



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 2024, as entidades devem efetuar um **Independent Assessment do CSCF v2024 até ao dia 31 de dezembro de 2024**.

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 v2024 até 31 de dezembro de 2024 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)

v2024

O SWIFT Customer Security Program (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 7 são opcionais
Arquitetura A3	30 controlos dos quais 7 são opcionais
Arquitetura A4	29 controlos dos quais 9 são opcionais
Arquitetura B	23 controlos dos quais 7 são opcionais

Alterações identificadas no CSCF v2024

1 Controlo 2.8

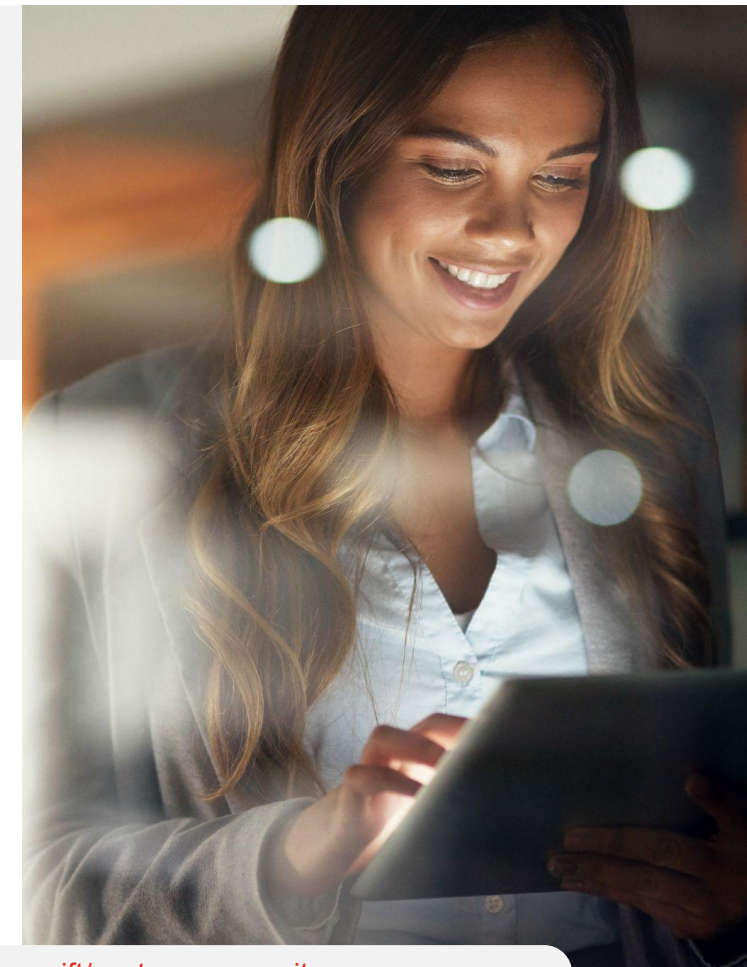
Em apoio ao aumento da terceirização e da cloudização o controlo 2.8 (Outsourced Critical Activity Protection) torna-se obrigatório e sujeito a alguns esclarecimentos.


2 Controlo 2.4

Para apoiar uma promoção faseada do controlo 2.4A (Back Office Data Flow Security) para obrigatório, diversas alterações foram feitas neste controlo para identificar adequadamente:

- os servidores que conectam o *back office* e a zona segura;
- os mecanismos que protegem a troca de fluxo de dados, seja
 - pela proteção de dados de ponta a ponta; ou
 - protegendo cada segmento de fluxo e os *middlewares* de suporte que são a segurança dessa troca de dados.

Embora o controlo 2.4A permaneça opcional, a SWIFT recomenda já identificar esses fluxos e avaliar sua postura de segurança.



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

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



Equipa qualificada com competências distintas de apoio aos nossos clientes

A nossa equipa detém as seguintes certificações:

- **ISO 27001** – Information Security Management System
- **CISSP** – 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 Auditor
- **ITIL** – Information Technology Infrastructure Library
- **CFE** – Certified Fraud Examiner
- Microsoft Certified **Azure Fundamentals**
- Microsoft Security, Compliance, and Identity Fundamentals



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**.

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 Lead

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



pwc.pt/swift



© 2024 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.