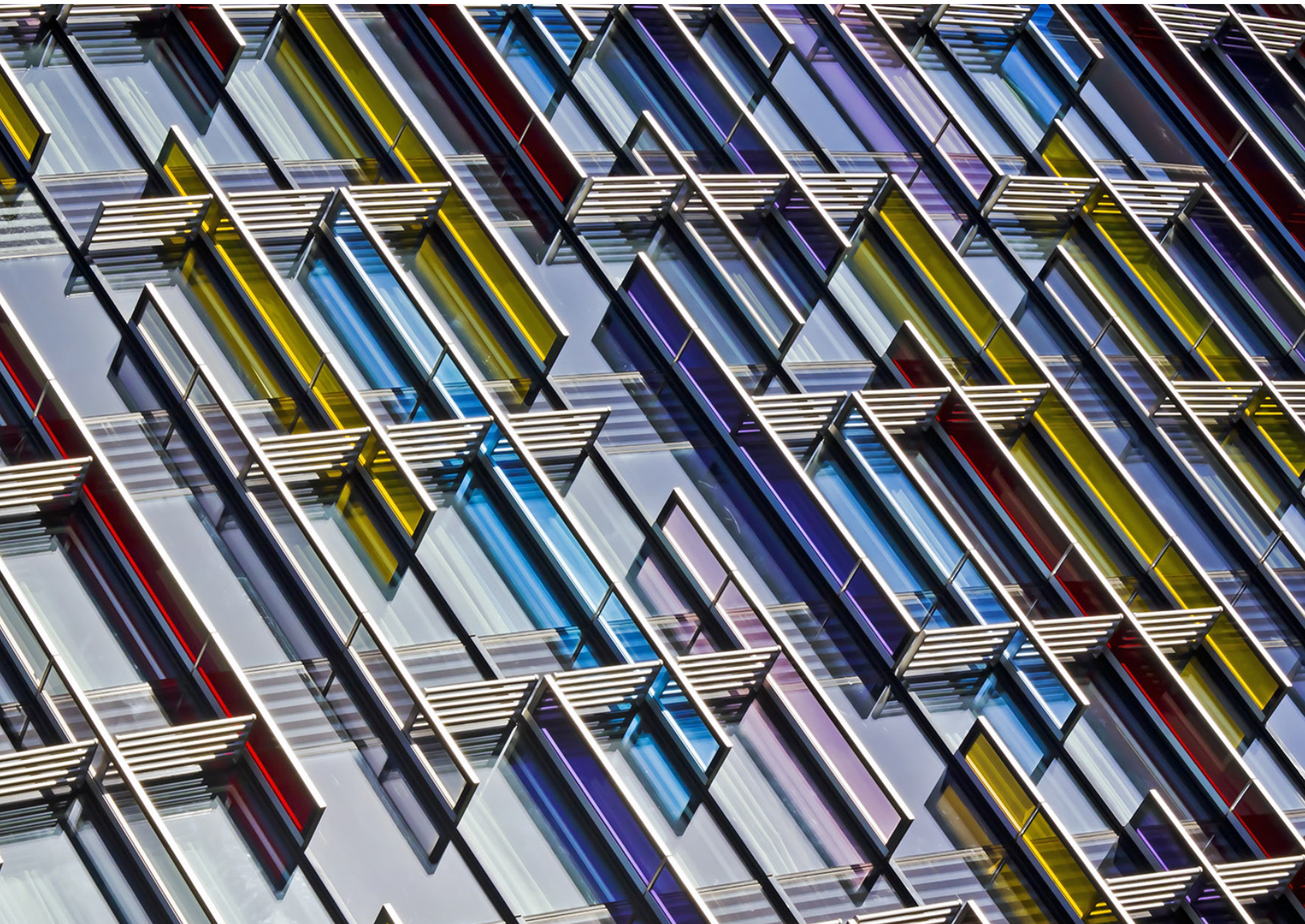# Swift Customer Security Program

Broadridge Consulting Services

An introduction to Swift Customer Security Controls Framework (CSCF)

Gain visibility into your organization's cyber risk

What is the Swift Customer Security program?

The financial sector is a key target for cyberattacks, and after incidents involving breaches of users' local environments, Swift launched its Customer Security Program (CSP) in 2017 to help institutions implement robust cybersecurity controls through a shared framework of mandatory and advisory measures that evolve to address emerging threats.

Why is Swift CSP so important?

The CSP helps create security standards and a shared framework, which outlines which security measures users should follow to secure their own financial ecosystem and ensure that they maintain high security standards while securely operating their Swift environment.

Swift adapts the framework to existing and new threats and encourages its users to implement, monitor and assess their security controls as part of a broader cyber risk management program.

Why choose Broadridge?

Broadridge is Swift-certified as a **2025 Swift Provider – Customer Security Program Assessment** and has been recognized as an independent assessor of choice.

With 25 years' experience managing a Swift service bureau, Broadridge offers in-depth product knowledge and technical expertise to help clients protect their IT infrastructure by keeping their Swift environment secure and compliant.

Broadridge provides a comprehensive service to help clients assess and attest to the Swift customer Security Control Framework and ensure that they implement robust security controls fully aligned to the CSCF objectives and principles.

Broadridge will perform a thorough control gap assessment of the client's Swift environment, and all the processes associated with it.

3 Objectives

7 Principles

32 Controls

Secure your environment

- Restrict internet access and segregate critical systems from general IT environment
- Reduce attack surface and vulnerabilities
- Physically secure the environment

Know and limit access

- Prevent compromise of credentials
- Manage identities and segregate privileges

Detect and respond

- Detect anomalous activity in system or transaction records
- Plan for incident response and information sharing

How can Broadridge assist?

Broadridge offers a broad range of CSP assessment and attestation services which can be fully tailored to our client needs.

We propose three different types of risk and control assessment options

Option 1

In-Depth Assessment – Compliant with CSP assessment and self-attestation requirements. Service includes:

- In-depth assessment of all Swift security controls (25 mandatory / 7 advisory) to attest to the full compliance with the Swift CSP Control Framework.
- Review effectiveness of security controls applied to IT systems, applications and processes connected to Swift
- Effort required: **10-15 days****

Option 2

Standard Assessment - Compliant with CSP assessment and self-attestation requirements. Service includes:

- Assessment of mandatory controls only. Focus is on understanding key infrastructure changes, identifying potential gaps and reviewing full CSP compliance with the latest Swift standards.
- Well suited for users with a mature Swift support model and a more established risk and control business function.
- Effort required: **6-10 days****

Option 3

Full risk and control review. Service includes:

- Full risk and control assessment: Initial Swift risk assessment, provide a prioritisation framework and a review of current controls
- Risk Mitigation Planning: Develop a remediation strategy and implementation roadmap to address identified gaps
- Implementation Support: Implement business governance, project management and implementation execution
- Effort required: **Dependent on scope**

**Time and effort will vary based on client architecture type, number of entities or BICs to be assessed

Trusted Expertise

Cyber risk: Broadridge can help you stay protected

We offer CSP assessment and attestation services to enable users to become fully compliant with Swift's Customer Security Control Framework (CSCF) and are adequately protected against cyber-threats.

Risk leaders

- We provide experienced risk managers
- We can identify gaps and risk areas to improve your cyber security

Control managers

- We understand cyber risk and help identify vulnerabilities
- We can guide you through the implementation of robust controls

Client centric

- We provide guidance and practical solutions to support your business

Security focused

- We can help you fight cyber threats
- We enforce CIA (Confidentiality, Integrity, Availability) in every part of our organization

Data experts

- We will assess your data quality and level of protection
- We understand privacy rules and can help you keep your data secure

Broadridge CSP process and key activities

CSP Assessment Period (Yearly)

Swift CSP Activities

Q1 (January - April)
- Swift publishes new CSP framework for next calendar year assessment (typically July of the previous year).
- Broadridge reviews in detail all updates and changes.
- Clients should begin reviewing new CSP details to ensure full readiness and understanding of all control changes.

Q2 (April - June)
- Swift hosts information session for all its users to introduce key changes to CSCF.
- Broadridge updates in-house CSP training materials and artifacts.
- Broadridge provides Swift CSP guidance and updates to its clients before the assessment period begins.

Q3 (July - September)
- Swift attestation window opens in July in Swift KYC-SA.
- Clients can begin CSP assessment and attestation with their independent assessor.
- Broadridge initiates CSP engagements and assesses client evidence.

Q4 (October - December)
- Client and Broadridge discuss and agree assessment results and findings.
- Broadridge delivers the final CSP assessment report to be submitted to Swift.
- Clients must provide final sign-off and self-certify in Swift KYC-SA by December 31st

Ready for Next

Broadridge Financial Solutions (NYSE: BR) is a global technology leader with trusted expertise and transformative technology to help the financial services industry operate, innovate, and grow. We power investing, governance, and communications for our clients – driving operational resiliency, elevating business performance, and transforming investor experiences.

Our technology and operations platforms process and generate over 7 billion communications per year and underpin the daily average trading of over $15 trillion of equities and fixed income trades. A certified Great Place to Work®, Broadridge is part of the S&P 500® Index, employing over 15,000 associates in 21 countries.

For more information about us, please visit **Broadridge.com**

Broadridge®

Ready for Next