SmartSuite

Framework / Cybersecurity / SWIFT Security Framework

Swift Customer Security Controls Framework (CSCF) v2026

The SWIFT Customer Security Controls Framework (CSCF v2026) sets 32 mandatory and advisory controls that every Swift user attests to each year under the Customer Security Programme.



What it is

The SWIFT Customer Security Controls Framework (CSCF) is the set of security controls that Swift requires every user of its messaging services to implement and to attest to each year under its Customer Security Programme (CSP). The current edition, CSCF v2026, is dated July 1, 2025 and contains 32 controls, 26 mandatory and 6 advisory, which users attest against between July and December 2026.

The framework is organized under three objectives (Secure your Environment, Know and Limit Access, Detect and Respond) and seven principles. Advisory controls carry an A suffix, such as 2.5A, and a user's architecture type (A1, A2, A3, A4 or B) decides which controls are mandatory for it. Version 2026 made control 2.4, Back Office Data Flow Security, mandatory, brought customer client connectors such as API endpoints, middleware and file transfer clients into scope of 14 basic hygiene controls, and means some users that attested as type B may now attest as type A4.

At a glance

PUBLISHER
Swift (Society for Worldwide Interbank Financial Telecommunication)

TYPE
Framework

VERSION
CSCF v2026 (32 controls: 26 mandatory, 6 advisory)

EFFECTIVE
July 2026 (attestation window July to December 2026)

DOMAIN
Cybersecurity

FAMILY
SWIFT Security Framework

REGION
Belgium

INDUSTRY
Financial Services

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: swift.com/myswift/customer-security-programme-csp/security-controls

Why it matters

- **One baseline for every user** CSCF v2026 sets 32 controls, 26 mandatory and 6 advisory, under three objectives and seven principles.
- **Scope that fits the setup** Architecture types A1, A2, A3, A4 and B decide which controls are mandatory for a given user.
- **Independent assurance** Attestations are assessed internally, externally or by a mix of both, and an assessor with the CSP Certified Assessor status earns a distinct label in KYC-SA.
- **Counterparty visibility** Published attestations are visible to counterparties once the user grants access, so the result is a trust signal as well as a requirement.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports SWIFT CSCF

Architecture and Scope Register

Record the architecture type (A1 to A4 or B), the in-scope components in live, back-up and disaster recovery environments, customer client connectors and the back-office data flows behind control 2.4.

CSCF v2026 Control Library

Hold the 26 mandatory and 6 advisory controls with owners, implementation status and applicability by architecture type.

Independent Assessment Tracking

Log whether the assessment is internal, external or mixed, the assessor, the findings and the remediation actions through closure.

Attestation Evidence

Attach policies, configurations and logs to the controls they support so the evidence is ready before the KYC-SA window opens.

Service Provider Oversight

Track connectivity providers, service bureaus and customer connector vendors with Third Party Risk Management, including the responsibilities they share with you.

Attestation Reporting

Report readiness by objective and principle, open items and the submission status for each BIC before the window closes.

Common framework mappings

CIS Controls v8.1 | EU DORA | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

SWIFT Customer Security Controls Framework

Defines mandatory and advisory security controls for organizations using the SWIFT network.

swift.com/myswift/customer-security-programme-csp/security-controls

SWIFT Customer Security Controls Policy

Provides the official security policy related to the SWIFT CSF implementation.

swift.com/about-us/legal/compliance/customer-security-programme-policy

SWIFT CSP Compliance Guidance

Outlines guidance on achieving and maintaining compliance with SWIFT CSP controls.

swift.com/myswift/customer-security-programme/your-compliance

SWIFT Customer Security Programme Overview

Describes the objectives and components of SWIFT's Customer Security Programme (CSP).

swift.com/myswift/customer-security-programme-csp

Frequently asked questions

What is the SWIFT Customer Security Controls Framework and who must follow it?

The CSCF is the set of security controls Swift requires its users to implement and attest to under the Customer Security Programme. It applies to every user of Swift messaging services, whether it connects through its own infrastructure, a connectivity provider or a Swift connector. The current edition is CSCF v2026, dated July 1, 2025.

How many controls are in CSCF v2026 and which are mandatory?

CSCF v2026 has 32 controls: 26 mandatory and 6 advisory. Advisory controls carry an A after the number, for example 2.5A, and users must attest against all mandatory controls and may attest advisory ones. Some controls are mandatory for certain architecture types and advisory for others.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What changed in CSCF v2026?

Control 2.4, Back Office Data Flow Security, became mandatory, while legacy direct data exchanges stay advisory with 2028 as a tentative date to make them mandatory. Customer client connectors, such as API endpoints, middleware and file transfer clients, are now in scope of controls 1.2, 1.3, 1.4, 2.2, 2.3, 2.6, 2.7, 3.1, 4.1, 4.2, 5.1, 5.4, 6.1 and 6.4. Some users that attested as architecture type B may now attest as A4.

How and when do users attest, and does it need an independent assessment?

Users submit the attestation in Swift's KYC Security Attestation (KYC-SA) application between July and December; for the current cycle that is July to December 2026 against CSCF v2026. Swift's Customer Security Controls Policy requires every attestation to be independently assessed, internally by a function independent of the CISO organization, externally, or by both. Counterparties can see the published attestation once the user grants access.

What are the architecture types A1, A2, A3, A4 and B?

The type describes how the user connects to Swift. A1 users own the communication interface, A2 users own the messaging interface but not the communication interface, A3 users run a Swift connector such as Alliance Cloud, A4 users have no Swift footprint but run a customer connector, and B users have no local Swift infrastructure and use a service provider's interface. The type decides which controls are mandatory, and Swift offers a decision tree for choosing it.

License included / downloadable: No Swift publishes the CSCF and its Customer Security Controls Policy on swift.com, and some Customer Security Programme resources sit behind a Swift login. The platform links to Swift's pages and does not reproduce the control text.

Full framework page and mappings: smartsuite.com/frameworks/swift-customer-security-framework-csf