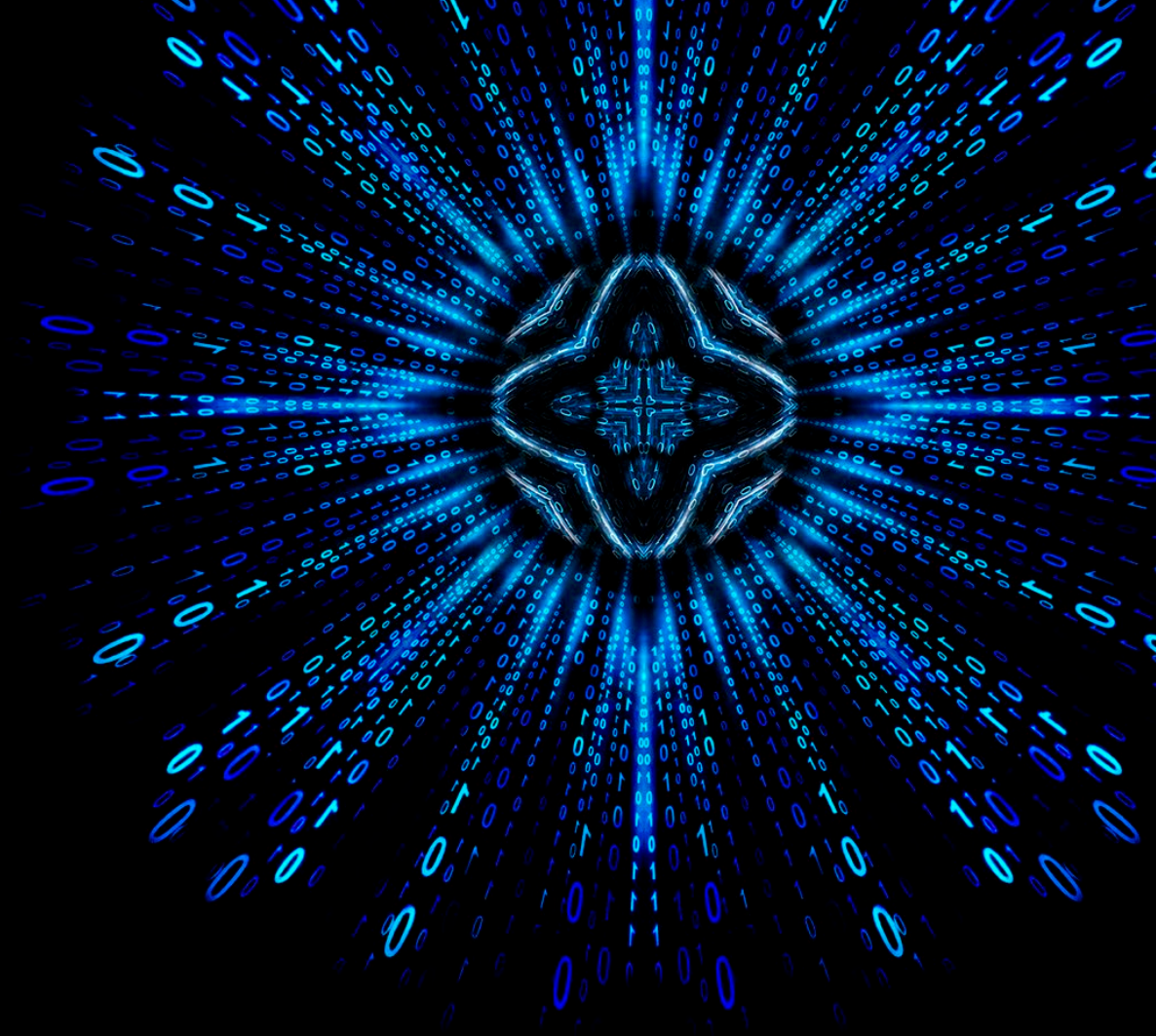
Deloitte.

SWIFT Customer Security Program

Since the Bangladesh Bank Heist of 2016, banks have seen a steady increase in high-profile cyberattacks on customers using Society for Worldwide Interbank Financial Telecommunications (SWIFT).

Deloitte can help business leaders navigate the issues associated with implementing SWIFT's Customer Security Controls Framework (CSCF) as well as address SWIFT dependencies and ultimately disrupt through innovation.



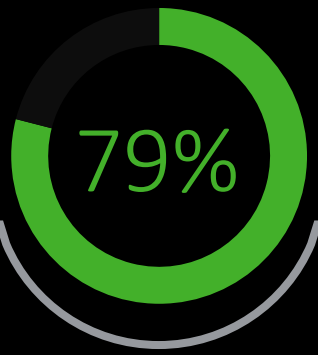
MAKING AN IMPACT THAT MATTERS since 1845

The issue: Growing risk from cybersecurity threats

A variety of cyberattacks have prompted banks and regulators to focus increasingly on managing cybersecurity risks

50% increase in attacks by banking malware, especially mobile banking malware, in the first half of 2019 compared to the same period in 2018

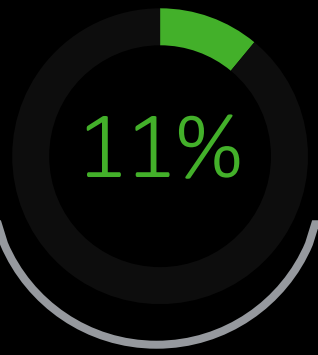
Source: ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk



ranked cyber threats as a top 5 concern for their organization

$1trillion

annual cost of cybercrime in 2019



reported high degree of confidence in their cyber resilience measures

Source: 2019 Global Cyber Risk Perception Survey

Cyberattacks ranked…

7th most likely to occur

8th most impactful risk

2nd most concerning risk for doing business

… globally over the next 10 years

In 2021, cybercrime damages may reach …

$6trillion

Source: Global Risks Report 2020

Limiting future cyberattacks

In response to recent cyberattacks, SWIFT issued baseline security requirements through its Customer Security Controls Framework. While the SWIFT network itself was not compromised in the attacks, in some cases hackers successfully breached the local operating environment established by SWIFT users.

To help limit hackers' opportunities to exploit weaknesses in SWIFT users' local environments in the future, SWIFT created the Customer Security Program (CSP), a framework designed to help users set up cybersecurity controls that they can implement themselves in their local environments.

The CSP's main components are the Customer Security Control Framework (CSCF) and the Customer Security Controls Policy (CSCP). An Independent Assessment Framework (IAF) has also been defined to guide the clients while assessing the CSP.

How SWIFT users can protect themselves

After its original release, the CSP has been updated on an annual basis to improve its coverage and to take into account the evolution of the cyber threat landscape. Compliance assessment declarations are expected at the end of each year.

SWIFT encourages its users to implement and monitor these customer security controls as part of a broader cybersecurity risk management program, which should be regularly evaluated and adjusted based on leading industry practices and changes to the individual users' security position and infrastructure.

CSCF and CSP Policy Evolution

2017

27 Controls
16 mandatory + 11 Advisory
Self-attestation by
31 Dec 2017/2018

2018

2019

29 Controls
19 mandatory + 10 Advisory
Self-attestation
by 31 Dec 2019

3 Controls Promoted to Mandatory
2.6 Operator Session flows
2.7 Vulnerability Scanning
5.4 Password Storage

2 New Advisory Controls
1.3A Virtualization Platform
2.10A Application Hardening

2020

31 Controls
21 mandatory + 10 Advisory
Independent assessment by
31 Dec 2019

2 Controls Promoted to Mandatory
1.3A Virtualization Platform
2.10A Application Hardening

2 New Advisory Controls
1.4A Restrict Internet Access
2.11A RMA Controls

1 Control with Scope Extension
2.4A Back-office data Flow
– MQ / Middleware Server

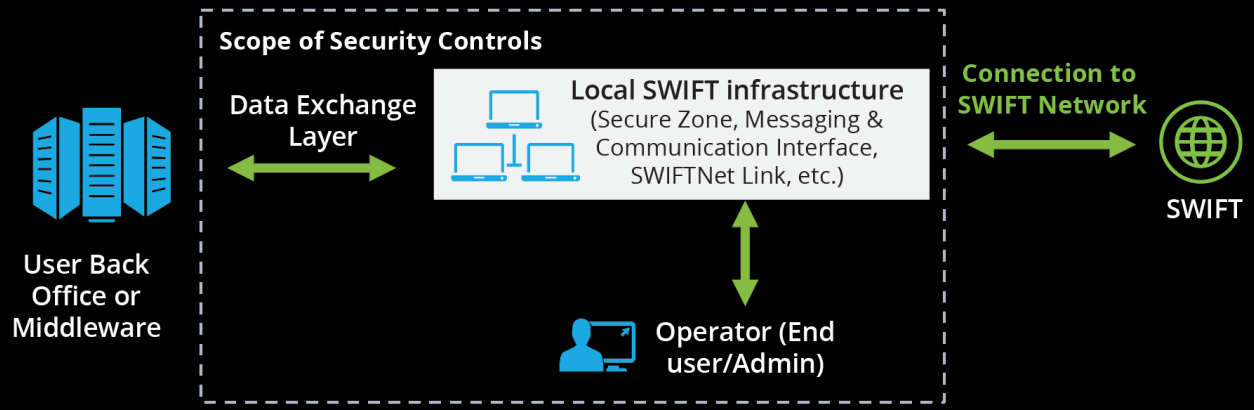
As of 2020, all SWIFT customers are mandated to support their self-attestation by an independent assessment.

- Self-attestation must be completed between June and December and will then be valid till the end of the following year.
- Self-attestation must be supported by an independent external/internal assessment.
- An annual update cycle is foreseen for CSP policy and CSCF updates.
- User Guide section transferred to KYC-SA documentation

SWIFT's strategic security principles

The Customer Security Controls Framework is a set of core security controls that are mandatory for SWIFT users. The controls are intended to help mitigate specific cybersecurity risks that SWIFT users face due to the cyber threat landscape.

Scope of SWIFT Security Controls



SWIFT Customer Security Controls Framework

Objectives	Strategic Security Principles
O1. Secure your Environment	P1. Restrict Internet access and Protect critical systems from general IT environment
	P2. Reduce attack surface & vulnerabilities
	P3. Physically secure the environment
O2. Know and limit access	P4. Prevent compromise of credentials
	P5. Manage identities & segregate privileges
O3. Detect and respond	P6. Detect anomalous activity to system or transaction records
	P7. Plan for incident response & information sharing

The framework can be applied to four types of SWIFT user architectures, titled A1, A2, A3, and B. SWIFT users must first identify which architecture applies to them before identifying and implementing the applicable controls.

How different will your declaration be on 31 December 2020?

In order to improve the level of assurance currently provided by the self-attestations, an independent assessment framework (IAF) has been developed by SWIFT and will require all attestations to be supported by an independent assessment from the CSCF 2020. The self-assessment will no longer be possible and SWIFT customers will now have to rely on an independent assessment performed either by their internal second or third line of defense (e.g., risk management, internal audit, etc.), or by an external third party organization.

AUGUST 2019

CSCF v2020 release

- **Change** identifications, such as advisory controls promoted to mandatory
- **Gap** assessment
- **Projects** plan
- **Budget** definition

JANUARY 2020

CSCF v2020 projects

- Implementation of **new** requirements
- **Improvement** of previously identified gaps
- **Preparation** of next audit

Independent Assessment Framework preparation

- Mandatory controls
- Method: Point in time evaluation of **user's implementations**

JANUARY 2021

Reporting analysis

- Assessments are **analyzed** by SWIFT
- **Additional evidence** requested by SWIFT
- Communication to third parties and business partners

CSP assessment

- Compliance assessment
- Compliance declaration

How Deloitte can support your organization

The SWIFT messaging platform, in particular, has been under concerted attacks since the Bangladesh Bank heist in 2016. Faced with highly sophisticated and organized cyberattacks, global banks need to do more to protect themselves against the rapidly evolving and adaptable cyber threat landscape.

Deloitte offers holistic services that can support your organization as you address your SWIFT dependencies, balancing the need to reduce risk with the goal of meeting productivity, business growth, and cost optimization objectives:

Impact Assessment: Deloitte will conduct initial SWIFT risk assessment, provide a prioritization framework, and review current controls

Risk Mitigation Planning: Deloitte will develop a remediation strategy and a roadmap for implementation for identified gaps in controls and processes

Testing: Deloitte will assist in establishing a testing framework and conduct testing to meet CSP requirements

Implementation Support: Deloitte will assist with governance establishment, implementation execution, and war gaming

Independent Assessment: Deloitte will review and validate your compliance with the SWIFT CSP controls and issue independent assurance reports under recognized standards (e.g., ISAE, SOC 2).

While Deloitte is prepared to assist you in connection with the SWIFT Customer Security Controls Framework, please note that Deloitte does not represent or speak for SWIFT, and the Customer Security Controls Framework is part of the contractual framework between SWIFT and its users.

How Deloitte can support your organization

SWIFT CSP Workshop

- Deloitte consultants with deep SWIFT CSP experience will conduct a workshop to review your self-attestation and provide you with high level opinion on remediation activities defined by your organization.
- Our team will interview your staff and inspect system configurations and documentation to deliver a management report that can be used for the self-attestation.

Added values: quick confirmation of your self-attestation, confirmation of your team understanding of the CSCF, and high level assessment of your remediation plan

Testing

- Deloitte can assist you in establishing a testing framework and conduct testing to meet CSP requirements.
- We will conduct initial SWIFT risk assessment, provide a prioritization framework, and assess your readiness to meet new SWIFT CSP requirements.

Added values: review of SWIFT environment, assessment of controls, and identification of compliance gaps

Controls implementation

- Through years of experience with different implementation methods, using all kinds of software and hardware, the Deloitte Cyber team is exceptionally placed to provide assistance with the implementation of controls in the CSCF.
- Our team will design and deploy process and technology solutions to mitigate control gaps, and develop a remediation strategy and a roadmap for implementation for identified gaps in controls and processes.

Added values: Deloitte team that understands the CSCF will implement controls that will fully mitigate gaps with minimal disruption to your current environment

Independent assessment

- Deloitte team has the depth of experience to review and validate your compliance with the SWIFT CSP controls and issue independent assurance reports under recognized standards (e.g., ISAE, SOC 2).

Added values: independent assessment of your SWIFT environment by a dedicated team with relevant SWIFT cybersecurity assessment experience

Our experience and credentials

SWIFT CSP tailor made methodology
Deloitte has a strong track record of performing operational and security risk assessments based on the SWIFT CSCF. Using that experience, we created a tailor made methodology based on SWIFT CSCF and international security standards specific to this type of engagements.

Selection of relevant experience

Client	Relevant experience
Multilateral development bank in the Philippines	Deloitte is conducting compliance assessment using the CSCF. This includes a compliance assessment against all mandatory controls on their onsite and disaster recovery site.
Provider of secure financial messaging services	Security assessment review program based on SWIFT Customer Security Controls Framework for a global financial messaging provider. As part of this program, we have assessed more than 100 financial messaging services connectivity providers across the world.
Provider of secure financial messaging services	Deloitte provided Quality Assurance to the provider of secure financial messaging services with their Customer Security Program (CSP). The goal of CSP is to reinforce the security of clients' wider ecosystem by engaging with its customers to make sure the security of their locally managed infrastructure is up to par. Deloitte helped analyze the attestation data and reported on the findings. Further, Deloitte advised on how to improve the program.
Central bank in Europe	Review for self-assessment of the internal controls relevant to the SWIFT environment in place at the bank and their (controls) compliance with the mandatory controls as published by SWIFT in the CSP framework.
Several major banks across EMEA region	Review of self-assessment related to the internal controls relevant to the SWIFT environment in place at the bank, and their compliance with SWIFT Customer Security Programme framework.

About Deloitte Cyber

As a recognized leader in cybersecurity consulting, Deloitte Cyber can help better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen our clients' ability to thrive in the face of cyber incidents. Using human insight, technological innovation, and enterprise-wide cyber solutions, we manage cyber everywhere, so society can go anywhere.

Value to our clients

- Unrivaled depth of technical knowledge and breadth of industry experience
- Comprehensive suite of solutions from advisory to managed security services
- Ability to develop a cyber risk program in line with the organization's strategic objectives and risk appetite
- Investment in emerging technologies, training, infrastructure, and people
- Global network of 31+ Cyber Centers provide consistency and high level of service

Cyber is everywhere. So are our services.

The ubiquity of cyber drives the scope of our services. Deloitte Cyber advises, implements, and manages solutions across the following areas:

Strategy
- Cyber strategy and transformation
- Cyber risk management
- Cyber training and awareness

Application Security
- ERP process, systems, and integrity controls including SAP S4/HANA & Oracle
- GRC, CRM, and HR security controls
- SecDevOps lifecycle

Emerging Technology
- Internet of Things
- Industrial Control Systems
- Artificial intelligence
- Robotics

Detect and Respond
- Threat intelligence
- Threat monitoring and analytics
- Vulnerability management
- Incident management and response
- Security automation and response

Cloud Infrastructure Security
- Core infrastructure security
- Cloud security
- Asset management
- Mobile and endpoint security
- Technical resilience

Data and Privacy
- Strategy
- Reporting/validation
- Architecture
- Privacy
- Protection

Identity
- Identity governance
- Advanced authentication
- Privileged access management
- User access governance
- Identity analytics
- Digital consumer identity
- Directory services and certificate lifecycle

Contact us

Anna Pabellon
Risk Advisory Leader
Deloitte Philippines
apabellon@deloitte.com

Talk to our team in the Philippines

Bel Del Castillo
Risk Advisory Manager
idelcastillo@deloitte.com

Akee Papa
Risk Advisory Senior Manager
arpapa@deloitte.com

17,000+
Cyber practitioners worldwide

125
Offices across Australia, China, India, Japan, Korea, New Zealand, Southeast Asia, Taiwan

26+
Years providing cyber risk services

30+
Cyber Intelligence Centres

Strength in numbers
What sets Deloitte Cyber apart from the competition is the know-how. Deloitte has the experience in dealing with many of the world's toughest cyber issues, helping clients solve the most complex business challenges. We have a team that doesn't quit; we have the experience you can depend on; and we have a commitment that we stand behind. Why trust anyone else?

Managed security services - a global partner with a local approach
Cyber Intelligence Centres (CICs) provide a high added value to our managed security services and act as front offices and last mile of delivery for clients. We tailor our offering to the needs of the client in each location.

NavarroAmper&Co.

Deloitte.