BAE SYSTEMS
INSPIRED WORK

SWIFT Customer Security Programme: Controls Framework

Readiness Assessment

The Challenge

Recent payment fraud in SWIFT customers' local environments demonstrates the necessity for industry-wide collaboration to fight against these threats.

In response SWIFT have launched the Customer Security Programme (CSP), which aims to improve information sharing throughout the community, enhance SWIFT-related tools for customers and provide audit frameworks.

SWIFT Customer Security Programme (CSP)

As part of the CSP SWIFT have introduced the Customer Security Controls Framework. The framework describes a set of 16 mandatory and 11 advisory security controls for SWIFT customers.

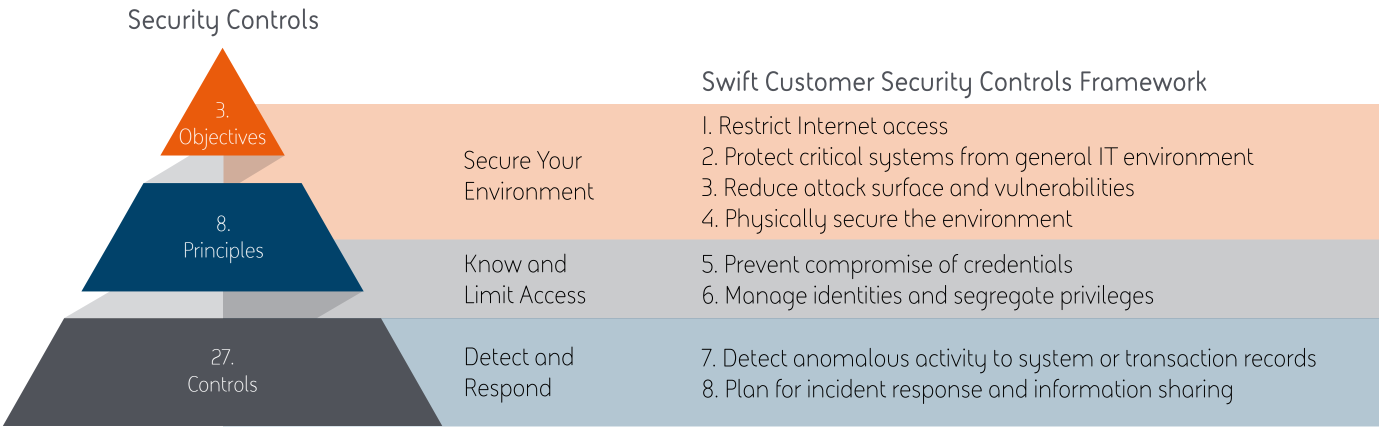
By 1 January 2018, all SWIFT customers will need to provide self-attestation against the mandatory controls and on an annual basis thereafter. The self-attestation may be tested and proof of compliance may be required.

Have you got the processes in place to ensure compliance?

The SWIFT Customer Security Controls are articulated around three overarching objectives:

1. Secure your Environment
2. Know and Limit Access
3. Detect and Respond

These are defined by the 8 principles shown below and detailed in 27 controls.



Swift Customer Security Controls Framework

Secure Your Environment	1. Restrict Internet access 2. Protect critical systems from general IT environment 3. Reduce attack surface and vulnerabilities 4. Physically secure the environment
Know and Limit Access	5. Prevent compromise of credentials 6. Manage identities and segregate privileges
Detect and Respond	7. Detect anomalous activity to system or transaction records 8. Plan for incident response and information sharing

How we can Help

Readiness Assessment

BAE Systems' cyber security experts will work collaboratively with you to understand your current security posture against the SWIFT Security Controls Framework. We will:

- Educate you on the controls programme and how you will need to demonstrate compliance. We will also brief senior management on the risks faced to ensure you have the right levels of support for your improvement programme
- Achieve an overview of your existing security controls associated with the in-scope payment services/platforms
- Understand planned technology enhancements which may impact remediation and recommendations
- Review existing practices and controls in place for each of the applicable 27 controls and measure your maturity
- Conduct a gap analysis against the mandatory level expected by SWIFT

Based on our review, we will produce a remediation report with a set of actionable recommendations targeted at addressing specific areas of focus and a prioritised high level roadmap to implement the recommendations outlined.

Readiness Assessment Benefits

- Understand how your organisation stands in relation to compliance with SWIFT's Security Controls Framework
- Develop your existing security controls with a tailored set of recommendations for your organisation, based on a set of domain-level standards
- Identify potential opportunities to enhance security across your payments services, providing targeted recommendations to achieve compliance with SWIFT's Controls Framework
- Provide you with independent assurance that you are pro-actively managing the increasingly sophisticated threat of cyber-criminal activity

Why BAE Systems?

- BAE Systems has been appointed by SWIFT as their Cyber Security Partner. We support the Customer Security Intelligence (CSI) team to investigate cyber incidents within SWIFT customer environments
- This engagement and partnership gives us direct first-hand experience combatting and developing remediation and preventative measures for SWIFT-related incidents
- Our Security Consulting Practice – including our Incident Response, Threat Intelligence, and Enterprise Security Consulting teams – have extensive experience in SWIFT customer environments through the partnership
- We support SWIFT customers in assessing their environments and helping them remediate deficiencies in order to comply with the Customer Security Controls Framework

About BAE Systems

We help nations, governments and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulation and transform their operations.

Stay compliant in the fight against fraud with BAE Systems and SWIFT

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
UK: +44 (0) 1483 816000
E: learn@baesystems.com | W: baesystems.com/businessdefence

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

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

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

CREST
CESG Certified Service
Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure