KPMG

监管快讯

监管洞察

2021年9月

监管机构聚焦云计算

要点

*监管机构目前注意到金融服务机构正在大规模快速向云计算转型（还注意到少数大型云服务提供商占主导地位），并已指出金融机构应重点关注的某些领域，以维护运营的安全性和稳健性以及保护数据安全和消费者数据。各监管机构关注的主题一致，涉及**网络安全、数据隐私、第三方管理和业务连续性**。主要考虑因素包括：金融服务机构对遵守所有适用　法律法规的最终责任；第三方服务提供商的选择、监督、测试和审查；合同所载企业和云服务提供商责任的明确性和全　面性；通过身份验证和访问控制实现数据安全；应对潜在服务中断/数据泄露以及降低集中度风险的方案。金融服务机构应确保制定明确的云计算数据战略和存储，并确保云计算方案与所有部门和流程的业务目标相一致。*

监管机构最近发布的文件和措施包括：

- **FINRA 研究报告 | 证券业中的云计算。**美国金融业监管局 (FINRA) 为弄清楚证券业云计算采用状况及相关影响进行了一项研究，并在近期发布了研究结果。研究涵盖了“证券业近 40 家市场参与者，包括经纪自营商、云服务提供商、行业分析机构和技术咨询公司。”报告指出：
  - 与云计算采用相关的**常见主题**：
    - “现成的”云产品通常用于非核心业务职能；
    - 云基础设施的推出往往具有针对性，采用逐步升级和迭代的方式；
    - 市场参与者开发了以云为中心的增强型治理结构、政策和程序，以保护云环境中的数据和系统。
    - 对技术专业知识的重新评估（包括员工培训和招聘需求）通常与云服务的采用同时进行。
  - 与云计算采用和迁移相关的**监管注意事项**：
    - **网络安全** — 网络安全应该是任何基于云的应用程序的评估、开发和测试过程的重要一环，且任务分工（例如，威胁检测、事件响应、修补/更新）应反映在证券公司与云服务提供商之间签订的合同中；
    - **数据隐私** — 证券公司可能需要根据客户数据收集、存储、分析和共享方式的变化更新与客户数据隐私相关的政策和程序（包括与供应商协议相关的政策和程序）；

- **外包/供应商管理** — 证券公司将某项业务活动或职能外包给云服务提供商或其他云供应商，并不能免除证券公司遵守与外包活动或职能相关的所有适用证券业法律法规以及 FINRA 规则的最终责任。证券公司应意识到集中度风险，并视情形考虑多云或混合云方案，并制定缓解不利锁定情形的退出策略；
- **业务连续性** — 证券公司每年需复核更新与紧急情况或严重业务中断相关的书面业务连续性计划。由于云服务提供商的数据中心可以提供冗余存储和计算能力，云服务被认为具有提高业务韧性的潜力，但证券公司应考虑测试冗余配置，以确保业务服务在遇到中断时的连续性，并相应更新测试方案和程序；
- **存档** — 在评估云提供商提供的存储产品或服务时，应考虑存储义务（例如，保存期限、格式、媒介）。

— FINRA 在 2021 年 10 月 16 日前**征求意见**。意见反馈者可以指出其认为适合 FINRA 考虑的“符合投 资者保护和市场诚信原则”的与云计算应用程序及 其对 FINRA 考虑制定规则相关的任何事项。

— **FFIEC 指引| 金融机构服务及系统验证和访问。**联邦金融机构检查委员会（FFIEC）成员就**身份验证和系统访问**发布了关于有效风险管理原则和实践的更新指引。指引应对与网络安全风险面扩大相关的重大风险（部分归因于金融机构使用应用程序编程接口 (API) 并与云服务提供商等第三方的连接增加）。指引面向所有可以访问数字银行系统和金融机构信息系统的用户，包括商业和零售客户、员工、第三方以及系统间通信。（参见毕马威监管快讯）。

— **拟定机构间指引 | 第三方关系：风险管理**。FRB、FDIC 和 OCC 联合发布了关于管理**第三方关系**（包括与以金融科技为业务重点的实体的关系）相关风险的拟定指引。拟定指引将第三方关系描述为银行机构与其他实体之间通过合同或其他方式订立的业务安排。常见问题部分（可能纳入指引）阐明，云服务提供商属于第三方，证券公司的**尽职调查和监督**应与使用云计算的活动或数据面临的风险相称，且合同应**载明相关责任**。此外，证券公司应进行尽职调查和监督，以确认第三方云服务提供商有能力以令人满意的方式监督和监测任何云服务分包商。（参见毕马威监管快讯）。

- 上述机构分别发布了专门面向社区银行的有关如何**针对金融科技公司开展尽职调查**的指引。

— **FFIEC 声明 | 云计算环境的安全性**。FFIEC 成员发布该联合声明，旨在解决在金融服务领域使用云计算服务和安全风险管理原则的问题。该声明强调了健全的安全控制和管理层理解云服务提供商与金融机构客户之间的共同责任的重要性。声明提供了风险管理实践和控制示例，包括保护客户敏感信息免受可能对消费者造成伤害的风险的防卫措施，涵盖多个领域， 包括：

- **治理** — 金融机构使用云计算服务的计划应与其整体信息技术战略、架构和风险偏好保持一致。如果没有适当的风险缓解措施，金融机构的风险敞口不得高于所确定的风险偏好；
- **云安全管理** — 云计算环境通常具有独特的关键安全考虑因素和控制；示例涵盖尽职调查、监督与监测、合同责任、存储流程、身份与访问管理、敏感数据控制和培训等方面。

— **变更管理**、系统迁移 — 金融机构在云落地中通常使用微服务，这可能会引起安全性、可靠性和延迟方面的问题；利用多个微服务可能增加金融机构的受攻击面。管理层应评估符合金融机构安全要求的落地方案。

— **韧性与恢复**、事件响应 — 云服务产品中不一定包含韧性和恢复功能；因此，合同应概述金融机构所需的韧性和恢复功能。根据云服务合同，管理层应评估确定基于云的运营如何影响业务连续性计划和恢复测试计划；此类计划应相应地更新，并进行定期测试和验证。同理，云服务合同应列明在响应事件时采取的行动和各方的责任。

— **审计和控制**评估（关键系统定期测试、云服务提供商控制的监测、互操作性和可移植性、数据销毁和清理）。

— **云计算金融科技峰会**。里士满联邦储备银行计划于今年9月29日至30日举办云计算金融科技峰会。期间将举行小组讨论，主题包括云计算采用、云环境中的网络安全和数据、疫情期间及疫情结束后的业务韧性和第三方风险管理，以及云环境中的创新与协作。

— **COSO ERM 框架 | 云计算企业风险管理**。美国反对虚假财务报告委员会（Treadway Commission）下设的发起人委员会 COSO 发布了关于云计算企业风险管理的指引，以指导金融机构通过利用 COSO《*企业风险管理 - 与战略和绩效集成*》框架（更新版见2017）的原则建立云计算治理。

COSO 表示，使用 COSO 企业风险管理框架有助于云计算与金融机构的企业风险管理职能集成。指引解释了如何在 COSO 企业风险管理框架的以下五个组成部分实施云计算治理：1）治理和文化，2）战略和目标设定，3）绩效，4）复核和修订，及 5）信息、沟通和报告。指引的附录部分包含云计算落地“路线图”（附录A.云计算路线图）以及角色和职责描述（附录 B. 角色 和职责）。

Amy Matsuo
主管合伙人
ESG及监管洞察中心

徐捷
金融业治理、风险与合规服务
主管合伙人
毕马威中国
电邮：jessica.xu@kpmg.com

作者：
Amy Matsuo（ESG及监管洞察中心主管合伙人）
Karen Staines（监管洞察中心总监）

kpmg.com/socialmedia