

SWIFT Customer Security Programme — Preparing for Cyberattacks

In response to fraud and cybersecurity threats that have grown more sophisticated and global, SWIFT introduced a new Customer Security Programme (CSP) in late 2016 that includes the SWIFT Customer Security Controls Framework (CSCF). The SWIFT CSCF is aimed at enhancing local user controls around the SWIFT environment to avoid potential exploitation by hackers.

The CSCF is based on three overarching objectives and is supported by eight principles, from which emanate 16 mandatory and 11 advisory controls. The SWIFT CSP requires all users to implement the 16 mandatory controls on their local SWIFT infrastructure and perform a self-assessment against the requirements on an annual basis. Institutions are required to submit a self-attestation on their compliance with the 16 mandatory controls based on the results of the self-assessment — with the first self-attestation due by December 31, 2017.

SWIFT Cyberattacks

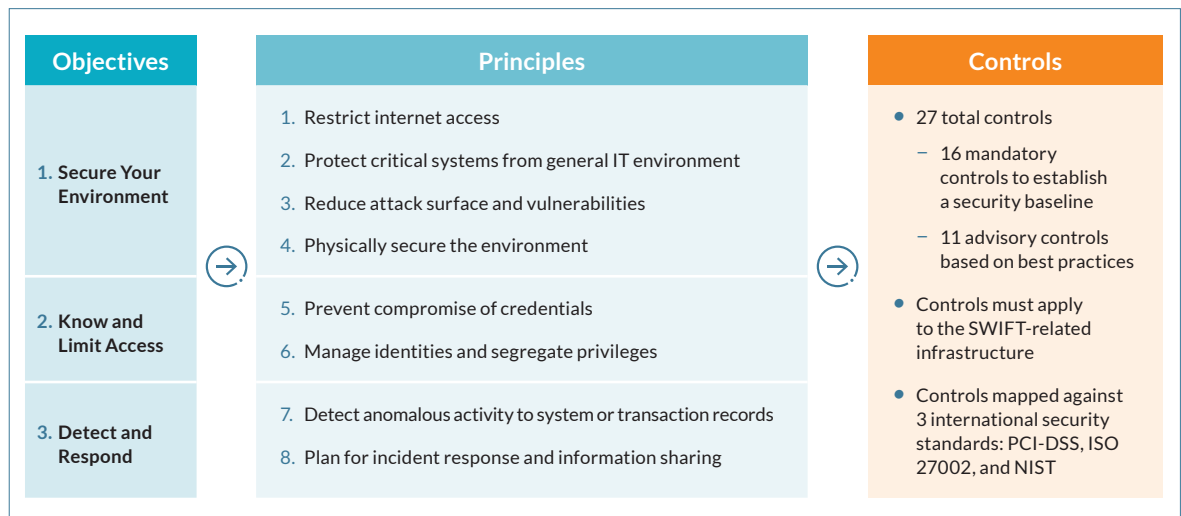
Bangladesh Central Bank

In 2016, hackers obtained Bangladesh Central Bank employees' SWIFT credentials and attempted to transfer \$1 billion to outside bank accounts. Lax cybersecurity practices were likely to blame for the bank's vulnerability to attack.

Vietnam Tien Phong Bank

Using fraudulent SWIFT messages, hackers attempted to transfer \$1.1 million from Vietnam's Tien Phong Bank. The hackers used malware to access the SWIFT network, which could have been prevented through stricter cybersecurity controls at the bank.

• • • SWIFT Customer Security Controls Framework (CSCF)

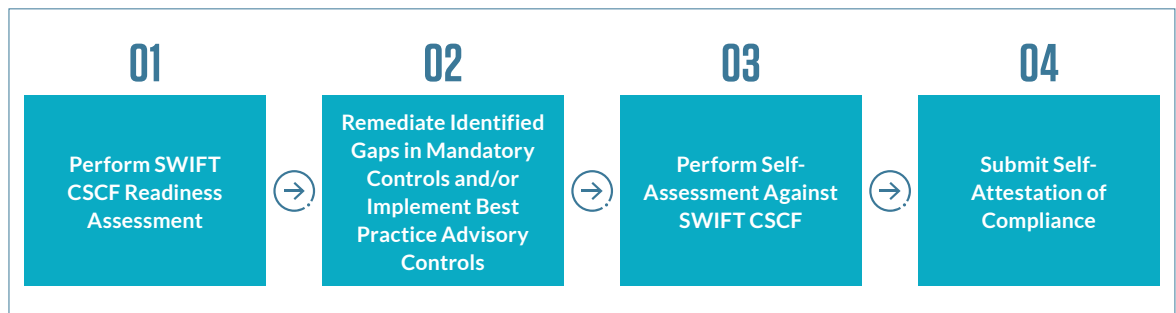


What's Next?

To meet the December 31, 2017 deadline for submitting the self-attestation and avoid counterparty restriction and reports to local regulators on noncompliance, institutions must first understand how their control environment measures up against the SWIFT CSCF mandatory controls. Protiviti's Security & Privacy practice professionals can perform a readiness assessment of your institution's SWIFT control environment against the CSCF requirements to help you understand the effort needed to reach compliance. From our

extensive experience working with CISOs, CIOs, and other senior leaders, Protiviti can recommend the improvements needed for organisations to comply with the SWIFT CSCF mandatory controls, as well as consult on the 11 optional advisory controls. Protiviti can design a customised, actionable, and realistic remediation plan to be executed by either your team or with Protiviti's assistance. Finally, Protiviti can serve as an external service provider to perform the required annual self-assessments that will inform your institution's self-attestation process.

• • • Steps to Compliance



What's the Impact?

Larger financial institutions will likely see similarities and overlap with existing security control assessments, although consideration should be given to control differences across geographies (the assessment/attestation is Bank Identifier Code (BIC) specific). While some control enhancements may be identified, particularly with regard to the CSCF advisory controls, the majority of the assessment effort should leverage existing compliance activities, e.g., Gramm-Leach-Bliley (GLBA) and the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT).

For smaller institutions, the SWIFT CSCF readiness assessment will be key to understanding the existing gaps in compliance with the CSP. These banks should consider whether the manual processes surrounding SWIFT transactions create control gaps that require remediation prior to the Q4 2017 self-attestation.

Why Protiviti?

As a firm, Protiviti has performed hundreds of cybersecurity framework and assessment engagements in recent years. Protiviti's Security

& Privacy professionals have deep experience in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Payment Card Industry Data Security Standard (PCI-DSS) assessments and remediation activities. Given the importance of those frameworks and their direct association within the CSCF, Protiviti understands how the controls can be designed for long-term sustainability and integration into the broader cybersecurity programme. Our recommendations are strategic in nature, with an eye toward tactical implementation rather than a list of one-off projects that simply delay regulatory issues to a later date.

Protiviti focuses on bringing together a knowledgeable team, with members ranging from the youngest consultant to our seasoned leadership, that can work closely with you to develop a custom solution to fit your culture, technology stack, and budget. We pride ourselves on solving the real problem without being constrained by regimented work programmes that don't adapt to your specific control implementations and supporting processes.

GLOBAL CONTACTS

ARGENTINA

Yves Davila
+5411.4001.3124
yves.davila@protivitiglobal.com.pe

GERMANY

Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

PERU

Marco Loayza
+51 1 208 1070
marco.loayza@protivitiglobal.com.pe

AUSTRALIA

Gary Anderson
+61.3.9948.1200
gary.anderson@protiviti.com.au

INDIA

Sanjeev Agarwal
+91.124.661.8600
sanjeev.agarwal1@protivitiglobal.in

QATAR

Andrew North
+974.4421.5300
andrew.north@protivitiglobal.me

BAHRAIN

Arvind Benani
+973.1.710.0050
arvind.benani@protivitiglobal.me

ITALY

Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

SAUDI ARABIA

Saad Al Sabti
+966.11.2930021
saad.alsabti@protivitiglobal.me

BRAZIL

Raul Silva
+55.11.2198.4200
raul.silva@protivitiglobal.com.br

JAPAN

Hyo Kambayashi
+81.3.5219.6600
hyo.kambayashi@protiviti.jp

SINGAPORE

Sidney Lim
+65.6220.6066
sidney.lim@protiviti.com

CANADA

David Dawson
+1.647.288.4886
david.dawson@protiviti.com

KUWAIT

Sanjeev Agarwal
+965.2242.6444
kuwait@protivitiglobal.me

SOUTH AFRICA

Fana Manana
+27.11.231.0600
fanam@sng.za.com

CHILE

Soraya Boada
+56.22.573.8580
soraya.boada@protivitiglobal.cl

or

Rakesh Kabra
+965.2242.6444
kuwait@protivitiglobal.me

UNITED ARAB EMIRATES

Arindam De
+9714.438.0660
arindam.de@protivitiglobal.me

CHINA (HONG KONG)

Albert Lee
+852.2238.0499
albert.lee@protiviti.com

MEXICO

Roberto Abad
+52.55.5342.9100
roberto.abad@protivitiglobal.com.mx

UNITED KINGDOM

Peter Richardson
+44.20.7930.8808
peter.richardson@protiviti.co.uk

CHINA (MAINLAND)

David Cheung
+86.21.5153.6900
david.cheung@protiviti.com

NETHERLANDS

Anneke Wieling
+31.20.346.0400
anneke.wieling@protiviti.nl

UNITED STATES

Matthew Moore
Managing Director
+1.704.972.9615
matthew.moore@protiviti.com

FRANCE

Bernard Drui
+33.1.42.96.22.77
drui@protiviti.fr

OMAN

Shatha Al Maskiry
+968 24699402
shatha.maskiry@protivitiglobal.me

VENEZUELA

Gamal Perez
+58.212.418.46.46
gamal.perez@protivitiglobal.com.ve

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.