Summary of Change to SWIFT Customer Security Controls Framework V2024

Document History

Version	Date	Changed By	Description
1.0	February 2024	Geoff Poulter and Matthew Neall	Document Creation

Copyright and Confidentiality

Contents

1. Introduction

Under their Customer Security program (CSP), SWIFT have updated their required client standards and published their Customer Security Controls Framework (CSCF) 2024 requirements. As introduced in 2021, the CSCF standard required independent review to ensure and confirm that at least all the mandatory controls are in place and meet the SWIFT requirements, before you complete your 2024 attestation.

This short document aims to advise you, a SWIFT CSP audit client of AJC, of the key changes in the V2024 requirements. This document is intended as a briefing guide, to help you assess if you require remedial work from your current SWIFT topology, policies, procedures and practices. You have access to the full CSCF V2024 documentation on the MySwift portal, for fuller explanations and exact wording, or we can supply a copy on request.

In V2024, there are no changes compared with v2023, to which reference architectures each control applies to. There are no new controls introduced in V2024.

2. Definition Changes

Throughout the revised CSCF standard, SWIFT now refer to the "user's SWIFT Infrastructure" environment instead of the "local environment". This is to reflect that the SWIFT infrastructure covered by the standard may be on-premise or remotely hosted, and managed, hosted or operated by a third party and/or the user organisation. It covers virtualisation and cloud platforms. The broader definition is simply to describe the intended scope, and in practice is no different to what we audited you against in 2023.

The CSCF standard document now also refers to bridging servers in several places. These are message/file transfer servers, used as an interim stage to get two systems to communicate. An internal SFTP server would be a simple example.

3. An Outsourcing Agent Changes Your Audit Architecture

If you outsource the hosting of your back-office application, then there is a potentially a significant scope change to your audit.

Where you outsource your back office SWIFT application or hosting infrastructure, but that provider has no SWIFT relationship or connection, they are referred to as an Outsourcing Agent. You are now required to get from that provider, their SWIFT architecture (most likely an A4 or B if they have no SWIFT connection). You must then be audited against the composite greater architecture. You will now need to provide the evidence in your audit for the controls applicable to their outsourced activities. Exactly what must be provided depends on the scope of the outsourcing, but in many cases most of the controls will apply to them if they host the application and they will need to participate in providing a full set of SWIFT control evidence.

For example:

▲ If your users only use a browser to access an outsourced back-office application, giving you no SWIFT 'footprint' and making you Architecture B.

▲ Your outsource provider, an Outsourcing Agent, host the back-office application on your behalf, and includes in their service an SFTP server to send SWIFT message files, to a SWIFT connection location of your choice/service, making them an architecture A4,

▲You pay for the SWIFT bureau service that provides you with a connection to SWIFT. They must be audited as part of the SWIFT SIP programme. You have your Servicing Agent send your SWIFT message files to that SWIFT bureau.

▸ As a result, for your audit, you must be audited as A4, not B, because your Outsourced Agent is A4 and higher than your B. The Bureau service must be SIP compliant, but their architecture does not affect your audit architecture.

4. Promoted Controls

4.1 Control 2.8 Outsourced Critical Activity Protection

Existing Advisory Control 2.8A (Critical Activity Outsourcing) has been renamed and promoted to a mandatory Control.

It applies when a critical** SWIFT-related activity(s) is outsourced to a third party or a service provider.
For each critical** third-party you must:

- You must obtain their SWIFT architecture type and include in your attestation, when outsourcing your SWIFT infrastructure (but for a using a service bureau).
- Provide evidence to the auditor that your SWIFT infrastructure provider is registered in the SWIFT SIP programme or the Lite 2 Application Provider Directory. See https://www.swift.com/about-us/partner-programme/shared-infrastructure-programme/service-bureau-directory and https://www.swift.com/about-us/swift-partner-programme/find-partner/lite2-business-application-providers-directory

- Get reasonable comfort that services and activities are performed to the same standards and care as if operated by you (no change)
- When relying on an outsourcing agent to collect, process and further submit Swift-related transactions to a service bureau, an L2BA provider or even directly to Swift (through for instance Alliance Cloud, Lite2, Transaction Manager or another Swift channel), the users remain responsible for the conformance with the security controls and must seek compliance from that outsourcing agent to complement their attestation. In other words, you remain responsible for the security controls delegated to your third party(s).
- Show SLAs and NDAs are in place
- Show a security risk assessment you conducted supporting the outsourcing to the third party on an ongoing and regular basis. This is security-related, so it is more than financial due diligence checks. For example, demonstrate whether they had accreditation for ISO27001, SIP Accreditation, Cyber Essentials, etc.

** Critical is defined by SWIFT in the CSCF standard.as falling into one of eight categories: relating to the control the provider has within the SWFT infrastructure, SWIFT secure zone, user accounts or SWIFT data. It is not a regulator defined definition, or a financial risk definition.

You should maintain a table of which SWIFT-related suppliers meet these critical criteria, and therefore for which you will be providing evidence relating to the compliance checks you conducted on them.

4.2 Existing Control 2.4A Back Office Data Flow Security

This control has been significantly reworded, ahead of it becoming a mandatory control over two phases, with phase 1 expected in CSCF 2025. This control is not applicable to Architecture B.

The control objective remains unchanged: Ensure the confidentiality, integrity, and mutual authenticity of data flowing between on-premises or remote Swift infrastructure components and the back-office first hops they connect to. In other

words, the objective is to stop “internal” man-in-the-middle attack or the internal injection of a spoofed fraudulent message. However, the scope and requirements have changed.

Phase 1 will apply to “new flows” and phase 2 will apply to “legacy “flows”.

An inventory is required, detailing the flows and how each is currently secured, and a planned method of how it will be secured if not already. This will need to be presented to the auditor but could be a simple spreadsheet. A migration to secure mechanism(s) is expected, with the organisation first migrating from opportunistic protocols if used to enforced protocols, and then migrating other connections to secure protocols with the order based on internal risk assessment.

Then for each phase, you must:
1. Protect the point to point connection between the back office system first hop and the components in the secure zone.
2. Protect flows that are not point to point and rely on a bridging server (such as an internal file transfer server).

The protection must come from:
1. Use of a secure protocol (or mechanism) in the point to point of bridging server communication that ensures authentication, integrity, and confidentiality of data exchange.
2. Ensuring bridging servers are secure, if used (The CSCF controls apply to these servers such as control 2.3 Hardening.)

For many AJC clients, the SWIFT back-office connection will simply be to one back-office system. However, others might have more than one back-office application, especially if in parallel they feed their inbound SWIFT messages directly into the General Ledger system, rather than a feed from the back-office system.

The confidentiality, integrity and authentication assurance need to be achieved in one of four methods and is more precise than just demanding encryption. The SWIFT document is technical given it is about secure communication protocols and requires either:

- Secure data transmission and authentication validation at the recipient end. It suggested an encryption protocol such as ASE-GCM, where the ASE encryption also has the GCM “mode” of the protocol checking the credentials.
- Use of Local authentication (LAU) in combination with an encryption protocol such as two-way TLS.
- Secure protocols with commonly accepted cryptographic algorithms and industry standard key lengths i.e. 2048 bit
- Credentials and private/bilateral key combinations.

This may be a substantial piece of work for your organisation.

5 Extended Scope and Revised Working

Several of the controls have had amendments to their working. Whilst some are for the purpose of clarity, others are a deliberate extension of the scope to which the Control applies.

The following highlights, in AJC’s view, some of the key wording changes.

Control 1.3 Virtualisation or Cloud Platform Protection	The Control has been renamed to include “or cloud”. The control details have not changed but the title change makes it clear the scope does apply to cloud-platform provided virtual infrastructure as well as on-premise or remote third party hosted systems i.e. Co-location and managed services.
Control 2.3 System Hardening	This control now explicitly states USB ports and serial bus devices must be restricted: “disabling them to the maximum extent possible, while still supporting operations (for example, when USB tokens are required to authenticate users, …).“
Control 3.1 Physical Security	The scope now includes secure removal of data and configuration from equipment being disposed or re-used. Typically, independent destruction or wipe certificates would be presented to the auditor for disposed of equipment.
Controls 4.1 Password Policy	The Control Objective remains unchanged: Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy. AJC interpret this to require a password minimum length of 12 or more characters, in line with industry standards, on devices forming or within the SWIFT secure zone including network equipment.
Control 5.2 Token Management	Software tokens, including One Time Password (OTP) SMS systems, are now in scope. Therefore, the existing controls that applied to hardware tokens now apply to software tokens. This includes having a documented, demonstratable process for assignment, holding records of assignments for SWIFT access, and an annual review (or more frequent) of assigned tokens to check access needs to be retained.
Control 5.4 Password Repository Protection	This control has been renamed from Physical and Logical Password Storage to Password Repository Protection. However, the content and scope are substantially unchanged.
Control 6.2 Software Integrity	The control statement, defining intent, includes an additional sentence: “Origin and integrity of the software is ensured at download and at deployment time. “ The principal implementation guide point is replaced with the statement: Before applying downloaded software, operators should validate the legitimate source/site and perform. When technically possible, integrity checks such as checksum validation to support the change and release management process up to the deployment of the software
Control 6.4 Logging and Monitoring	Whilst this control has not changed, a number of the other controls have been explicitly cross-referenced, better defining the scope of what has to be logged and monitored.

Appendix B of the V2024 SWIFT CSCF document has improved reference Architecture diagrams.

6 Questions

AJC remains available on a consultancy basis for architectural design and/or audit detailed scope questions.