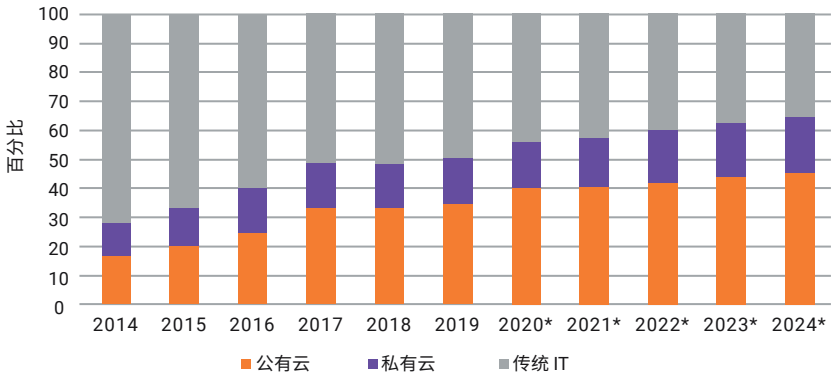
# 金融服务行业的云计算演变和监管

云计算服务经过一段时间后才被接纳和采用，但如今，包括金融行业在内的许多企业每天都在使用云。

数字化程度的提高影响了消费者的习惯和业务交互，导致许多金融机构关闭了实体分支机构并将流程、服务或活动外包。最常见的外包活动之一就是 IT；因此，外包安排管理在数字化战略中起着至关重要的作用。

**图 1**

全球 IT 基础设施支出
（按部署类型划分；* 代表预测）




**KILIAN TRAUTMANN** | CISA

存款保险领域涉及监管银行业务的 IT 审计资深专家。作为职业作家，他曾在各大国际知名期刊上发表过文章。其文章中针对 IT、合规性和审计的交叉问题提出了相关见解和解决方案。过去他曾在一家审计公司工作，该审计公司隶属于德国知名的以税务为中心的法律咨询公司。他也是隶属于 ISACA® 德国分会的“数字信任”专家组的创始成员兼副总监。

从按部署类型划分的全球 IT 基础设施支出（**图 1**）中可以观察到这一趋势[1]。到 2023 年，云服务预计将占全球 IT 基础设施支出的 60% 以上，对应的云 IT 基础设施年度支出为 1000 亿美元（比上一年增长 10%）（**图 2**）[2]。云应用市场价值将达到 1540 亿美元（比上一年增长 5%，比 2013 年增长 400%）（**图 3**）[3]。

尽管有多家云服务提供商 (CSP)，但市场高度集中，少数主要参与者（所谓的大科技公司）占据了大部分市场份额。2022 年第三季度 (Q3)，全球云计算收入领先的企业分别为 Amazon Web Services (AWS) (32%)、Microsoft Azure (22%) 和 Google Cloud (9%)（**图 4**）[4]。

对于执行银行交易和提供其他金融服务相关的基本流程、服务或活动，鉴于外包的性质、范围、复杂性和风险，实施充分且有效的控制措施至关重要。

实施云计算监管表明，数字化对金融服务和银行业的影响在不断演变。这种监管是动态的，欧盟最近颁发了《数字运营韧性法案 (DORA)》，将通过该法案对云服务实施进一步监管。

新冠肺炎疫情凸显了迅速扩展 IT 能力和远程系统可访问性的价值，同时还表明依赖现场技术存在风险，因为一旦出现漏洞或不可预见的外部因素，现场技术就可能无法使用。在这方面，DORA 解决了依赖云服务提供商的风险。

金融机构必须了解云计算在日益数字化的银行业中所发挥的作用、如何降低依赖云服务的风险，以及分布式账本技术 (DLT) 的兴起可能带来的进一步发展。

## 银行业数字化

数字化的增长催生了新的银行[5]产品。从消费者的角度来看，银行提供的数字解决方案通常包含新的交互方式（如机器人顾问、实时信用评分、数字预算跟踪和视频识别）和支付选项（如即时和移动支付）[6]。在监管方面，《支付服务指令 (PSD2)》 特别为提供金融解决方案的精通技术组织打开了银行业的大门。PSD2 引入了对支付账户提供商的要求，允许第三方交换账户信息并开始支付。该法规允许并鼓励创新，促使银行业进一步转型和创新，例如开放银行。

开放银行可以轻松整合各种类型的金融账户和服务，这些账户和服务来自众多以前互不关联的机构，从而创造出新的消费者金融服务。开放银行是一组金融机构使用软件即服务 (SaaS) 提供和支持各种金融服务而实现的一种金融即服务 (FaaS)。因此，开放银行建立在云计算基础之上。如果利用应用程序编程接口 (API) 遵守开放银行规则并获得客户批准，则开放银行生态系统将使第三方提供商能够访问来自不同企业的消费银行、国际和其他金融数据。一个现有的用例是先买后付 (BNPL)[7]。

目前，DLT 的兴起引发更多银行产品创新[8]。DLT 使人们更容易获得融资选择（为没有银行账户的人提供银行服务）并简化支付流程（结算和清算更快）。总体而言，DLT 能够减少以前必需的中介数量。

DLT 包含技术预防措施，使得欺诈和伪造极其困难。这也是为什么这项技术能够在数字信任文献和运动中发挥重要作用的原因。例如，DLT 可以通过将数字证券转化为智能金融工具来实现新型功能，这些智能金融工具具有嵌入式业务逻辑和自动执行的生命周期功能，如自动支付股息。这与仅仅使证券具备数字化性质形成鲜明对比。在金融证券领域使用 DLT 的主要潜在优势包括：数字证券的即时发行、分销和结算，以及更快的执行、降低的风险和每笔交易的成本[9]。

**图 2**

全球云 IT 基础设施支出
（单位：十亿美元；* 代表预测）

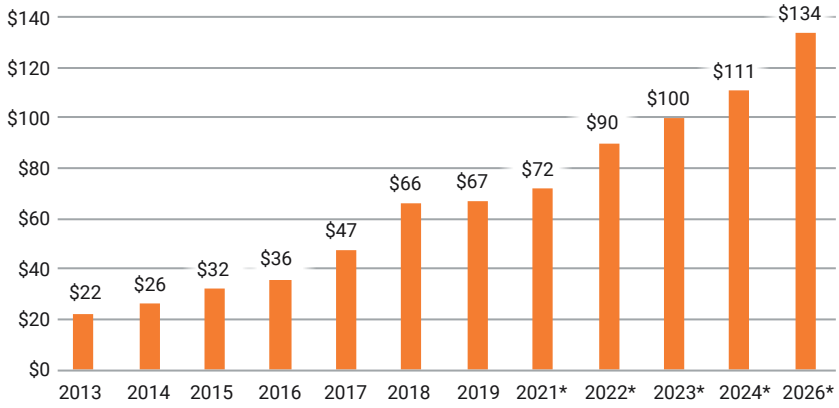
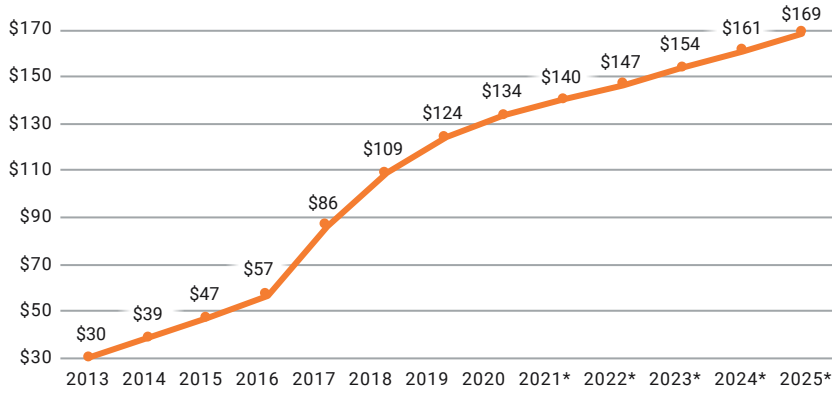



**图 3**

全球云应用市场规模
（单位：十亿美元；* 代表预测）




## 金融服务中的云计算

银行业务需要广泛使用技术。在银行自己的计算机基础设施上安装的本地系统代表传统金融行业的传统设置。然而，一份行业报告显示，40% 的服务器每年至少经历一次意外中断。平均中断时间持续 78 分钟，停机成本估计为每分钟 1,467 美元（每小时 88,000 美元）[10]。由此可见，现场实施和管理服务器存在风险。

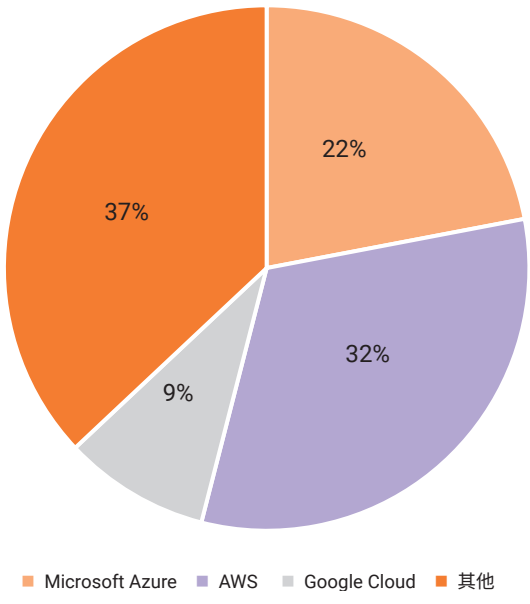
## 要与进入市场的其他不受监管的企业竞争，传统金融机构必须利用云计算服务。

无论使用哪种 IT 基础设施，业务目标的实现都需要广泛的信息安全，包括运营韧性任何程度的停机或数据丢失都是不可接受的。机构可以借助先进技术服务提供商的云服务来降低这些停机成本。与现场运行和管理系统相比，这些云服务可以提供更高的安全性。

到目前为止，云计算已经发展成为在数字领域创造新的金融服务、创新、团队合作和竞争的重要工具。银行和金融机构必须接受这一变化才能保持竞争力。对于这些机构而言，灵活性和上市速度至关重要。而云计算可以同时实现这两种要求。要与进入市场的其他不受监管的企业竞争，正如将 IT 视为业务推手的适当 IT 战略中所表述的那样，传统金融机构必须利用云计算服务。

**图 4**

2022 年第三季度领先云计算提供商的全球市场份额




历史上，欧洲金融服务机构采用云计算花了一段时间。主要原因涉及法律问题、信息安全和性能问题、可靠性、处理的复杂性、运营控制和治理。数据泄露是一个备受关注的云相关安全问题。另一个问题是锁定效应。使用专有 API 和 Web 界面访问云服务意味着必须在机构的 IT 环境中实施特定于 CSP 的架构。总的来说，锁定效应会带来一定程度的风险依赖和高转换成本。

同样重要的是，CSP 实际上是一个黑箱。尽管审计可以打开黑箱，但云市场的高度集中和由此产生的市场力量可能会阻碍访问、信息和审计能力。

最初，金融服务机构采用云服务专门用于 IT 开发和应用程序基础架构。如今，核心业务功能系统（例如企业资源规划、数据存储、投资管理）也概念化为涉及云计算技术。

### 欧洲外包和云服务指南

一旦金融服务机构充分意识到使用云的益处并开始采用，当局就会推动加强外包方面的监管。目的是借助云计算资源来解决可能影响金融市场稳定性和消费者保护的风险，例如数据泄露。金融行业的外包业务领域包含业务处理服务，其中包括承保和托收等利基领域、企业服务功能的技术平台部分、信息和通信技术 (ICT) 基础设施、应用程序开发和维护、行政流程，甚至包括完整的业务流程。这些领域都亟需使用云计算技术。

2018 年，欧洲银行管理局 (EBA) 发布了第一版金融服务机构外包及其他方面的通用法律标准[11]。国家监管机构和超国家监管机构必须协调各自的合规政策和程序。

针对使用云服务带来的风险因素，2017 年 EBA 发布了针对使用这些服务的机构的建议和指南[12]。指南中规定了对外包云服务的要求。例如，EBA 要求机构保证对 CSP 拥有不受限制的信息、审计和控制权。

实际上，这些指南涉及很高的成本。由于外包机构对其外包的流程、服务或活动负有全部法律责任，因此必须实施充分有效的控制措施。问题在于，由于 CSP 市场高度集中，谈判权已经从金融服务机构转移到 CSP 手中。结果导致标准化合同几乎没有回旋余地，机构也难以获得有合同保障的监管要求。

## 许多外包协议并未给出充分的保障措施，无法全面监控分包流程。

EBA 建议指出，审计权是确保重要外包职能按照合同约定提供并符合监管要求的关键[13]。主管当局的审计和访问权必须纳入所有外包安排，以确保实现对金融服务机构的有效监管。不过，这与 CSP 的实际能力矛盾，如果客户行使审计权，CSP 会给运营带来风险（例如，如果同时执行多项审计，数据中心可能会不堪重负）。因此，CSP 更倾向于通过服务组织控制 (SOC) 或国际标准化组织 (ISO)/国际电工委员会 (IEC) 标准提供审计报告等认证，而不是授予完整且不受限制的审计权[14]。即使只允许对一小部分 Microsoft Azure、AWS 和 Google Cloud 客户进行昂贵的现场审计或检查，CSP 也将无法运行其核心业务，从而面临服务水平履行方面的威胁。这些相互依赖的关系造成了一个两难的局面。

即使按照 EBA 的要求将合同审计授予有要求的企业，国家监管机构也无法直接影响 CSP，因为审计权并未直接授予该机构本身。国家当局只能通过依赖合作 CSP 的机构间接监督 CSP。所以 EBA 指南规定机构应确保 CSP 授予他们及其主管当局完全的访问、信息和审计的权利。尽管如此，许多外包协议并未给出充分的保障措施，无法对分包流程进行全面监控。这会影响机构评估相关风险因素的能力。

在不影响对外包安排的最终责任的情况下，金融服务机构可以使用与同一服务提供商的其他客户共同组织的联合审计。此外，也可以使用 CSP 提供的第三方认证和第三方或内部审计报告。

## 实践和立法对策

德意志交易所(Deutsche Börse)是一家德国国际交易所组织和市场基础设施提供商，于 2017 年成立了协作云审计集团 (Collaborative Cloud Audit Group)。这一全行业范围内的举措共同审计 CSP ，减少了所有相关方的工作量。[15]

2021 年，12 家欧洲金融机构成立了欧洲云用户联盟。该联盟的宗旨是在欧洲金融服务领域推广公共云系统的使用[16]。联盟中的金融机构一直在针对 CSP 制定通用安全标准和最佳实施规程。

机构目前借助一组来自不同组织的审计师开展的联合审计，并制定标准规则（自我监管）。云客户必须定期从 CSP 获得证据，证明满足商定的安全要求。证据应基于一套公认的规则，例如 ISO/IEC 27001:2022，该标准通常适用于金融服务行业的信息安全管理系统 (ISMS)[17]；ISO/IEC 27002:2022，适用于信息安全控制[18]；以及 ISO/IEC 27018:2019，适用于在充当个人可识别信息处理器 (PII) 的公共云中保护 PII[19]。在德国，云计算合规性控制目录 (C5) 是一套众所周知的综合性云服务安全标准[20]。

云客户必须核实适用范围和保护要求是否涵盖使用云服务的时间段。如果 CSP 使用分包商，则必须定期向云客户证明分包商执行了必要的审计。

同时，与 CSP 市场集中度相关的风险也在不断增加。如**图 4** 所示，因市场规模大，少数企业拥有大量全球数据。这引起了人们的关注。作为回应，欧盟委员会拟定了 DORA，根据该法案，关键信息和通信技术的第三方服务提供商（如 CSP）将受到所谓“牵头监督机构”的监督[21]。

## 云计算、创新与监管展望

在云计算的早期，反对使用云计算的主要理由之一是数据需要安全和保护。在合规方面，关于虚拟化计算资源的使用仍有激烈的讨论。外包数据流需要谨慎对待数据安全和保护问题。为评估综合现状而查看经验性的公共数据时，可能有人会问，乌克兰政府如何能够在 2022 年俄罗斯入侵期间访问和使用包含敏感数据的计算资源。乌克兰法律规定，某些政府数据和特定私营企业数据必须保存在实际位于乌克兰的服务器上。在俄罗斯入侵前一周，乌克兰议会出台了允许将公共和私营企业数据传输到云端的法规。此外，乌克兰政府为此公开呼吁援助。AWS 是最早做出回应的实体之一，该企业在 2022 年第三季度占据全球云服务市场的 32%[22]。

**少数占主导地位的 CSP 市场份额不断增长，与此同时风险也在不断增加。**

今天，云计算主要发生在提供服务器访问的各个数据中心。然而，这种趋势可能会发生变化。少数占主导地位的 CSP 市场份额不断增长，与此同时风险也在不断增加。我们对这些供应商的依赖程度非常高。CSP 的不可用、故障或其他一些事件可能危及金融实体的稳健性，最终，整个金融系统可能面临无法提供关键职能的风险，或面临其他不利影响的风险，包括巨额损失甚至破产。

虽然云服务可以使用多台服务器，但传统的云服务高度集中。这些资源由一个大型实体托管，该实体控制着客户的所有数据和应用程序。

大量的威胁和漏洞可能会危及云存储数据的完整性[23]。Microsoft 承认，由于存储服务器配置错误（机密性威胁），他们在 2022 年 10 月无意中暴露了与潜在客户的业务交易信息。Microsoft 试图将泄露的严重性降至最低，但据一家网络安全公司报告称，有 65,000 个实体（其中许多是企业）受到了此次泄露的影响[24]。若发生服务器中断，依赖度越高，损失越大。诸多企业在由三大 CSP 之一运营的数据中心托管他们的网站并存储其他数据。在过去几年中发生过多次中断事故，期间无法访问数据和服务（可用性威胁）[25]。

**ENJOYING THIS ARTICLE?**

- Read *Cloud Fundamental Study Guide. www.isaca.org/emerging-tech-cloud*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

因此，CSP 必须保证其机密性、完整性和可用性。例如，银行客户的个人数据可能因服务器配置错误而泄露（机密性威胁），或者客户尽职调查 (KYC) 数据可能因身份和访问管理薄弱而导致被更改或删除（完整性威胁）。由于无法访问其集中托管服务（可用性威胁），通过 Web 浏览器提供金融工具的多边贸易机构可能突然意识到没有交易费用。显然，依赖 CSP 存在风险。

为保护个人数据免受隐私侵犯，欧盟推出了《通用数据保护条例 (GDPR)》。GDPR 由三个主要部分组成：数据主体、数据控制者/联合控制者和数据处理者。当用户不能直接控制数据处理所涉及的各个阶段时，GDPR 会将共同责任分配给处理者，而不是控制者或联合控制者。例如，为了遵守 GDPR，向用户提供托管服务的基础架构即服务 (IaaS) 提供商负责处理该基础架构生成的数据（如记录和管理系统和访问日志）。在参与涉及个人数据的活动之前，参与者需要满足多项要求。在存储数据之前，必须满足以下条件：必须获得客户同意、数据必须加密、数据必须随时可擦除、保留期限必须短于所有数据活动所需的总时间。

要正式或自动验证是否符合这些 GDPR 要求已经变得很困难。此外，实际上违规行为时有发生。2021 年 7 月，卢森堡国家数据保护委员会发布了一项针对 Amazon Europe Core 的决议。据发现，亚马逊在对个人数据的处理方面不符合 GDPR。该委员会对其处以 7.46 亿欧元的罚款，并强制修订相应做法[26]。

金融机构有义务控制其外包企业。ISO/IEC 27001 的补充标准于 2014 年获得通过，这是首个全球云隐私行为准则 (ISO/IEC 27018:2014)，最新版本已于 2019 年发布[27]。该标准基于欧盟数据保护规则，为作为个人身份信息 (PII) 处理者的 CSP 提供了详细的指导，帮助进行风险评估并实施充分且有效的保护措施以保护 PII。

## 寡头垄断市场（例如云行业）可以通过使用 DLT 的去中心化服务补充。

根据**图 4**，最大的电子商务平台 (Amazon) 约占全球云市场的三分之一。因此，与 AWS 的其他细分市场可能存在利益冲突。

另一方面，从利用 DLT 作为治理技术的去中心化服务的演变，可以观察到：

> *如果区块链是一种无需可信中介即可实现可信交易的新方式，那么很快就能获得无中介信任……中介控制的信任存在一定的摩擦，但现在，有了区块链，可以拥有无摩擦的信任*[28]。

这可能会产生一种新的技术驱动型组织激励模式，在这种模式下，数据所有者和创新者（即应用程序开发人员和平台运营商）之间可以平等地共享利益。DLT 通过将权力从中心化的大科技公司部分重新分配，使其进一步去中心化，从而帮助去平台化[29]。可以通过使用 DLT 的去中心化服务补充寡头垄断市场（例如云行业）。

去中心化系统是分布式系统的一个子集。“去中心化”一词意味着决策制定过程中没有单一的点。每个网络节点决定自己的行为，由此产生的系统行为属于聚合响应。“分布式”一词意味着处理是在多个节点上共同进行的，但决策仍可能是集中的，并且使用完整的系统知识[30]。这个理念可以应用于分散式云存储，以了解云市场可能如何进一步发展。通过使用 DLT 池化（免费）个人的计算资源，云市场可以实现分布式和去中心化，创建一个没有单一网络故障点的存储网络[31]。该网络可以完全冗余地托管应用程序和网站，并为有需求的实体提供大量的服务器资源。这种架构没有单点故障，并且在地理上是分布式的。当一个网络节点遭到攻击者破坏时，可以自动创建一个新节点，

随着技术成为战略性考虑因素，金融机构必须监控颠覆性技术，并根据需要不断修改其产品组合和内部流程。

这样攻击就不会太有效。节点跨越网络，正如传统集中式系统内的服务器一样。在这样的去中心化模式中，需要激励这些网络节点，使它们为网络提供计算能力。正如传统的云领域一样，运营成本（例如构建和运营数据中心以及管理网络的成本）由客户支付。因此，去中心化模式中的节点运营商会获得货币补偿。

DLT 不是在一个中央数据中心甚至现场托管数据，而是提供了一种分散的、低风险的数据存储形式，这种存储形式基于数千个地理上分布的节点。考虑到不同区域的监管要求，地理定位功能可用于选择网络节点的地理位置。每个节点仅存储数据碎片，没有读写权限（数据保护）。加密技术用于确保数据只能由目标接收人处理和读取，并防止对数据进行任何更改或操作。

由此可见，DLT 创建了一个创新的生态系统。DLT 第一个广为人知的用例是加密资产（如比特币）。围绕这种新资产类别的监管已经变得动态化，欧盟加密资产市场 (MiCA) 法案就说明了这一点，该法案的初衷是为投资者提供必要的保护，同时维护金融市场的完整性和金融系统的稳定性。正如 MiCA 所展现的那样，监管基于 DLT 的应用程序和服务而不试图监管技术本身是可行的[32]。

一旦去中心化的云基础设施达到一定的程度，就需要新的办法监管金融服务环境下的这些服务提供商。这是由于该行业具有基于技术（尤其是去中心化和分布式）的特征[33]。

FTX 在 2022 年 11 月申请破产和涉嫌欺诈活动之前，一直是一家加密货币交易所。FTX 的崩溃可能会刺激金融监管机构在金融 DLT 领域制定更多的法律规则，尤其是在风险管理和 IT 安全方面[34]。

使用任何第三方都必然会有交易对手风险。FTX 及其附属实体涉嫌的欺诈活动本可以借助 DLT 在技术上加以防护，因为 DLT 可以存储和安全管理加密资产。

## 最佳实践

以信息和数据的创建、收集和保护为中心的数字经济正在发展。云计算等颠覆性技术的出现，孕育着新的市场和商机。银行业尤其如此。然而，随着数据成为不可或缺的资产和关键的竞争差异化因素，这一过程也加剧了竞争、监管和网络安全方面的担忧。因此，针对云计算相关问题，我们提出了一些实用建议：

- 管理层应评估混合和多云方法来解决依赖风险。依赖性评估和退出方案必须给予定期审查。
- 在金融领域，IT 系统、IT 流程和信息网络的其他组成部分必须确保数据的完整性、可用性和机密性。为此，IT 系统和流程设计必须基于通用标准。关于外包协议，内部审计团队需要定期根据公认的标准（例如 C5:2020、ISO/IEC 27018:2019）评估审计报告。在任何时候，金融机构都必须控制其外包服务提供商，包括分包商。如果发现问题，内部审计团队必须执行进一步检查。
- 无论如何，仅仅依赖审计报告是不够的。必须制定相应的机构控制措施，并且这些措施必须充分且有效。有些审计报告（例如 C5:2020）确实描述了相应的控制措施。客户需要检查这些控制措施，并且补充其他控制措施。
- 建议欧盟的金融机构以及为这些机构提供服务的 CSP 接受健康检查，了解其 DORA 合规状态。
- 随着技术成为战略性考虑因素，金融机构必须监控颠覆性技术，并根据需要不断修改其产品组合和内部流程。

## 结论

新技术、新参与者和有利的监管制度的出现影响了欧洲的金融业。金融科技公司 (Fintech) 推出了新的服务并改变了企业与客户互动的方式，进而满足了客户的金融需求。云计算技术是一个重大的颠覆性力量，它的出现引发了动态监管指引。

云计算具有诸多优势。IT 服务可以按需使用，这些服务具有可扩展性和灵活性，可以根据功能范围、使用时间和用户数量计费（如果需要）。此外，还可以利用 CSP 的专业知识和资源，将内部资源释放出来用于其他任务。除了流程之外，银行产品也可以通过云服务创新。

然而，在实践过程中，使用云的预期效益并不总能实现。一个常见的原因是，在购买云技术之前，没有充分考虑关键的成功因素。

很明显，云计算在带来益处的同时也存在风险。具体而言，近年来对领先 CSP 的依赖已显著增加。与此同时，正如 DORA 所述，金融行业对云服务的监管也在加强。根据该规则，CSP 有义务向其金融行业的客户及其主管当局授予完全的访问、信息和审计权限。很快，所谓的牵头监督机构将成为欧盟的新监管机构，监督 CSP 以确保金融市场的稳定并保护消费者。

开放银行和 DLT 构成了基于云计算的互补用例，金融机构可能会提倡 DLT 以提高效率和创新收益。基于 DLT 的云计算使企业能够最大限度地降低依赖风险。由于没有单点故障，单个网络节点对存储在区块链即服务 (BaaS) 数据库中的数据没有读写权限。这些新产品的定价较低，因此云计算可能会得到 DLT 领域参与者的补充。

要使金融市场源源不断地创新，监管必须允许和培养开放且无需许可的关系，而创新是收入的关键。

从金融监管的角度看，这项技术本身是否需要像互联网一样受到监管是值得商榷的。然而，要使金融市场源源不断地创新，监管必须允许和培养开放且无需许可的关系，而创新是收入的关键。

通过开放银行，第三方提供商可以访问金融系统，这种系统的采用率可能会有所增加。因此，对外包管理的要求仍将是监管部门的重点，确保金融市场的稳定，同时有利于保护消费者。

## 尾注


1 Statista, *Cloud Computing Dossier*, Germany, 2022, *https://www.statista.com/study/15293/cloud-computing-statista-dossier/*
2 *同上。*
3 *同上。*
4 Statista, *Marktanteile der führenden Unternehmen am Umsatz im Bereich Cloud Computing weltweit im 3*, Quartal 2022, Germany, 2022, *https://de.statista.com/statistik/daten/studie/150979/umfrage/marktanteile-der-fuehrenden-unternehmen-im-bereich-cloud-computing/*
5 在本文中，“银行”一词表示广泛的金融服务。
6 IDW Verlag, Kreditinstitute, *Finanzdienstleister und Investmentvermögen*, Germany, 2020
7 Kassab, M.; P. Laplante; “Trust Considerations in Open Banking,” *IT Professional*, vol. 24, iss. 1, 2022, p. 70–72
8 Heckel, M.; F. Waldenberger (Eds); *The Future of Financial Systems in the Digital Age: Perspectives From Europe and Japan*, Springer, Singapore, 2022
9 Gramlich, V. et al.; “Decentralized Finance—The Rise of a New Paradigm?” REthinking Finance, vol. 6, 2022 p. 30–40
10 Veeam Software, *2022 Data Protection Trends Report*, Switzerland, 2022, *https://go.veeam.com/wp-data-protection-trends-2022*

11 European Banking Authority (EBA), *Consultation Paper: EBA Draft Guidelines on Outsourcing Arrangements*, France, 22 June 2018
12 European Banking Authority (EBA), "Recommendations on Outsourcing to Cloud Service Providers," 20 December 2017
13 *同上。*
14 Hashemi, J. B.; A. Yavuz; D. Akdeniz; J. Putters; "Pooled Audits on Cloud Service Providers, Part 1," *de IT-Auditor*, 11 May 2020, *https://www.deitauditor.nl/wp-content/uploads/2020/03/pooled-audits-on-cloud-service-providers.pdf*
15 Deutsche Börse Group, "Deutsche Börse and Microsoft Reach a Significant Milestone for Cloud Adoption in the Financial Services Industry," 6 May 2019, *https://deutsche-boerse.com/dbg-en/media/press-releases/Deutsche-B-rse-and-Microsoft-reach-a-significant-milestone-for-cloud-adoption-in-the-financial-services-industry-1540058*
16 European Cloud User Coalition (EUCU), "Why Did We Form a Coalition?" *https://ecuc.group/about-us/*
17 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection—Information security management systems—Requirements*, Switzerland, October 2022, *https://www.iso.org/standard/82875.html*
18 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection—Information security controls*, Switzerland, February 2022, *https://www.iso.org/standard/75652.html*
19 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27018:2019 *Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, Switzerland, January 2019, *https://www.iso.org/standard/76559.html*
20 Amazon Web Services (AWS), "Cloud Computing Compliance Controls Catalog (C5)," *https://aws.amazon.com/compliance/bsi-c5/*
21 European Council of the European Union, "Digital Finance: Digital Operational Resilience Act (DORA)," 28 November 2022, *https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/*
22 Data Center Dynamics, "Ukraine Awards Microsoft and AWS Peace Prize for Cloud Services and Digital Support," 7 July 2022, *https://www.datacenterdynamics.com/en/news/ukraine-awards-microsoft-and-aws-peace-prize-for-cloud-services-digital-support/*
23 Kaya, D. et al.; "Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques," *International Journal of Research Publication and Reviews*, vol. 3, iss. 2, 2022
24 Kan, M.; "Microsoft Leaks Business Customer Data via Misconfigured Storage Server," *PC Mag*, 19 October 2022, *https://pcmag.com/news/microsoft-leaks-business-customer-data-via-misconfigured-storage-server*
25 Gunawi, H. *et al.*; "Why Does the Cloud Stop Computing? Lessons From Hundreds of Service Outages," Proceedings of the Seventh ACM Symposium on Cloud Computing, October 2016
26 DataGuidance, "International: CNPD Imposes €746M Fine on Amazon for Targeted Ad System," 30 July 2021, *https://www.dataguidance.com/news/international-cnpd-imposes-746m-fine-amazon-targeted-ad*
27 *Op cit* ISO/IEC 27018:2019
28 Mougayar, W.; *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, John Wiley and Sons, USA, 2016
29 Flux, XDAO, *https://runonflux.io/xdao.html*
30 Eagar, M.; "What Is the Difference Between Decentralized and Distributed Systems?" *Medium*, 4 November 2017, *https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462*
31 Krishnaraj, N. *et al.*; "The Future of Cloud Computing: Blockchain-Based Decentralized Cloud/Fog Solutions—Challenges, Opportunities, and Standards," Blockchain Security in Cloud Computing, Springer, Switzerland, 2022
32 Beck, B.; J. C. Schmike; M. Hörauf; P. Scholl; "EU Markets in Crypto-Assets (MiCA) Regulation Expected to Enter Into Force in Early 2023," Mayer Brown, 14 December 2022, *https://www.mayerbrown.com/en/perspectives-events/publications/2022/12/eu-markets-in-crypto-assets-mica-regulation-expected-to-enter-into-force-in-early-2023*
33 De Filippi, P.; A. Wright; *Blockchain and the Law*, Harvard University Press, USA, 2018
34 Smith, T.; "What Is FTX?" Investopedia, 22 December 2022, *https://www.investopedia.com/ftx-exchange-5200842*