The Society of Worldwide Interbank Financial Telecommunication (SWIFT)

The Society of Worldwide Interbank Financial Telecommunication (SWIFT) network provides a global community of financial institutions (11,000 customers across 200+ countries), the ability to exchange sensitive information involving international financial transactions.

This highly sensitive data has become a prime target for cyber criminals, as some of the most well-known breaches to date have involved fraudulent payment instructions being sent directly across the SWIFT network.

To establish a consistent secure framework and baseline for accountability, SWIFT introduced the SWIFT Customer Security Controls Framework (CSCF).

What is the SWIFT Customer Security Controls Framework?

The SWIFT Customer Security Controls Framework was developed to help financial service providers fight against cyber threats increasingly targeting their SWIFT-related infrastructure.

This framework focuses on three mutually reinforcing areas, including:

- Secure Your Environment
- Know and Limit Access
- Detect and Respond

These three objectives are supported by eight security principles, along with 16 mandatory and 11 advisory controls.

SWIFT Customer Security Controls Framework - Principles

The eight principles outlined in the SWIFT Customer Security Controls Framework can be easily broken down by objective:

- 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 and 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 do these requirements impact my organization?

The 16 mandatory controls must be implemented by all users on their local SWIFT infrastructure to establish a security baseline for the entire SWIFT community. These mandatory controls are subject to change to reflect the evolving threat landscape.

Institutions are required to submit a self-attestation of their compliance with the 16 mandatory controls based on the results of their self-assessment. The first self-attestation deadline was December 31, 2017 and must be submitted on a yearly basis thereafter. Organizations who fail to comply with these controls will be reported to the local supervisory authority as well as have the non-compliance status be viewable to all other users and counterparts within the SWIFT network.

The 11 advisory controls are based on security best practices that SWIFT recommends users to implement as part of a broader cybersecurity program.

Where do I start and why?

The security requirements outlined in the SWIFT Customer Security Controls Framework are in line with existing information security industry standards such as NIST 800-53, PCI DSS, and ISO, and should be complementary to your organizations existing IT strategy.

Netwrix combines intelligent change control with continuous system integrity monitoring, maintaining compliance for your systems, network and applications with a single solution that addresses over half of all the mandatory and advisory controls across the eight security principles.

SWIFT	Purpose	Netwrix Solution	Change Tracker
Requirement 1: 1.1: SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	Netwrix Change Tracker incorporates pre-built hardening templates derived from the Center for Internet Security (CIS) to audit for any vulnerabilities present and then continuous monitor for any configuration drift from that hardened state	✓
Requirement 1: 1.2: Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level operating system accounts.	Adopting the CIS best practice approach ensures correct settings are adopted from day one, but any account escalations will also automatically be captured.	✓
Requirement 2: 2.2: Security Updates	Minimize 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.	Change Tracker maintains host and application security settings, even for bespoke applications, and records all software patch updates.	
Requirement 2: 2.3: System Hardening	Reduce the cyber-attack surface of SWIFT-related components by performing system hardening.	Prebuilt device hardening template derived from CIS Benchmarks are used to audit for any vulnerabilities present: database systems, servers and network devices are then continuously monitored for any drift from the desired, hardened state.	✓
Requirement 1: 1.1: SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	Adopting the CIS best practice approach ensures correct settings are adopted from day one, but any account escalations will also automatically be captured.	✓

SWIFT	Purpose	Netwrix Solution	Change Tracker
Requirement 2: 2.2: Security Updates	Minimize 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.	File integrity monitoring (FIM) across all systems is an essential defense against malware and insider threats. Change Tracker includes a library of predefined FIM templates to detect and report unauthorized changes.	✓
Requirement 2: 2.9: Transaction Business Controls	Restrict transaction activity to validated and approved counter-parties and within the expected bounds of normal business.	Initial hardening audit will verify correct password and authentication policies are in use, with all subsequent account and privilege changes audited.	✓
Requirement 4: 4.1: Password Policy	Ensure passwords are sufficiently resistant against common password attacks by implement-ing and enforcing an effective password policy.	Prebuilt device hardening templates derived from CIS Benchmarks are used to audit for any vulnerabilities present: database systems, servers and network devices are then continuously monitored for any drift from the desired, hardened state.	✓
Requirement 5: 5.1: Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.	Initial hardening audit will verify correct password and authentication policies are in use, with all subsequent account and privilege changes audited. At all times, Netwrix Log Tracker will provide a 'checks and balances' audit trail for all account privilege changes.	✓
Requirement 6: 6.1: Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.	Change Tracker will check that AV services are activated and running, Log Tracker will alert on all significant AV events.	✓

SWIFT	Purpose	Netwrix Solution	Change Tracker
Requirement 6: 6.2: Software Integrity	Ensure the software integrity of the SWIFT-related applications.	Change Tracker file integrity monitoring (FIM) works on a zero-tolerance basis, reporting any changes to an operating system and program file systems. FIM ensures that nothing changes on your protected systems without being reported for validation.	✓
Requirement 6: 6.3: Database Integrity	Ensure the integrity of the data-base records for the SWIFT messaging interface.	Change Tracker file integrity monitoring (FIM) works on a zero-tolerance basis, reporting any changes to an operating system and program filesystems. FIM ensures that nothing changes on your protected systems without being reported for validation.	✓
Requirement 6: 6.4: Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	Netwrix Log Tracker provides a complete audit trail of all network activity, providing intelligent correlation threads to anomalous actions & operations. Alerting & ITSM ticket creation where appropriate.	✓
Requirement 6: 6.5: Intrusion Detection	Detect and prevent anomalous network activity into and within the local SWIFT environment.	Change Tracker provides real-time change detection to anomalous activity, whilst utilizing the CIS best practice processes, will reduce the attack surface and limit hacker activity significantly.	✓
Requirement 7: 7.3: Penetration Testing	Validate the operational security configuration and identify security gaps by performing penetration testing.	File integrity monitoring across all systems is an essential defense against malware and insider threats to card & customer data.	✓

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social