protiviti®
Face the Future with Confidence

SWIFT Customer Security Program — Preparing for Cyberattacks

In response to fraud and cybersecurity threats that have grown more sophisticated and global, SWIFT introduced a new Customer Security Program (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

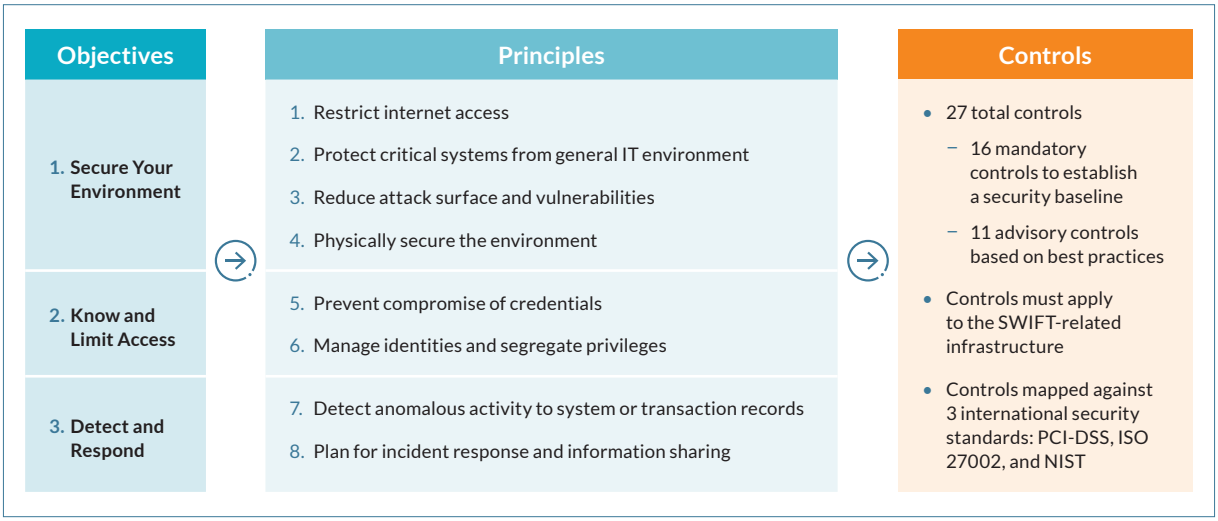
Bangladesh Central Bank

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.

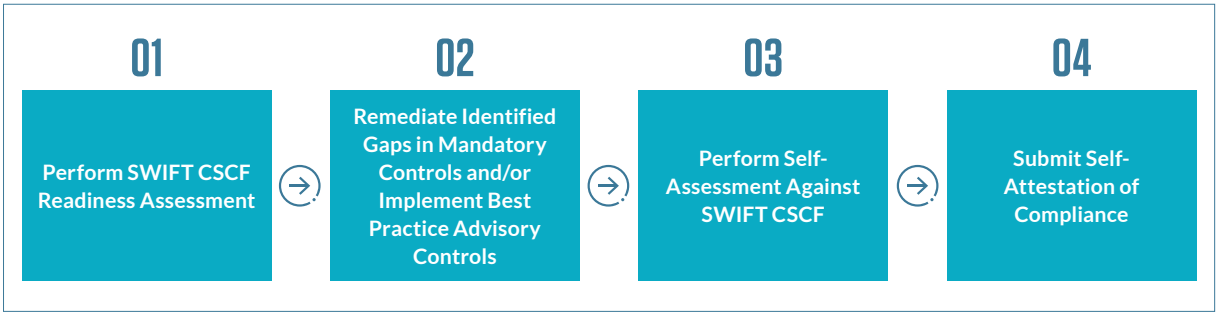
SWIFT Customer Security Controls Framework (CSCF)



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 organizations to comply with the SWIFT CSCF mandatory controls, as well as consult on the 11 optional advisory controls. Protiviti can design a customized, 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 program. 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 programs that don't adapt to your specific control implementations and supporting processes.

Contacts

Cory Gunderson
Managing Director
+1.212.708.6313
cory.gunderson@protiviti.com

Daniel Hansen
Managing Director
+1.415.402.3697
daniel.hansen@protiviti.com

Ed Page
Managing Director
+1.312.476.6093
ed.page@protiviti.com

Jeffrey Sanchez
Managing Director
+1.213.327.1433
jeffrey.sanchez@protiviti.com

David Taylor
Managing Director
+1.407.849.3916
david.j.taylor@protiviti.com

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

Mark Lippman
Managing Director
+1.571.382.7807
mark.lippman@protiviti.com

Michael Porier
Managing Director
+1.713.314.5030
michael.porier@protiviti.com

Cal Slemp
Managing Director
+1.203.905.2926
cal.slemp@protiviti.com

Michael Walter
Managing Director
+1.404.926.4301
michael.walter@protiviti.com

Scott Laliberte
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

Todd Musselman
Managing Director
+1.469.374.2454
todd.musselman@protiviti.com

Andrew Retrum
Managing Director
+1.312.476.6353
andrew.retrum@protiviti.com

David Stanton
Managing Director
+1.469.374.2488
david.stanton@protiviti.com