Approach to SWIFT security assessment

1. Setting the context

SWIFT (Society for Worldwide Interbank Financial Telecommunications) is a vast messaging network used by banks and other financial institutions to quickly, accurately, and securely send and receive information, such as money transfer instructions.

In Vietnam, we have had a vast amount of opportunity in conducting SWIFT system security gap assessment projects for Vietnamese banks. Through this article, we would like to provide you a short introduction about the Customer Security Controls Framework for the SWIFT system, as well as sharing best practices that the client should consider while implementing and securing the SWIFT system according to SWIFT requirements.

2. Introduction to SWIFT's Information Security Risk and Controls

The SWIFT Customer Security Controls Framework describes a set of mandatory and advisory security controls for SWIFT users. Mandatory security controls establish a security baseline for the entire community and must be implemented by all users on their local SWIFT infrastructure. SWIFT has chosen to prioritise these mandatory controls to set a realistic goal for near-term, tangible security gain and risk reduction.

Advisory controls are based on good practice that SWIFT recommends users to implement. Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

All controls are articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. The controls have been developed based on SWIFT's analysis of cyber threat intelligence and in conjunction with industry experts and user feedback. The control definitions are also intended to be in line with existing information security industry standards.

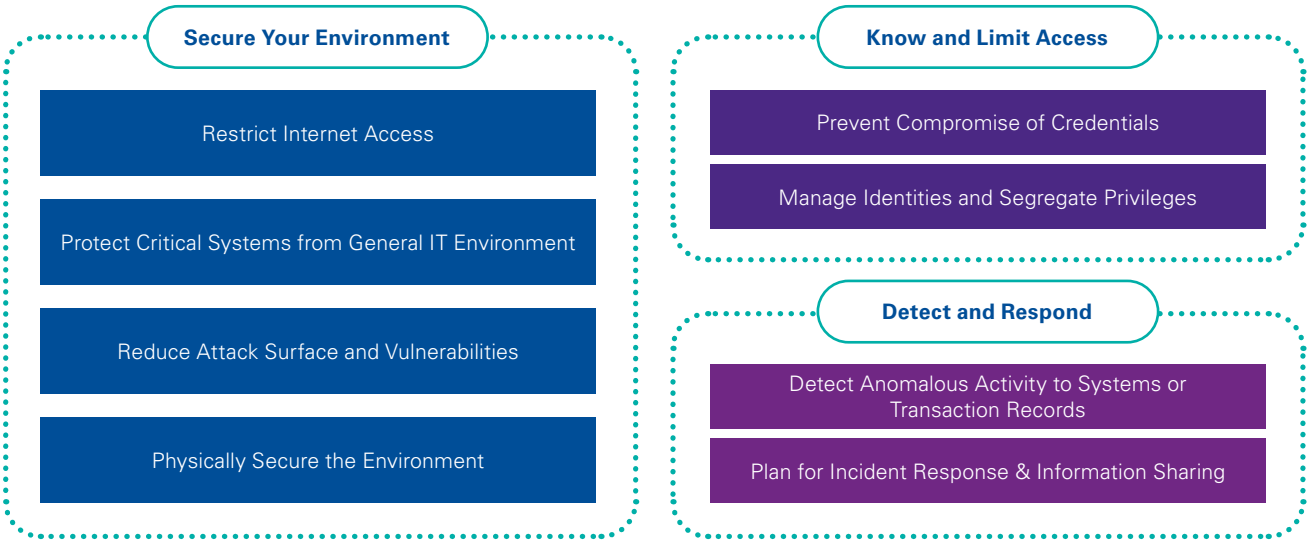

Figure 1: SWIFT security objectives and principles

SWIFT CSP 2021 has defined the 31 security controls (22 mandatory and 9 advisory controls) that underpin these objectives and principles. The controls are intended to help mitigate specific cybersecurity risks that SWIFT users face due to the cyber threat landscape. Within each security control, SWIFT has documented the most common risk drivers that the control is designed to help mitigate. Addressing these risks aims to prevent or minimise undesirable and potentially fraudulent business consequences, such as:

- Unauthorised sending or modification of financial transactions;
- Processing of altered or unauthorised SWIFT inbound (i.e. received) transactions;
- Business conducted with an unauthorised counterparty;
- Confidentiality breach (of business data, computer systems, or operator details);
- Integrity breach (of business data, computer systems, or operator details).

Ultimately, these consequences represent enterprise level risks, including:

- Financial Risk
- Legal Risk
- Regulatory Risk
- Reputational Risk

3. Common Violations with SWIFT Security Controls

During the gap assessment for the SWIFT system, we have noticed a number of common issues that financial institutions often violate compared to SWIFT's security requirements:

- The network separation for applications and SWIFT systems is not done clearly and completely. For example, email or AD applications still have common connections to the SWIFT system.
- Security policies and procedures (for example: Security vulnerability management procedure, malware prevention procedure, etc) are not detailed, correct and aligned to the current situation of the system.
- System hardening guidelines/standards are not fully and completely developed, and they are not periodically reviewed and updated.
- The security vulnerability scanning is only conducted on important applications and servers. For network devices or databases, the scanning is almost ignored.
- The password policy (password length, complexity, lockout, change, etc) is only applied to Windows servers and not on network devices, security devices or Unix/Linux platforms.

4. Key notes to assessment exercise

In order to fully assess the security controls of the SWIFT system, the following important points should be noted:

- **Understanding of client's SWIFT architecture:** The current architecture of SWIFT is divided into 4 types - A1, A2, A3 and B. Each architecture has a difference in components and the connection from the client to SWIFT. So, understanding each type of architecture will help you identify the scope and assess the systems involved that may affect the security of the SWIFT system.
- **Understanding of the scope of security controls to be assessed:** SWIFT's security controls are only applied to a certain scope - SWIFT systems and indirect infrastructure related to SWIFT. You need to be aware of connections and

determine which scope would apply SWIFT security controls to avoid assessing unnecessary components that are outside the scope.

- **Understanding of "Mandatory" and "Advisory" Controls:** SWIFT's security controls are divided into two categories: (1) Mandatory controls, and (2) Advisory controls. Depending on the requirements of the customer and the scope of the assessment, you should decide which controls should be reviewed and evaluated in the most appropriate way.
- **Understanding of the ultimate objective of each control:** SWIFT CSP 2021 includes a total of 31 security controls (22 mandatory controls and 9 advisory controls) divided into 8 groups. Understanding the objective of each control makes it easier to identify alternative controls if they exist and avoids misjudging the customer's current security level, because during the assessment, it is realised that customers could use different security controls than required by SWIFT and still meet the final objective and ensure the safety of the SWIFT system.
- **Understanding of the purpose and role of components in the SWIFT system:** SWIFT includes many components with different roles such as Messaging interface, Communication interface, GUI, SWIFTNet Link, HSM, Connector, v.v. These components connect, interact, and have mutual security relationships. Therefore, understanding the roles and functions of each component helps you determine which security controls are appropriate for which component, thereby assessing most accurately and effectively for potential risks.

5. Conclusion

Nowadays, as international transactions and commerce become more popular, SWIFT obviously becomes one of the important components of financial institutions, especially banks. Therefore, SWIFT security needs to be paid close attention to properly minimise fraud in international transactions, protect user data and safeguard the reputation of the organisation.

If you need any assistance with regard to SWIFT security consulting and assessment, please do not hesitate to drop your request here with your contact information. Our professionals will get in contact with you within 24 hours at the earliest convenience.

Contact us

Tran Phuong Hong

Director, IT Advisory

T: +84 90 9988 753
E: hptran@kpmg.com.vn

Do Kim Hien

Senior Solution Consultant,
IT Advisory

T: +84 94 5417 791
E: hiendo@kpmg.com.vn

Hanoi

46th Floor, Keangnam Hanoi Landmark Tower, 72 Building,
Plot E6, Pham Hung Street, Cau Giay New Urban Area,
Me Tri Ward, South Tu Liem District, Hanoi, Vietnam

T: +84 (24) 3946 1600
F: +84 (24) 3946 1601
E: kpmghanoi@kpmg.com.vn

Ho Chi Minh City

10th Floor, Sunwah Tower,
No. 115, Nguyen Hue Street, Ben Nghe Ward,
District 1, Ho Chi Minh City, Vietnam

T: +84 (28) 3821 9266
F: +84 (28) 3821 9267
E: kpmghcmc@kpmg.com.vn

Danang

Unit D3, 5th Floor, Indochina Riverside Tower,
No. 74, Bach Dang Street, Hai Chau 1 Ward,
Hai Chau District, Danang, Vietnam

T: +84 (236) 351 9051
F: +84 (28) 3821 9267
E: kpmgdanang@kpmg.com.vn

Follow us on:

kpmg.com.vn