur Umsetzung empfohlener Kontrollen zum Meldezeitpunkt an SWIFT

Abb. 3 – Modulare Services

Implementierung SWIFT CSP	**SWIFT CSP Readiness Assessment**	**Externes Independent Assessment** (bei einmaliger Beauftragung)
Externes Independent Assessment und Delta Assessment (alternierend bei mehrjähriger Beauftragung)	**Gemischtes Independent Assessment**	**Integrierte Assessments** (bspw. TARGET2, PCI-DSS, ...)

Unsere Expertise im Bereich Zahlungsverkehr und Cyber

Deloitte verfügt in Deutschland, EMEA sowie weltweit über mehr als 1.500 Berater:innen und Prüfer:innen mit ausgewiesener Expertise in den Bereichen Zahlungsverkehr und Cyber-Resilienz. In zahlreichen erfolgreich abgeschlossenen Einführungsprojekten und Assessments des SWIFT CSP konnten wir unseren Beratungs- bzw. Prüfungsansatz sowie unsere Kompetenz in den genannten Bereichen erfolgreich unter Beweis stellen. Mit unserem Netzwerk zur SWIFT, anderen Marktinfrastrukturbetreibern sowie zu relevanten Aufsichtsbehörden können Spezialfragen zu Einzelsachverhalten aus Ihrem Projekt zeitnah und vollumfänglich beantwortet werden.

Einbindung von Subject Matter Experts mit breiter Erfahrung in Bezug auf SWIFT und Zahlungsverkehr

- Deloitte pflegt eine enge Beziehung zu SWIFT und hat bereits eine Vielzahl von Aufträgen für SWIFT durchgeführt
- Unser Team hat tiefe Einblicke in die Funktionsfähigkeit sowie den Funktionsumfang des SWIFT-Netzwerks und liefert umfassendes Expertenwissen
- Regelmäßige Abstimmungsgespräche sorgen für einen Wissenstransfer zwischen Deloitte und dem Auftraggeber

Berücksichtigung des SWIFT CSP Independent Assessment Framework in unserem Beratungs- und Prüfungsansatz

- Unser Assessment-Ansatz beruht auf den SWIFT-Vorgaben und lehnt sich an den Prüfungsstandard ISAE 3000 an, um eine umfassende Marktakzeptanz zu gewährleisten
- Der Beratungs- oder Assessmentumfang wird durch Ihre genutzte SWIFT-Infrastruktur (Architekturtyp) sowie die Anforderungen des jeweils gültigen SWIFT Customer Security Controls Framework definiert

Modularer Ansatz zur Berücksichtigung zusätzlicher FMI-Anforderungen

- Aufsichtsbehörden und FMI-Institutionen definieren Anforderungen an die Teilnehmer des Zahlungsverkehrs
- Unser modularer Ansatz ermöglicht eine einfache Integration von weiteren Anforderungen (bspw. TARGET2, PCI-DSS, ...)
- Dieser modulare Ansatz schafft Synergien bei zukünftigen Assessments und reduziert die Gesamtkosten

Ihre Ansprechpartner

Daniel Hellmann
Director
Risk Advisory | Payments
Tel: +49 30 25468 5879
dhellmann@deloitte.de

Jörg Lang
Senior Manager
Risk Advisory | Payments
Tel: +49 711 16554 7026
jolang@deloitte.de

Ann-Kathrin Sobotta
Senior Consultant
Risk Advisory | Payments
Tel: +49 69 75695 7691
ansobotta@deloitte.de

Deloitte.

Stand 04/2022