CSCF v2027 Controls Evolution
Swift Executive Report, ER 1281

Confidentiality Level 2
Distribution to National Member Group allowed

Summary:
The Customer Security Programme (CSP) seeks to maintain the appropriate level of cybersecurity hygiene across all users, reduce the risk of cyberattacks, and minimise the financial impact of fraudulent transactions.

This report:

- Summarises the CSP overall status.
- Outlines the recommended changes to the Customer Security Controls Framework (CSCF) v2027.
- Seeks Board approval for the proposed changes.

Governance
Board on 11 June 2026

Issued by
Mike Manos, Chief Technology Officer

1 CSP Overall Status

Launched in 2016 in response to sophisticated cyberattacks on Swift users, the Customer Security Programme (CSP) seeks to maintain the appropriate level of cybersecurity hygiene across all users, reduce the risk of cyberattacks, and minimise the financial impact of fraudulent transactions.

As a non-commercial programme, the CSP offers free cybersecurity intelligence and supports customers in the continued development of cyber-risk management frameworks. This programme provides transparency on counterparty risk and allows enhanced customer and service provider risk-management through compliance status consumption.

Now well established, the CSP continues to innovate and delivers tangible results. It is one of the largest cyber initiatives of its kind in the world and one of only a few global programmes that is mandatory. The programme's control framework is recognised as an excellent and mature cybersecurity standard, setting the right protection and defence mechanisms against cyberattacks.

As such, the CSP is a comprehensive, multi-year, multi-facetted initiative with many stakeholders. Since its inception, considerable progress has been made across the various streams of activity:

- **Incident Response**: As an integral part of the CSP, the Customer Security Incident Response Team (CSIRT) undertakes incident response coordination. CSIRT works with stakeholders in the incident chain (i.e., victim bank, large correspondent banks, the end beneficiary bank) to detect and react upon fraudulent activity, stop and recall in-flight messages, and/or freeze accounts to support the recovery of funds.
- **Controls, Attestation and Compliance**: As of April 2026**,** the Attestation rates against the Customer Security Control Framework (CSCF) v2025 reached 90%, representing a 3% increase compared to the attestation rate in the previous quarter and covering over 99% of FIN traffic. Most non-attested entities are corporates (40%) and banks (36%), and non-attesting banks are reported to their supervisor. The global CSP compliance rate reached 86% (a 2% increase compared to Q4 2025 with the remaining 14% covering less than 0.5% of all FIN traffic).
- **Assurance**: As of April 2026, 94% of attested BICs were supported by independent assessments. In addition, approximately 30% of the v2025 attestations supported by an external assessor were conducted by a Swift CSP-certified assessor – compared to 18% in v2024 – strengthening quality and consistency.
- **Supervisory Transparency:** Supervisors are responsible for driving the efficiency and cyber-resilience of their local markets. Through the Know-Your-Customer Security Attestation (KYC-SA) for Know-Your-Customer for Supervisors (KYS) application, the CSP allows supervisors (i) to have visibility on non-attested or non-compliant supervised users and (ii) to request access to the attestation details of their supervisees.
- **Counterparty Risk Management**: The CSP provides the ability for each user to access the detailed compliance information of their respective counterparties through a 'request' and 'grant' process. Once 'granted,' users can 'consume' the counterparty data, allowing users to measure and/or manage the risk posed by counterparties. The newly granted Access Requests (AR) in 2025 account for an increase of 1% in all granted ARs since the inception of the CSP back in 2016.

- **Intelligence Sharing**: The CSP actively shares the technical Indicators of Compromise (IOC) that have been identified as part of forensics investigations conducted by the CSIRT after a customer has experienced a cyberattack. These IOCs are made available to all users via the Swift Information Sharing and Analysis Centre (ISAC) portal bulletins and associated feeds.

While it is difficult to categorically attribute the reduction of customer compromises to the CSP, the trend is due to a combination of several factors:

1. Raised customer awareness through local and regional engagement and continued sharing of IOCs, modus operandi, and other insights via the Swift ISAC, allowing customers to further secure their environments and undertake additional scrutiny for higher risk transactions.
2. Hardened interfaces which have further levels of protection and detection built-in and evolve as the threat landscape and attack techniques evolve.
3. Implementation of the security controls addressing protection of Swift-related components, detection, and response. These facilitate stopping adversaries from gaining easy access in the first place or detecting their activities early enough to minimise the impact.
4. Early detection of in-flight fraudulent messages and use of critical tools such as Swift's Payment Controls Service (PCS).
5. Strong collaboration of Swift with impacted stakeholders across the chain.

While these indicate that the CSP is making a difference, the programme should not lose focus and must remain vigilant to address the ever-changing threat landscape.

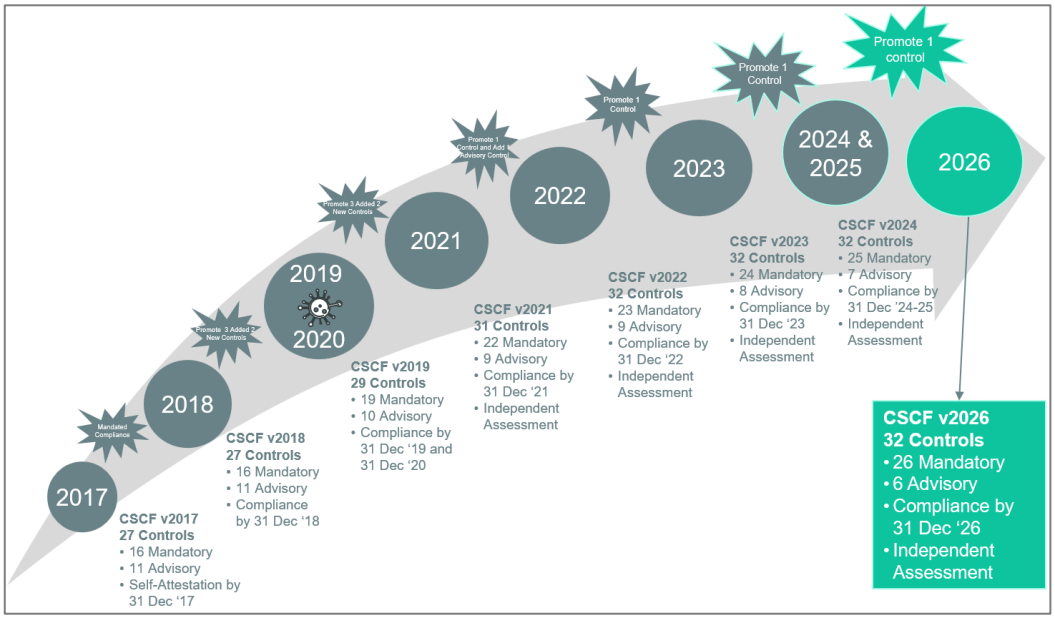
2 CSCF v2027 Controls Evolution

2.1 Controls Evolution

At the core of the CSP is a set of cybersecurity controls, the Customer Security Control Framework (CSCF). The CSCF is based on industry-standards, such as National Institute of Standards and Technology (NIST), ISO 27002 and PCI-DSS. This set of controls is split into 'mandatory' and 'advisory' controls.

Since its start, the CSCF has evolved, and Swift has ensured the right level of cybersecurity by promoting some controls from 'advisory' to 'mandatory,' by adding new advisory controls, and by the addition of guidance or clarifications. Refer to the following CSCF Controls Evolution graphic.

Figure 1 – CSCF Controls Evolution



Since the start of the programme in 2016, the pace of CSCF changes has slowed as the framework has become well established; however, it will continue to evolve pragmatically based on sound threat risk analysis, the technology evolution and lessons learned from customer attack cases, as appropriate.

At minimum, the CSP team anticipates a continued yearly CSCF release cycle with text updates and clarifications.

2.2 Community Consultation

The process for identifying the proposed changes for CSCF v2027 followed the existing CSCF change management procedure. The CSCF Working Group undertook extensive consultation. Established in 2021, this Working Group consists of primary and secondary representatives from 35 National Member Groups (NMG), comprising of large and smaller users, and users consulted for previous CSCF versions. Their role is to discuss Swift's CSCF proposal; centralise, prioritise, and review all formal and informal feedback from the community; and confirm the recommended changes.

Swift internal risk analysis started in October 2025. Community consultation on potential changes commenced in December 2025 and concluded in April 2026. Swift Oversight was kept informed of the potential changes. The final version of the CSCF v2027 document is expected to be published to the community in July 2026.

2.3 Summary of Recommended Changes

The CSCF Working Group reviewed 21 Change Requests (CR), covering the impact of new Swift initiatives, guidance clarifications, cosmetic improvements, and open questions. Seventeen CRs were accepted for inclusion in CSCF v2027 and four were rejected. Most proposed changes (12) were driven by Working Group participants, reflecting continued strong community engagement.

2.3.1 Summary

The majority of CSCF v2027 recommended changes are **clarificatory and non-disruptive**, reinforcing consistent interpretation of existing controls while ensuring

alignment with Swift's strategic initiatives, evolving technologies and operational experience. The framework remains stable, proportionate, and forward-looking, supporting effective implementation by the community and continued confidence by assessors.

2.3.2 Promotion of Advisory Control to Mandatory

Consistent with recent CSCF releases, **no** advisory controls or advisory in-scope components are proposed for **promotion to mandatory in CSCF v2027**. This approach maintains stability for the user community while allowing the framework to evolve through clarifications and guidance.

2.3.3 Additional Guidance Changes and Clarifications

The suggested changes include **guidance clarification and editorial refinements** aimed at improving usability and consistency of interpretation, while ensuring the CSCF remains aligned with Swift's strategic and technological evolution. These changes do not introduce any new security principles nor additional mandatory requirements. The following are examples of the most relevant clarifications and enhancements:

Alignment with Swift strategic initiatives

The CSCF clarifies its applicability to major Swift initiatives such as the **Swift Digital Ledger** and the **Swift Payment Scheme**. While these initiatives do not introduce new CSCF requirements at this stage, the framework confirms the continued applicability of existing controls to customer interfaces, connectors and outsourced components. Future CSP expectations, particularly for the Swift Digital Ledger, will be progressively defined via Knowledge Base guidance, with a view to integration into a subsequent CSCF release (targeting v2028).

Evolution of Alliance Connect connectivity

In support of the migration to **Software-Defined Wide Area Network (SD-WAN)** technology and the introduction of the **Secure Services Router (SSR)** model, the CSCF clarifies the treatment of new VPN deployment options, including a **Virtual on-Premises VPN**. These components are explicitly identified as in scope where relevant, ensuring continuity of security expectations across legacy, cloud, and emerging connectivity models.

Clarified responsibilities in outsourced, cloud and hybrid models

Guidance across multiple controls strengthens clarity around outsourced critical activities, regarding the handling of Public Key Infrastructure (PKI) keys and certificates managed via O2M. The CSCF reiterates that outsourcing does not shift accountability and provides clearer guidance on reliance on third-party assurance programmes.

Improved clarity on transaction, Relationship Management (RMA) and back-office controls

Several business-focused controls have been refined, notably:

- **Transaction Business Controls (2.9)**, with clearer expectations for outbound transaction activity across operating models and an emphasis on layered controls and service availability commitments

- **RMA Business Controls (2.11)**, emphasising regular business reviews of existing relationships and clarifying expectations for locally defined relationships, in the context of the central RMA model
- **Back-Office Data Flow Protection (2.4)**, including clearer definitions of the "back-office first hop" and the role of bridging servers, improving consistency of implementation and assessment.

Introduction of a technology-agnostic approach to secrets and keys management

A new generic concept, the **Secrets and Keys Vault (SKV)**, has been introduced to clearly frame CSCF expectations for the secure storage and management of credentials, keys and certificates. The CSCF confirms that such solutions are in scope, must be protected proportionately to the systems they support, and remain subject to outsourcing controls where externally hosted.

Operational clarity and alignment across controls

Additional refinements address recurring implementation and assessment questions, including:

- Risk-based mitigation of brute-force attacks within password policy expectations
- Confirmation that the Swift HSM is explicitly in scope for logging and monitoring
- Clearer expectations for penetration testing scoping, coverage and programme-based testing over time
- Updated guidance on internet access restrictions, micro segmentation, architecture selection.

Terminology, editorial consistency, and future automation

Definitions and glossary terms have been expanded to include concepts such as AI Agentic operators, micro segmentation, remote Group Hubs, Secrets and Keys Vaults, the Swift Digital Ledger, and the Swift Payment Scheme. Structural editorial changes, such as integrating footnotes into the main text, prepare the CSCF for future machine-readable and automation-friendly formats, without changing control intent.

3 Recommendation

The Board is asked to approve the proposed security enhancement changes to CSCF v2027 (Section 2).

End of Document