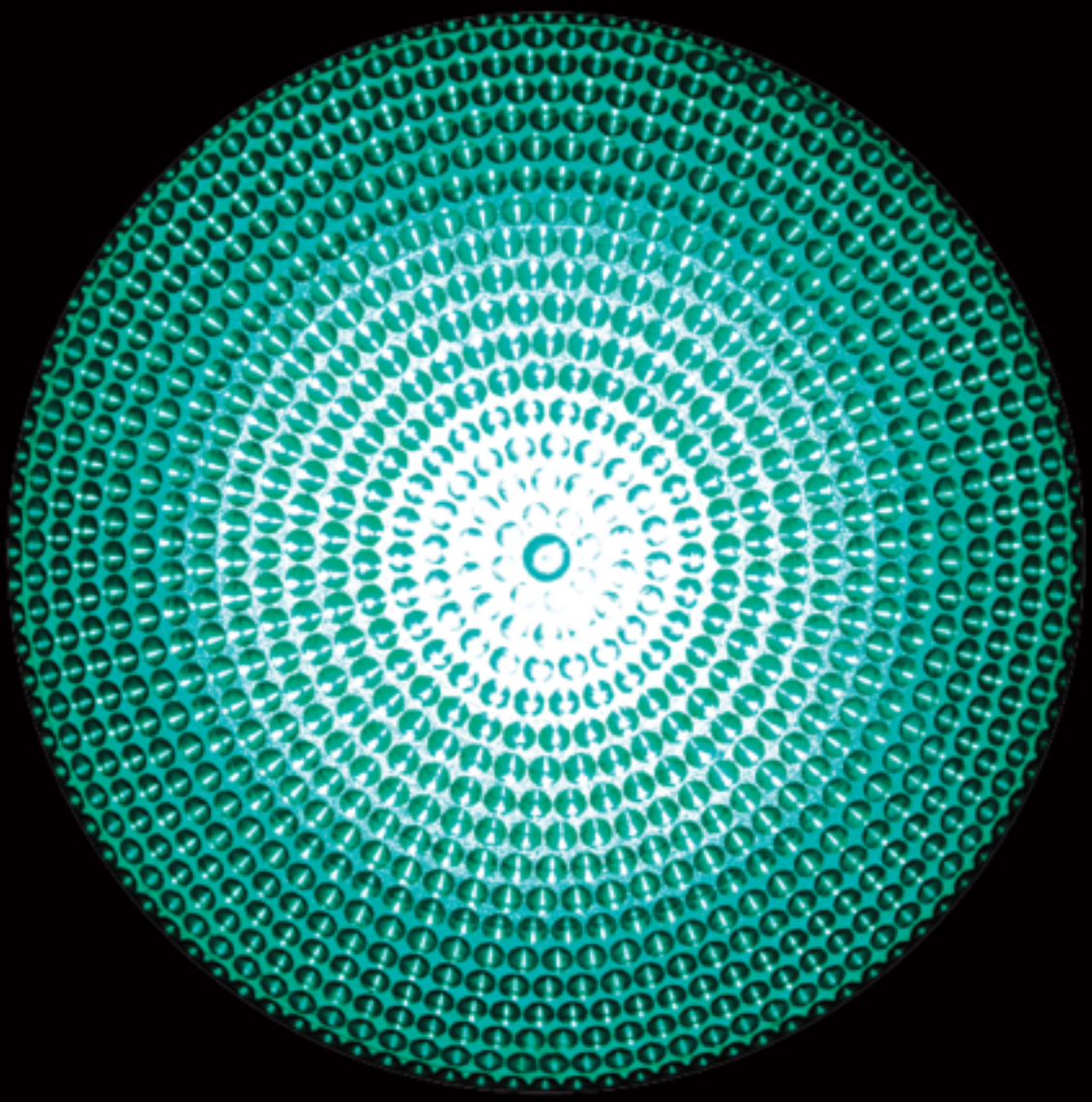
Deloitte.



SWIFT Customer Security Program (CSP)

Neuerungen 2020

SWIFT hat im Juli 2019 umfassende Neuerungen an dem SWIFT Customer Security Program vorgenommen, die ab dem Jahr 2020 von den Teilnehmern zu berücksichtigen sind. SWIFT zielt mit den Anpassungen auf eine weitere Erhöhung der Cyber-Resilienz bei den Teilnehmern sowie Verlässlichkeit der Implementierung des SWIFT Customer Security Controls Framework ab.

Die wichtigsten Neuerungen sowie die Herausforderungen bei der Umsetzung fassen wir in diesem Whitepaper zusammen.

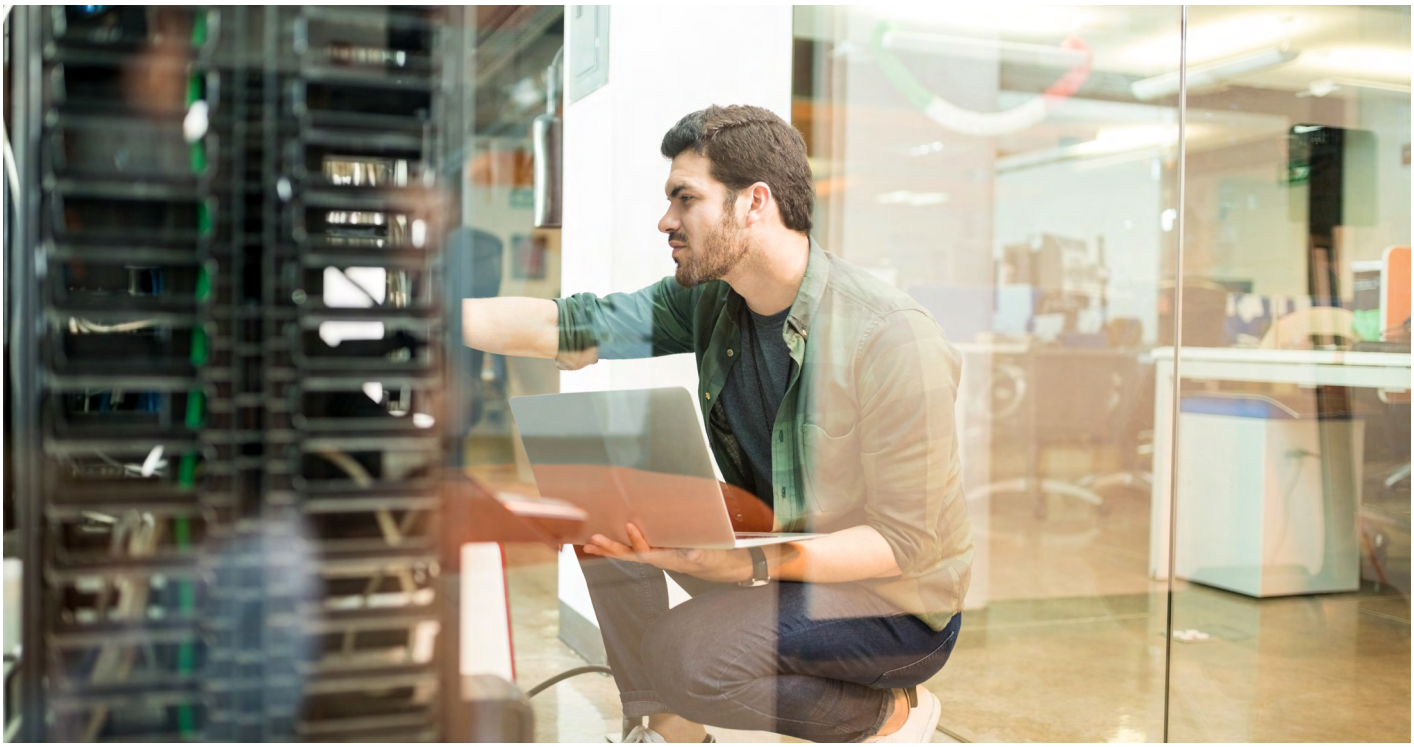
Einführung einer neuen Assessment-Methodik

Zur Erhöhung der Aussagekraft des Assessments der Compliance gegen die verpflichtenden („mandatory“) und freiwilligen („advisory“) Kontrollen des dem SWIFT CSP zugrunde liegenden SWIFT Customer Security Controls Framework (CSCF) wurde von SWIFT ein unabhängiges Rahmenwerk (IAF – Independent Assessment Framework) für die Durchführung der Assessments im Juli 2019 eingeführt. Das IAF konkretisiert die Anforderungen an Art und Umfang des Assessments, die Dokumentation sowie den Umgang mit den Ergebnissen aus dem durchgeführten Assessment.

Eine wesentliche Änderung ist die Anpassung der Anforderungen an die Durchführung des Assessments. In der Vergangenheit war es möglich, dieses im Form eines Self-Assessments durch die operativ verantwortlichen Bereiche (1st Line of Defense) durchführen zu lassen.

Mit dem CSCF v2020 entfällt diese Möglichkeit und wird durch das Community Standard Assessment ersetzt. Mit dessen Einführung ist das Assessment der Compliance gegen das CSCF nun unabhängig von den für das SWIFT CSP operativ verantwortlichen Bereichen durch geeignete interne Einheiten der 2nd Line of Defense (bspw. Compliance oder Risikomanagement), der 3rd Line of Defense (Interne Revision) oder durch qualifizierte externe Prüfer durchzuführen.

Parallel zu der verpflichtenden Durchführung des Community Standard Assessments behält sich SWIFT das Recht vor, anlassbezogen die Durchführung eines externen Assessments bei ausgewählten Teilnehmern einzufordern. SWIFT-Teilnehmer, die das Assessment bereits durch externe Prüfer haben durchführen lassen, sind von dieser Anforderung befreit.



Anpassung der zu betrachtenden SWIFT-Umgebung (Secure Zone)

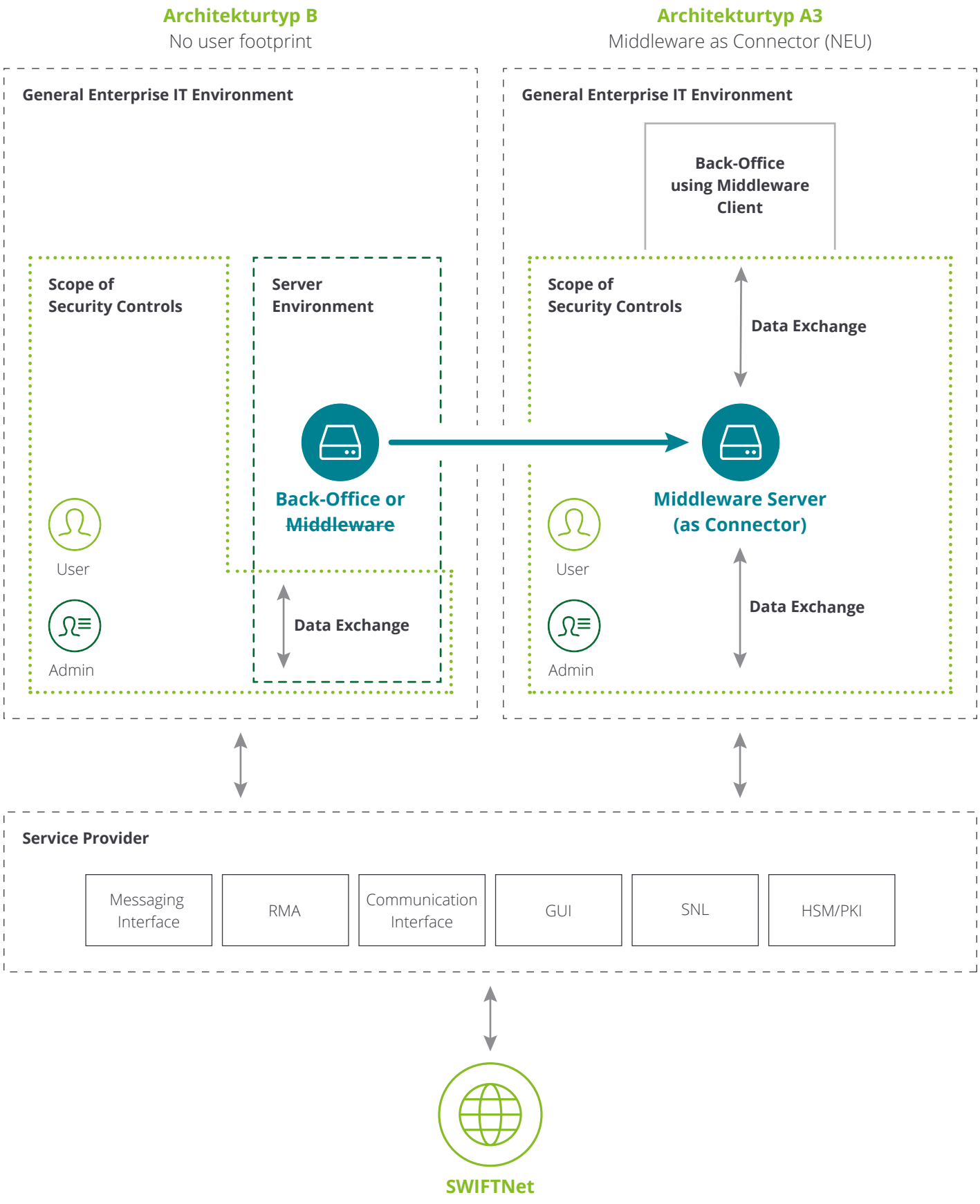
Im SWIFT CSCF v2020 erfolgen Anpassung und Konkretisierung der zu betrachtenden SWIFT-Umgebung mit Auswirkungen auf die definierten Architekturtypen sowie damit verbunden den Umfang der zu implementierenden Mandatory und Advisory Controls.

Die wesentliche Änderung ergibt sich für SWIFT-Teilnehmer, die über keine eigene SWIFT-Infrastruktur verfügen und über eine Middleware als Connector über einen Serviceprovider SWIFT-Nachrichten versenden und empfangen. Diese Middleware-Komponenten werden von SWIFT im CSCF v2020 in den Architekturtyp A3 überführt, sodass durch SWIFT-Teilnehmer mit Middleware-Komponenten ein erweitertes Set an Mandatory und Advisory Controls zu berücksichtigen ist.

Daneben wird konkretisiert, dass Testsysteme, die nicht vollständig von der SWIFT-Produktivumgebung getrennt betrieben werden, ebenfalls unter die Anforderungen des SWIFT CSCF v2020 fallen. Dies kann die zu betrachtende SWIFT-Umgebung zusätzlich erweitern.

Kunden, die über eine Middleware-Komponente an SWIFT angeschlossen sind, müssen ab 2020 sämtliche verpflichtenden Kontrollen des SWIFT CSCF implementieren.

Abb. 1 – Umgliederung innerhalb der von SWIFT definierten Architekturtypen



Weiterentwicklung des Customer Security Controls Framework

Mit der Veröffentlichung des CSCF v2020 erfolgen Anpassungen an ausgewählten Kontrollen, um Änderungen in den Angriffsvektoren und den technischen Fortschritt zu reflektieren sowie das Kontrollumfeld zu optimieren.

Überführung von zwei Advisory Controls (eingeführt in v2019) in Mandatory Controls

- **1.3 – Virtualization Platform Protection**
  Ziel ist, Virtualisierungsplattformen und virtuelle Server, auf denen SWIFT-relevante Komponenten betrieben werden, im gleichen Maße wie physische Systeme zu schützen

- **2.10 – Application Hardening**
  Ziel ist, Angriffsflächen von SWIFT-relevanten Komponenten durch die Härtung von Schnittstellen und Anwendungen zu verringern

Aufnahme von zwei neuen Advisory Controls

- **1.4A – Restrict Internet Access**
  Ausgliederung dieser Kontrolle aus den Kontrollen 1.1 (SWIFT Environment Protection) und 1.3 (Virtualization Platform Protection) und Bündelung der Vorgaben für Internetzugang

- **2.11A – RMS Business Control**
  Ausgliederung dieser Kontrolle aus der Kontrolle 2.9A (Transaction Business Controls), zur Trennung der Vorgaben für Transaktionen und Relationship Management Application (RMA)

Erweiterung einer Advisory Control

- **2.4A – Back-Office Data Flow Security**
  Aufnahme von Middleware-Komponenten in den Anwendungsbereich der Kontrolle

Vorgehensweise zur Umsetzung der Neuerungen im SWIFT CSP

Abb. 2 – Meilensteine bei der Umsetzung der Neuerungen im SWIFT CSP

Herausforderungen

Die Einführung einer neuen Assessment-Methodik ab 2020 erfordert ein Umdenken und einen neuen Ansatz zur Prüfung der Angemessenheit sowie Wirksamkeit der im SWIFT CSCF v2020 definierten Anforderungen und stellt SWIFT-Teilnehmer vor umfassende Herausforderungen:

- Umsetzung neuer und angepasster Advisory und Mandatory Controls
- Überprüfung und Validierung der Tiefe der Implementierung durch die 2nd oder 3rd Line of Defense bzw. externe qualifizierte Prüfer statt wie bisher durch den für die Umsetzung verantwortlichen Bereich (1st Line of Defense)
- Zusätzliche, unerwartete/ungeplante Aufwände durch potenzielle Anordnung eines externen Assessments durch SWIFT

Neben der Einführung einer neuen Assessment-Methodik stellen die Anpassungen der zu prüfenden SWIFT-Umgebung die Teilnehmer vor weitere Herausforderungen:

- Ausbau bereits implementierter Kontrollen durch die Erweiterung der Definition des „Data Exchange Layer“
- Implementierungsaufwand durch Erweiterung des Anwendungsbereichs um Middleware-Systeme (z.B. IBM MQ Server)
- Neubewertung der SWIFT-Umgebung und ggf. Neuzuordnung von SWIFT-Umgebungen des Architekturtyps B zu den Architekturtypen A1, A2 und A3 durch angepasste Definitionen sowie einhergehende Berücksichtigung sämtlicher 31 statt zuvor 22 Kontrollen

Durch die Überführung von zwei Advisory Controls in Mandatory Controls müssen Unternehmen, die Erstere bisher nicht oder nur teilweise implementiert haben, nun ggf. weitere Anforderungen verpflichtend umsetzen. Die Einführung von zwei neuen Advisory Controls sowie die Erweiterung des Anwendungsbereichs der Advisory Control 2.4A auf Middleware-Komponenten sorgen zusätzlich für akuten Handlungsbedarf bis Ende 2020.

Die Einführung des Community Standard Assessment und die Anpassung der zu prüfenden SWIFT-Umgebung stellen Teilnehmer vor neue Herausforderungen.

Unsere Services

Deloitte unterstützt Sie zum einen bei der Implementierung der geänderten Anforderungen oder bietet Ihnen zum anderen die Durchführung eines SWIFT CSP Readiness Assessment in Vorbereitung auf beziehungsweise die Durchführung eines unabhängigen Assessments in Bezug auf die Angemessenheit und Wirksamkeit der im SWIFT CSCF definierten Kontrollen an.

Unterstützung bei der Implementierung

- Durchführung einer Gap-Analyse in Bezug auf die Änderungen des SWIFT CSCF v2020 sowie ggf. etablierter Best Practices in der Umsetzung des SWIFT CSCF
- Entwicklung einer Roadmap zur Implementierung der geänderten bzw. neuen Anforderungen aus dem SWIFT CSCF v2020 unter Berücksichtigung bestehender SWIFT-Release-Wechsel sowie ggf. weiterer interner Projekte
- Unterstützung der Implementierung der geänderten und neuen Anforderungen aus dem SWIFT CSCF v2020 sowie sonstiger Gaps unter Berücksichtigung der entwickelten Roadmap

SWIFT CSP Readiness Assessment

- Bewertung des Reifegrades der implementierten SWIFT-CSCF-Kontrollen vor dem unabhängigen intern oder extern durchgeführten Assessment
- Identifizierung von Schwachstellen und Optimierungsbedarfen in Bezug auf die Angemessenheit und Wirksamkeit der Mandatory und Advisory Controls
- Ableitung von Handlungsoptionen zur Behebung identifizierter Schwachstellen und Sicherstellung der Compliance sowie zur Realisierung identifizierter Optimierungbedarfe
- Unterstützung bei der Umsetzung identifizierter Handlungsbedarfe und Optimierungspotenziale vor Durchführung des unabhängigen internen oder externen Assessments

Unabhängiges Assessment des SWIFT CSP

- Durchführung eines unabhängigen Assessments in Bezug auf die Angemessenheit und Wirksamkeit der implementierten SWIFT-CSCF-Kontrollen inkl. Berichterstellung in den von SWIFT bereitgestellten Vorlagen
- Soweit notwendig, Darstellung von Handlungs- und Optimierungsbedarfen inkl. Unterstützung bei der Umsetzung kurzfristiger Maßnahmen zur Sicherstellung der Angemessenheit und Wirksamkeit der Mandatory und Advisory Controls zum Meldezeitpunkt an SWIFT
- Optional: Durchführung integrierter Assessments in Bezug auf Anforderungen anderer Marktinfrastrukturen (bspw. Target2-Selbstzertifizierung)

Unsere Expertise im Bereich Zahlungsverkehr und Cyber-Resilienz

Deloitte verfügt über mehr als 1.500 Berater und Prüfer mit ausgewiesener Expertise bei Zahlungsverkehr und Cyber-Resilienz in Deutschland, EMEA sowie weltweit. In zahlreichen erfolgreich abgeschlossenen Einführungsprojekten und Prüfungen des SWIFT CSP konnten wir unseren Beratungs- bzw. Prüfungsansatz sowie unsere Kompetenz in den genannten Bereichen erfolgreich demonstrieren.

Mit unserem Netzwerk zu SWIFT, anderen Marktinfrastrukturbetreibern sowie zu relevanten Aufsichtsbehörden können Spezialfragen zu Einzelsachverhalten aus Ihrem Projekt zeitnah und vollumfänglich beantwortet werden.

Abb. 3 – Unser Mehrwert für Ihr Projekt

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 SWIFT 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

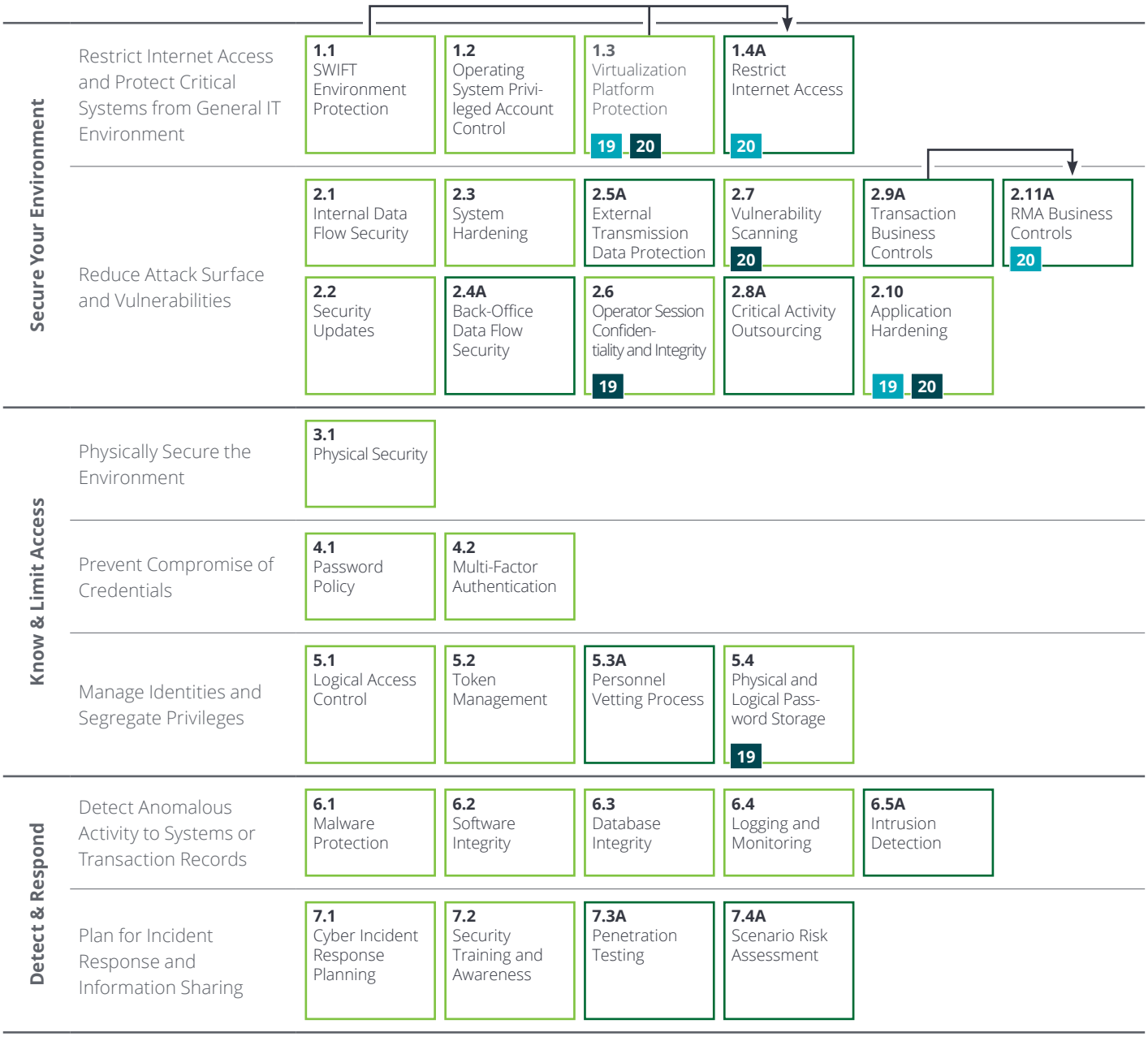
- Unser Prüfungsansatz beruht auf den SWIFT-Vorgaben sowie dem Prüfungsstandard ISAE 3000, um eine umfassende Marktakzeptanz zu gewährleisten.
- Der Beratungs- oder Prüfungsumfang wird durch Ihre genutzte SWIFT-Infrastruktur (Architekturtyp) sowie die Anforderungen des jeweils gültigen SWIFT CSP definiert.

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 Prüfungen und reduziert die Gesamtkosten.

Übersicht der Advisory und Mandatory Controls des SWIFT CSCF v2020

Abb. 4 – Änderungen in den Kontrollen des CSCF v2020



Ihre Ansprechpartner

Daniel Hellmann
Director
Risk Advisory | Payments
Tel: +49 (0)30 25468 5879
dhellmann@deloitte.de

Jörg Lang
Senior Manager
Risk Advisory | Payments
Tel: +49 (0)711 16554 7026
jolang@deloitte.de

Deloitte.

Stand 05/2020