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 2025, as entidades devem efetuar um ***Independent Assessment* do CSCF v2025 até ao dia 31 de dezembro de 2025.**

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 v2025 até 31 de dezembro de 2025 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

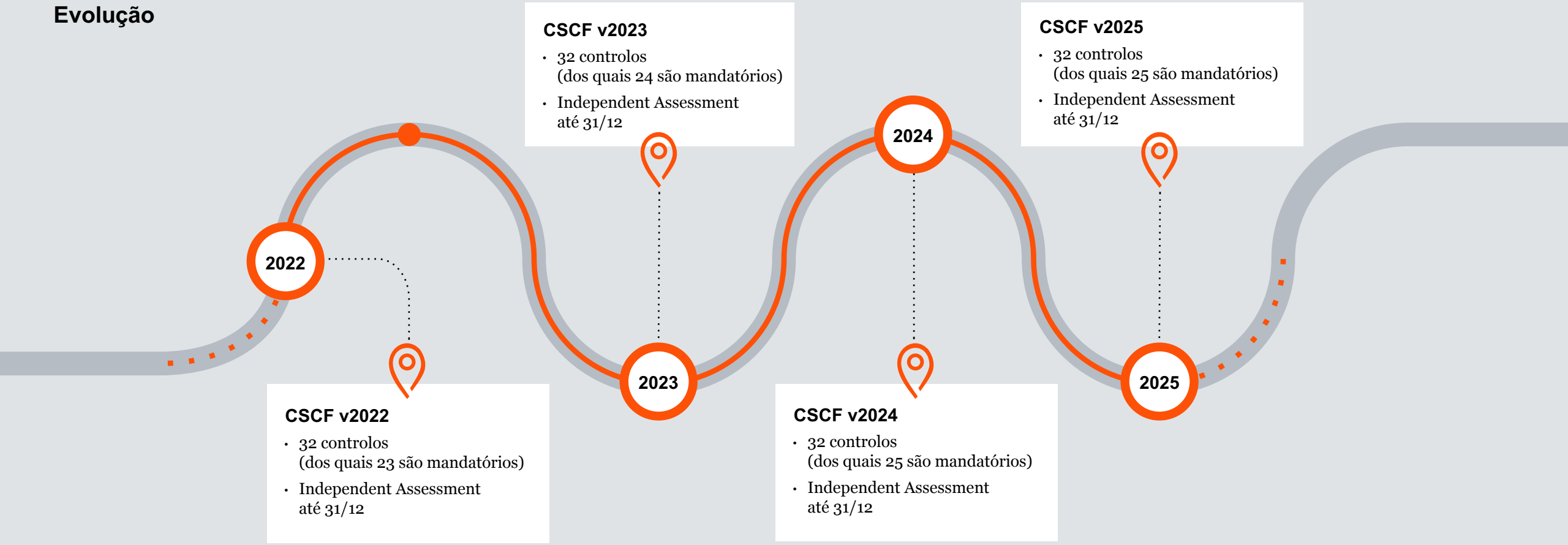
O não cumprimento expõe a Instituição ao aumento do risco cibernético inerente aos seus processos de pagamentos.

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



CSCF v2022
- 32 controlos (dos quais 23 são mandatórios)
- Independent Assessment até 31/12

CSCF v2023
- 32 controlos (dos quais 24 são mandatórios)
- Independent Assessment até 31/12

CSCF v2024
- 32 controlos (dos quais 25 são mandatórios)
- Independent Assessment até 31/12

CSCF v2025
- 32 controlos (dos quais 25 são mandatórios)
- Independent Assessment até 31/12

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 7 são opcionais **Arquitetura A3** 30 controlos dos quais 7 são opcionais **Arquitetura A4** 29 controlos dos quais 9 são opcionais **Arquitetura B** 24 controlos dos quais 8 são opcionais

Alterações identificadas no CSCF v2025

1

Controlo 2.4

Para apoiar uma promoção gradual do controlo 2.4A (Back Office Data Flow Security) para obrigatório, diversas alterações foram feitas neste controlo com o objetivo de:

- proteger os servidores que conectam o *back office* e a zona segura do cliente;
- proteger o fluxo entre *back office* e a zona segura do cliente.

Embora o controlo 2.4A permaneça opcional, a SWIFT recomenda a preparação de um plano de priorização de fluxos identificados entre a zona segura do cliente e o *back office* de acordo com:

- a postura de segurança do cliente; e
- uma abordagem baseada no risco.

2

Customer Client Connector

Gradualmente a SWIFT indica que todos os *endpoints* de clientes conectados indiretamente à SWIFT, serão classificados como *Customer Client Connector*.

Na versão de 2025, irá traduzir-se como uma mudança opcional, que passará a ser **obrigatória** com o CSCF v2026.

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

Customer Client Connector

Enquadramento

O *Customer Client Connector* é um *endpoint*, que facilita o fluxo entre o utilizador e o fornecedor e serviços. O conceito de *Customer Client Connect*, vai ser alargado e passará a abranger tanto um servidor como o cliente, ou seja o *endpoint* de cliente que se liga a um fornecedor de serviços ou à ao SWIFT.

Próximos passos

- Utilizador da arquitetura do tipo B que operem um *Customer Client Connector* devem certificar-se como arquitetura A4.
- Foi adicionado em todos os controlos o *Customer Client Connector* como opcional para 2025. No entanto é esperado que se torne obrigatório na versão de 2026 para a maioria dos controlos.

Objetivo?

Proteger transações financeiras no *endpoint* do cliente, e **alinhar a proteção** de todos os tipos de *endpoint* de aplicações.

Como é que estas mudanças afetam a minha organização?

Utilizadores que operem num ***Customer Client Connector***, que previamente utilizavam uma **arquitetura do tipo B**, **passam a utilizar uma arquitetura A4** em conformidade com o CSCF v2025.

Notas importantes

Utilizadores de arquiteturas do tipo B com operadores que usam apenas a interface gráfica da aplicação não devem mudar para uma arquitetura do tipo A4.

Segundo o CSCF v2025, este é o único tipo configuração aplicável a uma arquitetura do tipo B.

Credenciais PwC

Experiência em SWIFT

Os elementos da equipa de Risk Assurance 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
SWIFT CSCF Principal

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

pwc.pt/swift

© 2025 PricewaterhouseCoopers & Associados - Sociedade de Revisores Oficiais de Contas, Lda. Todos os direitos reservados. PwC refere-se à PwC Portugal, constituída por várias entidades legais, ou à rede PwC. Cada firma membro é uma entidade legal autónoma e independente. Para mais informações consulte www.pwc.com/structure.