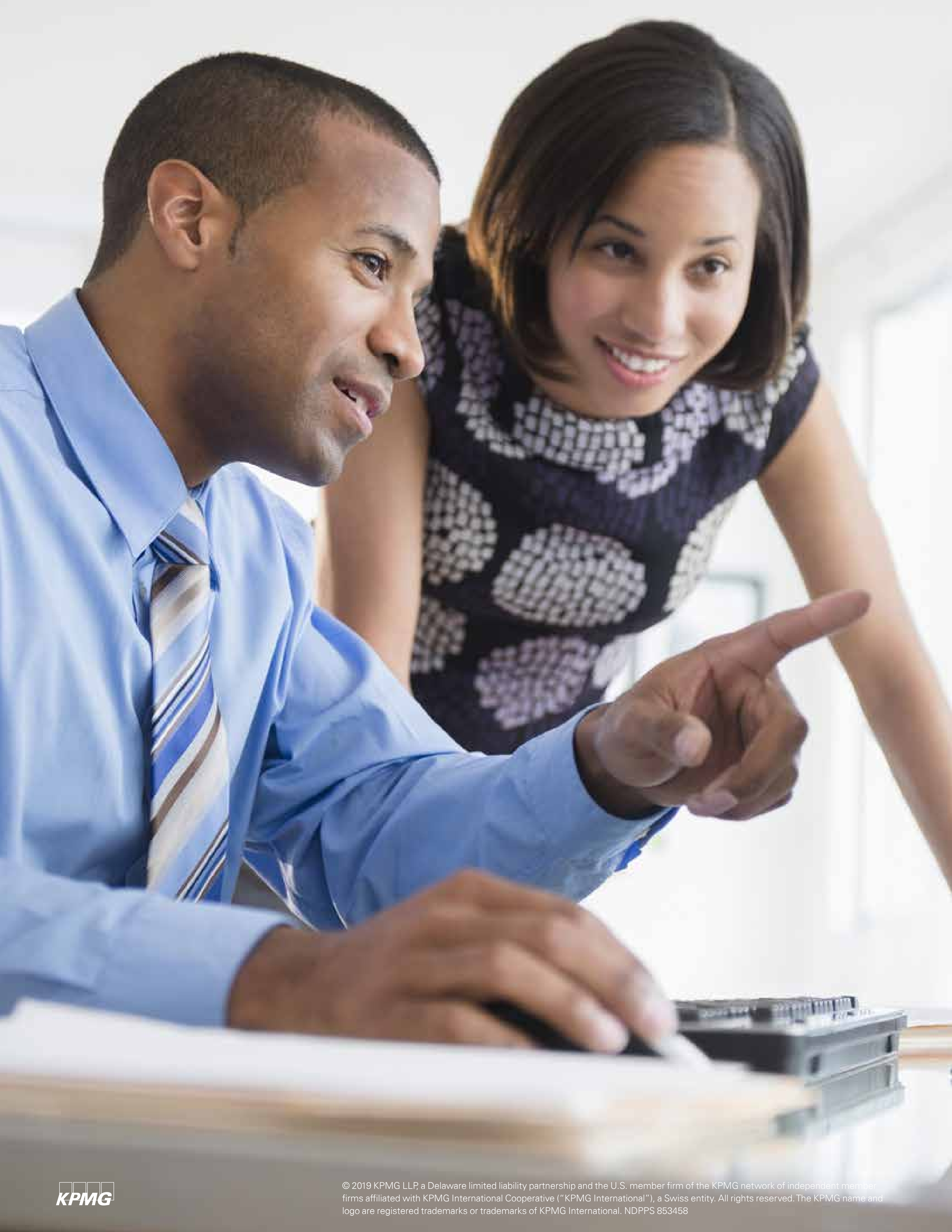
Cybersecurity assurance and the SWIFT Customer Security Program

kpmg.com



The financial sector continues to be a prime target for highly sophisticated, customized attacks. In particular, several financial institutions around the globe have had their SWIFT platforms hacked by cyber thieves resulting in the loss of hundreds of millions of dollars. In response, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) introduced a Customer Security Program (CSP) in 2017 that requires all member organizations who use the interbank messaging network to implement core security standards as well as a related "assurance framework." SWIFT has published an assurance framework (Customer Security Control Framework—CSCF) that requires SWIFT members to self-attest their compliance with the mandatory controls on an annual basis.

> **The growing threat of cyberattacks has never been more pressing, SWIFT customers are responsible for the security of their own environments; but the security of the industry as a whole is a shared responsibility requiring full collaboration within financial services.**
>
> **—Alain Desausoi,**
> Chief Information Security Officer (CISO), SWIFT
> Source: Sibos conference, London (Nov. 23, 2018)

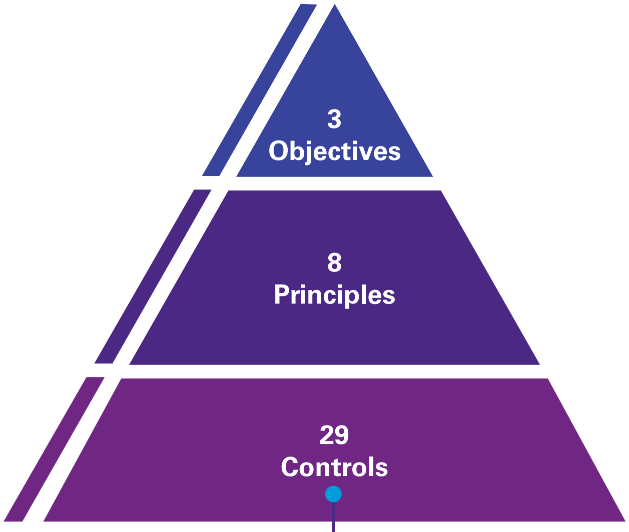
SWIFT's CSCF evolves in 2019

The SWIFT CSCF has been updated, moving three controls to the mandatory category and introducing two new controls into the advisory category.

The v.2019 of the SWIFT CSCF now comprises 19 Mandatory controls to which members must self-attest compliance and 10 Advisory controls. These changes provide SWIFT's response to the ever-changing cyber threat landscape and provides their user community with an enhanced, standardized assurance framework.

CSP secure and protect—customer security controls framework v.2019

Security controls



CSP security controls framework

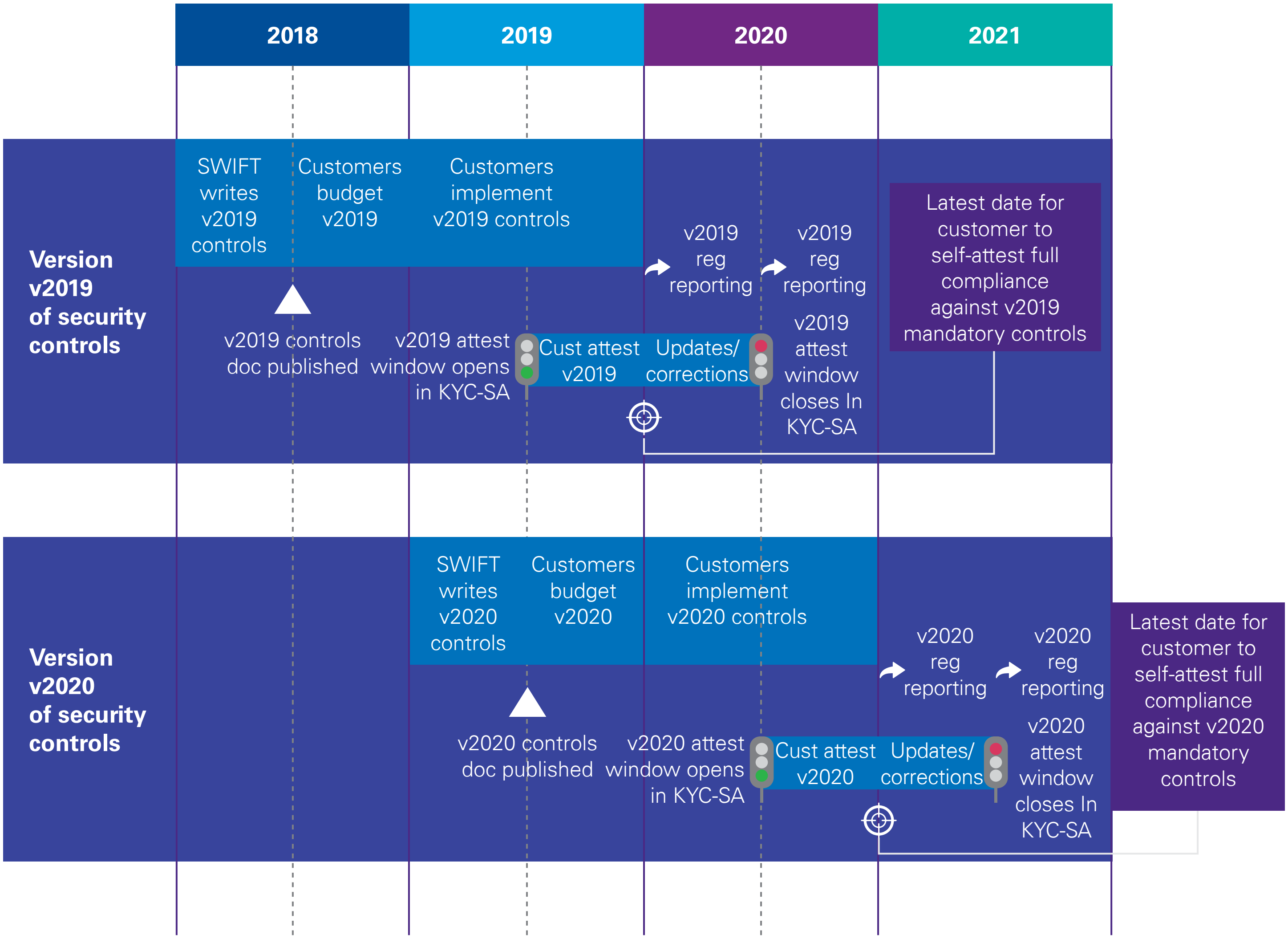
Secure your environment	1. Restrict internet access
	2. Segregate critical systems from general IT environment
	3. Reduce attack surface and vulnerabilities
	4. Physically secure the environment
Know and limit access	5. Prevent compromise of credentials
	6. Manage identities and segregate privileges
Detect and respond	7. Detect anomalous activity to system or transaction record
	8. Plan for incident response and information sharing

- 19 controls are mandatory—3 advisory promoted:
  - 2.6 Secure operator sessions
  - 2.7 Yearly vulnerability scanning
  - 5.4 Physical and logical password storage
- 10 controls are advisory—2 new ones: 1.3A Virtualization platform protection and 2.10A Application hardening
- Full compliance against mandatory ones by end of 2019

Source: SWIFT (August 10, 2018)

With the introduction of v.2019 of the CSCF, SWIFT has also published a timeline for members. This provides a schedule for the introduction of changes to the framework and the reporting requirement. SWIFT member organizations will be expected to assess and implement these changes in accordance with the published timeline.

CSP update secure and protect—CSCF v2019 (aka v2) timeline


2018
2019
2020
2021
Version v2019 of security controls
SWIFT writes v2019 controls
Customers budget v2019
Customers implement v2019 controls
v2019 reg reporting
v2019 reg reporting
Latest date for customer to self-attest full compliance against v2019 mandatory controls
v2019 controls doc published
v2019 attest window opens in KYC-SA
Cust attest v2019
Updates/ corrections
v2019 attest window closes In KYC-SA
Version v2020 of security controls
SWIFT writes v2020 controls
Customers budget v2020
Customers implement v2020 controls
v2020 reg reporting
v2020 reg reporting
Latest date for customer to self-attest full compliance against v2020 mandatory controls
v2020 controls doc published
v2020 attest window opens in KYC-SA
Cust attest v2020
Updates/ corrections
v2020 attest window closes In KYC-SA

Source: SWIFT (August 10, 2018)

SWIFT reporting requirements:

All SWIFT members are required to self-attest to their conformity with the CSCF's 19 mandatory controls and have the option to self-attest to the 10 advisory controls on an annual basis (i.e., no later than December 31).

Additionally, as mentioned in SWIFT's Q4 newsletter, SWIFT has begun requesting a select number of members to arrange for an independent external assessment to validate the members' self-attestation. These assessments will need to be performed by independent specialists that possess the necessary technical capabilities to undertake the work. If the assessments highlight that the members' current implementation does not match that self-attestation recorded in the SWIFT tool, then a new selft-attest will need to be performed.

KPMG's point of view

With the changes noted in the preceding, and the increase in pressures from counter-party requests for greater security transparency and a higher level of assurance, automation in trading and payments systems, the broad array of interconnected platforms, and the increased speed of executed transactions, there is a heightened demand on SWIFT members' ability to consume these change drivers while simultaneously maintaining an effective, rigorous cybersecurity controls framework.

By design, the SWIFT CSP will continue to change over time as the threat landscape and attack vectors evolve. The most effective management of risk takes the view of incorporating the SWIFT controls into an ongoing governance, risk, and compliance strategy within the organization and not a one-time, "check-the-box" activity. Below are some of the better practices we have assisted clients with in meeting their SWIFT requirements.

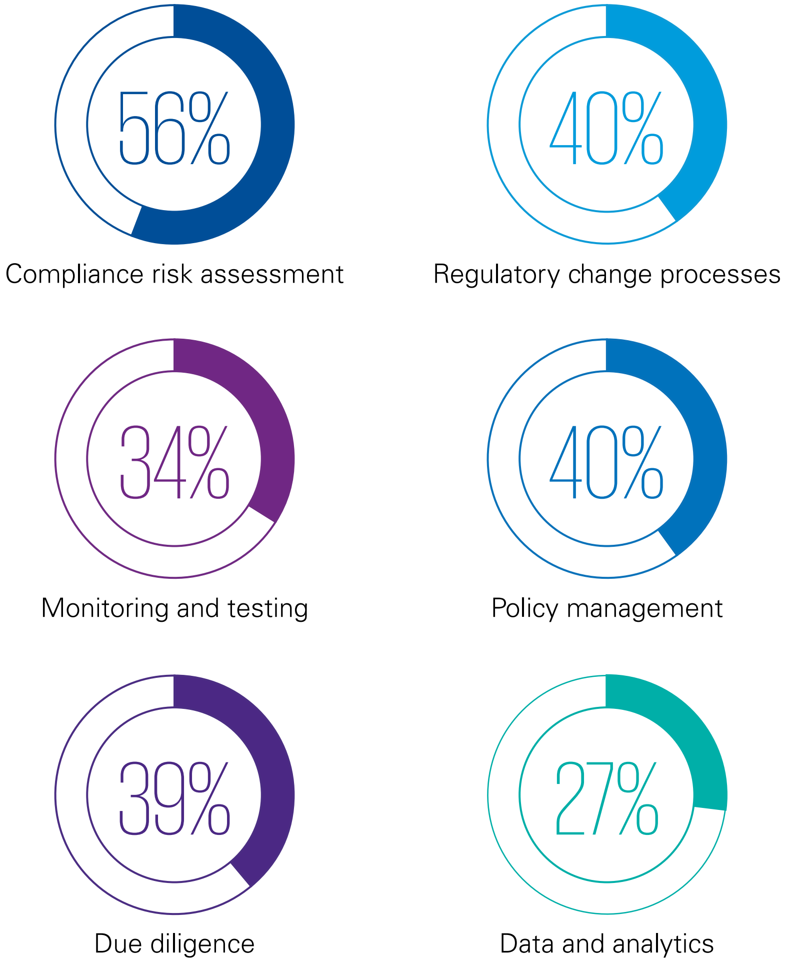
— **Risk identification:** Understanding the types of transactions, data flows, and systems used to process transactions is a critical first step for organizations. By identifying and documenting the end-to-end transaction chain and the accompanying infrastructure, management can understand the relevant risk points and design a well-structured security and risk framework in accordance with the SWIFT CSCF requirements.

— **Documentation will ease compliance pain.** With SWIFT set out to enforce compliance against its framework, it is critical for SWIFT users to understand their IT control environment and to clearly document how processes and controls implemented address the mandatory controls to alleviate the stress of going through the compliance process. Complete and accurate data flow diagrams that provide an end-to end transaction flow across multiple systems and interfaces will help to accurately identify key risk points and control gaps and increase the assurance of proper SWIFT CSCF control coverage.

— **Integration and standardization is key:** Many organizations are faced with multiple security frameworks—some imposed by their regulators and others imposed by their counterparties or business relationships. Implementing and maintaining these frameworks can be a costly and time-consuming burden. A key component in addressing the SWIFT CSCF, often times overlooked, is integrating it into the organization's enterprise governance, risk, and compliance (GRC) model. Integration into an effective GRC program provides clarity on roles and responsibilities, consistent risk assessment and change processes, a streamlined library of controls to reduce redundancy, and coordination of reporting and monitoring of control effectiveness. This integration provides organizations with an enhanced ability to achieve compliance and operational performance goals as well as reduce costs and increase the sustainability of compliance.

— **Compliance automation:** With technology changes, the evolving nature of cyber threats, updates to the CSCF Implementation Guide, and changes associated with new business strategies and processes, organizations are looking at automation solutions to reduce compliance costs, increase efficiencies, and better understand complex risks that can impact their business. Automation can be used to extract textual information from non-machine-readable documents to review transaction activity, analyze source documentation, aggregate test results for a more holistic view of risk, and assist with proactive identification and escalation of compliance failures. Automation can provide greater risk coverage and consistency and help identify more meaningful patterns in transactional data, ultimately providing stakeholders with improved insight into the organization's compliance practices.

In the shift toward automation, organizations are focused on automating the following top compliance activities:



Source: KPMG's Compliance Automation Survey (2018)

- **Independent attestation has additional benefits:** SWIFT has already started requesting some of its members to hire an independent third party to validate the members' self-attestation as a part of SWIFT's Quality Review Program. An independent, objective attestation of the member organization's adherence to the SWIFT CSCF controls helps SWIFT members provide their counterparties and correspondents with a higher, globally recognized vehicle of assurance around their SWIFT infrastructure while reducing the burden on internal resources. The independent attestation report could also be used to satisfy a SWIFT quality audit or regulatory request. Additionally, an independent, globally recognized third party can provide SWIFT members with a broader industry perspective and better practices through a readiness assessment that may lead to a more efficient and effective way of addressing their SWIFT CSP requirements.

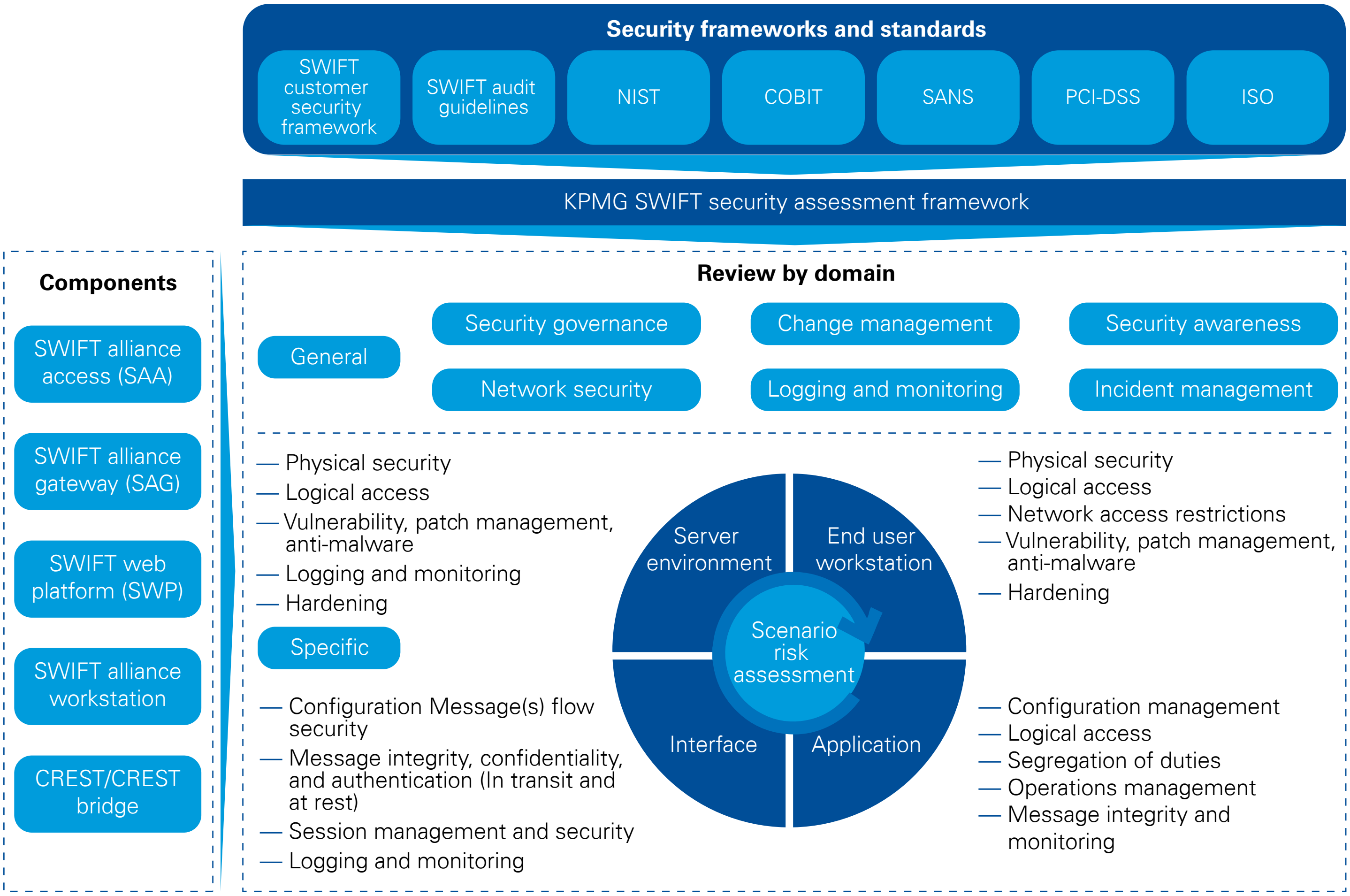
KPMG's approach

KPMG recognizes participating in a trusted SWIFT network, supported by the SWIFT CSP, is a strategic imperative for clients in the financial services industry. Since the inception of the SWIFT CSCF in 2017, KPMG has assisted clients globally in assessing their current-state SWIFT controls framework to identify gaps and provide practical, actionable recommendations for addressing those gaps in accordance with SWIFT CSCF criteria. Additionally, KPMG has also provided independent attestation services under recognized standards to clients in accordance with the SWIFT CSCF that provides those clients with a globally recognized standard of assurance and a reduction of effort for their critical in-house resources.

KPMG brings a cross-functional team of professionals from the disciplines of IT Audit and Assurance and Cybersecurity who have experience in the financial services industry to deliver readiness assessments and/or attestation services tailored to the clients' needs and in accordance with the SWIFT CSCF criteria.

KPMG has developed a SWIFT security assessment framework and standardized reporting formats for the execution of SWIFT engagements that provides:

- A consistent, holistic approach to assessing cybersecurity frameworks for the latest iteration of the SWIFT CSCF
- Globally recognized reporting standards (ISAE 3000, AT-C 205, SOC 2+, or dual reporting)
- Entity-wide processes related to SWIFT
- Domain-specific controls
- Security and IT industry better practices


Security frameworks and standards
SWIFT customer security framework
SWIFT audit guidelines
NIST
COBIT
SANS
PCI-DSS
ISO
KPMG SWIFT security assessment framework
Components
SWIFT alliance access (SAA)
SWIFT alliance gateway (SAG)
SWIFT web platform (SWP)
SWIFT alliance workstation
CREST/CREST bridge
Review by domain
General
Security governance
Network security
Change management
Logging and monitoring
Security awareness
Incident management
— Physical security
— Logical access
— Vulnerability, patch management, anti-malware
— Logging and monitoring
— Hardening
Specific
— Configuration Message(s) flow security
— Message integrity, confidentiality, and authentication (In transit and at rest)
— Session management and security
— Logging and monitoring
Server environment
End user workstation
Scenario risk assessment
Interface
Application
— Physical security
— Logical access
— Network access restrictions
— Vulnerability, patch management, anti-malware
— Hardening
— Configuration management
— Logical access
— Segregation of duties
— Operations management
— Message integrity and monitoring

KPMG has an established global footprint in security risk management and assurance services. KPMG is investing heavily in cyber consulting services and our global leadership position was confirmed by Forrester Research who named KPMG as a market leader in 2017. KPMG's capabilities are also recognized by SWIFT. As a member of SWIFT's partner ecosystem, KPMG's specialists are up to date on the latest SWIFT standards.

KPMG

SWIFT CSP: KPMG experience and global reach

KPMG is listed as a consultancy partner for SWIFT, providing SWIFT subject matter and cyber expertise

56+ The number of countries with available KPMG resources (Cyber, Audit, Swift)

25+ Number of SWIFT CSP assessments and attestations performed in the US and globally since SWIFT CSP inception

180+ Number of SWIFT CSP practitioners and SWIFT SME’s in KPMG’s global network

3.200+ Cyber Security professionals available from our global Cyber team

Reputation

KPMG is a listed Global Consultancy Partner for SWIFT

How we can help your team

As noted above, cybercrime is one of the fastest growing risks, and audit committees and executives are rushing to understand their company's position as it relates to cyber risk management. KPMG has a dedicated team who can work with your team to help challenge their thinking or assist in determining which attest vehicle best suits your specific needs.

Contact us

Chris Mottram
Partner, Advisory
T: 404-979-2100
E: cmottram@kpmg.com

Aleksandr Lembrikov
Partner, Advisory
T: 917-774-7274
E: alembrikov@kpmg.com

Tim O'Rourke
Director, Advisory
T: 404-222-3470
E: tjorourke@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.