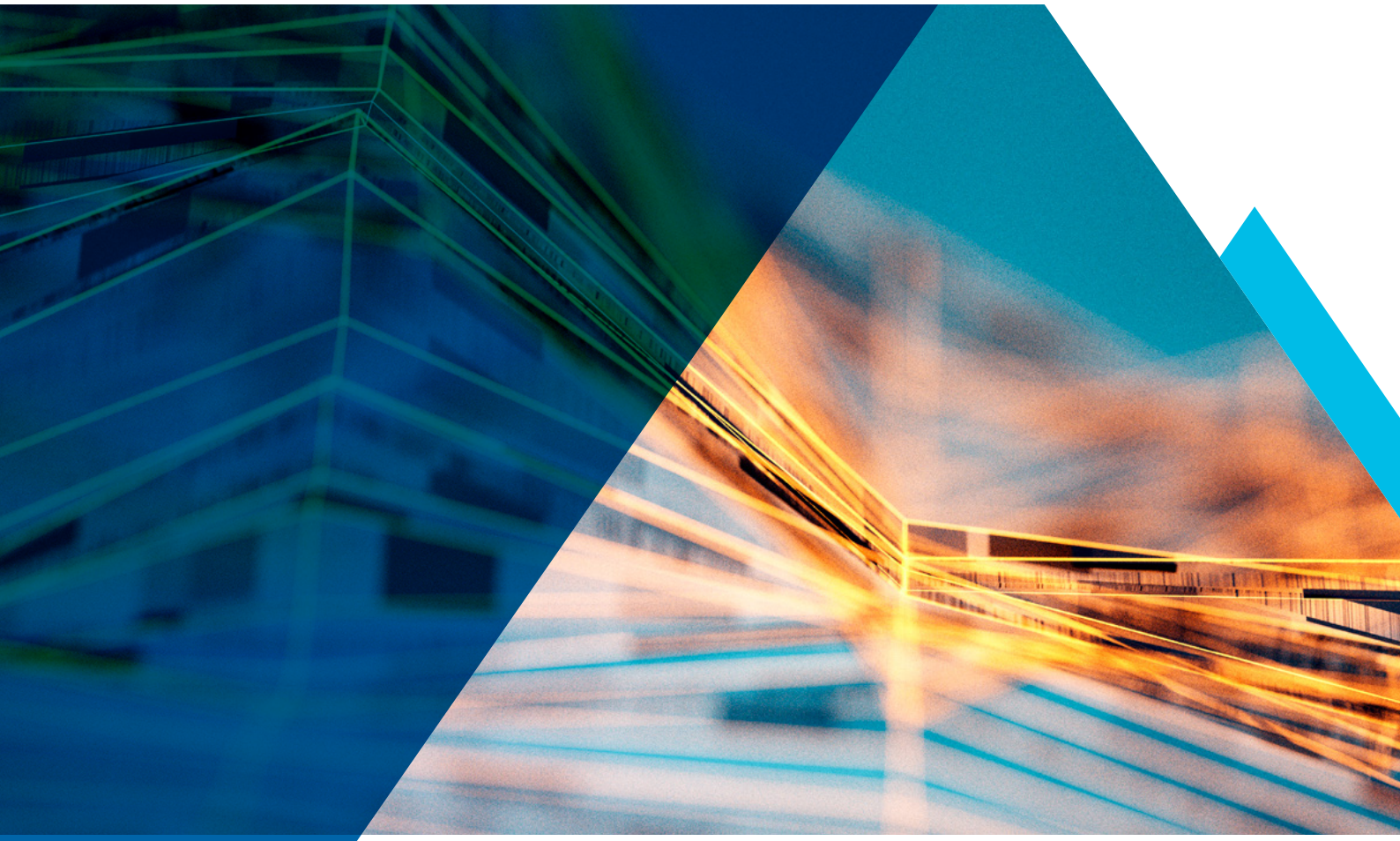

国际商会金融科技合作指南

2022年5月

目的和范围

贸易金融行业正在经历前所未有的数字化浪潮。整个贸易金融生态体系正在越来越多地通过科学技术和扩大合作，来迅速解决纸质贸易金融的局限性。金融机构和企业对包括分布式记账技术(DLT)（含区块链）、机器学习、人工智能、应用程序接口 (API) 以及技术独立的数字网络等科学技术产生越来越多的兴趣。

随着这一行业趋势的发展，贸易金融的数字化显然需要越来越多的行业参与者相互连接，并使用第三方（金融科技公司Fintechs）提供的服务/信息/数据。目前，业内大多数参与者都有自己的一套标准来进行尽职调查、交换贸易信息和引入第三方供应商。这些标准很少是一致的，而且还在不断发展过程中。从而导致第三方很难将他们的解决方案迅速商业化。

本文件旨在汇总一套通用标准，贸易金融数字生态体系中的各方可以使用这些标准以数字化的方式相互连接。这是一份动态的文件，会随着时间的推移而扩展。这些标准涵盖了第三方合作普遍考虑的事项，并力求实现一定程度的标准化，以确保服务提供商和用户之间的合作更快、更高效、更有效。主要由于《通用数据保护条例》（GDRP）、监管要求、审计、认证公司等方面的发展，贸易金融受到许多监管约束，这些约束要求银行内部部门（合规、法律、风险、安保等）履职。银行整合了这些方面，而2-5年前的情况并非如此。银行必须和客户一起处理这些方面的问题。

在第三方参与之前或期间，通常会考虑三个主要的主题标准。这些是：

1. 信息安全 **(Infosec)**标准，
2. 商业标准，以及，
3. 技术标准。

这份文件列出了在每个主题下所采用的共同考虑因素和标准。需要注意的是，这些标准仅供参考，不应被视为法律建议或咨询意见，也不应被视为已涵盖所有内容。此类第三方服务的接收者应考虑其特定情况，并寻求自己独立的财务、法律、税务和其他相关建议。

注：本文档末尾为术语表

标准

1. 信息安全 (Infosec) 标准

这些标准适用于技术供应商或服务提供商；负责向客户（*客户可能是金融服务提供商和/或企业终端用户）提供平台和相关服务的人员。更多内容详见附件1。

主题	推荐标准	说明
数据分类	• 根据信息类型对信息或数据进行分类。例如，公开/内部/受限/高度受限/机密/绝密信息等。 • 限制数据访问	数据分类被广泛定义为按相关类别组织数据的过程，以便更有效地使用和维护数据。
数据托管	• 数据服务的位置 • 保护静态数据 • 数据传输控制 • 数据访问控制 • 监管要求	数据托管是在第三方或外部服务提供商的基础设施上部署和托管数据中心的过程。 资产分类必须根据业务重要性、服务水平预期和操作连续性需求。应定期维护和更新位于所有地点和/或地理位置的关键业务资产的完整库存及其随时间的使用情况，并按规定的角色和职责分配所有权。 应设置物理安全边界(如围栏、墙壁、屏障、警卫、大门、电子监控、物理认证机制、接待处和安全巡逻)，以保护敏感数据和信息系统。 用户和支持人员对信息资产和功能的物理访问应受到限制。 了解监管环境和客户对某些特定数据/信息的托管要求，例如，《海外账户税收合规法案》（FATCA）。
数据管理	• 数据丢失防护 • 安全补丁管理 • 数据可逆性和删除流程 • 受当地法规约束的数据保留标准	数据丢失防护 (DLP) 是一种确保终端用户不会将敏感或关键信息发送到企业网络之外的策略。 安全补丁管理不断提供应用更新，可帮助解决系统中应用程序的代码漏洞或错误。 应制定政策和程序，并实施配套的业务流程和技术措施，以安全处理和完全删除所有存储介质中的数据，确保数据不能通过任何计算机取证手段恢复。 数据保留政策应考虑监管层面，关于特定的数据说明必须保留多长时间的要求。

主题	推荐标准	说明
		应制定程序以允许数据对客户端的完全可逆性，并确保一旦可逆性完成，在服务提供商端数据将被全部删除。 实际删除的日期应由供应商和银行商定。
网络安全	• 备份级别 • 网络渗透测试 • 预防、检测和恢复控制 • 定期审查，以应对不断变化的威胁 • 异地灾难恢复	通过公共网络传输与电子商务有关的数据，应适当保密以防止欺诈活动、未经授权的披露或修改，从而避免合同纠纷和数据泄露。 生产数据不得在非生产环境中复制或使用。任何在非生产环境中使用客户数据都需要得到来自所有数据受影响的客户明确、书面的同意，并且必须遵守所有法律法规对敏感数据元素进行数据清理的要求。这应该是有时限的（或偶发的）和/或受合同约束。这应基于时间（或发生）和/或受合同约束。如果是个人账户，则应以时间为基础的“明确同意”。 **网络安全标准案例** SWIFT启动了客户安全计划(CSP)，以推动全行业在打击网络威胁方面的合作。这包括一套核心安全控件。这是网络安全行业标准的一个例子。 国际商会没有检查或验证这些标准是否可以直接适用于您的业务。这里仅作为示例。 https://www.swift.com/myswift/customer-security-programme-csp 金融科技公司应具备相关流程，以便他们识别客户并与客户沟通。
应用程序安全	• 管理应用程序的开发过程 • 用户测试 • 用户认证/识别	应用程序接口(APIs)应按照领先的行业标准进行设计、开发、部署和测试，并遵守适用的法律、法规或监管合规义务。

主题	推荐标准	说明
		此类法律、法规或监管合规要求的清单应形成一套文件，并告知客户。 在授予客户对数据、资产和信息系统的访问权限之前，应解决关于客户访问权限的识别安全、合同和监管上的要求 应用程序接口和数据库应实现数据输入和输出完整性例程(即核对和编辑检查），防止手工或系统处理错误、数据损坏或误用。
恶意软件识别和修复活动	• 本地安装或基于云的反恶意软件程序 • 在协议的时间线内和基于优先级的基础上快速修补漏洞的能力 • 为移动设备开发的应用程序	应制定政策和程序，并配套业务流程及技术措施，以防止在机构中所有的或被托管的用户终端设备（例如，发布的工作站、笔记本电脑和移动设备）以及网络基础设施和系统组件中的恶意软件运行。
入侵防御	• 文件完整性（主机）和网络入侵检测(IDS) 工具的实施	审计日志的保护、保留和生命周期管理需要更高级别的保证，遵守适用的法律、法规或监管合规义务，并提供唯一的用户访问责任，以检测潜在的可疑网络行为和/或文件完整性异常，并在发生安全漏洞时提供司法鉴定能力。
访问控制（有条件的访问）	• 管理用户ID和密码 • 职责的划分 • 不再需要访问控制时，删除访问控制（包括但不限于用户ID和密码） • 限制对访问信息安全管理系统（例如，管理程序、防火墙、漏洞扫描器、网络探查器、APIs等）的访问。. • 对用户级别的访问进行日志记录和监控	访问控制是一种安全技术，它规定谁或什么人可以查看或使用计算机环境中的资源。 应适当细分和限制与组织机构信息系统交互的审计工具的访问和使用，以防止日志数据的泄露和滥用。 应制定用户访问政策和程序，以及实施业务支持流程和技术措施，以确保为所有公司内部用户以及能够访问数据、公司拥有或管理

主题	推荐标准	说明
	• 可审计性——谁做过什么，日期，时间戳，构建都应能够被内部和外部审计员审计。	的(物理和虚拟)应用程序接口以及基础设施网络和系统组件的客户用户（租户）提供适当的身份、权限和访问管理。用户日志应包括识别用户登录时间和运行活动的能力。 此类日志应能以正常的机器可读格式和/或可转换为人类可读格式被“随时”读取。
监管	• 遵守数据隐私法，例如GDPR（《通用数据保护条例》）和新加坡PDPA（《个人资料保护法案》） • 数据托管所在地的监管机构进行沟通了解。国家法规将会对云端托管数据、跨境共享数据以及按需访问数据方面做出规定 • 与监管就使用第三方渠道与客户沟通这一方式进行交流。这是否被视为一种新的分销渠道? • “了解你的客户”（KYC）/第三方准入要求 • 编程语言的互操作性 • 透明度、制裁、反洗钱甄别 • 跨境许可证 • 金融科技公司应准备好共享分包商信息	数据合规性是指确保敏感数据的组织和管理能够使组织机构遵守企业商业规则以及法律和政府法规的做法。

2. 商业标准

领域	推荐标准	基本原理
风险管理	**商业政策—**除了数据和技术相关政策外，服务提供商还应具备合适的商业政策。例如包括: • 反洗钱/恐怖主义和制裁政策;反贿赂与腐败、欺诈、环境/社会治理 • 股息 • 操作风险控制 • 为了管理潜在的反垄断风险或利益冲突，当金融科技公司的多数股权被包括政府或主要企业/银行持股时，此类信息应予以披露。 • 员工政策，包括： ◦ 如适用，激励措施 ◦ 确保职能划分清晰 ◦ 任何背景调查需求 ◦ 满足当地雇佣劳动力的法定要求 ◦ 任何分包 ◦ 员工离职时的书面记录 ◦ 健康和安全 此外，如果服务提供商是由银行建立的，则可能需要制定另外的政策: • 反垄断 • 利益冲突	供应商展示合适的风险治理和管理。
风险管理-业务连续性	**业务连续性规划(BCP)有两个方面:** 1. 考虑服务提供商(技术提供商)采用足够的BCP和相关政策以及 2. 在业务接收端(如金融机构或企业)有适当的规划和回退手段。 **BCP政策的主要考虑领域包括:** • 分析关键服务领域中断的影响 • 恢复计划/冗余 • 建立可容忍的中断期间 • 定期回顾BCP计划 • 金融科技公司应该公布他们业务连续性保障的位置以及能够出现在保障现场的关键员工的编号。	

<table>
<tr><th>领域</th><th>推荐标准</th><th>基本原理</th></tr>
<tr><td>义务</td><td>责任和义务
明确界定双方义务。
以下列举了义务及可能的限制：
<table><tr><th></th><th>%合同金额
或名义金额
（以高者为准）</th><th>供应商补偿
客户</th><th>无限制</th></tr><tr><td>欺诈</td><td></td><td></td><td>✓</td></tr><tr><td>故意违约</td><td></td><td></td><td>✓</td></tr><tr><td>故意放弃</td><td></td><td></td><td>✓</td></tr><tr><td>知识产权违约</td><td></td><td>✓</td><td></td></tr><tr><td>一般供应商义务</td><td>✓</td><td></td><td></td></tr><tr><td>数据丢失</td><td>✓</td><td></td><td></td></tr></table>
“不可抗力”，金融科技公司需要澄清在这种情况下发生了什么，涵盖了什么，或有什么影响（如：若不可抗力因素持续存在，协议将在一定期限内终止）</td><td>明确界定发生各种违约或损失时，哪一方应承担责任。</td></tr>
<tr><td>保险</td><td>保险单
服务供应商应提供保险单。例如：
专业赔偿
公共责任
一般产品责任
员工欺诈
雇主责任
财产损失
数据保护
一般而言：各方应对保险人的地位和声誉感到放心。
有关保险单的其他需要考虑的问题：
转让或签发给持有人。需确保银行能够主动提出索赔
各方应重点关注保险金额，确保其与基础活动有关的风险相匹配
在某些情况下：可以免费进行试点或“概念验证”。然而，在这些情况下，如果由于试点/概念验证而导致各种损坏和/或损失，仍可购买保险单。</td><td>确保发生索赔时已有合适的保险单。</td></tr>
</table>

领域	推荐标准	基本原理
知识产权(IP)	**知识产权归属** • 适当地定义技术供应商与服务供应商的安排下产生的“知识产权”；以及哪一方拥有它。 列出具体示例可能会有所帮助。 • 确保知识产权在法律框架中是“保密的”。	在做安排时确定所有权以避免将来发生纠纷。
数据共享原则（非技术）	**金融机构/企业与金融科技/供应商共享数据的标准。 应就主要原则达成一致：** • 任何数据共享均需征得客户同意，这可能包含在银行的条款中 • 数据只能用于所述目的 • 监管机构可能要求访问数据 • 在网络/解决方案供应商没有数据，客户和银行拥有自己数据的所有权，其他方无法访问该数据的情况下（如：一个节点内，仅可查看无用信息），可以设定一个替代模型。 • 数据提供者（如银行）仍然是该数据的保管人 • 数据保管人保留删除或发送/迁移数据的权利，并有权要求提供这样做的证明 • 除非另有规定/约定，交易数据仅能共享 • 提供担保以遵守GDPR(《通用数据保护条例》) • 技术/服务提供商可以在投资组合级别与银行共享和平台/产品使用相关的信息，前提是这些信息是隐藏的	建立透明的普遍接受的原则（尽管数据共享可能取决于具体安排的情况）
金融科技/供应商引入要求	• 在准入的过程中，可能会出现与供应商信用/财务稳定性/声誉、不利消息、制裁等相关的问题 • 妥善管理因分包产生的风险。这包括与新外包相关的风险，以及承包商和分包商之间的合作或沟通不足 • 披露所提供的技术/服务方面的分包安排，包括其司法管辖区	与银行建立关系时需提供的主要信息。 便于银行考虑不同的许可证。
全球监管环境	**需要考虑的全球以及国家监管项目：** • 《通用数据保护条例》（GDPR）— 欧盟法律 • 金融科技/供应商的监管报告义务 • 合同可能涉及跨地区的当事方和服务供应。银行和服务/技术提供商应就具有约束力的法律和法院达成一致，以便在发生合同违约或纠纷时执行服务合同中规定的法律 • 合适的税务条款（可能存在的增值税，代扣所得税等） • 金融科技公司应共享合规批准的监管通知。	概述金融科技/供应商应了解的主要银行注意事项

领域	推荐标准	基本原理
	• 在需要跨境实施的情况下，金融科技公司应提供实施计划，以及预期服务中的任何考虑因素和差异性。	
可审计性	根据合同关系，银行有权审计金融科技/服务提供商（如果适用），或金融科技/服务提供商有义务为银行的报告要求提供数据	
品牌/标识等的使用	根据合同关系，应考虑以下情况： • 金融科技/服务提供商用白标显示银行的品牌/标识等 • 银行使用金融科技/服务提供商的品牌/标识等 • 使用联合品牌/标识等	
成本和收入	银行与金融科技/服务提供商之间的成本/收入分配（如适用）	

3. 技术标准

技术标准因使用案例和应用目的而可能有所不同。同时，还应考虑到技术标准将持续发展，因此有时可能会有所不同。所以，以下不是提供明确的标准，而是以常见问答形式提供的包括相关的技术领域的考量因素建议。

领域	推荐考量因素
技术支持与维护	• 描述您的解决方案如何提供清晰的事件状态，以便以简单明了的方式与客户和支持团队共享。 • 描述您的支持管理服务（本地化、语言理解、覆盖时间等）。 • 描述升级支持管理（1 级、2 级等）。 • 产品支持哪些离线/批次处理的作业调度工具？例如TWS, Autosys 等。 • 描述您的解决方案如何管理应用程序的相互依赖性，例如实时制裁检查。 • 您的解决方案是否具有在数据量反常的情况下识别并自动通知支持人员的功能？ • 描述您的解决方案如何支持客户端设置阈值和指标以确定应用程序运行状况的能力？请描述解决方案的所有要素。 • 描述您的解决方案如何公开应用程序运行状况的指标。 • 描述您的应用程序如何实施有针对性的日志记录以支持事件解决和/或过程监控。 • 描述您的解决方案支持或集成的监控和警报工具/实用程序。 • 描述如何监控您的产品在银行生产环境中的性能。说明您自己提供的用于监控性能的任何工具，或对与您的产品一起使用的其他金融科技工具的建议，例如Wily/AppDynamics。 • 支持产品的数据/配置是否存在某些方面，在解决事件的情况下无法用于支持团队？请描述所有实例。 • 客户希望在生产环境中运行分析工具来检查应用程序的状态。它支持哪些实时分析工具？ • 确认具备强大的灾难恢复功能，并定期进行测试。 • 金融科技公司应描述其预期框架，以支持正在进行的审查和监控以及终止指南。 • 对SLA级别的承诺，并针对不同严重性问题共享不同SLA的框架。（即为不同级别提供修复的周转时间）。 • 金融科技公司应评论其解决方案是否有自动审核日志，跟踪每个用户的操作，以便轻松识别问题可能发生的位置。

领域	推荐考量因素
软件安装（部署）	• 谁来负责部署的策略？ ◦ 仅客户 ◦ 仅服务提供商 ◦ 两者都有 解释每一个策略和选项。 • 如果客户负责（全部或部分）解决方案的部署策略，解释以下两种情况应如何实施： ◦ 与客户合适的CI/CD流水线进行整合 ◦ 不与客户CI/CD流水线实施整合，解释你的解决方案使用的工具。 • 可应用什么样的部署： ◦ 非颠覆性和整个系统 ◦ 非颠覆性和渐进的（即在向新的版本转换过程中，现有版本仍部分使用） ◦ 颠覆性和整个系统 ◦ 颠覆性和渐进的 ◦ 为A/B测试做好准备 ◦ 对每一个选项解释如何实施。 • 如果有多个云服务商支持，解释转换到另一个云服务商的影响。 • 对于联合实施，金融科技公司应对合作预期进行分享，即应由银行承担的测试比例或者银行应承担哪些其他工作。
基础设施	• 提供图表对各参与者要使用的基础设施概貌进行展示： ◦ 机器 ◦ 服务器 ◦ 防火墙 ◦ 负载均衡器 ◦ 应用设备（如，硬件安全模块等） ◦ 边缘基础设施（信标技术、传感器等） ◦ 网络区域 ◦ 数据中心 • 你支持哪个云服务商？ ◦ IaaS ◦ PaaS ◦ SaaS ◦ 对上述每个选项你支持哪个云区域和可用区？ ◦ 你与上述每一个服务商的合作经历（特殊要求、限制等）？ ◦ 你的解决方案在不同服务商之间是否便于转换？ • 解释基础设施的尺寸（如服务器型号和数量、存储、带宽等）以及对响应非功能性请求（见后）的影响因素（如用户数量、请求数量、峰值等）。 • 对保障基础设施“恢复点目标”（RPO）和“恢复时间目标”（RTO）的要求？ • 如果使用上述（X）aaS云服务，备份在哪里？ • 使用过的可用区和区域是什么？

领域	推荐考量因素
架构适用性	• 描述你的产品设计如何具有错误容忍度，描述你的解决方案如何解决失败？是否所有程序都可以从失败时间点重新开始，如果是，如何实现这一点？你是否将失败测试纳入你的产品测试？ • 数据分析和可视化应用的设计纯粹为满足终端用户的消费，而不是数据提炼的目的；描述你的解决方案如何体现这一声明。 • 描述你如何审核商业情报功能的使用，使得数据使用可以获得。 • 描述你的解决方案可支持的测试自动化的工具（自动化测试工具加上测试数据获取机制） • 一项应用程序的各个方面和它的运行时间必须可通过代码进行配置，代码通过版本进行控制—请描述你的解决方案如何实现并支持这一原则。 • 提供你如何管理产品升级诉求的细节。 • 描述你的产品如何支持定制化，以及如何实施并管理。请注意基于你的产品、产品升级及其依赖的技术路线图，如何管理定制化。 • 描述你的解决方案如何管理应用程序和状态数据，该解决方案是否以不可变的模式建设和运行？如，没有状态数据存储在应用实例中。 •«通过提供的容积数据描述应用效果的细节。其中要包含适用你的产品流程的相关绩效标准。 • 示例；吞吐量每秒处理量（TPS）、均值、探针、峰值、数据量、服务器负载、应用程序和网络延迟和多样性，应用程序争用、数据层表现、用户交互表现、API接口表现。 » • 描述你的解决方案如何支持工作量管理——不断波动的工作量峰值批量负载处理时间和并行用户接入。 • 提供产品范围详情，有没有区域或全球限制？ • «描述你的解决方案如何支持操作系统和浏览器独立性？UI必须可运行windows、Mac OS、安卓、iOS、Linux操作系统并且完全兼容和响应HTML5。 • 确认产品不依赖Silverlight、ActiveX、Flash和客户端Java. 请提供需要在桌面/浏览器安装/下载的其他构件的相关信息。 » • «解释你的解决方案如何满足“残障歧视法”相关要求？ • 你如何测试对法规的合规性？ • 你的解决方案如何适应法规的变化？» • 列举解决方案界面针对设备的特点/方面。支持哪些设备？请提供未来支持的路线图。 • 请描述UI架构，包括逻辑层（如商业逻辑）与UI层的隔离。同时提供信息说明你提供服务时如何考量设备的局限性，如带宽问题。 • 提供信息说明解决方案对标准接入和外围设备的兼容性，如对标准微软Office软件接入的兼容性。 • 你的解决方案接入用户界面进入客户网络分析工具是否存在制约？ • 你可以支持应用程序、操作系统和和中间件技术多少个之前的版本？ • 对于新发布产品你的管理流程有何变化？

领域	推荐考量因素

应用程序设计	• 描述环境管理以满足发布交付和用户参与需要（生产前解决方案、用户测试、客户做出是否可行决策等）
	• 描述用户信息和与应用发展相关的培训。
	• 你如何向我们分发软件以及你是否有完整的发布说明样本？
	• 描述系统支持区块链或API等新技术的能力，以及成功实施的案例
	• 你的解决方案是否利用了SWIFT MT报文等现有标准？
	• 描述你的解决方案如何采用正在研发的新标准或支持ISO20022等更广泛的行业标准？
	• 你多快可以支持新的操作系统或平台？
	• 是否存在一个专用架构可交付或提供给接收方？当某一客户数据以环境共享/公有云的方式建立在另一客户数据的原型上，详细描述如何隔离并确保安全。
	• 如果需要，是否可安装一个专用过滤器以确保向客户的用户交付服务仅能通过特定场所获取（如使用互联网IP过滤器、VPN等）？
	• 测试结果指引，用以确定产品是否可从用户验收测试（UAT）转移到银行共享的生产中。
	• 银行可发起请求的特定数据的指引应予以共享。银行是否能请求行业匿名报告或该报告是否可自动发布？
	• 指引说明产品多大程度可对每个银行或客户提供定制化？如，在融资方面，是否可支持不同银行授权要求？
	
	• 你的解决方案遵循的主要架构原则？提供解决方案的软件构成图表并解释解决方案应用的设计原则（如分层架构）。在移动设备支持的情况下，不要忘记移动设备的组成部分。
	• 描述每个组件的安装功能或能力，并识别所用组件与外界的整合能力。
	• 实施逻辑是什么和如何运转，以及你为何选择实施这种逻辑？
	  ◦ 展示逻辑
	  ◦ 整合逻辑（数据转换、协议转换等）
	  ◦ 处理逻辑
	  ◦ 商业逻辑
	  ◦ 数据逻辑
	• 解释所做的设计选择如何对你的解决方案未来变化提供便利（模块化、复杂性、依赖性、风险关注的隔离性等）
	• 说明属于系统核心的组件且不能被第三方解决方案替换
	• 为更好理解应用程序并确认是否覆盖客户需求：
	  ◦ 提供所用的逻辑数据模型
	  ◦ 提供每一实体类型及相关类型的定义（逻辑数据模型可不同且可大于规范的数据模型）
	
	• 哪些组件用来增加可用性？解释如何在以下方面加强可用性：
	  ◦ 数据存储组件（如分发）
	  ◦ **处理**组件（如**多维/分布式实例**）

领域	推荐考量因素

	• 与帽子原理相关要考虑哪些选项？
	  ◦ 一致性：系统关注信息一致性并对每一次请求做出正确响应。
	  ◦ 可获得性：系统关注可接受的响应时间而非响应的正确性。
	  ◦ 分区容错性：系统关注保持操作性且可处理间歇性的网络中断。
	• 分区容错性：系统关注保持操作性且可处理间歇性的网络中断。
	• 提供与你的解决方案互动或交流的数据模型图表。
	• 为每一种实体类型提供定义。
	• 你的解决方案接触点有哪些？
	  ◦ 网络
	  ◦ 移动应用程序
	  ◦ 桌面应用程序
	  ◦ 其他
	• 解释解决方案多大程度可被用于“面向服务架构（SOA）”:]
	  ◦ 你的解决方案体现出的服务哪些功能可称为SOA（如，内部流程的状态）。
	  ◦ 你希望客户服务或第三方解决方案提供哪些功能。
	• 解释你的解决方案多大程度基于“事件驱动架构（EDA）”:
	• 你发布哪些事件、哪些内容、以何种频率（如，内部商业流程事件、通知、数据事件等）？
	• 你希望从客户收到哪些事件、哪些内容、以何种频率?
	• 你的解决方案遵循的主要架构原则？提供解决方案的软件组件图表并解释方案设计适用的原则（如分布式架构）。如果支持移动设备，不要忘记移动设备组件。可提供详细描述和图表作为附件。
	• 提供解决方案对技术的见解（平台、中间件、框架和协议）。即使对于SaaS解决方案这些信息对于缓释风险也是有用的。
	• 提供架构图表，提供实现组件图表中每一组件功能所用技术堆栈的完整视图。列举所有技术:
	  ◦ 操作系统
	  ◦ 中间件平台
	  ◦ 存储
	  ◦ 数据库技术
	  ◦ 结构化
	  ◦ 非结构化
	  ◦ 数据湖
	  ◦ 分布式
	  ◦ 内容管理技术
	  ◦ 集成技术
	  ◦ 排队技术 (面向消息的中间件-MOM)

领域	推荐考量因素
技术概述	◦ 服务总线 (ESB) ◦ 数据库集成技术 ◦ 处理引擎 (BPMS) ◦ 事件代理 ◦ 流媒体技术 ◦ 调度程序 ◦ 导出转换负载 (ETL) ◦ 执行 ◦ 网络服务器 ◦ 应用软件服务器 ◦ 规则引擎 (BRMS) ◦ 处理引擎 (BPMS) ◦ 浏览器 (IE, Chrome, Edge, Safari, Firefox等) ◦ 运行时库 (.Net, JRE等.) ◦ 其他 • 说明技术堆栈何处可将一项已有技术替换成另一项技术。 • 你的解决方案遵循的主要架构原则？提供解决方案的软件组件图表并解释方案设计适用的原则（如分布式架构）。如果支持移动设备，不要忘记移动设备组件。 • 解释你的解决方案适用的每一个组件，其扩展、配置和开发所用的语言。 • 如果涉及边缘计算请予以考虑。 • 你能否一直符合客户标准： ◦ 前端：HTML5, CSS3, Javascript ◦ 语言：Java, Python» • 说明属于系统核心的组件且不能被第三方解决方案替换（如一项客户已经拥有的解决方案）。 • 为更好理解应用程序并确认是否覆盖客户需求： ◦ 提供所用的逻辑数据模型 ◦ 提供每一实体类型及相关类型的定义（逻辑数据模型可不同、且可大于规范的数据模型）» • 解决方案的哪部分基于第三方产品，如由其他金融科技公司交付的组件（解决方案、流程、数据等）？ • 你的解决方案哪些模型可被第三方或客户内部解决方案替代？如何替代？» • 对于所有相关技术事项，你跟进金融科技公司技术发布和标准迭代有多快？ ◦ 操作系统 ◦ 所有相关中间件 ◦ 所有相关架构 ◦ 所有相关第三方组件 ◦ 对于所有相关事项，当前可支持的版本 ◦ 展示你在该领域创新的速度 说明以上每一项技术主题如何进行文本化（如，通过线下文本、放在公共或有防护协助或支持的网站等）。

领域	推荐考量因素
安全&接入	• 描述你的解决方案如何支持RBAC和ABAC接入控制方法。 • 解释在不同用户类型（如管理员用户和普通用户）情况下产品有何差异。 • 解释在不同用户类型及其授权下产品有哪些不同特点。 • 解释如何管理用户，使其只能看到被授权的数据? • 描述授权功能并解释如何进行定制。 • 解释各项功能如何进行明确分配或屏蔽。 • 用户特权/角色如何持续；如在服务器、网络文件/URL参数方面？ • 解释你的产品如何实现用户验证和单点登录。 • 系统必须控制接入数据和操作。请解释在使用API接口和其他后端处理的情况下，如何实现这一点? • 是否所有数据都放在可验证的数据存储中？请解释如何进行数据存储的验证，是通过个人用户账户还是系统账户? • 对于系统账户，请解释密码循环流程及控制，即解决方案如何满足常见的系统密码过期问题并利用Cyberark等产品。 • 解释产品如何支持多点登录? • 描述产品如何确保用户安全。请列举所有技术，包括有关用户安全的版本和维护，如幻灯片制作工具Struts。 • 解释可为产品提供的标准强化指引。 • 你的管理团队能否接入用户数据库? • 是否存在你可向客户建议的远程接入方式? • 对于特殊权限用户（管理员），解决方案是否可与强验证机制交互（多因素验证）? • 描述系统组件之间的通讯如何确保（HTTPS, MQ , JDBC/ODBC等）。是否存在任何组件间通讯不能保证的因素? • 第三方评估人的系统安全评估，即渗透测试，是否已完成以确认脆弱性？如果是，可否告知对系统的哪个版本、在何时完成以及评估结果。 • 解决方案必须具有抗病毒和抗恶意软件保护。请解释产品在这方面的能力。 • 解释建议的方案如何防范网络安全攻击。请清楚说明客户应承担哪些责任。 • 描述解决方案的安全特性，包括对第三方安全和加密软件的兼容性? • 解释在研发和测试过程中如何保障产品安全性。 • 你的产品源代码是否通过源代码安全漏洞检测工具扫描，作为管理流程变更的一部分？如果是，请说明使用了哪个/哪些产品。 • 解释在你的产品源代码开发过程中，如何解决10大OWASP漏洞和25大SANs问题? • 要求使用哪种数据对你的产品进行测试（生产数据、模拟数据还是清洁数据)? • 一旦发现解决方案存在漏洞，客户安全团队可以向你的公司提出问题；描述发现问题的方法，包括有关披露政策和流程。 • 应要求客户对解决方案应用程序所集成的源代码进行评估，解释这些源代码的交付如何可以便利化。 • 有时客户可能要求确保消息级别（MLS）的数据安全而非仅是传输级别（TLS）的安全。解释应用程序如何支持端到端的加密和 / 或消息签署。

领域	推荐考量因素
	• 描述应用程序对N层架构DMZ拓扑的支持情况，展示层、应用层以及数据库层通过防火墙区域进行分隔。 • 解释应用程序如何在客户与主机或用户与主机之间保持对话状态。 • 解释如何防止本地隐藏数据被篡改。 • 解释应用程序对敏感操作如何支持双人/多级授权。 • 展示在屏幕上、打印材料或审计日志上的数据可能因保密原因需要隐藏（解释应用程序可如何 配置使特定数据模糊化）。 • 解释应用程序如何配置可与基于互联网的防病毒产品相融合。 • 你的解决方案是否支持预先安排的银行用户数据摘要以及重新认证的角色权限? • 你的网络是否对互联网通信和电信通信进行隔离？ • 你的内部IT网络（局域网办公室）是否与客户主机网络（客户网络）连接？如果是，你如何避免来自你内部IT网络的病毒攻击客户主机网络？ • 在你的安全基础设施出现严重安全漏洞的紧急情况时，你是否有应用补丁的流程? • 能否提供你的安全保障计划和质量保障计划? • 描述你如何应对分布式拒绝服务攻击。
认证	• 列举对所需服务提供商的认证条件。 • 能否确认所有主机数据中心符合相关规定（HVAC等）和（国家）有规定的精确标准? • 服务是否依赖有标准安全规范的系统或流程（如EAL x产品信息安全认证或ISO y）？ • 描述你确保以下事项的措施： ◦ 应用程序代码质量 ◦ 数据质量
邮件服务—网络协作服务	• 描述邮件服务设计和管理规则（通知流程、申请确认、电子邮件地址处理、附件处理、加密服务）。 • 如果已提供，描述自动化平台（工作流、激活、监控等需要与客户互动的设备/服务）。

领域	推荐考量因素
文件传输	• 如文件需要上传到互联网网站，描述可用的解决方案。 • 采用何种机制可确保文件的一致性和完整性? • 如果出现原文件与互联网版本错配，你能获取何种信息用于审计跟踪? • 如果服务商和客户发生了信息自动交换（如资源自动输送），描述可提供的解决方案。

术语表

术语简称	含义
ABAC	基于属性的访问控制模型
AML	反洗钱
AppDynamics	应用性能监测工具
Autosys	工作规划软件
BI	商业情报
CAP-theorem	一致性、可获得性、分区容错性原理
CI/CD	持续集成 (CI)和持续交付 (CD)
CSP	SWIFT客户安全计划
Cyberark	防网络威胁软件
DDoS	分布式拒绝服务
DLP	数据丢失防护
EDA	事件驱动架构
FATCA	海外账户纳税法案
GDPR	通用数据保护条例
HSM	硬件安全模块
IaaS	基础设施即服务
ISO 20022	贸易和支付行业标准
KYC	了解你的客户
OWASP	开放式Web应用程序安全项目
PaaS	平台即服务
R&R's	角色和责任
RBAC	基于角色的访问控制
RPO	恢复点目标
SaaS	软件即服务
SANS	系统管理、审计、网络和安全
Secure data at rest	保护未使用或未传输到系统端点的数据
SOA	面向服务的架构
SWIFT MT	SWIFT 报文类型如MT7xx
Throughput TPS	每秒交易吞吐量
TRO	恢复时间目标
TWS	企业作业调度软件 (IBM) 工作规划软件
VPN	虚拟私有网络
Wily	应用性能监测工具 (IBM)

附件1
其他信息安全（Infosec）标准

中间商和/或数据加工商通知客户他们所采取的与其服务或产品相关的组织措施和技术安全措施，通过这种方式，基于客户想要使用的服务或产品以及可能的对个人数据的处理，客户可以评估这些措施是否充分。数据加工商要在行为准则（或SoC/ISO）中说明这些内容。

数据加工商以及发布声明或已经将上述内容纳入数据加工协议。

《声明》应至少包括以下内容:

- 数据处理系统所选的信息安全管理，安全标准或标准;
- 数据加工商证明文件（如适用）；
- 数据加工商是否以及选哪个（次级）数据加工商;
  - 客户的个人数据以何种方式可被删除;
  - 保留期限，与3个月销毁期相比是否存在偏离;
- 在数据加工商的组织内部，对联系人详细联系方式的数据保护；或数据加工商使用声明和标准的行业标准或经行业审批的行为准则;将数据加工条款作为（加工商）协议的一部分。
- 数据加工商在合同管理中持续跟踪，看数据加工运营的标准条款是否适用。
- 数据加工商在合同管理中持续跟踪，看（某一项）其他加工协议或标准条款是否适用。
- 数据加工商通知客户其设计的流程和程序，客户可针对数据主体的权力进行回应。
- 数据加工商通知客户关于数据主体的现有权力；包括但不限于：被告知的权力、获取的权力、更正的权力、删除的权力、限制加工的权力、数据便携性的权力、反对的权力以及与机器自动决策和画像相关的权力.
- 如果数据加工商检测到数据违约，数据加工商应尽快告知客户，从而使管理者可满足在知悉的72小时内应履行的法律义务，以及在适用的情况下，将数据违约情况报告当地数据保护监管机构（DPA）和/或有关的数据主体。选择向当地DPA报告，是管理者的责任。
- 如有需要，数据加工商可对报告流程向客户或管理者提供支持.
- 一旦发生数据违约，数据加工商应至少提供以下所需信息：
  - 事件描述，侵权性质，个人数据性质或涉及的数据主体类别，涉及的数据主体数量预测，可能涉及的数据库，事件发生时的表现（如，发生了什么？）；
  - 联系人详细联系方式（管理者如有疑问可以问谁？）；
  - 可能的结果（可能发生什么，管理者或数据主体应注意什么，指出确认欺诈的可能性，如社会安全码等详细信息，登录和密码详情，护照复印件可能出现在不该出现的人手里）；
  - 采取的措施（数据加工商做了什么以在未来去避免、限制或阻止这种损失）；
  - 管理者或涉及的数据主体采取的措施（数据主体可做些什么，如关注邮件和密码变更）；
  - 数据加工商让客户知悉未来发展。

数据加工商经常测试并评估其数据保护政策，采取安全措施并在需要时进行调整。

数据加工商经常测试并评估其信息安全管理系统，并在需要时进行调整。

评论和监督

1. 使用标准时，独立监管人和指定的治理主体在适用时可作为监管人，
2. 数据加工商负责对过程评估是否符合其声明进行监督.
3. 标准或行为准则被使用或引用时，数据加工商应由独立审计机构进行评估。

中国国际商会/国际商会中国国家委员会组织翻译

翻译：张毅琳　奚琳

译审：徐　珺

关于国际商会（ICC）

国际商会（ICC）是在100多个拥有4500多万家会员的国际民间组织。国际商会的核心使命是让商业服务于每个人、每一天、每个地区。通过政策建议、争议解决和标准制定的独特组合，除了提供市场领先的纠纷解决服务外，我们还促进国际贸易，负责任的商业行为和全球监管方式。我们的会员包括许多世界领先的公司、中小企业、商业协会和当地商会。

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo