

SWIFT CUSTOMER
SECURITY PROGRAMME.

SWIFT's own network has never been the point of failure in a major payment fraud incident — **the customer's local messaging environment consistently is, which is exactly the gap the Customer Security Programme exists to close.**

- LOCAL ENVIRONMENT SECURITY
- SEPARATION OF DUTIES
- ANNUAL ATTESTATION
- COUNTERPARTY RISK

01 THE MECHANISM



Shared Responsibility Model

SWIFT secures its core network; each connected institution is responsible for its own local messaging environment — **CSP exists because most real incidents happen on the customer side**, not inside SWIFT's network.



Three Control Objectives

The Customer Security Controls Framework organizes mandatory and advisory controls around **securing the local environment, limiting and monitoring access, and detecting and responding** to anomalous activity.



Annual Attestation, Visible to Counterparties

Every connected institution self-attests compliance annually, and that status is visible to counterparty banks — **non-compliance becomes a real correspondent-banking risk**, not just a compliance gap.

02 THE FLOW

The Hardened Local Environment CONTAINED

1

The local SWIFT messaging interface runs in a dedicated, segmented environment isolated from the general corporate network, with **strict access controls on who can operate it.**

2

Operator credentials require MFA, and message creation is separated from approval so **no single compromised account can send a fraudulent transfer alone.**

3

Anomalous message patterns — unusual amount, destination, or timing — trigger real-time alerts **before the transfer settles**, giving a window to intervene.

The Compromised Local Environment EXPOSED

1

Malware on an operator's workstation captures valid SWIFT credentials, exactly as in the 2016 Bangladesh Bank heist, where **attackers never touched SWIFT's own network at all.**

2

A single compromised account has both the access and the authority to create and approve a payment message, so **nothing internally challenges a fraudulent instruction.**

3

The fraudulent message looks completely legitimate to SWIFT and the receiving bank — by the time anyone notices, **funds have already moved through correspondent accounts.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Secure Your Environment	Segmenting and hardening the local SWIFT infrastructure — messaging interface, connectivity, and operator workstations — from the broader corporate network.
Know and Limit Access	Multi-factor authentication, least-privilege operator accounts, and separation of duties between payment creation and approval.
Detect and Respond	Logging, anomaly detection, and an incident response plan specific to the payment messaging environment, not just general IT security.
Annual Attestation & Independent Assessment	Self-attesting against the CSCF every year, independently validated rather than self-reported alone, visible to counterparty institutions.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Trusting SWIFT's Network Security Alone	No	SWIFT's core network being secure does nothing for a compromised local messaging environment — Bangladesh Bank's heist never touched SWIFT's infrastructure.
One Account With Both Creation and Approval Rights	No	A single compromised credential can originate and authorize a fraudulent transfer with no internal check to catch it.
General IT Security, No Dedicated Messaging Hardening	No	Standard IT hygiene doesn't address the specific local attack surface the CSCF's controls are built around.
Self-Attestation With No Independent Validation	No	An unverified self-report gives counterparty institutions no real assurance the controls are actually implemented.
Segmented Environment + MFA + Separation of Duties + Anomaly Detection + Validated Attestation	Yes	Addresses the local environment where real incidents actually happen, with assurance counterparties can verify.

SWIFT CUSTOMER SECURITY PROGRAMME.

SECURE · LIMIT · DETECT

05 PROGRAM OPERATIONS

SWIFT's core network has never been the weak point in major fraud incidents. The customer's own local environment consistently is, which is exactly why CSP exists.

Separation of duties between creating and approving a payment message is one control that would have stopped several real-world SWIFT fraud incidents outright.

Attestation status is visible to counterparty banks, which turns non-compliance into a correspondent-banking relationship risk, not just an internal audit finding.

Independent assessment matters because an unverified self-report gives no real assurance to counterparties, or the institution itself, that controls are actually in place.

06 CONTROL MAPPING

CSCF

Customer Security Controls Framework — the specific mandatory and advisory technical controls institutions must implement, organized around CSP's three objectives.

KYC-SA

Know Your Customer Security Attestation — the application through which institutions self-attest CSCF compliance annually, visible to counterparties.

INDEPENDENT ASSESSMENT

Required validation of the attestation by internal audit, a competent independent function, or a third party — not simply self-reported.

ARCHITECTURE TYPE (A1-A4, B)

SWIFT's classification of how an institution connects, which determines the applicable control set based on local attack surface.

07 WHAT THIS DOES NOT SOLVE

Correspondent Banking Risk Beyond SWIFT

CSP hardens the messaging layer; it **doesn't address every risk** in the broader correspondent banking relationship or settlement process.

Insider Fraud With Full Authorization

Separation of duties raises the bar, but a **coordinated insider scheme** involving multiple authorized parties isn't fully solved by controls alone.

General Enterprise Security

CSP scopes specifically to the SWIFT messaging environment; **broader corporate network and endpoint security** remain separate programs.

Real-Time Fund Recovery

Detecting a fraudulent message quickly still depends on **intervening before settlement completes** — detection doesn't guarantee recovery once funds have moved.

08 MYTHS VS. REALITY

MYTH "SWIFT's network was hacked in the Bangladesh Bank heist."	REALITY Attackers compromised Bangladesh Bank's own local systems and used valid credentials to send fraudulent messages — SWIFT's core network was never breached.
MYTH "Passing CSP attestation means we can't be defrauded."	REALITY Attestation validates a defined control baseline at a point in time; it's not a guarantee against a sophisticated or novel attack.
MYTH "Self-attestation is sufficient on its own."	REALITY Since 2021, attestations must be independently assessed — an unverified self-report gives counterparties no real assurance.
MYTH "CSP is just another general cybersecurity checklist."	REALITY Its controls are specifically built around the local SWIFT messaging environment's actual attack surface, not general IT hygiene.
MYTH "Non-compliance is just an internal audit issue."	REALITY Attestation status is visible to counterparty banks, and significant non-compliance can trigger mandatory regulatory reporting in some jurisdictions.

09 SPEAK THE PROGRAM — KEY TERMS

CSCF

Customer Security Controls Framework — the document defining the **specific mandatory and advisory security controls** SWIFT-connected institutions must implement.

KYC-SA

Know Your Customer Security Attestation — the annual self-attestation application, with status **visible to counterparty institutions.**

SEPARATION OF DUTIES

Splitting payment message creation and approval between different individuals so **no single compromised account** can complete a fraudulent transfer alone.

ARCHITECTURE TYPE

SWIFT's classification of how an institution connects to the network, **determining which set of controls actually applies.**

CORRESPONDENT BANKING

The network of relationships banks use to actually settle funds; **SWIFT carries the payment instructions, not the money itself.**

INDEPENDENT ASSESSMENT

Third-party or internal-audit validation of a CSCF attestation, **required rather than optional self-reporting.**