WHITE PAPER

Addressing the Challenges of the SWIFT Directive

Table of Contents

WHITE PAPER

Addressing the Challenges of the SWIFT Directive

Executive Summary

The Society of Worldwide Interbank Financial Telecommunication (SWIFT) is a global member-owned co-operative and the world's leading provider of secure financial messaging services. SWIFT's messaging services are used and trusted by more than 11,000 financial institutions in more than 200 countries and territories around the world.[1] Naturally this network is a high-value target for attackers, as it provides a community of financial institutions worldwide the ability to exchange sensitive information relating to international financial transactions.

Recent history has revealed some of the largest ever cyberheists involving fraudulent payment instructions being sent directly over the SWIFT network.

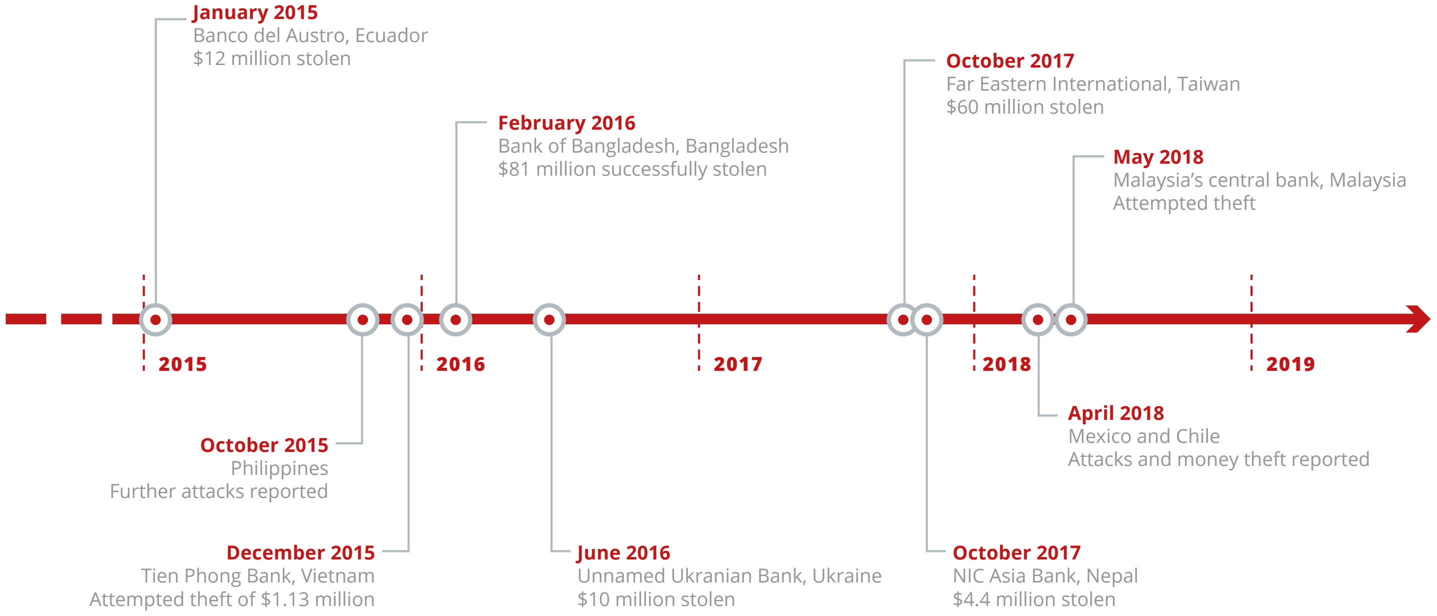

Figure 1. History of targeted attacks against SWIFT.

Connect With Us

In an effort to respond to such attacks and establish a consistent secure framework and baseline, SWIFT has introduced the SWIFT Customer Security Controls Framework (CSCF).

What Is the SWIFT Customer Security Controls Framework?

The SWIFT CSCF 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 practises that SWIFT recommends users implement. Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

In March 2017, SWIFT published the first version of CSCF. Initially, this was a set of security controls—16 mandatory and 11 advisory—that set a security baseline for all SWIFT users. Now SWIFT has published the new CSCF v2019, which sets out a number of changes to the existing controls and provides some additional guidance and clarification on the implementation guidelines. As a result, the CSCF v2019 is now composed of 19 mandatory and 10 advisory controls. All controls are articulated around three overarching objectives: “Secure your Environment,” “”Know and Limit Access,” and “Detect and Respond.”

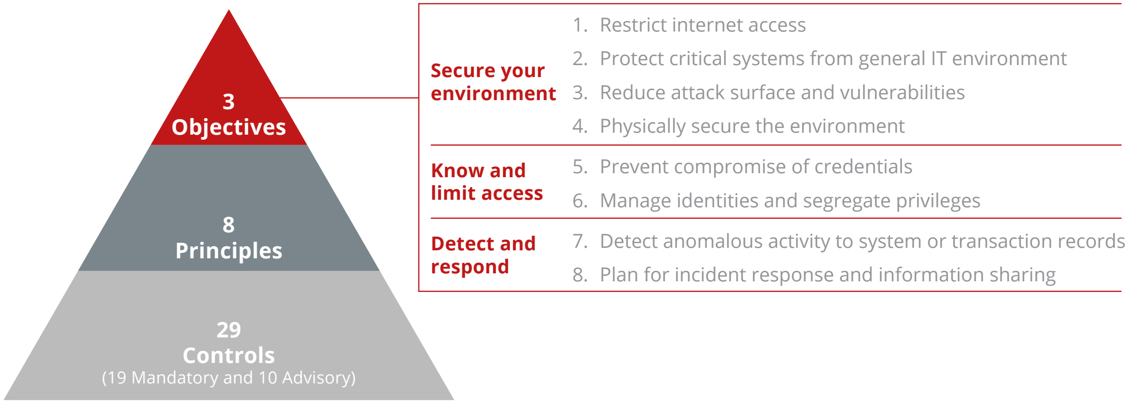
3
Objectives
8
Principles
29
Controls
(19 Mandatory and 10 Advisory)
Secure your environment
1. Restrict internet access
2. Protect critical systems from general IT environment
3. Reduce attack surface and vulnerabilities
4. Physically secure the environment
Know and limit access
5. Prevent compromise 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

Figure 2. The three primary objectives of CSCF v2019.

To ensure adoption of the controls, SWIFT has developed an attestation and compliance process that will require users to self-attest compliance against the mandatory and, optionally, the advisory security controls. All users must self-attest compliance against the mandatory security controls outlined in a specific release at first by the end of the version year (as an example, by the end of 2019 at the latest for v2019). Users will be required to resubmit their attestation on an annual basis thereafter.

How McAfee Helps Support SWIFT Compliance Role[2]

The Customer Security Programme (CSP), launched by SWIFT in 2016, is designed to help customers implement the practises that are critical to help defend against, detect, and recover from cybercrime.

Customers will first need to protect and secure their local environment and then turn to preventing and detecting fraud, continuously sharing information, and preparing to defend against future cyberthreats.

Our analysis finds that CSP is articulated around three mutually reinforcing areas:

- **Secure and protect:** Securing local SWIFT-related infrastructure and putting in place the right people, policies, and practises are critical to avoiding cyber-related fraud.
- **Detect and respond:** Even with strong security measures in place, attackers are very sophisticated and you need to assume that you may be the target of cyberattacks. That's why it is also vital to put in place strong detection measures to increase the chances of stopping or mitigating fraud in case your environment is breached.
- **Share and prepare:** The financial industry is truly global, and so are the cyber challenges it faces. What happens to one company in one location can easily be replicated elsewhere in the world. That is why it is really important to consume, operationalise, and share threat intelligence information. This allows the whole community to protect itself, take mitigating actions, and defend against further attacks.

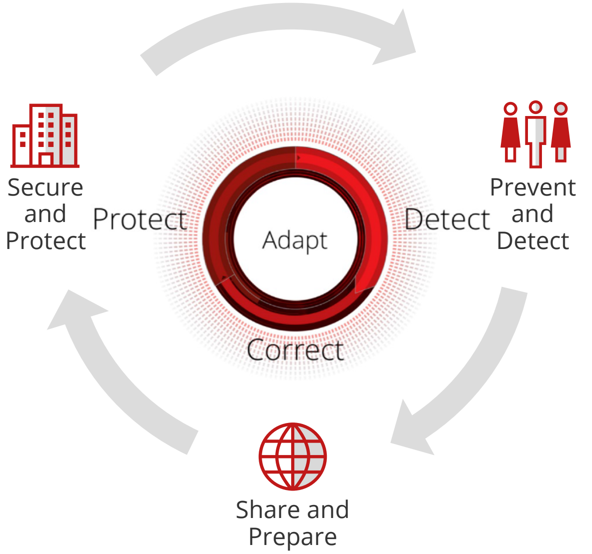

Figure 3. The integrated McAfee Threat Defense Lifecycle.

The integrated McAfee® Threat Defense Lifecycle based on the Protect, Detect, and Correct paradigm is aligned to the SWIFT strategy.

McAfee products are designed to enable customers to **protect** their environment by putting controls on devices, over the networks, and in the cloud.

Moreover, acting like sensors, every single protection product is able to collect and bring information to different layers of inspection, intelligence, and analytics for deeper **detection** of malicious activity or abnormal behaviour.

Then, once a new threat is uncovered and detected, the information about the threat is immediately shared across the whole environment in order to empower every other protection technology with such information and proceed to **correct** the incident.

The Importance of Collaboration and Information Sharing

Since the first publication of the Customer Security Programme[3] in 2016, the SWIFT consortium has placed an emphasis on topics that are currently widely considered central for prevention and detection: collaboration and intelligence sharing.

Initially, the approach was to share information inside the community, mainly tactical and strategic intelligence, such as high-level information about changes in risk status for the whole community or protection and configuration best practises.

Continuing and expanding this way, the SWIFT Information Sharing and Analysis Centre (SWIFT ISAC) service was activated in June 2017 to allow SWIFT members to quickly receive more technical and operational threat intelligence. The information shared by SWIFT ISAC includes malware details, such as file hashes and YARA rules, indicators of compromise (IoCs), and details on the modus operandi used by the cybercriminals and formats that can be consumed by security tools.

It is, therefore, essential that the protection and detection tools in use can interact quickly and natively with these sources of threat intelligence. McAfee solutions are designed to be integrated with external threat intelligence sources in order to consume this information and increase protection and detection.

Embedded in most McAfee products is Data Exchange Layer (DXL), which enables secure and fast messaging communication and information sharing across different products. The DXL communication fabric connects and optimises security actions across multiple vendor products, as well as internally developed and open source solutions. In this way, enterprises gain secure real-time access to new data and take advantage of lightweight, instant interactions with other products. Moreover, the DXL communication fabric can be virtually connected and extended to any other technology thanks to OpenDXL, an open standard and ecosystem developed by McAfee and released for free as an open source project with the aim of helping developers and enterprises to freely leverage DXL.

The OpenDXL community and resources at OpenDXL.com empower DXL integrations, provide a catalogue for available applications, support implementations, and nurture new ideas.

Control Mappings

The table below highlights some of the mandatory and advisory controls where the McAfee security architecture and solutions can help with meeting the requirements and describes the key capabilities provided for implementing those controls.[4]

SWIFT Control	McAfee Solution
1.1 SWIFT Environment Protection **Control Type:** Mandatory **Control Objective:** Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	McAfee® Network Security products such as McAfee® Network Security Platform and McAfee® Web Gateway provide network-level separation, access restrictions, and connectivity restrictions. McAfee Network Security Platform is the next-generation intrusion prevention system (IPS) for physical and virtual environments, empowering boundaries segmentation between the local SWIFT infrastructure and the larger enterprise network. It reduces the attack surface and defends against cyberattacks that commonly involve compromise of the general enterprise IT environment. Moreover, McAfee® Virtual Network Security Platform, the dedicated virtual IPS solution certified to work with VMware NSX, enables micro-segmentation of VMs and deep inspection of east-west traffic in order to restrict the communication between components in the secure zone. McAfee Web Gateway restricts and controls outbound internet access from the SWIFT Secure Zone, enabling web filtering functionality with content inspection and protection through both reputation and category-based filtering. **McAfee Products: McAfee Network Security Platform, McAfee Virtual Network Security Platform, McAfee Web Gateway**
1.3A. Virtualisation Platform Protection **Control Type:** Advisory **Control Objective:** Secure virtualisation platform and virtual machines (VM) as physical servers.	McAfee® Cloud Workload Security enables customer to discover, assess and automate virtual workload and container defence. McAfee Cloud Workload Security integrates comprehensive host and network countermeasures, including machine learning, application containment, virtual machine-optimised anti-malware, whitelisting, file integrity monitoring, and micro-segmentation that protect virtual workloads from targeted attacks. McAfee® Virtual Network Security Platform, the dedicated virtual IPS solution certified to work with VMware NSX, enables micro-segmentation of virtual machines (VMs) and deep inspection of east-west traffic in order to restrict the communication between components in the secure zone. **McAfee Products: McAfee Cloud Workload Security, McAfee Virtual Network Security Platform**
2.1 Internal Data Flow Security **Control Type:** Mandatory **Control Objective:** Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.	McAfee Network Security Platform, working at network level as the next-generation IPS for both physical and virtual environments, provides detection for policy violations and applications usage. McAfee Network Security Platform enables customers to detect, alert, or block usage of unencrypted network protocols, weak cipher protocols, or untrusted applications in order to assure protection of internal data flows and safeguard against unintended disclosure, modification, and access of the data while in transit. **McAfee Products: McAfee Network Security Platform**

SWIFT Control	McAfee Solution
2.2 Security Updates **Control Type:** Mandatory **Control Objective:** Minimise the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.	McAfee® Policy Auditor provides automatic patch assessment coverage for a wide range of platforms, operating systems, and applications commonly found in enterprise environments. Comprehensive patch benchmarks cover Windows, Linux, and Unix operating systems. Application patch assessment spans a wide spectrum of enterprise applications. In order to accelerate patch, security configuration, and compliance validation, automatic reports with up-to-date data can be scheduled and alerts delivered to management for review and resolution. McAfee Policy Auditor automates security audit processes and helps set up a security update process that is comprehensive, repeatable, and implemented in a timely manner. McAfee Products: McAfee Policy Auditor
2.3 System Hardening **Control Type:** Mandatory **Control Objective:** Reduce the cyberattack surface of SWIFT-related components by performing system hardening.	McAfee provides many security solutions aimed at protecting systems and reducing the attack surface. Among these, McAfee® Host Intrusion Prevention System and McAfee® Database Activity Monitoring have an important role. McAfee Host Intrusion Prevention hardens systems and defends against zero-day exploits and unpatched vulnerabilities, with coverage across all levels: network, application, and system execution. Vulnerability shielding automatically updates signatures to protect systems against attacks resulting from exploited vulnerabilities. McAfee Database Activity Monitoring hardens databases by detecting attacks that attempt to exploit known vulnerabilities, as well as common threat vectors. It can be configured to either issue an alert or terminate the session in real time. Virtual patching updates are provided on a regular basis for newly discovered vulnerabilities and can be implemented without database downtime, protecting sensitive data until a patch is released by the database vendor and can be applied. Furthermore, as keeping the configurations and compliance to industry-standard security configuration guidance under constant control is a central part of a hardening process, using McAfee Policy Auditor allows customer to regularly check the systems against the secure settings identified as per the preceding guidance to take any relevant corrective action. McAfee Policy Auditor software ships with templates that perform configuration assessment against the latest compliance standards, including CIS, CJIS, PCI DSS 3.2, SOX, GLBA, HIPAA, FISMA, EU GDPR, ISO 27001, NIST 800-171, and COBiT frameworks.[5] McAfee Products: McAfee Host Intrusion Prevention, McAfee Database Activity Monitoring, McAfee Policy Auditor
2.4A. Back Office Data Flow Security **Control Type:** Advisory **Control Objective:** Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.	McAfee Network Security Platform, working at network level as next-generation intrusion prevention system (IPS) for both physical and virtual environments, provides detection for policy violations and applications usage. McAfee Network Security Platform enables customers to detect, alert, or block usage of unencrypted network protocols, weak cipher protocols, or untrusted applications. It assures protection of internal data flows, safeguarding against unintended disclosure, modification, and access of the data while in transit. McAfee Products: McAfee Network Security Platform

SWIFT Control	McAfee Solution
2.5A. External Transmission Data Protection **Control Type:** Advisory **Control Objective:** Protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone.	McAfee Network Security Platform, working at the network level as the next-generation IPS for both physical and virtual environments, provides detection for policy violations and applications usage. McAfee Network Security Platform enables customers to detect, alert, or block usage of unencrypted network protocols, weak cipher protocols, or untrusted applications. It assures protection of internal data flows, safeguarding against unintended disclosure, modification, and access of the data while in transit. As part of this control requires encryption of sensitive data leaving the secure zone when it is extracted from its normal operating environment, McAfee® File and Removable Media Protection helps provide policy-enforced organisation-wide encryption to prevent unauthorised access to sensitive information. McAfee Products: McAfee Network Security Platform, McAfee File and Removable Media Protection
2.6. Operator Session Confidentiality and Integrity **Control Type:** Mandatory **Control Objective:** Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.	McAfee Network Security Platform, working at network level as next-generation IPS for both physical and virtual environments, provides detection for policy violations and applications usage. McAfee Network Security Platform enables customers to detect, alert, or block usage of unencrypted network protocols, weak cipher protocols, or untrusted applications in order to assure protection of internal data flows, safeguarding against unintended disclosure, modification, and access of the data while in transit. McAfee Products: McAfee Network Security Platform
3.1. Physical Security **Control Type:** Mandatory **Control Objective:** Prevent unauthorised physical access to sensitive equipment, hosting sites, and storage.	Because part of this control requires USB and other external ports and access points on both operator PCs and server environments to be disabled to the maximum extent possible, McAfee® Device Control can be used to specify and categorise which devices may or may not be used and enforce what data can and cannot be transferred to devices. Moreover, when remote working on SWIFT infrastructure is allowed, McAfee® Drive Encryption delivers centrally managed and enforced full disk encryption to devices used for "teleworking." McAfee Products: McAfee Device Control, McAfee Drive Encryption
6.1. Malware Protection **Control Type:** Mandatory **Control Objective:** Ensure that local SWIFT infrastructure is protected against malware.	McAfee® Endpoint Security delivers industry-leading protection using state-of-the-art techniques to identify malicious code based on appearance and behaviour. McAfee Endpoint Security ensures anti-malware protection on each system in the SWIFT infrastructure: operator PCs or server infrastructures on both Microsoft Windows and non-Windows systems. Additionally, McAfee Endpoint Security protection can be enhanced by integrating with McAfee® Advanced Threat Defense, which improves endpoint detection and enables investigation capabilities. McAfee Advanced Threat Defense combines in-depth static code analysis, dynamic analysis (malware sandboxing), and machine learning to increase zero-day threat detection, including threats that use evasion techniques and ransomware. McAfee Products: McAfee Endpoint Security, McAfee Advanced Threat Defense
6.2 Software Integrity **Control Type:** Mandatory **Control Objective:** Ensure the software integrity of the SWIFT-related applications.	McAfee® Application Control blocks unauthorised executables on servers, corporate desktops, and fixed-function devices. Using whitelisting, McAfee Application Control can prevent attacks from unknown malware by allowing only known-good whitelisted applications to run. McAfee® Change Control delivers file integrity monitoring (FIM) capabilities, continuously tracks changes to file and registry keys, and identifies who made changes to specific files. McAfee Change Control then protects critical system files, directories, and configurations from tampering. No changes to the server environment are permitted except those in accordance with set policies. McAfee Products: McAfee Application Control, McAfee Change Control

SWIFT Control	McAfee Solution
6.3 Database Integrity **Control Type:** Mandatory **Control Objective:** Ensure the integrity of the database records for the SWIFT messaging interface.	Database integrity checks provide a detection control against unexpected modification to records stored within the database. McAfee Database Activity Monitoring delivers real-time monitoring and intrusion prevention capabilities help stop breaches before they cause damage. Alerts are sent directly to the monitoring dashboard with full details of the policy violation for remediation purposes. High-risk violations can be configured to automatically terminate suspicious sessions and quarantine malicious users, allowing time for the security team to investigate the intrusion. McAfee Database Activity Monitoring helps safeguard database integrity by blocking any unauthorised deletion or modification of database records. McAfee Products: McAfee Database Activity Monitoring
6.4 Logging and Monitoring **Control Type:** Mandatory **Control Objective:** Record security events and detect anomalous actions and operations within the local SWIFT environment.	ll McAfee products listed so far produce logs that are indispensable for detecting abnormal behaviour and potential attacks. However, in order to perform adequate detection, centralised log collection should be empowered with advanced monitoring and analytics capability. McAfee® Enterprise Security Manager provides a security information and event management (SIEM) solution that collects logs from the enterprise, archives them, and delivers actionable intelligence to prioritise, investigate, and respond to threats. Moreover, McAfee Enterprise Security Manager provides a user behaviour analytics (UBA) Content Pack and risk correlation capabilities. The UBA Content Pack combined with the McAfee Enterprise Security Manager risk correlation engine provides behavioural analytics capabilities and helps analysts track risky user behaviour. McAfee Products: McAfee Enterprise Security Manager
6.5A Intrusion Detection **Control Type:** Advisory **Control Objective:** Detect and prevent anomalous network activity into and within the local SWIFT environment.	McAfee Network Security Platform is a next-generation IPS that enables organisations to detect and block advanced threats. It performs deep inspection of network traffic by using a combination of advanced technologies, including full protocol analysis, threat reputation, and behavioural analysis to detect and protect against malware callbacks, denial-of-service (DoS), zero-day attacks, and other advanced threats. Additionally, McAfee Network Security Platform has the capability to inspect encrypted flows with inbound and outbound SSL decryption. When using virtualisation inside the local SWIFT environment, a dedicated solution built as a virtual instance of our award-winning IPS is the preferred choice. McAfee Virtual Network Security Platform discovers and blocks advanced threats in virtual environments, software-defined data centres (SDDCs), and private and public clouds. McAfee Products: McAfee Network Security Platform, McAfee Virtual Network Security Platform
7.1. Cyber Incident Response Planning **Control Type:** Mandatory **Control Objective:** Ensure a consistent and effective approach for the management of cyber incidents.	The McAfee® Professional Services Incident Response Program Team is ready to provide you expert guidance in building a complete incident response (IR) programme. McAfee IR consultants have deep expertise in collaborative and cross-functional emergency planning. From the initial kickoff interview through plan signoff and adoption, we will deliver confidence throughout your organisation and help ensure you are prepared for any security challenge. Our goal is to help you build a plan that works. McAfee Products: McAfee Professional Services

SWIFT Control	McAfee Solution
7.2. Security Training and Awareness **Control Type:** Mandatory **Control Objective:** Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.	McAfee® Security Training from top industry experts helps your IT professionals gain proficiency in best practises to implement your security strategy and better respond to incidents. Our security courses provide training to help security professionals build secure software and applications, assess vulnerabilities to defend against hacker attacks, and gain critical computer forensics skills to better respond to incidents. McAfee Products: McAfee Security Training
7.3A. Penetration Testing **Control Type:** Advisory **Control Objective:** Validate the operational security configuration and identify security gaps by performing penetration testing.	McAfee® Security Assessments Services provide security evaluation, vulnerability assessment, and penetration testing on the target enterprise. Moreover McAfee® Red Team Services combine elements of social engineering with penetration testing to gain insights into how the environment will fare in a real-world attack scenario. McAfee Red Team services can assess the effectiveness and readiness of your security controls, user awareness, incident detection, and response capabilities. McAfee Products: McAfee Professional Services
7.4A. Scenario Risk Assessment **Control Type:** Advisory **Control Objective:** Evaluate the risk and readiness of the organisation based on plausible cyberattack scenarios.	McAfee® Enterprise Risk Assessment Services discover the threats that are likely to have the greatest impact on your organisation and provides strategies to mitigate risk while meeting compliance goals. McAfee Enterprise Risk Assessment services are based on industry best practises, such as ISO 27002:2013, NIST Cybersecurity Framework, or other best practises. McAfee Products: McAfee Professional Services

Summary of Controls Coverage

Mandatory and Advisory Security Controls	McAfee Coverage
1 Restrict Internet Access and Protect Critical Systems from General IT Environment	
1.1 SWIFT Environment Protection	•
1.2 Operating System Privileged Account Control	McAfee® Security Innovation Alliance*
1.3A Virtualisation Platform Protection	•
2 Reduce Attack Surface and Vulnerabilities	
2.1 Internal Data Flow Security	•
2.2 Security Updates	•
2.3 System Hardening	•
2.4A Back Office Data Flow Security	•
2.5A External Transmission Data Protection	•

Mandatory and Advisory Security Controls	McAfee Coverage
2.6 Operator Session Confidentiality and Integrity	•
2.7 Vulnerability Scanning	McAfee Security Innovation Alliance*
2.8A Critical Activity Outsourcing	
2.9A Transaction Business Controls	
2.10A Application Hardening	
3 Physically Secure the Environment	
3.1 Physical Security	•
4 Prevent Compromise of Credentials	
4.1 Password Policy	McAfee Security Innovation Alliance*
4.2 Multifactor Authentication	McAfee Security Innovation Alliance*
5 Manage Identities and Segregate Privileges	
5.1 Logical Access Control	McAfee Security Innovation Alliance*
5.2 Token Management	McAfee Security Innovation Alliance*
5.3A Personnel Vetting Process	
5.4 Physical and Logical Password Storage	McAfee Security Innovation Alliance*
6 Detect Anomalous Activity to Systems or Transaction Records	
6.1 Malware Protection	•
6.2 Software Integrity	•
6.3 Database Integrity	•
6.4 Logging and Monitoring	•
6.5A Intrusion Detection	•
7 Plan for Incident Response and Information Sharing	
7.1 Cyber Incident Response Planning	•
7.2 Security Training and Awareness	•
7.3A Penetration Testing	•
7.4A Scenario Risk Assessment	•

* For an up-to-date list of McAfee Security Innovation Alliance partners, please visit: https://www.mcafee.com/enterprise/it-it/partners/security-innovation-alliance/directory.html.

Summary

By partnering with McAfee, organisations will not only be able to manage many of the mandatory and advisory controls required by the SWIFT Customer Security Control Framework, they will also be able to increase their ability to protect, detect, and respond to threats faster. The McAfee security architecture and portfolio are natively built to share and collaborate in an integrated ecosystem so as to facilitate information sharing and allow its customers to adhere to the underlying principles of a Customer Security Programme: Secure and Protect, Detect and Respond, Share and Prepare.

McAfee can help you meet 18 of the 29 controls and, through the McAfee Security Innovation Alliance Program,[6] maximise coverage, and provide a truly integrated and connected security ecosystem of interoperable security products to maximise the coverage of the CSCF controls while safeguarding existing customer security investments.

1. http://www.swift.com/about-us
2. McAfee products and services may provide features that support and enhance your industry's compliance obligations. However, they are neither designed nor intended as holistic compliance solutions. The information provided herein is for information purposes only and does not constitute legal advice or advice on how to meet your compliance obligations.
3. https://www.swift.com/myswift/customer-security-programme-csp
4. McAfee solutions are not designed to be holistic SWIFT compliance solutions. However, our product portfolio helps customers meet the requirements.
5. McAfee products and services may provide features that support and enhance your industry's compliance obligations. However, they are neither designed nor intended as holistic compliance solutions. The information provided herein is for information purposes only and does not constitute legal advice or advice on how to meet your compliance obligations.
6. https://www.mcafee.com/enterprise/en-us/partners/security-innovation-alliance.html

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com