通过 Swift CSP 评估提高金融安全

作者：atsec 李攀

关键词：Swift、CSP、金融交易安全、KYC-SA、CSCF、安全评估、客户安全计划、客户安全控制框架

atsec information security

Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.com

目录

1 引言

在全球金融体系高效运转的背后，是安全、可靠的信息流作为基石。Swift 网络作为这一信息流的核心通道，其安全性不仅关乎每个机构的稳健运营，更关系到全球金融生态的稳定与信任。然而，随着网络威胁的日益复杂化和严峻化，保障 Swift 环境安全已成为所有接入机构必须面对的核心挑战。

为应对这一挑战，Swift 推出了客户安全计划（CSP：Customer Security Programme），建立了一套成熟、严谨的安全评估体系。然而，对于许多金融机构而言，如何准确理解其架构分类、客户安全控制框架（CSCF ：Customer Security Controls Framework）与合规流程，并有效执行以满足合规要求，依然是一项充满困难的任务。

本文旨在协助金融机构更好的理解 Swift CSP 体系及其价值。atsec 作为专注于信息安全的评估机构，结合丰富的 Swift 客户安全计划（CSP）评估经验，对 Swift 客户安全计划（CSP）体系进行了系统性的梳理与解读。我们将从基础概念入手，逐步剖析架构类型、客户安全控制框架（CSCF）、KYC-SA（Know Your Customer Security Attestation）合规流程以及评估的步骤与价值。希望协助金融机构更好地理解并开展 Swift CSP 评估，筑牢金融交易的安全防线。

2 概述

2.1 Swift 定义

环球银行金融电信协会（Swift：Society for Worldwide Interbank Financial Telecommunication），本文中简称为“Swift”，作为一家全球性同业合作组织，Swift 是世界领先的安全金融报文传送服务机构。Swift 为金融机构提供报文传送平台和通信标准，并在连接、集成、身份识别、数据分析和合规等领域提供产品和服务。

Swift 的报文传送平台、产品和服务对接了全球超过 11,000 家银行、证券机构、市场基础设施和企业用户，覆盖 200 多个国家和地区。Swift 不为客户持有基金或管理账户，而是帮助全球用户社区通过可靠途径，安全开展通讯并交换标准化金融报文，从而支持全球和本地市场的金融交流，并助力国际贸易和商业活动。

Swift 用户（Swift User）指的是接入并使用 Swift 网络和服务的金融机构或其他组织。每个 Swift 用户都由一个唯一的 BIC（Business Identifier Code） 来标识。

2.2 Swift 维护的标准

Swift 制定并维护一系列金融报文标准，用于统一全球金融机构之间的通信格式，主要包括：

- MT 报文标准：传统格式，用于支付、外汇、证券等（如 MT103、MT202）。
- MX 报文标准：基于 ISO 20022 的 XML 格式，更现代化、结构化，支持更丰富的数据字段。
- FIN、InterAct、FileAct 等服务协议，支持实时、批量文件传输等不同通信模式。

这些标准确保了不同国家和机构之间的金融交易能够无缝对接。

3 Swift 架构类型

3.1 概述

用户可以通过多种技术设计方式连接到 Swift 系统。有些用户拥有自己的 Swift 基础设施，而有用户则可能使用其他组织的基础设施，例如 Swift 连接服务提供商（Swift Connectivity Provider）或集团中心（Group Hub）。 客户安全计划（CSP）将这些技术设计称为架构类型。在客户安全计划（CSP）中，有五种架构类型。架构类型从宏观的角度描述了用户用于连接至 Swift 所拥有的技术组件。

可通过下图判断连接 Swift 或服务供应商方式，知晓所属的架构类型：

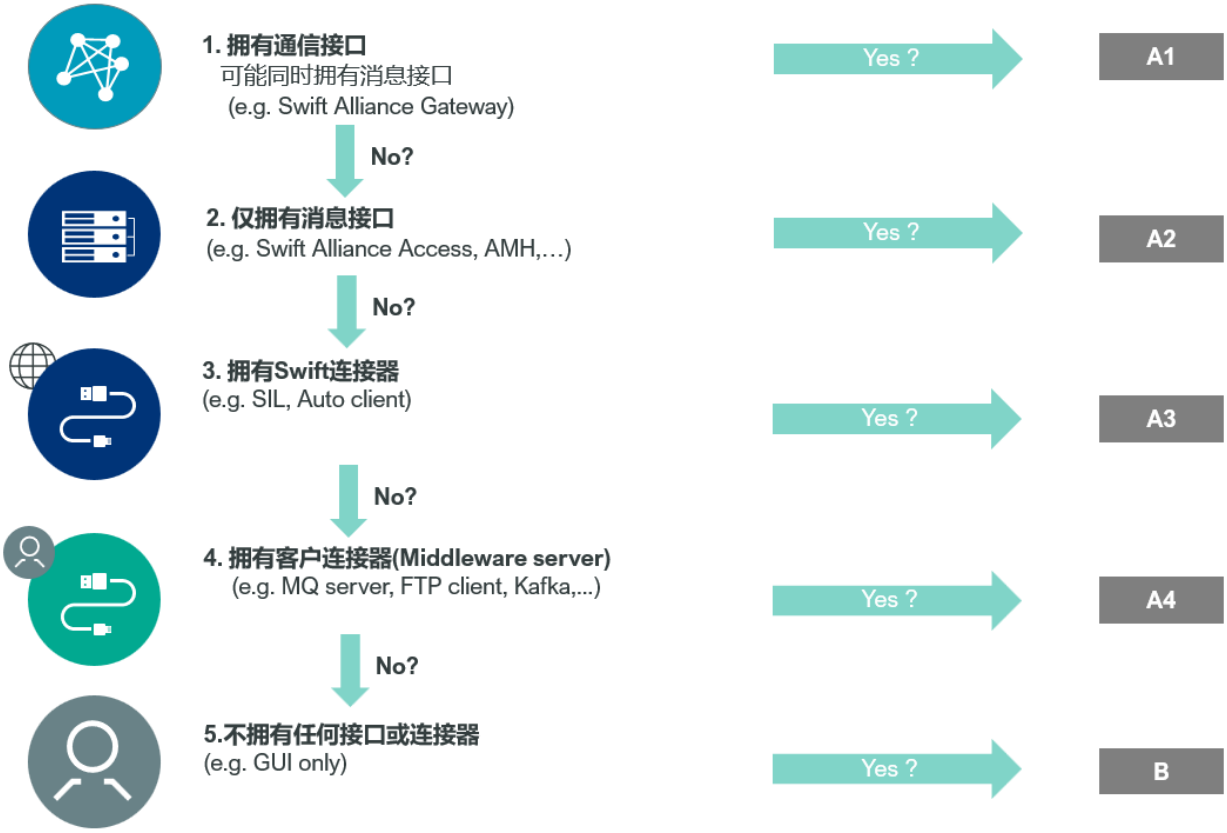

图 1：架构类型定义（图片源自 swiftsmart.swift.com，CSCF 总结）

3.2 五种 Swift 架构

3.2.1 A1 – 通信接口（Communication interface）

核心特征：拥有一个通信接口（Communication interface）。

典型组件：Swift Alliance Gateway 或 Alliance Gateway Instant。

连接模式：

- 可以直接连接到 Swift 网络。
- 可以拥有自己的报文接口，构成 A1 架构。
- 也可以不拥有报文接口，仅提供通信连接。

适用场景：拥有自己完整的 Swift 网络接入点，管理底层通信连接的大型机构。

3.2.2 A2 – 报文接口（Messaging interface）

核心特征：拥有报文接口，但不拥有通信接口。

典型组件：Swift Alliance Access 或 Alliance Messaging Hub。

连接模式：

- 依赖一个服务提供商（Swift connectivity provider or Group hub）来提供通信接口。
- 依赖 Swift 提供的 Alliance Remote Gateway 进行连接。

适用场景：拥有业务应用集成和报文处理能力，但将网络连接外包的金融机构。

3.2.3 A3 – Swift 连接器（Swift Connector）

核心特征：拥有一个 Swift 连接器。

典型组件：Swift Integration Layer，Alliance Lite2 AutoClient 或 Swift Microgateway。

连接模式：

- 通过该连接器连接到服务提供商（Swift connectivity provider or Group hub）的接口。
- 直接连接到 Swift 的云服务（如 Alliance Cloud）。

适用场景：希望通过轻量级、标准化的 Swift 提供组件实现应用与应用集成的用户。

3.2.4 A4 – 客户连接器（Customer connector）

核心特征：拥有一个客户连接器。

典型组件：

- 中间件或文件传输的服务器/客户端（如 IBM MQ，sFTP 服务器/客户端）。
- 使用 Swift SDK 的内部 API 端点。

连接模式：

- 通过该连接器连接到服务提供商（Swift connectivity provider or Group hub）的接口。
- 使用内部 API 端点直接连接到 Swift 的 API 平台。

适用场景：使用自有的或第三方中间件/文件传输/API 解决方案与服务提供商集成的用户。

3.2.5 B – 图形用户界面用户（GUI：Graphical User Interface）

核心特征：不拥有任何接口或连接器。

连接模式：

- 仅有操作员通过图形用户界面 访问服务提供商的业务应用。
- 仅有操作员通过图形用户界面 访问 Swift 服务（如 Alliance Lite2，Alliance Cloud）。

关键限制：不存在应用对应用的流，只有用户对应用的交互。

适用场景：仅通过网页浏览器使用 Swift 服务，没有后端系统集成需求的中小型用户。

4 Swift 评估体系

4.1 客户安全计划

客户安全计划 （CSP：Customer Security Programme）于 2016 年启动，旨在针对 Swift 用户的复杂网络攻击，为所有用户维持适当的网络安全标准，降低网络攻击风险，尽量减少欺诈性交易的财务影响。

核心组成部分

- **客户安全控制框架（CSCF）**
  - 包括强制性和建议性安全控制措施强制性安全控制为整个社区确立了安全基准，所有用户都必须在其 Swift 基础设施中实施上述基准。该框架会定期更新，以应对不断变化的威胁环境。
- **安全声明**
  - 用户必须每年提交其对 CSCF 中强制性控制措施的合规状态。这有助于您评估自身的安全状况，并与您的交易合作机构建立信任。
- **客户安全计划（CSP）评估**
  - Swift 提供工具和指导，帮助您独立的评估对客户安全控制框架（CSCF）的合规情况。
- **KYC-Security 合规信息**
  - 此功能允许您安全地与您的交易合作伙伴共享您的安全合规状态，帮助他们完成其安全尽职调查流程。

4.2 客户安全控制框架

Swift 客户安全控制框架（CSCF）包括强制性和建议性安全控制措施，它们基于行业标准框架，例如美国国家标准和技术协会（NIST：National Institute of Standards and Technology），ISO 27000 以及“支付卡行业数据安全标准”（PCI DSS）。强制性安全控制为整个社区建立了一个安全基线，所有用户都必须在其 Swift 基础设施上实施。Swift 优先考虑强制性控制，为短期、有形的安全收益以及降低风险设定一个现实的目标。建议性安全控制是基于 Swift 建议用户实施的最佳实践。随着时间的推移，强制性控制可能会随着威胁形势的演变而变化，一些建议性控制可能会成为强制性的控制要求。

4.2.1 版本发布周期

- **每年发布新版本**：CSCF 每年会发布一个新版本（例如：CSCF v2025）。
- **发布时间**：通常在每年 7 月发布新版本。
- **生效时间**：新版本中的控制要求将在次年 7 月正式在 KYC-SA（Know Your Customer Security Attestation）中生效。

例如：

- CSCF v2025 于 2024 年 7 月发布。
- 用户需在 2025 年 7 月至 12 月期间，依据 v2025 中的控制要求完成合规性证明。

4.2.2 控制的逐步升级

- **建议性控制（Advisory）可能转为强制性（Mandatory）：**
  - 例如：控制 2.4A（Back Office Data Flow Security）计划在 2026 年转为强制性。
  - 部分“遗留流程”的保护要求预计在 2028 年成为强制性。
- **新增组件逐步纳入范围：**
  - 例如：客户客户端连接器（Customer Client Connector）在 v2025 中为建议性组件，预计在 v2026 转为强制性。

4.2.3 控制框架内容

- **控制措施类型**

- 强制性控制：必须实施并在 KYC-SA 中声明的安全基线。CSCF v2025 包含 25 项强制性控制。
- 建议性控制：Swift 强烈推荐实施的最佳实践，能进一步提升安全性。CSCF v2025 包含 7 项建议性控制（在控制号后标“A”，如 2.4A）。

- **框架结构：**围绕三大目标和七大原则，共衍生出 32 项控制措施。具体信息如下：

三大目标	七大安全原则	核心焦点
1. 保护您的环境	1.1 限制访问并保护关键系统与通用 IT 环境隔离 1.2 减少攻击面与漏洞 1.3 物理保护环境	系统隔离、加固、物理安全
2. 了解并限制访问	2.1 防止凭据泄露 2.2 管理身份并分离权限	认证、访问控制、权限分离
3. 检测并响应	3.1 检测系统和交易记录中的异常活动 3.2 规划事件响应和信息共享	监控、日志、入侵检测、事件响应

- **安全控制概述表**

关于适用范围，控制措施的应用取决于用户的架构类型（A1，A2，A3，A4，B）。架构越复杂（如 A1），适用的控制越多；架构 B 适用的控制最少。以下图 2 是 CSCF v2025 安全控制概述表，我们可以了解到两个关键信息：第一，哪些是强制性控制，必须执行、哪些是建议性控制，建议执行（带 A 并标阴影）；第二，这些控制分别适用于哪种技术架构（A1 到 B 型）。每个机构的合规范围，完全取决于机构属于哪种架构类型。

强制性和建议性安全控制	架构类型				
	A1	A2	A3	A4	B
1 限制互联网访问和保护关键系统免受总体 IT 环境影响					
1.1 Swift 环境保护	●	●	●		
1.2 操作系统特权账户控制	●	●	●	●	●
1.3 虚拟化或云平台保护	●	●	●	●	
1.4 互联网接入限制	●	●	●	●	●
1.5 客户环境保护				●	
2 减少攻击面和薄弱环节					
2.1 内部数据流安全	●	●	●		
2.2 安全更新	●	●	●	●	●
2.3 系统强化	●	●	●	●	●
2.4A 后台系统数据流安全	●	●	●	●	●
2.5A 外部传输数据保护	●	●	●	●	
2.6 操作员会话的保密性和完整性	●	●	●	●	●
2.7 薄弱环节扫描	●	●	●	●	●
2.8 外包关键活动保护	●	●	●	●	●
2.9 交易业务控制措施	●	●	●	●	●
2.10 应用强化	●	●	●		
2.11A RMA 业务控制	●	●	●	●	●
3 保障物理环境安全					
3.1 物理安全	●	●	●	●	●
4 防止登录资料泄密					
4.1 密码政策	●	●	●	●	●
4.2 多重身份验证	●	●	●	●	●
5 管理身份和权限分离					
5.1 逻辑访问控制	●	●	●	●	●
5.2 译码器管理	●	●	●	●	●
5.3A 人员审批流程	●	●	●	●	●
5.4 密码库保护	●	●	●	●	●
6 检查系统或交易记录的异常活动					
6.1 恶意软件保护	●	●	●	●	●
6.2 软件完整性	●	●	●	●	
6.3 数据库完整性	●	●		●	
6.4 日志和监控	●	●	●	●	●
6.5A 入侵检测	●	●	●	●	
7 事故应对措施和信息共享计划					
7.1 网络事件反应计划	●	●	●	●	●
7.2 安全培训和意识	●	●	●	●	●
7.3A 渗透测试	●	●	●	●	●
7.4A 基于场景的风险评估	●	●	●	●	●

图 2：安全控制概述表（源自 Swift 客户安全控制框架 2025 年版）

4.3 Swift KYC-SA

KYC-SA 是 Swift 客户安全计划（CSP）中的核心合规工具和透明度机制。

- **合规声明**

- 内容：每个 BIC（Business Identifier Code）每年必须在 KYC-SA 中证明其符合所有适用的强制性控制措施。
- 评估方式：可以由内部团队（如合规、风控、内审）执行，也可由外部有资质的机构（例如 atsec）进行独立评估。

- **年度周期与关键时间点**
  - 7 月：Swift 发布新版本的 CSCF（例如，CSCF v2025 于 2024 年 7 月发布）。
  - 次年 7 月 - 12 月：用户必须依据上一年 7 月发布的 CSCF 版本进行评估。
  - 例如：针对 CSCF v2025 的评估，需在 2025 年 7 月至 12 月期间完成。
  - 12 月 31 日：提交合规声明和独立评估报告的最终截止日期。
- **评估的有效期**
  - 一次评估结果自提交后，有效期至该 CSCF 版本周期的第二年年底。
  - Swift 建议每六个月检查并更新一次评估状态，以保持信息的及时性。
- **信息的可见性**
  - 用户提交：用户自行在 KYC-SA 中提交声明。
  - 合作方查询：在获得授权后，交易合作方可以查看您的合规状态。
  - 监管监督：监管机构可通过专用工具实时查看其管辖范围内机构的合规情况。

5 atsec 安全评估方法论

5.1 Swift 评估类型

在提交安全评估合规声明前，Swift 用户必须根据客户安全控制框架（CSCF）完成强制性安全控制项的评估。评估路径主要分为以下三类：

1. 自我评估（不合规路径）

- 执行方：由用户内部的第一道防线（即业务和风险所属部门）执行。
- 性质：缺乏独立性，此评估类型被视为“不合规”，仅在特定过渡期或特殊情况下临时使用。

2. 独立评估（合规路径）

此为满足 Swift 合规要求的标准路径，包含两种执行模式：

- **独立外部评估**
  - 执行方：由独立的第三方专业安全评估机构执行。
  - 机构选择：建议从 Swift 官方提供的客户安全计划（CSP）评估服务提供商名录中选择，这些机构及其评估员均通过 Swift 的资质验证与认证考试。
  - 优势：专业机构（如 atsec 信息安全等名录内成员）能提供高可信度的评估报告，并凭借其丰富经验帮助客户切实提升安全状况。
- **独立内部评估**
  - 执行方：由机构内部独立的第二或第三道防线部门（如风险、合规或内审部门）执行。
  - 核心要求：必须确保评估部门在组织和职能上独立于批准认证的第一道防线（如 CISO 办公室）。评估人员需具备相关的网络安全评估经验及专业认证。

3. Swift 强制外部评估（特定情况）

- **执行机制：**Swift 每年会随机抽取一部分用户，强制要求其进行外部评估。
- **硬性规定：**在此情况下，必须指定选择有资质授权的第三方外部评估机构，内部评估不再被允许。
- **机构选择：**用户可自由选择合适的外部评估机构（但不能与现有认证的评估方相同），官方名录可作为重要参考。

综上所述，为确保认证顺利通过并有效提升安全水平，用户应优先选择 Swift 官方名录中的认证评估机构（如 atsec）进行独立的外部评估。

atsec 具有多年的独立的安全评估经验，且在产业内具有较高的品牌认可度；结合上述经验，atsec 具有完整且适用于金融机构的合规和评估方法论。

5.2 Swift 评估步骤

5.2.1 评估流程六步法

根据产业最佳实践，评估过程遵循结构化的六步流程，确保全面性和一致性，详细的评估流程图参见如下：

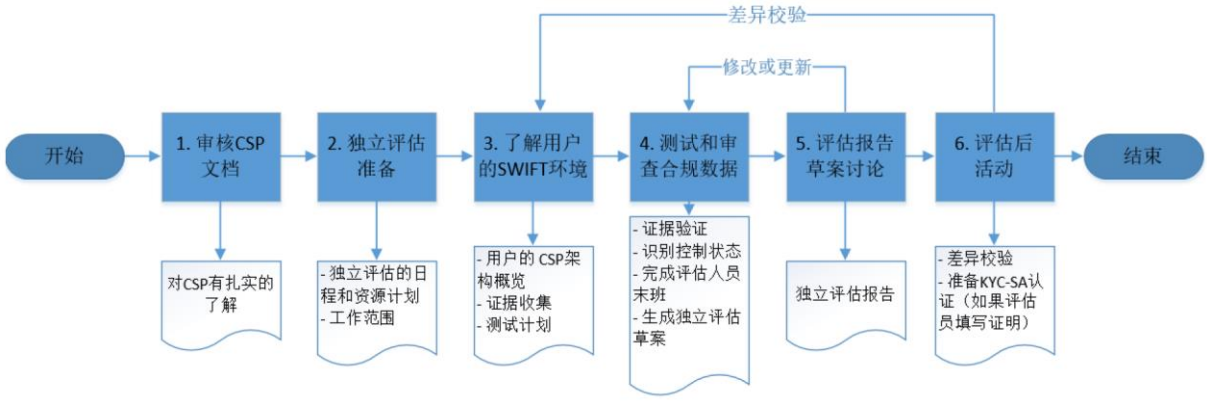

图 3：评估流程图（图片源自独立评估流程指南）

步骤一：准备与规划

- **审阅客户安全计划（CSP）文档：**评估师必须精通客户安全控制框架（CSCF）、独立评估框架等核心文件。
- **准备独立评估：**
    - 确认用户的架构类型（A1-A4, B）。
    - 明确评估范围（所有生产、灾备环境）。
    - 制定详细的评估计划与时间表。
    - 决定是否依赖往年评估结论或其他第三方报告。

步骤二：理解用户环境

- 收集并审阅架构图、配置文件、流程文档等证据。
- 访谈用户的业务和技术管理员，了解报文流和控制措施。
- 制定详细的测试计划。

步骤三：测试与审阅

- 执行测试计划，综合运用访谈、观察、检查、重新执行等方法。
- 使用评估模板记录每个控制措施的合规结论。
- 采用基于风险的方法，关注控制目标而非死板对照检查清单。

步骤四：出具报告

- 生成评估报告草稿，并与用户召开结项会议，讨论评估结果。
- 解决分歧，获取用户对最终结论的正式签批。
- 出具最终评估报告和完成函。

步骤五：评估后活动

- 用户根据最终报告，于 30 天内在 KYC-SA 平台提交或更新其安全声明。
- 所有评估证据和工作底稿需安全保存 5 年。

步骤六：监督与质量保证

- Swift 会对认证评估师进行服务监督，可能抽查评估报告以确保质量。

5.2.2 关键概念与要求

评估师资格与独立性

- 独立性：必须独立于所评估的 Swift 环境运营团队（第一道防线）。
- 资质：
    - 首席评估师必须持有行业认可的网络安全认证（如 CISSP，CISA，PCI DSS QSA，ISO/IEC 27001 主任审核员等）。
    - 必须具备近期相关的网络安全评估经验。

基于风险的方法

- 评估应关注控制是否实现了安全目标，覆盖了范围内组件，并缓解了风险驱动因素。
- 客户安全控制框架（CSCF）中的实施指南是建议性而非强制性的，用户可以采用替代方案，只要其能同等满足控制目标。

5.3 Swift 评估交付

- **正式评估报告**
    - **性质：**核心交付物，详细记录了评估的全过程和结果。
    - **必须包含的内容：**
        - 用户公司名称、BIC（Business Identifier Code）和地点。
        - 评估类型、目的和所依据的客户安全控制框架（CSCF）版本。
        - 评估方信息和评估团队成员。

- 评估起止日期和报告签发日期。
- 用户的架构类型、覆盖的环境和组件范围。
- 每个适用的控制措施的合规性确认，并说明结论是如何达成的（例如：通过测试、依赖往年评估等）。
- 需要整改的已发现缺陷的概述。

- **完成信函**
  - **性质**：一份总结性信函，由首席评估员或评估机构代表签署。
  - **内容**：确认评估方被用户任命，以评估其针对特定版本客户安全控制框架（CSCF）的控制措施合规水平。
  - **语言**：必须使用英文或经过正式翻译。
- **更新后的 KYC-SA 安全认证**
  - **性质**：评估结果的最终体现，在 Swift 网络中公开给交易合作方和监管机构。
  - **内容**：必须准确反映评估报告中的合规性结论。对于不合规的控制措施，需选择“我将在<日期>前遵守”或“我不遵守”。

5.4 Swift 评估结果的有效期

5.4.1 基本有效期原则

- **评估结论可被下一年度沿用**：同一评估结论最多可支持连续两个年度的认证周期。例如：2024 年完成的评估结论可用于支持 2024 年和 2025 年的认证，但不能用于 2026 年。
- **必须每两年重新评估**：Swift 客户安全计划（CSP）需要每年度进行安全评估，而且每两年必须进行一次完整的重新评估。

5.4.2 沿用评估结论的条件

若要沿用上一年度的评估结论，必须同时满足以下条件：

- **新版客户安全控制框架（CSCF）未对控制目标等做实质性变更**：当前评估所依据的客户安全控制框架（CSCF）版本，相较于上一次评估时，没有对该控制措施的控制目标、范围内组件或风险驱动因素造成实质性变更。
- **用户端控制设计或实施无重大变更**：在用户的架构、配置、设计或实施方法中，没有发生任何会影响到该控制措施有效性的重大变更。

5.4.3 依赖其他报告

- **Swift 评估结果可依赖其他保证报告**
  可接受符合条件的外部认证（如 ISO/IEC 27001、NIST、PCI DSS）或内部独立部门报告，减少评估范围。
- **条件**：必须准确审阅报告所覆盖的控制范围定义（包括控制目标、范围内组件和风险），确保其与所要支持的客户安全控制框架（CSCF）中的控制定义完全相同，但其覆盖周期不得超过提交认证前的 18 个月。

5.5 评估的价值

Swift 用户通过合规评估的主要价值如下：

- **满足强制性要求**：所有使用 Swift 网络用户必须每年完成合规性评估并提交结果，无法达到该要求可能会导致被 Swift 通报甚至中断服务，故而机构必须完成独立评估以达成合规认证（自评估视为无效）。
- **降低金融犯罪风险**： 通过实施 CSP 的控制措施，能有效防范诸如商业邮件欺诈、未授权交易、数据篡改等高发且高损失的金融犯罪。
- **建立信任与透明度**：一旦发生安全事件，金融机构的声誉将遭受重创。成功通过 CSP 评估并向合作伙伴证明自身的合规性，是维护市场信心和客户信任的强力凭证。
- 评估类型及是否采用认证评估员均在 KYC-SA 中公开，增强对交易合作方与监管机构的透明度，进而提升整个 Swift 生态系统的信任基础。

- **优化成本与效率**：用户可通过沿用往年合格控制的评估结论、采纳符合条件的外部保证报告（如 ISO/IEC 27001、PCI DSS），以及采用混合评估模式，显著减少重复工作，灵活控制评估成本。atsec 积累了诸多不同体系和标准评估的方法论，可以协助金融机构更好的实现体系融合。
- **保障评估质量与一致性**
    - 认证评估员受 Swift 定期监督，确保评估过程与结果的专业性及可靠性。
    - Swift 提供标准化模板与指南，统一评估流程与输出，帮助用户明确评估范围与合理定价，确保评估结果符合预期。
- **增强用户信心与决策便捷性**
    - 使用经认证的评估员本身即是对其专业能力的信任背书，该信息在用户合规证明中明确体现，可以有效增强用户对所选服务商的信心。
    - Swift 官网公开认证评估机构与人员名录，提高信息透明度，简化用户的选择决策过程。

6 结语

通过本文的阐述，我们可以看到，Swift CSP 体系不仅仅是一套强制性的合规要求，更是一个全面提升金融机构网络安全防御能力的战略性框架。从精准界定自身的架构类型，到深入理解并落实 CSCF 中的每一项安全控制，再到通过 KYC-SA 平台完成透明的合规声明，这一过程本身就是一次对自身安全状况的全面审视与升华。

面对不容松懈的网络安全形势，满足 CSP 要求已从“可选项”变为“必选项”。一次成功、严谨的独立评估，不仅是打开 Swift 网络合规运营的“钥匙”，更是向交易合作方、客户和监管机构传递信任的“信号”。它有力地证明，您的机构已经建立了符合全球公认标准的安全保障，能够有效地抵御和应对潜在的网络威胁。

作为 Swift 官方认可的评估机构，atsec 深刻理解这一体系背后的安全逻辑与评估精髓，atsec 持续关注 Swift 产业动态，积极参与每年度标准演进发展相关的培训和考核，并形成自身的评估方法论，为全球的金融机构提供 Swift CSP 安全评估服务。我们相信，通过社区各方的共同努力，持续加固 Swift 环境的安全基线，能够共同构建一个更具韧性、更值得信赖的全球金融生态系统。如果您在 Swift CSP 的合规之旅中需要专业的支持与指引，atsec 团队时刻准备着，以我们深厚的技术积淀和严谨的评估经验，为您保驾护航。

A 参考资料

(i) https://www.atsec.com

(ii) https://www.swift.com

(iii) Decision Tree (16 October 2025)

(iv) Swift Customer Security Controls Framework - Detailed Description v2025 - 1 July 2024

(v) Independent Assessment Framework - Detailed Description v2025 - 08 July 2025