GET FIT FOR SWIFT CSP

accenture

ACCENTURE CYBER COMPLIANCE FOR SWIFT CSP

GETTING READY FOR THE SWIFT CUSTOMER SECURITY PROGRAM (CSP)

Recent Accenture research has just found that—on average—a financial services firm will face 85 targeted cyber-attacks each year. 1 out of 3 of those results in a security breach which means 2 to 3 effective attacks per month in principle.

If you think about this, it is no surprise that cyber-attacks could be a huge threat to the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system with its today 11.000 users and processing up to 30 million financial messages per day.

INTRODUCING THE SWIFT CUSTOMER SECURITY PROGRAM

SWIFT is now launching an initiative to support its customers. As the security is as weak as its weakest link, the responsibility for higher security involves each customer, their counterparts, and the entire community. Hence, SWIFT has now introduced the Customer Security Program (CSP) to support its customers in reinforcing the security of their SWIFT-related infrastructure. SWIFT has developed and published a specific list of requirements for banks to fulfill on an ongoing basis—and banks must document and self-attest their compliance with these requirements. Participants failing to reach compliance with CSP may be subject to specific actions taken by SWIFT and the local regulator.

FIRST DEADLINE, DECEMBER 2017

To help financial institutes meeting CSP controls and assessment as well as developing an effective response to SWIFT-related cyber threats, Accenture has launched the Accenture Cyber Compliance for SWIFT CSP to help financial services across the globe to work on compliance with SWIFT's CSP.

Accenture is included in SWIFT's official Cyber Security Services Provider Directory. Beyond the Cyber Compliance for SWIFT CSP, Accenture can draw on broad network of highly skilled people with industry (payments), security and technical knowledge to help also with the definition and implementation of any resulting actions after the assessment of the current state.

DETAILS OF THE SWIFT CUSTOMER SECURITY PROGRAM

SWIFT's Customer Security Program asks its participants to undertake three basic initiatives:

1. SECURE YOUR ENVIRONMENT.

SWIFT network participants are asked to restrict access of unauthorized parties to the secure zone hosting the SWIFT components as well as to the internet from this zone. Banks should, in addition, examine vulnerabilities and reduce the overall attack surface while stepping up measures to secure their own physical environments.

2. KNOW AND LIMIT ACCESS.

SWIFT asks its users to implement controls to detect activity that is unusual or anomalous, whether it appears within systems or in transaction records. If and when anomalies are spotted, financial institutes should have detailed plans for responding to the incident.

3. DETECT AND RESPOND.

Under CSP, financial institutes will take new measures to prevent the compromise of credentials, to manage identity recognition of authorized individuals, and to make sure that SWIFT privileges are carefully reserved for those needing access.

DETAILS OF THE ACCENTURE CYBER COMPLIANCE FOR SWIFT CSP

A disciplined, systematic response to CSP can keep financial institutes compliant with SWIFT requirements. The Accenture Cyber Compliance for SWIFT CSP is a comprehensive approach to identifying vulnerabilities and to implementing an effective response.

Through this offering, Accenture will:

- Assess all prerequisites of the original SWIFT catalogue, divided by chapter and subchapter
- Question and evaluate each item transparently against the bank's implementation
- Provide a clear picture of the bank's compliance grade for each component of the CSP catalogue
- Recommend implementation measures and guidelines to close possible gaps
- Indicate a typical cost range for these implementation measures

ACCENTURE ACCELERATORS AND TOOLS

In the **Cyber Compliance for SWIFT CSP**, Accenture uses custom-designed tools including:

CSP QUESTIONNAIRE

The questionnaire by Accenture includes more than 180 granular questions based on the detailed control descriptions (all 7 chapters) of the SWIFT Customer Security Controls Framework.

CSP MEASUREMENT CATALOGUE

Based on the controls predefined by SWIFT, Accenture has developed a measurement catalogue which covers external standards and clusters all components related to categories, sub-categories and classes.

CSP DASHBOARD

The CSP Dashboard is an overview of all results at both a general and at a cluster level. Results are separated into categories of compliance with all controls and with mandatory controls.

REPORTING TOOLS

These tools cover all clusters and sub-clusters, both mandatory and non-mandatory.

Being listed in **SWIFT's official Cyber Security Services Provider Directory**, Accenture can help financial institutes comply with CSP while leveraging its technological and cybersecurity expertise and solutions to ensure an additional layer of protection for banks' revenues and reputations. Accenture also offers a multi-year security checkup service that helps banks stay compliant even as SWIFT standards continue to change. The SWIFT CSP deadlines are approaching quickly.

To learn more about the Accenture Cyber Compliance for SWIFT CSP, contact any of the individuals listed:

Diane Nolan
Managing Director Financial Services
Brussels
diane.nolan@accenture.com

Thibaut Roisin
Senior Manager Security
Brussels
thibaut.roisin@accenture.com

Björn Zaksek
Manager Payments Services
Vienna
bjoern.zaksek@accenture.com

Martin Metz
Manager Security
Hamburg
martin.metz@accenture.com