SWIFT

Customer Security Programme (CSP)

BDO

SWIFT Customer Security Programme (CSP)

Breve Enquadramento

O **SWIFT Customer Security Program (SWIFT CSP)** foi estabelecido pela Society for Worldwide Interbank Financial Telecommunication (SWIFT) para ativamente suportar os seus utilizadores no reforço da cibersegurança dos seus ambientes de negócio locais e que suportam a troca de informação das transações financeiras processadas através da infraestrutura SWIFT e à qual se encontram conectados.

Este programa foi estabelecido pela SWIFT em resposta a um conjunto de incidentes de cibersegurança originados nessas infraestruturas tecnológicas em 2016, sendo o mais notável, o incidente (infeção de malware) ocorrido no Bangladesh Bank que representou uma perda (desvios em contas bancárias) de $81 milhões de dólares (swift, Bangladesh Bank breach 2016, Euromoney, Centralbanking).

Este programa estabelece a Customer Security Controls Framework (CSCF) que implementa um conjunto de controlos de segurança alinhados com as melhores práticas da indústria constantes de três standards de segurança internacionais (PCI-DSS, ISO 27002 e NIST) e tem vindo a ser revista anualmente pela SWIFT para assegurar a sua relevância e a continuidade da segurança da sua infraestrutura e da informação dos seus utilizadores.

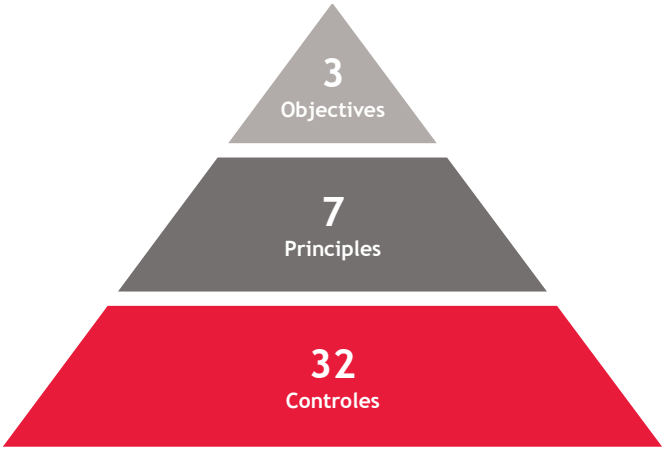
A framework (na sua versão vs2023) tem três objetivos orientadores ligados a sete princípios de segurança vertidos em controlos obrigatórios e opcionais/recomendados e a SWIFT requer que os seus utilizadores atestem a conformidade das suas infraestruturas numa base anual (entre julho e 31 de dezembro).

SWIFT Customer Security Programme (CSP)

Em 2023 foi melhorada a robustez da framework com a introdução de alterações nos controlos para assegurar que todos os componentes em âmbito estão protegidos dentro de um ambiente seguro e também com a clarificação de orientações para implementação dos controlos. A saber:

- Passagem de um controlo opcional para obrigatório, relacionado com a preocupação de proteção do ambiente em que estejam inseridos todos os conectores (um total de 23 controlos obrigatórios).
- Extensão do âmbito de vários controlos (1.2, 1.4, 2.1, 2.2, 2.4A, 4.1, 4.2 e 6.2) de forma a incluir o novo Hardware Security Module (HSM) com a utilização de Pin Entry Device (PED) remotamente.

Security Controls



Customer Security Controls Framework

Objectives	Principles
Secure Your Environment	1. Restrict Internet access & Segregate critical systems from general IT environment
	2. Reduce attack surface and vulnerabilities
	3. Physically secure the environment
Know and Limit Access	4. Prevent compromise of credentials
	5. Manage identities and segregate privileges
Detect and Respond	6. Detect anomalous activity to system or transaction records
	7. Plan for incident response and information sharing

Fonte: SWIFT, Reinforcing the security of the global banking system.

SWIFT Customer Security Programme (CSP)

Podemos esperar já em 2024 e nos próximos anos uma crescente preocupação com a garantia de segurança de controlos cuja responsabilidade seja total ou parcialmente delegada a terceiros, através da utilização da cloud e de serviços de outsourcing. Para além de nova clarificação de orientações para implementação dos controlos, podemos esperar para 2024:

- Novo controlo obrigatório: o controlo "2.8 Outsourced Critical Activity Protection" passa a ser obrigatório em vez de facultativo. A promoção deste controlo a obrigatório vem na sequência do crescimento da utilização da cloud e do outsourcing na comunidade SWIFT.
- Alterações relevantes no controlo "2.4A Back Office Data Flow, de forma a suportar a sua promoção a controlo obrigatório, de uma forma faseada. Ainda que este controlo se mantenha apenas facultativo em 2024, a SWIFT recomenda que seja já efetuada a identificação destes fluxos de dados em back office e que seja avaliada a sua postura de segurança.

Desde 2020 que o programa evoluiu com a alteração dos requisitos de garantia de compliance exigidos pela SWIFT, passando a ser requerida a submissão à SWIFT de uma avaliação independente realizada das seguintes formas possíveis:

- Avaliação externa efetuada por organização externa independente com reputação, experiência e credenciais em serviços e processos de avaliação de cibersegurança, bem como os consultores que realizam o trabalho tenham competências, certificações e experiência relevantes na área.
- Avaliação interna efetuada por departamento da 2ª ou 3ª linha de defesa da organização (por exemplo, a função de Compliance, Gestão de Risco ou Auditoria Interna) independente da 1ª linha de defesa. É relevante que o colaborador que conduz a avaliação tenha competências e experiência em cibersegurança e em avaliação de controlos desta natureza.

Deixa de ser possível submeter o "self-attestation" na aplicação Know Your Customer – Security Attestation (KYC-SA) sem os detalhes da avaliação independente.

Atualizações recentes no processo de avaliação de conformidade

Em 2023

Os utilizadores SWIFT têm de submeter a avaliação independente aos controlos obrigatórios da CSCF v2023 (mínimo de 15 controlos e máximo de 23 controlos, dependendo da arquitetura) que introduz alterações face à CSCF v2022, conforme referido atrás. Já no que respeita à metodologia de avaliação da conformidade, é obrigatória avaliação independente do desenho e implementação dos controlos obrigatórios (recomendável para os controlos facultativos "advisory").

Será necessário efetuar uma avaliação para cada controlo em âmbito, assegurando o cumprimento de 5 condições, cumulativamente, para poder existir reliance nas conclusões da avaliação independente do ano anterior.

O que configura não conformidade com a CSCF?

Estão em situação de incumprimento os utilizadores SWIFT:

- sem assessment de conformidade válido (não submetido ou expirado)
- que não implementam os controlos obrigatórios
- que se conectam à infraestrutura SWIFT através de um service provider não *compliant* ou que não apresentam avaliação externa obrigatória.

O que acontece nos casos de não conformidade com o SWIFT CSP?

Em primeiro lugar, as não conformidades em controlos SWIFT aumentam o risco de ciberataques e potenciam o impacto financeiro e reputacional resultante de transações fraudulentas.

Adicionalmente:

i. A SWIFT reserva-se o direito a reportar não conformidades com os controlos obrigatórios às autoridades de supervisão e às contrapartes (entidades com quem cada utilizador SWIFT troca mensagens financeiras);
ii. As autoridades de supervisão, mediante uma aplicação específica, possuem acesso em tempo-real ao estado atualizado de conformidade das entidades supervisionadas; e
iii. As contrapartes que tenham acesso à sua informação de attestation na plataforma KYC-SA também terão acesso em tempo real ao seu estado de conformidade. Cada membro com acesso ao KYC-SA deve consultar o estado de conformidade das entidades com quem se relaciona e integrar essa informação nos seus processos de gestão de risco (ciber, operacional, financeiro, regulatório) e de tomada de decisão no negócio. Pode, ainda, solicitar os dados do assessement submetido pelos membros com quem troca transações financeira e avaliar necessidades de controlos compensatórios no seu ambiente de negócio ou de limitação da relação de negócio estabelecida.

SWIFT Customer Security Programme (CSP)

Como pode a BDO ajudar?

Para além do conhecimento profundo das especificidades do SWIFT CSP/CSCF e da SWIFT Independent Assessment Framework, a BDO é uma entidade listada no diretório de Assessors da SWIFT e dispõe de recursos qualificados com certificações internacionalmente reconhecidas, tais como: CISA, PCI-QSA, CRISC, ISO 27k, ISO 20k, COBIT, ITIL e larga experiência na área Compliance de segurança da informação, cibersegurança e na realização de assessments com relação a standards e controlos de segurança, auditorias de segurança SI/TI, como uma diversificada experiência no setor financeiro em geral e de acordo com frameworks reconhecidos internacionalmente, tais como: PCI DSS, ISO 27001, NIST 800-53, NIST Cybersecurity Framework, ENISA, PSD2, EBA ITC Guidelines, NIS Directive, ISACA, ISF, CIS, SANS, SOX, FINRA, etc.

Desde 2021, ano em que se tornou obrigatório o independente assessment do SWIFT CSP, e até à data atual, a BDO adquiriu uma experiência considerável em trabalhos de independent external assessment num leque variado de entidades (bancos).

Para mais informações podem contatar diretamente o responsável do nosso Departamento de Information Systems Audit & Assurance, Vasco Jara Schiappa, através do telefone 937 990 180 ou do email vasco.schiappa@bdo.pt, ou formular um pedido de informação, através do link "CONTACTO", abaixo.

CONTACTO

www.bdo.pt