SWIFT

Customer Security Control Framework (CSCF)

pwc.pt/swift

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 dos 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 2026, as entidades devem efetuar um ***Independent Assessment* do CSCF v2026 até ao dia 31 de dezembro de 2026.**

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

Quem está abrangido?

Todos os proprietários de SWIFT BIC (‘*Bank Identifier Code*’).

Obrigações das Instituições?

Realização de um *Independent Assessment* do CSCF v2026 até 31 de dezembro de 2026 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

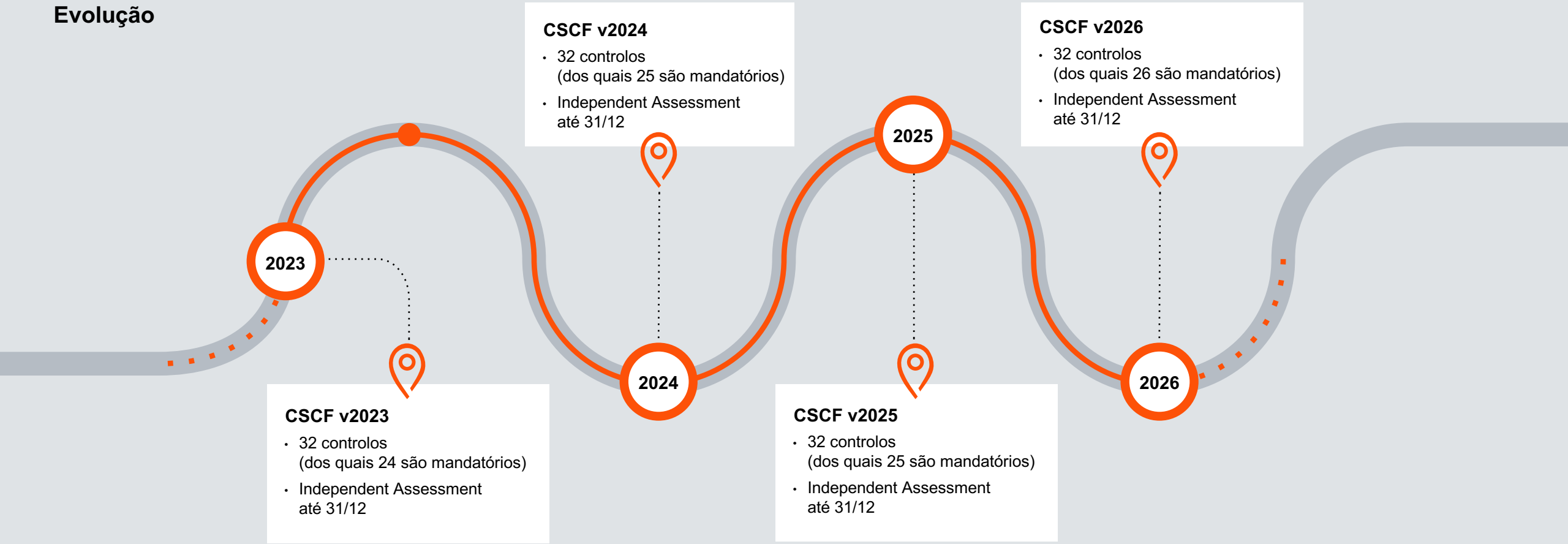
O não cumprimento expõe a Instituição ao aumento do risco cibernético inerente aos seus processos de pagamentos.

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)

v2025

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

Princípio base	Controlos
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 (v1.1 e v2.0), PCI-DSS, ISO27002.	**Arquitetura A1 e A2** 31 controlos dos quais 6 são opcionais **Arquitetura A3** 30 controlos dos quais 6 são opcionais **Arquitetura A4** 29 controlos dos quais 8 são opcionais **Arquitetura B** 23 controlos dos quais 7 são opcionais

Alterações identificadas no CSCF v2026

1

Controlo 2.4 — Back Office Data Flow Security
A implementação segue uma abordagem faseada, garantindo uma transição estruturada e segura. O que precisa de proteger?

Servidores de Bridging
Os guardiões que suportam a comunicação entre a sua zona segura e os *first hops* de *back-office*.

Fluxos entre Servidores
Todas as ligações entre servidores de *bridging* e entre estes e a zona segura, sempre que não exista proteção *end-to-end*.

Novos Fluxos Directos
Ligações diretas entre a zona segura e o *first hop* de *back-office*.

E os fluxos legados?
Mantêm-se em regime advisory... por agora.
Atenção: está prevista a sua obrigatoriedade em 2028.
Antecipe-se!

Agora é OBRIGATÓRIO!

2

Customer Client Connector
Os Customer Client Connectors passam agora a integrar o âmbito obrigatório de 14 controlos do CSCF, nomeadamente:
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 e 6.4.

O que é um Customer Client Connector?
É qualquer aplicação ou componente (como um *endpoint* que consome APIs, *middleware* ou cliente de transferência de ficheiros) que se liga indiretamente à SWIFT através de um prestador de serviços

Utilizadores que anteriormente atestavam como Arquitetura Tipo B poderão ter agora de atestar como A4, caso utilizem um Customer Client Connector.

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

Credenciais PwC

Experiência em SWIFT

Os elementos da equipa de Cybersecurity & Privacy da PwC possuem **experiência relevante** na realização de trabalhos SWIFT CSP.

A PwC realiza em Portugal trabalhos em todos os programas SWIFT:

- SWIFT CSP – Customer Security Program
- SWIFT PSP – Provider Security Program

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 ManageCISSP – Certified Information System Security Professional
- **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

Fale connosco

António Loureiro
Risk Assurance Partner

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

Marcelo Rodrigues
Cybersecurity Partner

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

Tiago Marques
Cybersecurity Principal

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

pwc.pt/swift