

SWIFT Customer Security Controls Framework (CSCF)

SWIFT Customer Security Framework establishes baseline cybersecurity controls for organizations using the SWIFT network to secure financial transactions.



What it is

The SWIFT Customer Security Framework (CSF) is a cybersecurity framework that establishes baseline security controls for organizations using the SWIFT network, aiming to reduce the risk of cyberattacks and ensure secure financial transactions. The framework defines mandatory and advisory security measures to help financial institutions protect the confidentiality, integrity, and availability of SWIFT-related assets.

Published by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the CSF is used globally by banks, payment service providers, and other entities that access the SWIFT network. Its control objectives focus on areas such as security governance, system integrity, user access controls, threat detection, and incident response, complementing broader financial sector regulations and cybersecurity standards.

At a glance

PUBLISHER SWIFT	TYPE Framework	VERSION SWIFT CSF 2023
EFFECTIVE 2017	DOMAIN Cybersecurity	FAMILY SWIFT Security Framework
REGION Belgium	INDUSTRY Financial Services	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.swift.com/myswift/customer-security-programme-csp/security-controls>

Why it matters

- **Strengthen cybersecurity governance** Establish consistent oversight and accountability for SWIFT-related security controls across all connected business units.
- **Enhance regulatory and industry alignment** Support conformity with financial sector regulations while bridging gaps with other global cybersecurity standards and frameworks.
- **Increase audit readiness** Provide a structured approach for validating control effectiveness, supporting internal audits and external regulatory inspections.
- **Improve threat detection and response** Enable faster identification and mitigation of potential cyber threats targeting SWIFT-related infrastructure and services.

How SmartSuite supports SWIFT CSCF

SWIFT Environment Scope Define SWIFT messaging components, interfaces, and supporting systems in scope.	SWIFT Control Library and Ownership Organize controls by requirement type with owners and implementation status.	Evidence for Annual Attestation Centralize proof for access, monitoring, vulnerability management, and segregation.
Incident Response and Fraud Readiness Run response workflows and track improvements tied to SWIFT risk scenarios.	Vendor Access and Shared Responsibility Manage vendor access, reviews, and shared responsibility evidence.	Attestation Reporting Report readiness and open items for annual control attestation.

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 Framework (CSF) used for?**

The SWIFT CSF is designed to establish and maintain baseline cybersecurity controls for organizations using the SWIFT network. Its primary purpose is to reduce cyber risk, safeguard SWIFT-related assets, and ensure secure financial transactions across global financial institutions.
- Is compliance with the SWIFT CSF mandatory?**

Yes, compliance with the mandatory controls of the SWIFT CSF is required for all SWIFT users, including banks and payment service providers. Organizations must complete annual self-attestations and, in many cases, obtain independent assessments to validate their compliance with CSF requirements.
- Who does the SWIFT CSF apply to?**

The SWIFT CSF applies to all entities that connect to and use the SWIFT financial messaging network, including banks, financial institutions, and service providers. It covers SWIFT-specific assets, infrastructure, and systems that process, store, or transmit SWIFT messages.

What are the core control objectives or required artifacts in the SWIFT CSF?

The SWIFT CSF defines mandatory and advisory controls across domains such as security governance, access management, system integrity, threat detection, and incident response. Core artifacts include the completed self-attestation, risk assessments, evidence of implemented security controls, and independent assessment reports.

How do organizations implement the SWIFT CSF?

Organizations implement the SWIFT CSF by mapping its controls to their internal security policies, conducting risk assessments, and applying technical and procedural safeguards across networks and systems related to SWIFT operations. They must also perform continuous monitoring, remediate gaps, and document compliance efforts for governance and audit purposes.

How does the SWIFT CSF relate to other cybersecurity frameworks?

The SWIFT CSF is complementary to other financial sector regulations and industry cybersecurity standards, such as ISO 27001 or NIST. Its controls can be mapped to internal frameworks and integrated with broader cybersecurity programs to achieve comprehensive risk management and regulatory compliance.

What are the ongoing compliance obligations under the SWIFT CSF?

Organizations must conduct annual self-assessments, address any non-compliance findings, stay current with SWIFT's evolving control requirements, and provide evidence of control effectiveness. Ongoing activities also include security incident response, regular risk reviews, and periodic independent assessments.

How would SmartSuite support SWIFT Customer Security Framework (CSF) compliance?

SmartSuite enables organizations to manage SWIFT CSF compliance by providing a mapped control library, consolidated risk register, and policy governance workflows. It supports automated evidence collection, continuous compliance tracking, remediation workflows, and audit-ready documentation. Reporting dashboards facilitate measurement of security practices and simplify preparation for attestations and independent assessments.

License included / downloadable: Yes The SWIFT Customer Security Framework documentation is publicly available through SWIFT resources for financial institutions.

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