





SWIFT Customer Security Programme («CSP») Independent Assessment Service Offering

June 2021



Our approach to assessing an organization's compliance with SWIFT CSP standards

Our approach allows us to independently assess an organization's level of compliance with the SWIFT Customer Security Programme. We report the gaps, recommended actions and their priority as soon as identified so that organizations can plan for relevant remediation activities in a timely manner. Once these activities are implemented, we assess them and finalize our report and the independent assessment completion letter.

	Phase 1 Kick-off meeting and preparation	Objectives <ul style="list-style-type: none">• Organize the kick-off meeting• Understand the organization's SWIFT environment• Determine which mandatory and advisory controls of the SWIFT Customer Security Control Framework ("CSCF") are implemented
	Phase 2 Assessment of implemented controls	Objectives <ul style="list-style-type: none">• Assess controls which are applicable to the organization's SWIFT architecture by reviewing the available documentation, interviewing key stakeholders, testing the design of controls, performing walkthroughs and reviewing systems parameters• Report on identified gaps, recommended actions and priorities for your management's consideration
	Phase 3 Remediation and re-assessment	Objectives <ul style="list-style-type: none">• Close identified gaps by leveraging provided recommendations (<i>performed by the organization</i>)• Perform final assessment of the remediation activities to determine if gaps are adequately closed
	Phase 4 Final report	Objectives <ul style="list-style-type: none">• Prepare the final report including an executive summary for Senior Management• Prepare the independent assessment completion letter• Submit the attestation on SWIFT's portal (<i>performed by the organization</i>)

Scope of the independent assessment for type A4 and B SWIFT architectures – Mandatory controls only

The scope of our assessment is usually limited to applicable mandatory controls. Upon request, we can also include one or several advisory controls within the scope of the independent assessment. The following tables lists the mandatory controls in scope for architecture type A4 et architecture type B.

Architecture A4 mandatory controls

1.2 Operating System Privileged Account Control

1.3 Virtualization Platform Protection

1.4 Restriction of Internet Access

2.2 Security Updates

2.3 System Hardening

2.6 Operator Session Confidentiality and Integrity

2.7 Vulnerability Scanning

3.1 Physical Security

4.1 Password Policy

5.1 Logical Access Control

5.4 Physical and Logical Password Storage

6.1 Malware Protection

6.4 Logging and Monitoring

7.1 Cyber Incident Response Planning

7.2 Security Training and Awareness

Total of 15 mandatory controls

Architecture B mandatory controls

1.4 Restriction of Internet Access

2.2 Security Updates

2.3 System Hardening

2.6 Operator Session Confidentiality and Integrity

2.7 Vulnerability Scanning

3.1 Physical Security

4.1 Password Policy

4.2 Multi-factor Authentication

5.1 Logical Access Control

5.2 Token Management

5.4 Physical and Logical Password Storage

6.1 Malware Protection

6.4 Logging and Monitoring

7.1 Cyber Incident Response Planning

7.2 Security Training and Awareness

Total of 15 mandatory controls

Flexible timeline to support organizations until they are ready to submit their attestation

We deliver independent assessments between June and December, depending on the preparedness of organizations we engage with. The indicative schedule of the work to be carried out for the standard independent assessment is described in the following table. The timeline highly depends on the amount of deficiencies identified and the remediation timeframe. Should no deficiency be identified, the independent assessment could be delivered in 5 to 6 weeks.

Activities	July	Aug.	Sept.	Oct.	Nov.	Dec.
Phase 1: Kick-off meeting and preparation	■	■	□	□	□	□
Phase 2: Assessment of implemented controls	□	■	■	■	■	□
Phase 3: Remediation and re-assessment	□	□	□	■	■	■
Phase 4: Final report	□	□	□	□	□	■

We are committed to exceeding your expectations



Yan Borboën

Cybersecurity Partner

Phone: +41 58 792 84 59

E-Mail: yan.borboen@pwc.ch



Benoit de Jocas

Cybersecurity Manager, SWIFT CSP Lead

Phone: +41 58 792 96 10

E-Mail: benoit.de.jocas@pwc.ch



Michiel Mannaerts

Partner, Leader Corporate Treasury Solutions Switzerland

Phone: +41 79 638 51 64

E-Mail: michiel.mannaerts@pwc.ch



Tobias Thayer

Senior Manager, Corporate Treasury Solutions Switzerland

Phone: +41 76 758 88 44

E-Mail: tobias.thayer@pwc.ch

pwc.ch

This document does not constitute a contract (or a binding offer) to perform services. The acceptance of an engagement by PricewaterhouseCoopers Ltd is contingent upon successful completion of our acceptance procedures. Any engagement arising out of this unbinding proposal will be subject to the execution of our formal engagement contract, including also our standard terms and conditions, by the client and PricewaterhouseCoopers Ltd.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers AG, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2021 PwC. All rights reserved. In this document, 'PwC' refers to PricewaterhouseCoopers AG, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.