

pwc.pt/swift

SWIFT

Customer Security Control Framework (CSCF)



SWIFT – Customer Security Control Framework (CSCF)

Enquadramento

A SWIFT definiu o **Customer Security Control Framework (CSCF)** com o objetivo de **incrementar a segurança cibernética da rede de pagamentos SWIFT**, aumentando a maturidade cibernética de seus membros.

De acordo com os requisitos SWIFT CSCF, as Instituições que utilizam SWIFT devem estar em **conformidade e submeter-se a avaliação independente do SWIFT CSP** (programa que determina os objetivos de controlo para cumprimento do CSCF). Para o ano de 2023, as entidades devem efetuar um **Independent Assessment do CSCF v2023 até ao dia 31 de dezembro de 2023**.

O **Independent Assessment** deve ser realizado por um avaliador independente da 1ª linha, seja ele interno ou externo à Instituição, devendo ter conhecimento e ser **acreditado pela SWIFT**.

Quem está impactado?

Todos os proprietários de SWIFT BIC ('Bank Identifier Code')

Obrigações das Instituições?

Realização de um Independent Assessment do CSCF v2023 até 31 de Dezembro de 2023 para reporte à SWIFT. Não é permitido pela SWIFT apenas um *self-assessment*.

Quais são os potenciais riscos?



Risco Reputacional

A não conformidade pode resultar em danos à marca e perda de confiança do cliente.



Risco Operacional

O não cumprimento expõe a Instituição ao aumento do risco cibernético inerente aos seus processos de pagamentos.

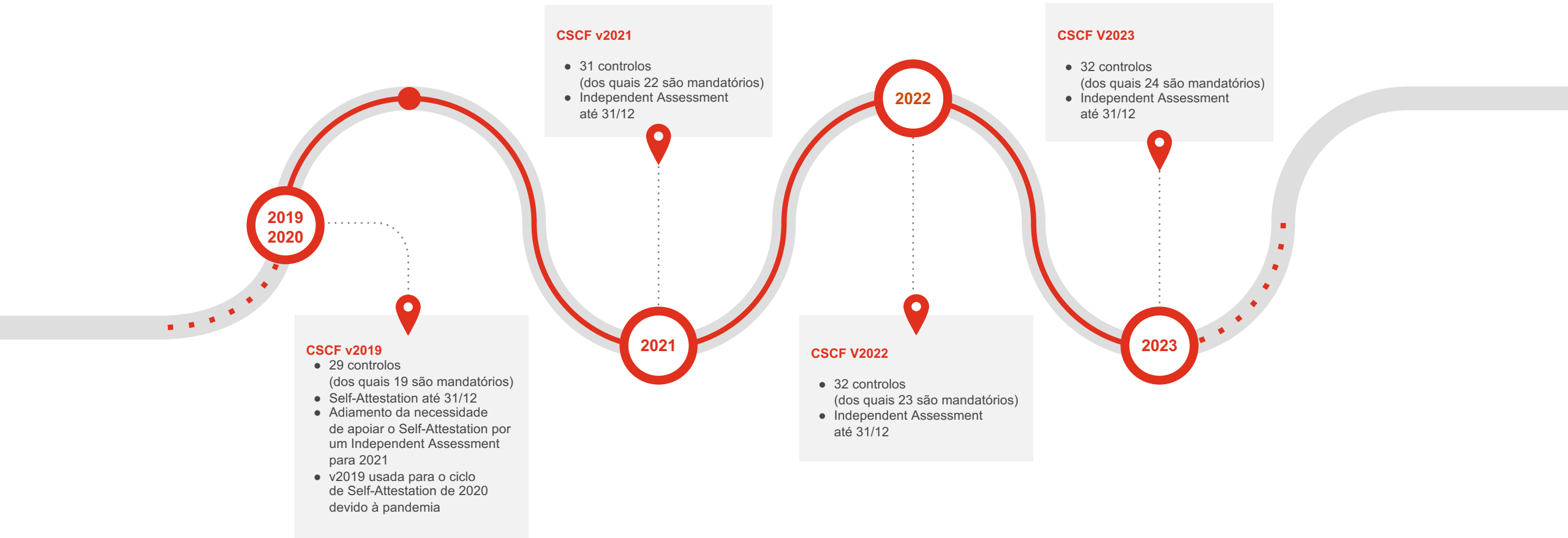


Risco Regulatório

Os reguladores poderão solicitar o envio de informação, realizar auditorias e/ou solicitar acesso local às instalações.

SWIFT – Customer Security Program (CSP)

Evolução



SWIFT – Customer Security Program (CSP)

v2023

O SWIFT Customer Security Programme (CSP) determina a obrigatoriedade do cumprimento do seguinte programa:

Princípio base

O CSCF exige às entidades que estas se certifiquem como estando em conformidade com um conjunto de controlos de segurança divididos em controlos obrigatórios e opcionais, dependendo do tipo de arquitetura implementada.

Controlos mapeados com os principais *standards* internacionais - NIST, PCI-DSS, ISO27002

Controlos

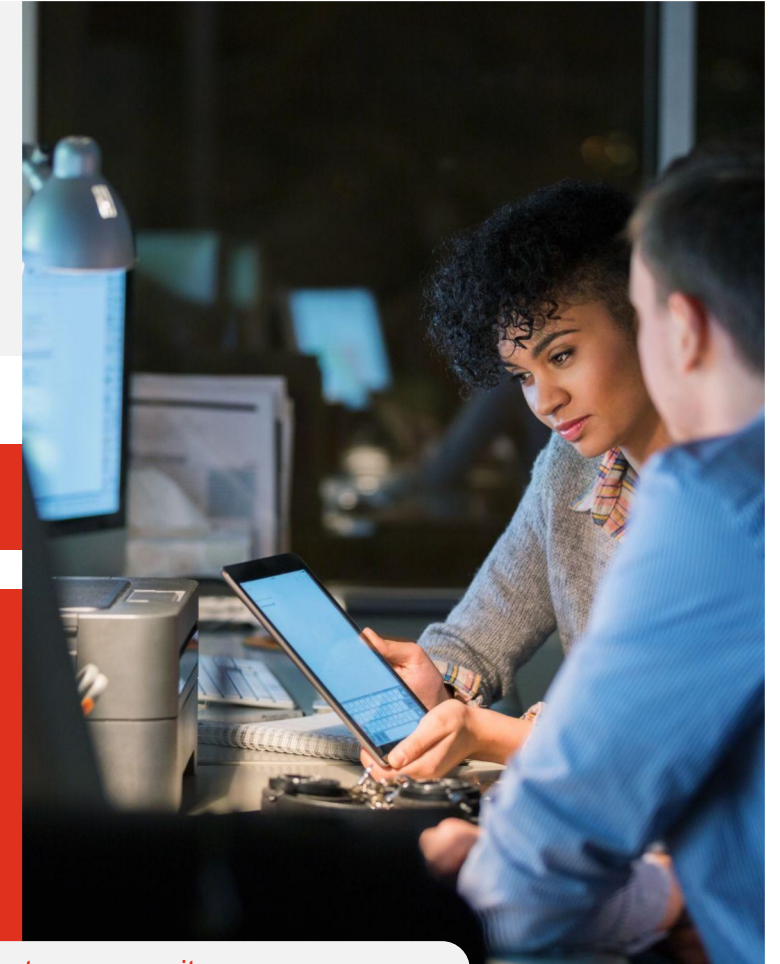
Arquitetura A1 e A2	31 controlos dos quais 8 são Opcionais
Arquitetura A3	30 controlos dos quais 8 são Opcionais
Arquitetura A4	29 controlos dos quais 10 são Opcionais
Arquitetura B	23 controlos dos quais 8 são Opcionais

Alterações identificadas no CSCF v2023

1 Controlo 1.5
O controlo do *Customer Environment Protection* passa a ser obrigatório na v2023 para a arquitetura A4.

2 Novo HSM
Nos seguintes controlos foi adicionado um componente em âmbito dos mesmos, nomeadamente no novo HSM, apenas devem ter atenção as entidades que já têm o novo HSM com utilização de PED's remotamente:

- 1.2 Operating System Privileged Account Control
- 1.4 Restriction of Internet Access
- 2.1 Internal Data Flow Security
- 2.2 Security Updates
- 2.4A Back Office Data Flow Security
- 4.1 Password Policy
- 4.2 Multi-Factor Authentication
- 6.2 Software Integrity



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

Credenciais PwC

Experiência em SWIFT

A equipa de Cibersegurança da PwC presta serviços no âmbito de todos os programas SWIFT:

- SWIFT CSP - Customer Security Program
- SWIFT SIP - Shared Infrastructure Program

As nossas credenciais



A PwC é entidade acreditada pela SWIFT como CSP assessment providers
Fonte: <https://www.swift.com/myswift/customer-security-programme-csp/find-external-support/directory-csp-assessment-providers>



A PwC é entidade credenciada em Segurança de Informação pelo **Gabinete Nacional de Cibersegurança de Portugal**

Equipa qualificada com competências distintas de apoio aos nossos clientes

A nossa equipa detém as seguintes certificações:

- ISO 27001 - Information Security Management System
- CISM - Certified Information Security Manager
- CISA - Certified Information Systems Auditor
- CeH - Certified Ethical Hacker
- CIAM - Certified Identity and Access Manager
- Security+ - CompTIA Security+
- CIA - Certified Internal Audit
- ITIL - Information Technology Infrastructure Library
- CFE - Certified Fraud Examiner
- Microsoft Certified Azure Fundamentals
- Microsoft Security, Compliance, and Identity Fundamentals



pwc.pt/swift



António Loureiro
Risk Assurance Partner

(+351) 916 601 370
antonio.loureiro@pwc.com



Marcelo Rodrigues
Cybersecurity Director

(+351) 911 747 740
marcelo.ferreira.rodrigues@pwc.com



Tiago Marques
SWIFT CSCF Lead

(+351) 961 645 688
tiago.david.marques@pwc.com

