指南

评估网络安全对手方风险

入门指南

目录

资格和限制条件

本文为 SWIFT 用户提供了一个综合且不具约束力的指南，旨在让金融服务生态圈内的用户了解如何使用和理解对手方所提供的网络安全数据信息。本文件就推荐的治理办法以及分享网络安全数据和将网络安全风险数据整合入机构现有的风险管理框架内的流程提供建议。

但它并不针对用户的具体问题或要求。

本文件中的信息并未详尽列出，它并不替代明智的判断或符合最佳惯例。

对于遵从该等指南或采纳该等建议后采取的任何措施或作出的任何决定以及对本文件所述数据的任何解读，用户承担完全和全部责任。对于本文件的内容，或基于本文件内容采取的任何措施或作出的任何决定或与本文件内容有关的任何措施或决定，或该等措施或决定所带来的后果，SWIFT 拒绝承担任何和所有责任。本文件的任何内容均不得解释或解读为构成 SWIFT 一方任何义务、陈述或保证。

SWIFT 发布本文件的唯一目的是提供信息。本文件中的信息可能随着时间的变化发生变更。用户必须始终参照提供的最新版本。

客户的声音

您在您对手方应用的网络风险管理体系中遇到的主要挑战是什么？

“我们遇到的一个主要挑战是访问我们对手方设置的网络控制系统。因为对每个对手方的控制级别缺乏认知，从而使网络风险管理颇具挑战。您最薄弱的环节决定了您的安全水平。这就是为什么开展对手方网络安全尽职调查如此重要的原因。

主要问题包括：

- 找到所有对手方都使用的、在做基准测试时可以利用的一致标准
- 让对手方分享关于其安全控制或缺乏安全控制方面的信息
- 核实对手方所提供信息的准确性
- 在某种程度上通过对提供有价值的风险信息的获取和处理对企业是有利的，可以使企业能理解并作出适当的业务决策
- 跟进任何问题，确保该问题得到纠正和解决，并同意在其间实施补偿性控制措施”

执行摘要

网络安全仍然是金融服务领域面临的一项主要威胁。本指南陈述银行和支付生态系统内的组织可以如何着手评估他们日常交易的对手方所带来的网络安全风险。

该指南涵盖各机构应该关注的四个方面：建立治理模型；建立网络安全风险管理框架；采用网络安全风险应对措施和融合对手方的网络安全“证明”资料。

网络安全风险（包括对手方带来的网络安全风险）需要同其他风险类型（运营、财务和监管风险）共同管理。许多机构正在努力将网络风险评估整合入其现有的对手方风险流程内。

需要完善对该过程的监管——**治理**，确保承担适当责任的人具有做决定的能力，且流程稳定并可重复。具备牢固的治理结构之后，机构可以着手实施网络安全风险**管理框架**。这包括对手方通过以下方式开展风险评估：

- 收集必要的数据，为以风险为推动因素做出的决定提供支持；
- 处理该数据并将该数据转换为可衡量的、基于风险的评估，通常以数字分数或红黄绿标示显示；
- 采用适合的应对措施，降低或“处理”风险。

机构可能具有不同的风险偏好，但是，作为示例的网络安全风险减缓措施可能包括：

- 对对手方的交易实施额外的监视级别；
- 限制与对手方进行的交易类别；
- 要求对手方实施额外的控制措施或欺诈检测措施；
- 要求对手方通过独立评估证实其信息；
- 重新评估对手方的协议和合同。

在使用该治理模型和进行风险管理过程中，机构应考虑在其对手方处于网络准备状态时融合数据。

SWIFT 引进的、作为其客户安全计划 (CSP) 一部分的客户安全控制框架 (CSCF) 在这一方面极有价值。CSCF 就针对 SWIFT 用户的一套强制性和建议性安全控制措施做了说明，确立了整个社区的安全基准。所有用户必须在其本地的 SWIFT 基础设施实施该框架，且必须自证其符合强制性安全控制措施。

一旦出具了自证声明，用户可以将该声明提供给其任何对手方，证明其符合每一项控制措施——同样地，对手方可以要求相互提供该声明。用户可以查看和按对手方或批量导出该数据，更好地“**获取**”数据和将数据整合入其基于风险的决策框架。

CSCF 有助于提高社区的透明度和标准化，更好地使组织将网络安全整合入其决策制定过程。该证明资料信息量庞大，是 SWIFT 用户网络安全风险数据的唯一来源。

背景

网络安全和欺诈始终是全球最大威胁。威胁行为人的老练程度正在提高，庞大的数据库是常见的受威胁地点，而对于高级持续性威胁 (APT) 网络攻击而言，实质上，任何人都有可能成为攻击目标，而有了“物联网”，无处不在的“智能”设备可用作 DDoS 武器。

在金融服务领域，该等威胁行为人通过精妙的网络安全攻击带来威胁，而在该等网络安全攻击中，罪犯的主要动机是**资产盗窃**。

但是，银行和支付生态系统内的组织自然不会在与外界隔绝的环境下运营 —— 他们每日与无数的对手方互动和交易。因为小数量精妙的、资金充足的威胁行为人继续对 SWIFT 客户进行网络攻击，所以风险确实存在。**组织该如何看待和处理他们可能正在与毫不知情的网络攻击受害人进行交易这一潜在风险呢**？若该风险未处于管理当中，且资金发生损失，财务风险可能很大。

本指南研究组织可以如何着手评估其对手方带来的网络安全风险，涵盖四个关键领域：

- 建立网络安全风险管理治理模型；
- 建立网络安全风险管理框架；
- 采用网络安全风险减缓措施；
- 包含 SWIFT 对手方的网络安全证明资料。

本文件剩余部分讨论该等四个主题。

客户的声音

网络安全证明资料是否已帮助您解决一项或几项此类难题，若是，那么如何帮助解决的？

“SWIFT 的客户安全鉴证过程是对我们整个成员管理计划的补充，有助于解决该等难题。通过收到的证明资料，我们现在有能力了解对手方实施的控制级别。理解各对手方实施的控制类型和控制级别之后，我们更适合开展网络风险管理。

SWIFT CSP 已为我们提供了一套所有对手方使用的、做基准测试时可以利用的一致响应措施。它之于我们，就像 SAT 测试之于大学招生团队。使用鉴证工具请求和同意访问对手方，非常简单。SWIFT CSP 计划为对手方提供了一种让对手方的回应获得内部和/或外部审计证实的手段，从而帮助提高我们对对手方回应的信任级别。我们开发了一种定量模型，获取来自鉴证工具的数据并生成报告和图表。”

建立网络安全风险管理治理模型

网络安全风险（包括对手方构成的网络安全风险）需要同其他风险类型（运营、财务和监管风险）共同管理。

应完善对该风险管理过程的监管——治理，确保承担适当责任的人具有做决定的能力，且流程稳定并可重复，例外情况能够得到管理。

高级委员会组织

网络安全风险治理应被视为一项整体职能。这意味着，它应由整体负责业务的人进行集中监管，而非局限于 IT 或运营部门内孤立的后勤支持部门。在实际操作中，对手方风险管理层应属于**高级委员会组织（例如风险委员会）**的一部分（或子集），拥有其自己的授权和充分资源。

在该跨部门治理中，也应考虑在“3 道防线”之间分配责任。在实际操作中，这意味着应在第一道防线（例如业务、运营、IT/网络部门）作出日常运营风险决策，因为其负责执行内部控制和运营程序。应在第二道防线（例如合规、风险部门）管理例外情形和逐步升级的情形，因为其具有一定程度的运营独立性。第三道防线（例如内部审计部门）监督风险保证情形，因为其独立于其他部门。

以业务为推动因素的利益相关人

应由具有充分资历、有权限作出影响适当的内部利益相关人小组的决策的个人发挥治理职能。

可以认为，很多关于对手方管理的日常运营风险决策应由**业务人员**而非仅由技术或网络安全人员推动。但是，总体治理应为全局性的，并包括来自以下部门的代表：

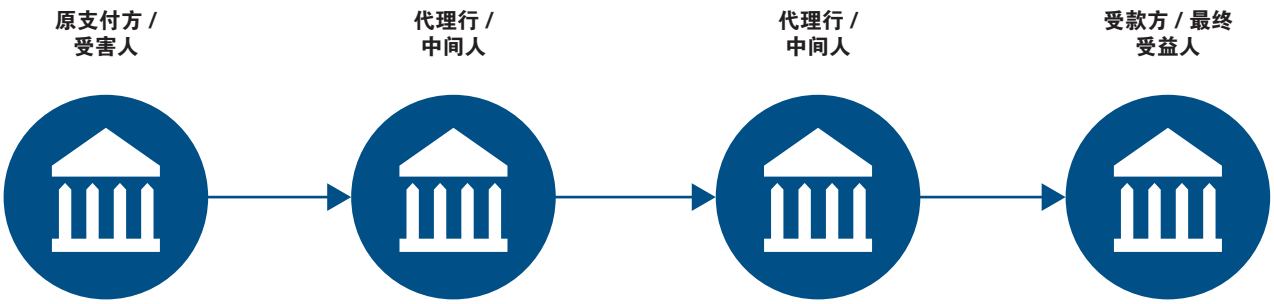
- **业务**和对手方密押关系，目的是评估市场和对手方风险以及与对手方联络；
- **支付运营部门，**目的是实施运营控制、调整限额和干预正常的处理操作；
- **技术部门，**例如 IT/信息安全/网络安全部门，目的是要求实施额外的技术控制措施或特定的欺诈检测措施；
- **风险、合规和审计部门，**目的是管理例外情形以及承担独立保证职能。

由于数据的敏感性和安全漏洞的潜在影响，应由高级管理人员监督该过程，且该高级管理人员应帮助推动风险评估和升级流程，并监督由此作出的应对决策。

明确的命令

监督对手方风险的高级委员会应具备说明长期战略以及日常运营模型（包括职务和责任）的明确命令或职权范围。
该命令也应包括需要就对手方风险范围、具体事件和进展情况以及发展趋势向董事会和高级管理层定期汇报。

网络安全对手方风险评估框架



本指南旨在：

- 收到原支付方指示的**小中型企业**。与拥有多个对手方关系和复杂的内部组织结构的较大型机构相比，该等小中型企业的对手方数量有限。
- 担任原支付方和最终受益人交易中间人的**代理行**（不考虑其规模）。

客户的声音

您能否说明一下，除了在工具内提交您的自证证明之外，您具体如何使用网络安全鉴证资料；更准确地说，您如何在您对手方的安全风险管理背景下使用他们。

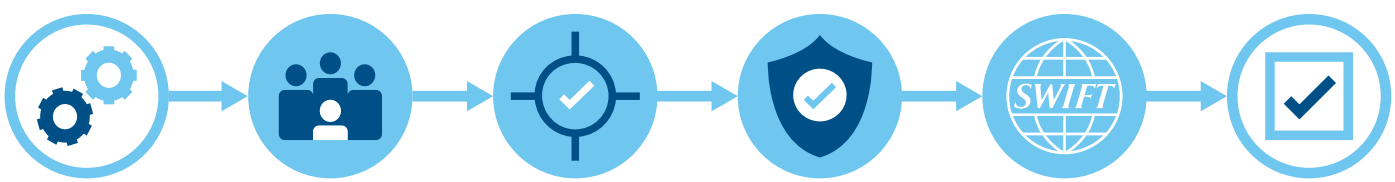
“该证明工具提供一致的响应，所以我们能够评估每项证明和基于反馈应用一个数值。这让我们能够为每项证明重复运用定量和定性测量方法。之前，我们仅依赖问卷，在很多情况下，问卷提供的回应不一致。”

建立网络安全风险管理框架

具备牢固的治理结构之后，机构通常将从风险角度着手处理网络安全。这意味着，他们评估风险级别和将预算用于最需要的地方，并接受低于风险临界值或风险偏好的风险。该网络安全风险管理流程或框架包含几个步骤：

1. **收集必要的对手方风险数据；**
2. **处理数据，评估风险级别。这通常以获得一个总评分结束，然后将该总评分与公司风险偏好级别对比；**
3. **根据该风险评分实施合适的办法，管理或“处理”风险。**

网络安全对手方风险评估框架



建立网络安全风险管理**治理**模型

建立网络安全**风险管理**框架

采用网络安全风险减缓**措施**

融合来自 SWIFT 对手方的网络安全**鉴证资料**

对手方风险数据

机构收集和处理各种数据，以从网络安全角度，帮助确定对手方风险预测。

该风险数据大体上分为三类：与对手方运营所处的外部环境相关的数据，说明与对手方之间的业务关系的数据，以及交易数据：

1. 与对手方运营所处的外部环境相关的风险

- **运营所在国/地区**——可作为对手方运营所在地所属司法管辖区的网络安全级别、法规和犯罪/欺诈的衡量标准。这可以使用可公开获得的资源（例如 Basel AML 风险报告）进行评估；
- **产业类型**——可以与被攻击的可能性做关联对比，因为与其他领域相比，一些领域遭受网络安全攻击和数据漏洞的频率更高；
- **对对手方的监管程度**以及当地监管机关实施网络安全法规或政策的范围。

2. 关于与对手方之间的业务关系的风险

- **对手方关系的深度 / 长久度**——与长久、深厚和受信任的关系相比，较新的关系可能具有更高的风险；
- **对手方的规模 / 所有制结构**——可以与预算、应对威胁的熟练资源和工具的可获得性作关联对比，尤其是，如果属于较大型集团的一部分时，例如全球系统性重要银行(GSIB)；
- **已知的网络或安全事件**或其他可以得到的新闻、信息或尽职调查资料；
- **对手方的现有风险评估，**例如运营、财务或规章方面。

3. 与交易相关风险

- **交易类型**——限制与对手方所进行交易的类型，因为某些交易类型天生比其他交易类型更易受攻击，例如凭单付款；
- **交易价值**——作为信用风险暴露的表现；
- **交易频率**——每期交易量越大，潜在攻击面就越大。

收集该对手方数据之后，即可应用风险评估流程。

风险评估流程

收集了对手方数据之后，机构即进行处理并将其转换为基于风险的评估。本评估方法可能因机构不同而不同，但是基本上遵循以下三种方法之一：

- **基于专家的**——评估是由专家的判断和专业人员对风险进行定量评估推动的；
- **基于规则的**——通过决策树，利用关于对手方在每个风险因素方面的评分的简单规则，作出评估；
- **基于模型的**——基于对手方在每个加权风险因素方面的评分，从而分析得出的评估。

无论采用哪种方法，对手方通常获得一个总评分，以红、黄或绿色指示器表示。

风险减缓措施取决于本评分与内部风险偏好的对比情况。例如，若对手方评分低或为绿色，可能被划分为不需要额外监视，但是若对手方评分高或为红色，可能成为风险减缓措施的实施对象。

采用网络安全风险减缓措施

该风险管理框架可以让机构评估和划分与对手方相关的安全风险程度。然后，机构可以决定接受风险或考虑采取风险减缓措施。

网络安全风险减缓措施可能包括：

1. 关于与对手方之间的业务关系的应对措施

- 主动**联系高级管理层**，以加强关系和提供总体保证；
- 要求对手方通过内部或第三方/外部独立评估或通过提供技术规范文件或测试结果**证实其信息**；
- 要求对手方实施**额外的控制措施**或**欺诈检测**措施；
- 重新评估对手方的**协议和合同**，包括“规避”对手方风险以及更改或终止合同的可能性。

2. 关于更严格地治理与对手方的交易的应对措施

- 对超出**事先确定的临界值**的交易做审查标记。这包括交易类型、交易值、交易币种或最终受益人的资料；
- 对于所有标记过的交易，实施**额外监视**，例如与对手方的交易受两人的监督和/或经双方确认。

以上应对措施并未穷尽列明，机构可能还有可以利用的其他控制措施和工具帮助管理风险。

对高风险对手方运用应对措施

对于高风险对手方，机构可能希望结合运用以上任何应对措施。通常情况下，机构将希望运用额外监视措施，监督超出预先确定值或临界量的付款指令。机构应有调整临界值的能力，也应具备处理增加的警报数量的工具和能力，以及人工处理交易的其他精力，包括需要最新的对手方联系信息。

所增加的监视措施不必为永久性的。对手方被重新划分为“低”风险类别之后，例如因为他们遵守额外的应对措施，即可更改或移除临界值。

除了实施风险减缓措施的任何决定，各机构仍单独和专属负责全部或部分更改、中止或终止与对手方的关系。

一旦建立网络安全风险管理流程，治理组织结构定期审查对手方，评估其风险预测是否已发生改变，是一项审慎的决定。

客户的声音

网络安全证明资料如何输送入网络风险管理之中，以及围绕这一点成立的治理机构有哪些？

“向我们的首席风险官和其他风险部门提供周报。我们追踪所同意证明的数量，并将其与未解决的请求数量相对比。对于同意的证明，我们对每项证明进行风险评级，然后在定性预测中应用每项经过评分的证明。我们的风险部门已经开始将预测结果融入其准则内。”

附件 A：包含 SWIFT 对手方的证明资料

2016 年 5 月发布的 SWIFT 客户安全计划 (CSP) 支持所有 SWIFT 用户类别增强其与 SWIFT 相关的本地基础设施的安全。

SWIFT 的客户安全控制政策 (CSCP) 界定了用户证明流程以及相关原则、职务和责任。SWIFT 也制定了客户安全控制框架 (CSCF)，该框架确立了针对整个用户社区的强制性和建议性控制措施的安全基准。

CSCP 政策要求用户对**强制性安全控制措施**的合规情形进行自证证明，还鼓励他们对建议性控制措施的合规情形进行自证证明。他们证明合规级别，而且他们的**证明**通过 SWIFT 提供的 KYC - 安全证明 (KYC-SA) 应用程序予以公布和管理。

KYC-SA 工具提供的一个关键功能是，能够让机构与其对手方按照共同协议，通过**“请求”和“同意”访问**交换证明资料。在这种情况下，机构可以评估对手方风险，然后根据证明的合规级别作出关于对手方风险的决策。本证明资料信息量庞大，是网络安全对手方风险数据的唯一来源。

因为机构开始将 CSP 证明资料整合入其对手方风险框架，所以应考虑数个因素：

- 对治理模型的考量；
- 对风险管理框架的考量；
- 更多风险减缓措施选项。

以下是在 KYC-SA 工具的整体背景下，对该等三个考量方面的讨论情况。

证明用户对用户的证明结果承担唯一责任且 SWIFT 并不核实用户证明结果的正确性，强调这一点非常重要。设计 CSP 的目的是建立所分享安全信息的**标准化**和**透明度**水平，之后，该标准化和透明度水平可由 SWIFT 用户使用。

请注意，附件 B 包含 CSCF 框架和 CSCP 政策文件的链接。

附件 B 也包含 KYC-SA 用户指南的链接，该用户指南就如何请求 / 同意访问证明资料以及如何按 excel 文件导出证明资料分步骤提供了分步的详情。该证明资料可由组织的安全官按对手方导出，或将所有相关对手方的证明资料批量导出。但是，该等指南未说明组织该如何利用数据，即分配治理、处理数据、评估风险和安排应对措施。该指南概述如下。

客户的声音

关于同意对手方访问您证明资料，有什么治理措施？ 是否属于共享责任（例如风险部、合规部、法律部等之间）？

“关于同意对手方访问我们的证明资料的治理流程需要多个团队的参与。确保同意访问我们证明资料这一过程的透明度。我们拥有一个内部工作流审批流程。一旦获得内部批准，行政管理团队利用证明工具同意访问。”

治理模型的考虑因素

在决定分享证明资料或请求他人分享其证明资料之前，应确定利用对手方证明资料的整个过程。这尤其需要包括将如何分享，以及什么人应该发挥什么作用。

尽管 SWIFT 提供了技术平台，机构的治理模型也需要调整，为评估对手方的安全证明资料提供支持。应考虑由机构范围内的适当代表“同意”或“请求”访问证明资料，该数据应视为机构现有对手方风险管理框架的额外元素。

同意（或拒绝）访问对手方

为了同意请求对手方访问，治理模型需要清楚地识别管理“是”或“否”审批决策流程的业务所有者。若没有明确的“同意人”，收到的证明请求将被搁置，不予答复。

用于同意所收到请求的审批决策标准应通常由风险委员会等高级委员会组织或 CISO、总法律顾问或首席合规官等高级管理层签字批准。

“同意人”使用的同意对手方访问的决策标准示例

- 将与全球交易银行共享证明资料，无论其位于何处
- 将与位于同一地域，受同一规管机构监管的对手方共享证明资料
- 一旦我们可以报告我们由外部评估或审计机构支持的“证明类型”，将共享证明资料
- 将与同我们保持积极通信关系的所有请求对手方共享证明资料
- 将与也同我们机构分享其证明资料的请求对手方共享证明资料
- 将与所有请求对手方共享证明资料

高级委员会组织或高级管理层应签字批准该决策标准。签字批准之后，中级管理层可以将此标准应用于收到的请求中，为技术操作人员提供决策，同意或拒绝访问请求。

例外情形应上报至高级委员会组织或高级管理层。

在操作层面，操作人员（或“同意人”）应定期（例如每周一次）向管理层提交一份有关所收到请求的概述并汇报采取的措施。

同意访问的流程示例

1. 向操作人员分配“同意人”角色
2. 操作人员收到对手方的访问请求
3. 操作人员比照审批标准审阅该请求，并作出肯定或否定回答的建议
4. 中级管理层审阅该建议，许可执行、提供替代性决策或上报至高级管理层
5. 操作人员“同意”或“拒绝”对手方请求。在拒绝访问请求时，操作人员应提供拒绝的理由。这可能包括与对手方之间没有业务关系或此时未准备好共享证明资料
6. 操作人员定期（例如每周一次）提交关于状态请求概述和措施的报告

证明工具还提供设立符合高级管理层所确立标准的对手方 BIC “白名单”工具。如此会实现经请求自动同意访问该等对手方，从而避免了人工审阅和批准流程。这一功能被称为“自动同意”。

向对手方请求访问权限

高级委员会组织或高级管理层应签字批准同意对手方访问的标准。也应由类似层面决定对手方证明资料的请求标准。

“请求人”请求访问对手方数据所使用的决策标准示例

- 我们将向我们的所有对手方请求证明资料
- 我们将仅向我们不定期互动的对手方请求证明资料
- 我们将仅向位于高风险地区的对手方请求证明资料
- 我们将仅向已被视为高风险的对手方请求证明资料

一旦高级管理层确定了决策标准，证明请求会由操作人员（“请求人”）通过证明工具执行。

访问对手方证明资料的请求的状态应定期（例如每周一次）汇报至管理层 —— 与关于同意对手方访问的状态报告类似。

请求访问权限的流程示例

1. 向操作人员分配“请求人”角色
2. 高级管理层确定对手方证明资料访问请求决策标准
3. 操作人员通过证明工具向对手方发出请求
4. 对手方“同意”或“拒绝”访问请求。若请求被拒绝，高级管理层应考虑与对手方进一步联络，在拒绝原因消解之后再次请求访问
5. 操作人员定期（例如每周一次）提交关于状态请求概述和措施的报告

客户的声音

在被同意访问对手方证明资料的过程中，您收到的任何信息中是否存在任何令您作出重大的网络安全决策的信息？ 若是，您能否详细说明？

“在被同意访问对手方的证明资料之后，我们查看控制措施的响应情况。尽管我们未基于对手方的证明作出网络安全决策。对手方的响应推动我们围绕网络感染开展内部对话。”

风险管理框架的考虑因素

被同意访问对手方证明资料的组织可以使用该工具“利用”该数据。此证明资料包含每项控制措施的合规水平，应被整合入该组织以风险为基础的决策框架，帮助管理对手方带来的风险。

希望将网络安全证明资料嵌入其现有的风险管理流程的机构可能希望基于该信息运用加权和评分。

对加权和评分作有意义的分配是一项非常详细的工作，机构应确保内部利益相关人就此相互协作，例如信息安全、运营、技术、风险、合规、业务和法律部门的利益相关人。

加权和评分方法示例

- 若对手方未作证明，应予以评分
- 若对手方未回应 KYC-SA 访问请求，应予以评分
- 对各项 CSCF 控制措施的合规水平应予以评分：例如，对指南的合规情形、替代方式的合规情形、不合规情形或未来截至规定日期的合规情形
- 每项具体（强制性或建议性）控制措施的权重分配可能不同
- 其他证明变量可能享有特殊权重，例如：
  - **基础设施类型**
  - **基础设施构成部分**——该对手方是否使用经验证的界面？
  - **服务供应商**——该对手方使用是否通过服务供应商链接以及该供应商的证明或合规状态如何？
  - **评估类型**——该对手方是否雇用了内部或外部第三方提供建议，或者其证明是否经内部或外部独立评估证实？见下文

解释“评估类型”

自证证明中的该字段记录对手方使用独立审查人证实其所宣称的合规级别的范围。

– **第三方独立评估（可能包括外部审计人的审计）**——机构通过使用独立外部评估人证实控制合规情况。其名称必须由证明机构宣布。 – **内部独立评估（可能包括内部审计）**——机构通过使用内部评估人功能证实控制合规情况。	可能容许较高程度的合理保证，即对每项控制措施的合规情况得到独立证实。可能暗示可以提供此保证水平的对手方有较高的信任级别。允许核查该外部评估人的名称。
– **外部事务所进行顾问复核**——机构在其合规评估中聘用第三方提供咨询服务。第三方的名称必须由证明机构宣布。 – **内部独立团队进行顾问复核**——机构在其合规评估中聘用独立内部方提供咨询服务。	可能在独立核实所列控制状态时给予一定的信任度。固定的、事先确定的框架不执行咨询性评估。若出具和提供完整的评估报告，信任度可能更高。可使用特定的评估或样本检查补充。
– **自我评估**——机构对其输入情况进行自我评估，例如通过 CISO、CRO 或其他管理人员签字批准。	可能确立最低的信任度，即对手方已经彻底评估其对 CSCF 控制措施的合规情况。

额外风险减缓措施

除了第 4 条列出的一般性应对措施，可考虑包括专门与 SWIFT 的使用相关的数个其他选项，如下所示。

要求符合建议性控制措施

除了已有的强制性措施合规情况自证证明义务，机构可能希望要求一些对手方也自证证明其对一些或所有建议性控制措施的合规情况。

对手方使用欺诈检测措施

SWIFT 用户可能希望要求一些对手方实施欺诈检测功能，寻找未表现出正常行为模式的异常行为或无关项。该措施目前在 CSCF (2019 版本) 中被界定为咨询性控制措施。

示例：SWIFT 每日验证报告 (DVR)

作为 CSP 计划的一部分，SWIFT 添加了一项交易模式检测工具，从而扩大了其金融犯罪合规服务产品组合。其设计目的是降低与付款欺诈相关的风险。

每日验证报告 (DVR) 使机构轻松验证支付交易活动、强调潜在风险以及发生欺诈事件时快速应对。

DVR 提供前一日付款活动的相关信息。每日的交易值和交易量总额与用户在过去 24 个月的日均值和日均量相对比，可以快速识别和了解任何重大活动变化。

涵盖两个关键领域：

- 活动报告可以让用户看到他们的日常活动合计情况——日常活动合计情况按通信类型、币种、国家和对手方提供。提供日总值和总量以及最大额交易的详细情况。
- 设计风险报告的目的是突出可能预示存在欺诈风险的大型或不寻常的消息流。它帮助用户挑选其看到的与收款和付款对手方之间的最大单项交易和最大合计交易流。与之前的日总值和日总量相对比，让用户评估活动变化。风险报告也强调该日交易的直接或间接对手方的任何新组合。

就以下关键 SWIFT 通信类型整合信息：
MT 103、MT 202、MT 202COV、MT 205 和 MT 205COV。
DVR 发布于 2016 年。

示例：SWIFT 付款控制服务 (PCS)

付款控制服务 (PCS) 尤其注重帮助 SWIFT 用户检测正在进行中的异常活动。PCS 实时检测对手方政策以外或不具特征性且暗示存在欺诈风险的付款。是在带外开展的，即远离用户地点。这意味着即使机构遭受损害，数据仍然可靠。

PCS 通过两个实时操作模式之一运行，使用订阅者确定的政策规则：

- 报文抄送和提醒，或
- 报文保留和提醒

其核心是，PCS 让用户为多个参数配置政策规则：

- 业务日历、非营业日和正常营业时间
- 币种白名单 / 黑名单，单次和累计付款限额
- 国家白名单 / 黑名单，单次和累计付款限额
- 国家、币种、单个实体或集团联合体的阈值
- 新机构：根据过去的报文流，识别向新参与人或链的付款
- 可疑账户：对照机构认为存在高风险的账号黑名单核实终端客户账号

PCS 发布于 2018 年 10 月。

请注意，机构实施接收人欺诈控制措施之前或机构请求对手方实施发送人欺诈控制措施之前，应审查条款和条件以及其他法律考量因素。

改善关系和应用 RMA

几年前建立的关系可能随着时间发生变化，不符合今日的业务模式。除了控制谁可以通过密押关系 (RMA) 发送消息，SWIFT 用户还可以限制通过 RMA+ 发送的消息类型。例如，用户可以同意接收理财或贸易消息但不同意接收付款消息。

示例：SWIFT RMA 和 RMA Plus

密押关系 (RMA) 是两个金融机构之间的关键交流和授权过程，能够让机构界定哪个对手方可以向其发送 FIN 消息。任何不需要的流量均可以在发送人层面被封锁，降低处理不需要的消息所带来的操作风险。

RMA Plus 是 RMA 的更精细版本，比 RMA 更进一步，可以让机构说明其想要发送和想要从其每个对手方处收到的消息类型。例如，机构可能仅希望收到某个代理行的信用证。

为了收到其对手方发来的消息，机构需要授予该等对手方 RMA 或 RMA Plus 授权，而且 RMA 功能内置于 Alliance Access 和 Alliance Entry SWIFT 界面。

随着时间的推进，很多机构已经和很多对手方建立了很多 RMA 关系。但是，当业务关系发生变化或终止时，RMA 授权名单可能不会始终更新。因此，机构可能存在大量的不活跃 RMA —— 机构可能甚至不知道他们的存在。

通过合理化和撤销休眠或不活跃的 RMA，机构能够使有关该等活动的时间和成本最小化并降低风险。

机构能够自己承担此项合理化任务。作为可供选择之一，SWIFT 提供 RMA “清除”和 RMA Plus 授权服务。

RMA 发布于 2009 年

附件 B：词汇表

术语	缩略词	说明
SWIFT 客户安全计划	CSP	**点击此处了解更多信息**
客户安全控制框架	CSCF	**点击此处了解更多信息**
客户安全控制政策	CSCP	**点击此处了解更多信息**
了解您的客户 —— 安全证明（应用程序）	KYC-SA	基线：**点击此处了解更多信息** 用户指南：**点击此处了解更多信息**
密押关系	RMA	**点击此处了解更多信息**
每日验证报告	DVR	**点击此处了解更多信息**
付款控制服务	PCS	**点击此处了解更多信息**
共享基础设施供应商	SIP	**点击此处了解更多信息**
业务识别码	BIC	**点击此处了解更多信息**
首席信息安全官	CISO	公司内负责信息安全、级别最高的管理人员的常见名称。

关于 SWIFT

SWIFT 是一家会员所有制全球合作企业，是世界领先的安全金融报文传送服务供应商。我们向我们的用户群提供报文传送服务平台和通信标准，我们以“方便访问，促进集成化，验证、分析和金融犯罪合规”为宗旨提供产品和服务。

我们的报文传送服务平台、产品和服务将 200 多个国家和地区 11,000 多家银行机构、证券机构、市场基础设施和企业客户连接在一起。让他们能够安全地进行通信、可靠地交换标准化金融报文。

作为客户信赖的供应商，我们促进全球和地区金融流动、推动世界范围内的贸易和商业发展；我们不懈地追求卓越运营，不停地寻找减少成本、降低风险和消除低效运营的方法。

SWIFT 总部位于比利时，其跨国治理和监督模式强化了其协作机制的中立性和国际性。SWIFT 遍布全球的分支机构网络确保其在所有主要的金融中心都能有一席之地。

若要了解更多信息，请访问
www.swift.com，或
联系您的客户经理，或
发送电子邮件至 weareswift@swift.com。

57386 – 2019 年 1 月