BAE SYSTEMS

SWIFT Customer Security Assessment Services

SWIFT have developed a Customer Security Control Framework (CSCF), made up of 21 mandatory and 10 advisory controls, that all companies using SWIFT must attest against publically and annually. V2020 is the most recent version of the CSCF to which companies must self attest by the end of 2020.

From July 2020, all SWIFT members will be obligated to carry out an independent assessment when self-attesting. This is either the Community Standard Assessment or the SWIFT mandated assessment. This can be performed by an independent external organisation with existing cyber security assessment experience.

3 Objectives

8 Principles

31* Controls

*Updates to Controls

- X2 advisory controls promoted to mandatory (to protect and reduce vulnerabilities in critical systems where virtualisation is being used more frequently.
- X2 new advisory controls to provide guidance on a) restricting internet access and b) Relationship Management Application (RMA) business control.
- X1 advisory control expanded to include middleware/MQ servers to help protect the upstream back-office application flows.

SWIFT CSP timeline

2016

BAE Systems were the original researchers to uncover what happened in the Bank of Bangladesh heist

2017

27 Controls

16 Mandatory + 11 Advisory

Self-Attestation by end of 2017

2018

27 Controls

16 Mandatory + 11 Advisory

Mandatory self-attestation by end of 2018

2019

29 Controls

19 Mandatory + 10 Advisory

Mandatory self-attestation by end of 2019

2020

31 Controls

21 Mandatory + 10 Advisory

Independent Assessment by end of 2020

Why BAE Systems?

We have been working with SWIFT since July 2016 to provide rapid insight, advice and solutions to compromised SWIFT members through Incident Response, Threat Intelligence and Security Consulting services. We have also collaborated with SWIFT in publishing thought leadership content including The Evolving Advanced Cyber Threat to Financial Markets.

We are approved on SWIFT's list of cyber security service providers and are independent, qualified and experienced in delivering CSP assessment services. We also bring to bear our unique SWIFT relevant financial sector threat intelligence to ensure we have the most current view of the relevant threats to SWIFT members. Visit https://www.swift.com/myswift/customer-security-programme-csp_/community-engagement/cyber-firms-directory

How we can help

Using our unique intelligence insights on the tactics, techniques and procedures used by threat groups to attack organisations' payment systems, we provide two complimentary services to assess your compliance and the effectiveness of your SWIFT Controls.

Standard Independent Assessment

Community-Standard Assessment or SWIFT Mandated Assessment

Review SWIFT environment configuration in alignment to architecture and security controls, and conduct an in depth evaluation of CSP controls verifying operational effectiveness.

Intelligence-led Testing Services

Simulated attack on your SWIFT environment using realistic attack scenarios based on real-world intelligence to test the effectiveness and resilience of your SWIFT controls.

For more information about contact us at learn@baesystems.com. Or to find out more about BAE Systems go to www.baesystems.com/financialservices

Assured Service Provider

in association with National Cyber Security Centre

Victim of a cyber attack?
Contact our emergency response team on:

UK:	0808 168 6647
US:	1 (800) 417-2155
Australia:	1800 825 411
International:	+44 1483 817491
Email:	cyberresponse@baesystems.com

Contact Details: UK: +44 (0) 1483 816000 | US: +1 (720) 6969 830 | AUS: +61 1300 027 001
BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/financialservices

linkedin.com/company/baesystemsai twitter.com/baesystems_ai