云环境下的金融服务现状

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

CSA 金融服务行业工作组官网地址是：

https://cloudsecurityalliance.org/research/working-groups/financial-services/

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

报告支持单位

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫、企业等各大行业用户与各类型企业用户提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立了海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

工商银行软件开发中心 1996 年 6 月在珠海成立，主要负责全行应用研发、新技术研究、技术管理、服务支持、生产运维、人才培养任务，目前分布在珠海、广州、上海、北京、杭州、成都、西安等 7 个城市办公。成立以来，软件开发中心聚焦科技创新能力提升，深耕行业应用，赋能业务发展，先后自主研发了 4 代核心银行系统，建设了 24 条业务线，涵盖 195 个业务系统，构建了支撑全集团经营管理、服务境内外客户、丰富完善的全功能应用产品体系。获得人行科技发展奖 169 项，人工智能、隐私计算、分布式技术能力获得行业最高评价，以科技创新助力全行高质量发展。

绿盟科技和中国工商银行是 CSA 大中华区的理事单位，支持该报告内容的翻译，但不影响 CSA 研究内容的开发权和编辑权。

英文版本编写专家

作者：Hillary Baron　Troy Leach　John Yeoh

贡献者：Josh Buker　Daniele　Catteddu　Ryan Gifford　Jez Goldstone

Sean Heide　Erik Johnson　Alex Kaluza　Stephen Lumpe (graphic design)

Vinay Patel

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正！ 联系邮箱 research@c-csa.cn； 国际云安全联盟 CSA 公众号。

序言

云计算技术的快速发展，如云原生、无服务器等概念层出不穷，催生了很多新的云服务模式，也带来了诸多安全风险，对云计算安全的关注将成为持续的话题。

同时，各行各业也开始大量采用云计算基础设施，构建基于云原生的服务。特别是金融行业，云优先（Cloud First）和只有云（Cloud Only）已经成为企业构建新业务的策略。云计算业务日益增加的使用，与不断增加的监管要求和有限安全投入之间形成了客观上的冲突。

对于企业的负责人而言，需要关注云安全新技术的发展，例如人工智能、量子计算和 DevSecOps；又要借鉴头部企业在云化趋势下安全的最佳实践，包括人员、流程和技术层面所需要做的工作。本白皮书通过对金融行业企业的安全相关负责人调查，给出了近年来的云环境下金融服务现状和机遇，以及 CSA 后续的行动计划。相信读者会从中受到启发，更好地执行适合自身的云化策略和行动。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

前言

云安全联盟（CSA）是一个非营利性组织，其宗旨在于广泛推广确保云计算和 IT 技术中的网络安全最佳实践。CSA 同时也向业界相关成员提供对其他各类网络安全问题的指导。CSA 的成员包括安全从业人员、安全厂商及其他专业团体。CSA 的主要目标之一是对信息安全趋势进行调查与评估工作。这些调查向组织提供当前信息安全技术成熟度、意见、兴趣和趋势等各类信息。

CSA 的金融服务社区的成员来自全球各类银行、金融科技公司、支付处理机构、金融咨询机构、保险公司、金融监管机构、数据保护机构和其他国家监管机构。随着金融业对云的使用持续增长，其所带来的挑战与关注度也在同步上升。过去几年中，CSA 为了更好地了解金融业对云计算技术的现状与挑战，从而进行了行业调研。今年研究的目标是为了更好地了解如下内容：

- 从金融机构的角度分析云解决方案的采用水平和需求，与 2019-2020 年进行的调查进行比较。
- 当前面临的挑战以及与云服务供应商的合作。
- 识别在保护金融数据及相关资产安全的云服务中创建指引的新机遇。

目录

摘要

近年来，金融服务业对云服务的使用大幅增长，预计其将伴随着使用和集成云服务提供商（CSP）所提供的功能进一步增长，以替代传统的银行业、商业和其他金融交易方式以及交换金融数据的方法。

本报告的目的是评估行业现状，并于与三年前行业初期 CSA 类似的调查结果进行比对，来证实金融服务业领导者正在进一步利用云服务来发现的当前问题和新的机遇。

在与本报告相关的访谈中，金融科技公司的首席信息安全官（CISO）和云架构师表示，利用可扩展性和快速推向市场的能力，将创新引入市场比以往的做法更划算。此外，银行业专业人员表示，受新冠疫情的影响，利用云服务实现远程办公或快速的动态更新、部署新的软件服务的主要原因是其能够提供符合法规的一致部署协调的安全策略。

本报告中的监管是最具影响力的因素之一。尽管将越来越多的云计算被用于托管受管控数据，但对于云服务提供商如何理解和确保其遵守各国法律仍是值得深思的问题

然而，新的方案伴随着新的风险，受访者表示，尽管云服务的使用正在不断增加，但其进展需要与 CSP 和金融服务业展示其符合法规、整体数据保护的能力以及员工对管理工作的舒适程度保持相对一致。

本报告中除了监管之外的主题还包含数据管理的重要性、访问的完整性、威胁情报和良好的企业风险管理。

本报告中最明显的一点是云服务正在不断深入金融服务的各个方面并有望被长时间使用。云服务是否被采用已不在是问题，而更多问题是“如何”使用。如何采取云原生安全策略，如何应用零信任方法，如何指导员工、监管机构和云合作伙伴等所有相关合作方。

本报告中与 CSA 共享的信息有助于明确未来的研究内容、标准要求、培训和指导等该社区可能感兴趣的内容。在报告的最后，我们将分享一些建议，以供我们的金融服务业领导委员会考虑。

调查方法

本报告的调查方式是通过与 2020 年《金融服务部门云使用情况调查报告》的调查结果进行对比，来确认金融服务业对云服务的使用和准备情况。许多问题与最初由 CSA 金融服务工作组最初的问题相同，以进行公正的对标。

同时，还包括了其他一些问题，以便更好地了解对云控制矩阵和 STAR 计划的现状，以及由金融服务业领导工作组、CSA 分析师和其他行业专家的问题。

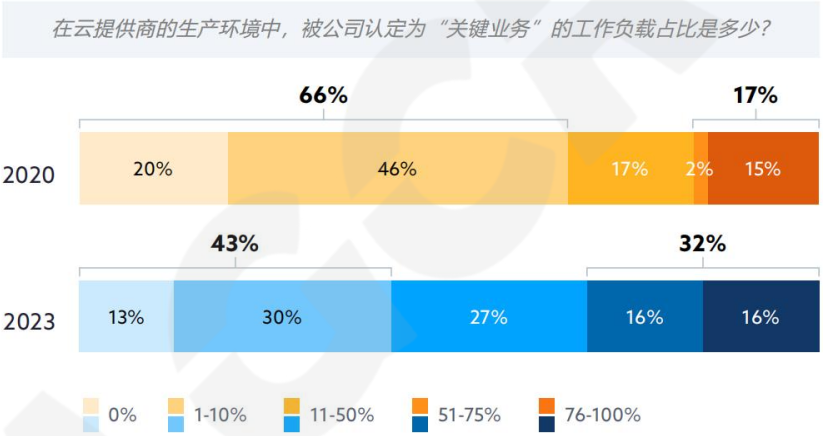
此外，我们还对首席信息安全官、首席风险官、金融服务内部云架构和数据治理的其他负责人进行了多次采访。

调查结果

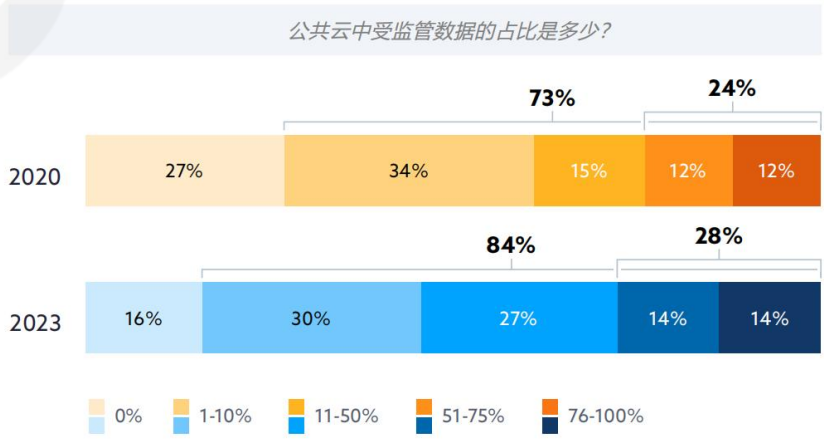
日益增长的云服务使用情况

自新冠疫情以来，金融服务业使用云服务的情况不断增长，几乎所有金融机构都在使用某类云计算服务。**98%的受访者**表示他们公司正在使用云计算服务，高于 **2020 年的 91%**。许多受访者讨论了增长的原因，其中一部分是疫情导致新工作场景带来新的发展需求，以适应远程办公和客户对其账户的远程访问。

目前，业界对于在业务关键中使用云计算工作负载的把握已有显著增加。2020 年的调查结果显示，当被问及在生产中的“关键业务”工作负载占比时，约 **66%**的服务提供商表示没有关键业务（20%）或关键业务占比小于十分之一（46%）。这些数字在 2023 年的调查结果中有了显著下降**(43%)**，拥有高占比关键业务工作负载的公司数量几乎翻了一倍，从 **17%**增加到 **32%**。

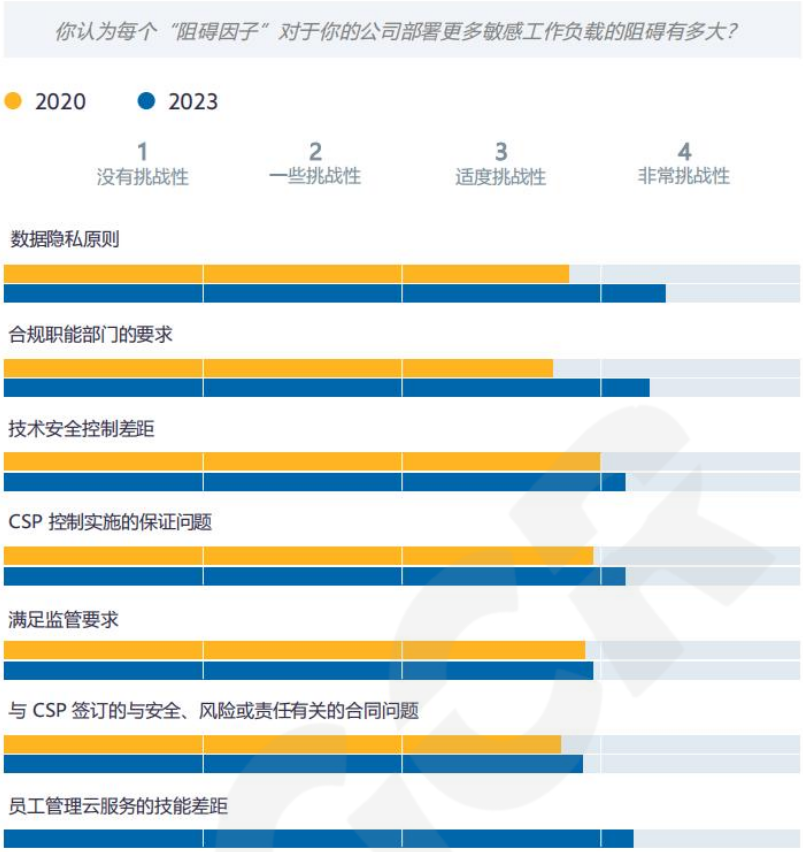


我们之前的调查相比，在公共云中使用受监管的工作负载的情况增加了，**84%** 的受访者表示他们的一些受监管数据存储在公共云中，前期调查比例为 73%。同时，许多金融服务机构采取了私有云和公共云混用的方式，并继续进行内部部署操作。然而，也有公司认识到许多服务提供商已经将软件服务迁移到云上，这也影响了云的更广泛使用。尽管如此，仅有 28%的受访者表



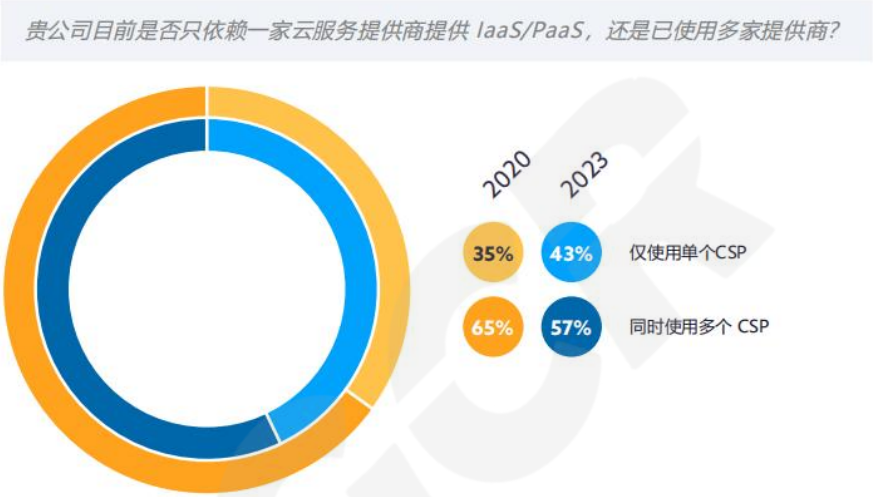
示他们的大部分（50%及以上的工作负载）受监管数据存储在公共云中，这与 2020 年的 24%相比略有增加。

有趣的是，在被问及是什么阻碍公司进一步采用敏感工作负载时，给出的第一个“阻碍因子”几乎都是“难度增加”。在监管和合规功能，尤其是隐私方面，仍是除了技术人员配备外最大的挑战。



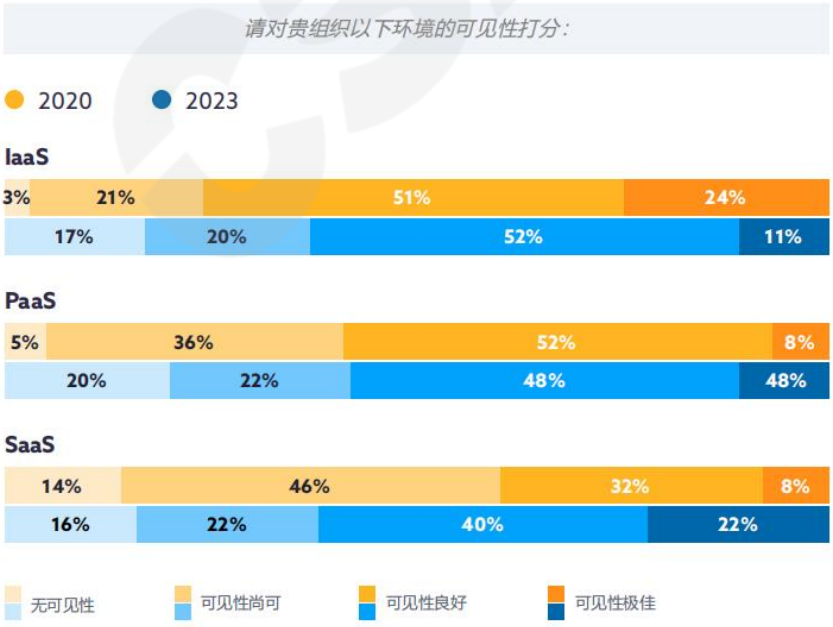
金融服务多云化是当前现状

依赖单一的云服务提供商，还是同时注册使用多家云服务，是困扰企业的一个普遍问题。对企业多云使用的目的表明，许多企业已经认识到云提供商多样化的好处，例如可以降低供应商锁定的风险，确保云环境更具有灵活性和弹性。通过使用多家云服务，企业还可以利用每个供应商的独特功能和最佳功能，避免被某一单一供应商绑定，从而优化其云战略，最大限度地提高投资价值。



调查显示，**57%** 的企业目前使用多家云服务来满足其 IaaS/ PaaS 需求。

尽管政府监管机构要求支持多云服务使用以提高企业业务弹性，但受访的企业首席信息安全官们提到了当前多云发展方面所面临的挑战。主要使用单一云服务商来提供 IaaS/PaaS 的受访者人数略有增加，这也从侧面印证了首席信息安全官们的观点。第三方云服务之间的信息互通可操作性、信息可移植性、可视性、数据管理、安全策略等方面的复杂性导致了使用多云环境的困难。



随着跨云堆栈的第三方管理对于多云部署变得越来越重要，可见性仍然是一个令人担忧的问题。

与上一份报告中的可见性对比显示，认为其对云堆栈不可见的受访者数量意外增加，尤其是对 IaaS 和 PaaS 云堆栈。总体而言，受访者对 SaaS 和 PaaS 的可见性从

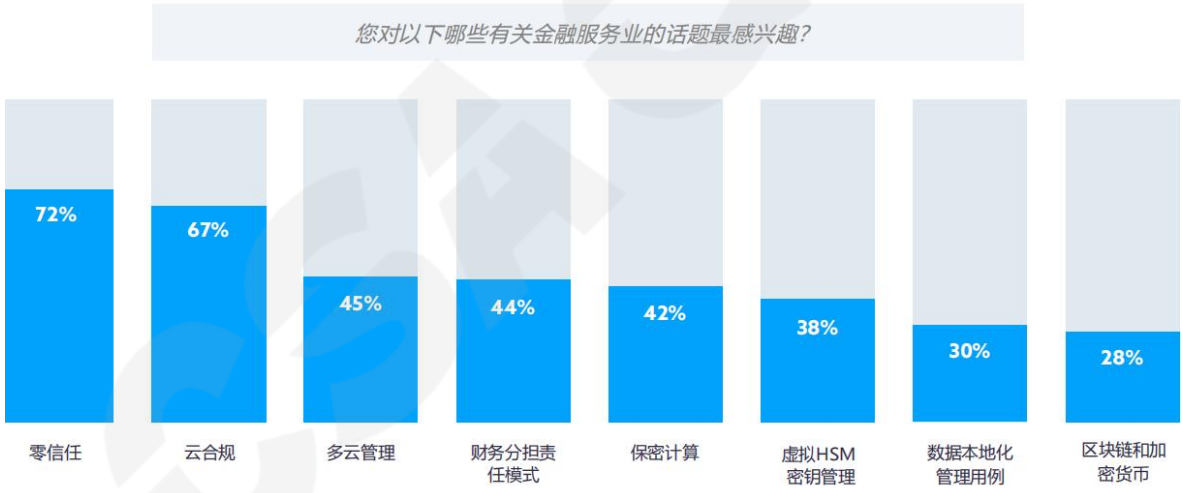
良好到优秀有所增加，但对 IaaS 环境的可见性却有所下降。对企业信息安全负责人的访谈的进一步评估显示，这不仅仅是可见性的问题，而是在跨云环境中缺乏通知和变更上下文信息，或者未披露。这为主要的 IaaS 提供商在操作和活动级别添加额外的可见性、控制和上下文层面留有余地。云原生应用保护平台（CNAPP）和变更通知标准等解决方案的改进将在这方面发挥主导作用。

这种可见性的缺乏可能导致未知的安全和合规风险，例如无保障、无法证明行规符合状态等。企业应该考虑实施健全的 SaaS 管理策略，以获得更好的可见性和对云环境的控制。

零信任为金融云访问增加完整性

金融组织对查看或操作财务记录的权限的完整性有多种期望。有几个因素促成了这一点，包括上述提到的数据管理方面，以保持机密性， 以及防止由于对数据的完整性保护不当而导致的数据丢失或损坏，如洗钱或盗窃。这也是调查中指出零信任是当前首要任务的一个可能原因。

零信任方法要求对敏感数据和资产的访问进行持续验证，同时最大限度地降低信息泄漏的影响。



在云环境中，应定期测试所有第三方访问的继承安全控制，以验证权限是否仍然相关。这种方法有可能实现保护金融资产的业务和技术目标，同时证明符合各种行业规定。

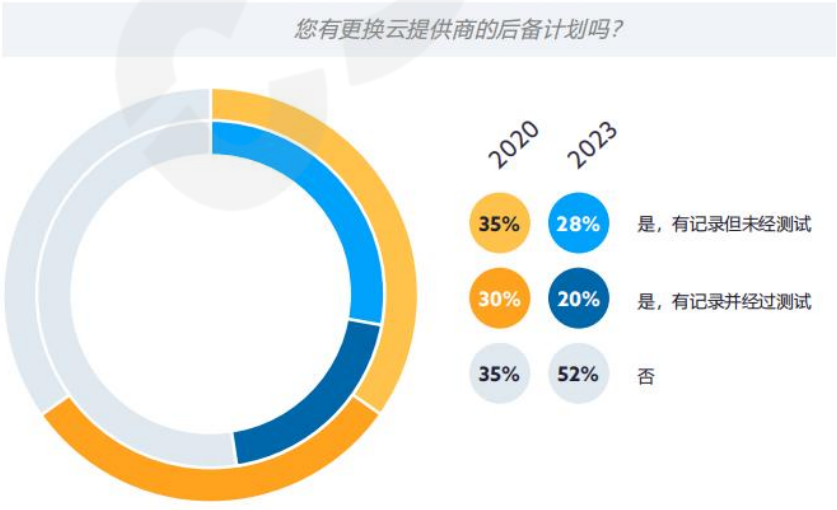
加强云的数据管理能力

对于金融服务业来说，数据的机密性以及了解数据的流向和路由方式至关重要。数据在存储、传输和使用过程中都必须受到保护，以便确认公司货币会计的合法性，并保护在该企业托管资金的所有消费者。此外，还需要数据的可追溯性和清晰的审计跟踪，随时了解数据的移动和保护情况。几位受访者表示，在云端记录财务数据的可扩展性优于许多本地部署方法，这为向云端迁移提供了保障，但必须保持数据可靠性和一致性。

然而，受访者对数据暴露表示担忧，这也导致对敏感数据迁移至公有云保持谨慎态度。通过使用零信任成熟度模型（例如 CISA 零信任成熟度模型 v2）来衡量云端的数据管理安全性，同时应用共享安全责任模型（SSRM）和专门针对云的控制措施（例如 CSA 云控制矩阵（CCM））帮助建立与数据外泄、机密性和配置错误相关的透明性要求。

业务连续性对云端业务至关重要

可用性对于保持业务连续性和确保机构平稳运行至关重要。美国财政部在近期报告中强调了金融机构的弹性和多云化支持的能力。欧盟（EU）在《欧洲网络安全法案》（EU- CSA）和《欧盟网络与信息安全指令》（NIS2 指令）2022/2555 中考虑到了网络弹性问题。



云计算通过将关键数据和应用程序安全地存储在第三方服务和基础设施中，以降低数据丢失和现场基础设施故障的风险，从而确保金融服务的业务连续性。同时，这些服务的设计必须始终符合不断变化的金融服务业安全标准和要求。金融监管机构、审计员和检查员一直在问类似于 "如果 云服务提供商完全瘫痪怎么办？”这样的问题。这凸显

了制定包括备份和灾难恢复解决方案在内的强大多云管理策略的必要性。但是，这可能需要付出云端的效率和运营成本。有趣的是，报告显示，与 2020 年调查的受访者相比，当前服务提供商的备份计划准备程度略有下降。

与首席信息安全官们探讨后发现（CISO）云端数据迁入和迁出成本存在不均衡性。将数据迁出的成本远远超过向公有云环境迁移数据的成本。

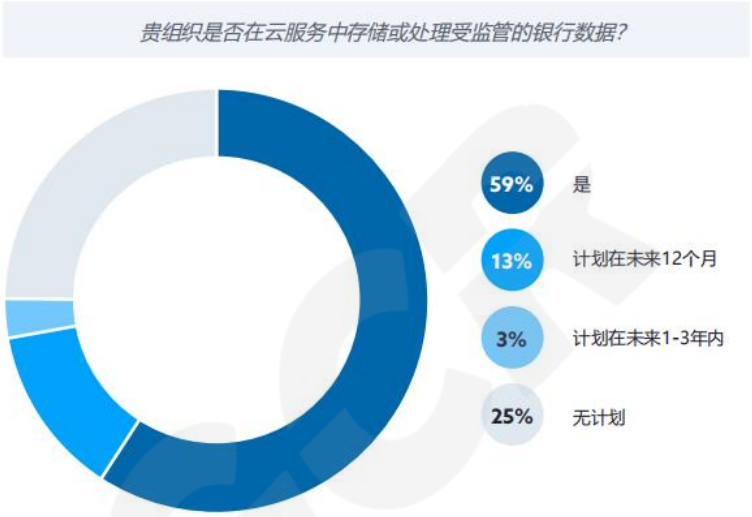
分布式拒绝服务（DDoS）和勒索软件等攻击的增加进一步加剧了对可用性的担忧，尤其是在金融服务业。

根据 Cloudflare 的数据，在 2022 年 6 月的 DDoS 攻击中，金融服务占 45%。《Verizon 数据泄露调查报告》（DBIR）连续将金融服务列为受数据泄露影响最严重的行业。CSA 早期的调查报告显示，DDoS 和勒索软件是与数据泄露、系统访问权限丢失、系统破坏、持续对抗性访问、帐户劫持和欺诈相关的最主要的安全关注点。DDoS 和勒索软件能够封锁组织的关键数据,使运营陷入停滞，因此它们在最新的 CSA 《云计算 11 大顶级威胁》 报告中被着重提及就不足为奇了。

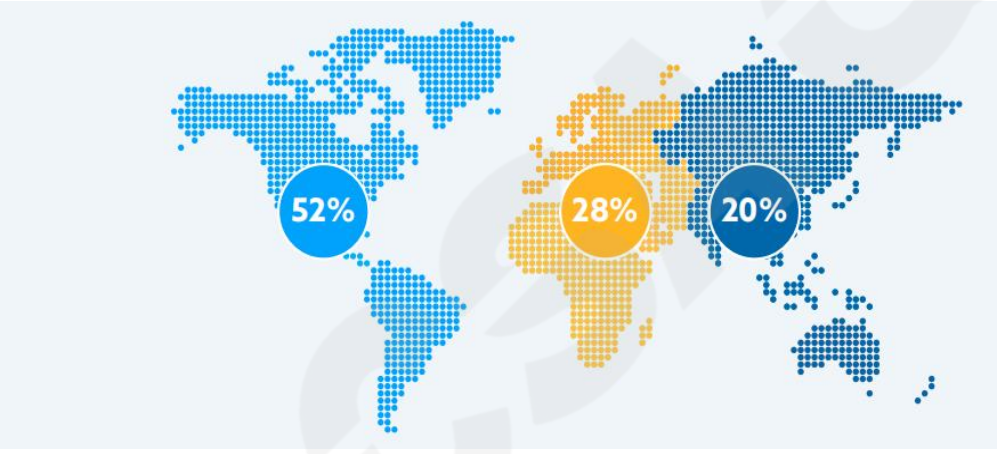
此类攻击会严重扰乱运营并导致声誉受损，因此金融服务机构必须制定有效的业务连续性计划（BCP）和事件响应计划（IRP）战略。企业组织需要投入强健的网络空间安全措施，定期测试其备份和恢复计划，降低宕机风险，确保系统始终可用。通过部署主动的安全防御措施并进行持续的改进，金融服务业可以自信地驾驭云环境，保护其关键数据和运营。

满足云端监管要求

金融服务机构在其运营或开展国际业务的所有司法管辖区都受到当地法律和联邦法律的监管。近年来，调查受访者指出，监管机构对第三方（尤其是云服务提供商）的审查力度加大，要求其提供文件并证明其符合各种标准框架，称监管机构对第三方的关注能够影响安全性。受访者提到，备受瞩目的金融数据泄露事件和新法规的出台是引起这种关注的催化剂。

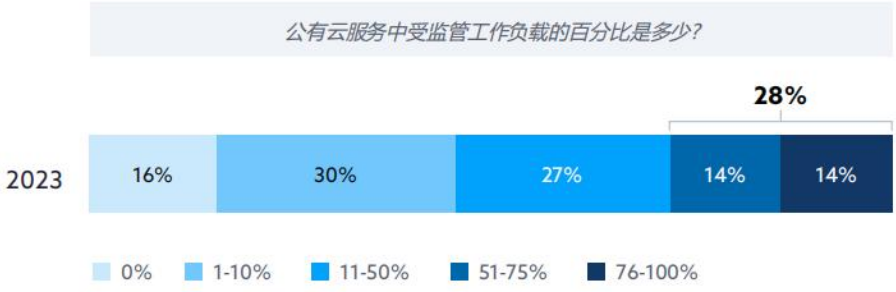


尽管如此，大多数金融服务机构在合规数据方面仍然使用云计算，其中有 **59%**的受访者表示其在云服务中存储或处理受监管的银行信息，只有 **25%**的受访者表示未来没有这样的计划。



参与调查的全球代表来自亚太地区（**20%** 的受访者）、欧洲、中东和非洲地区（**28%** 的受访者）以及美洲地区（**52%** 的受访者），这表明全世界都在关注如何解决云环境中的监管问题。

虽然大多数金融服务机构都在广泛部署云服务，但只有 **28%** 的受访者表示他们将大部分受监管的工作负载部署在公有云上在

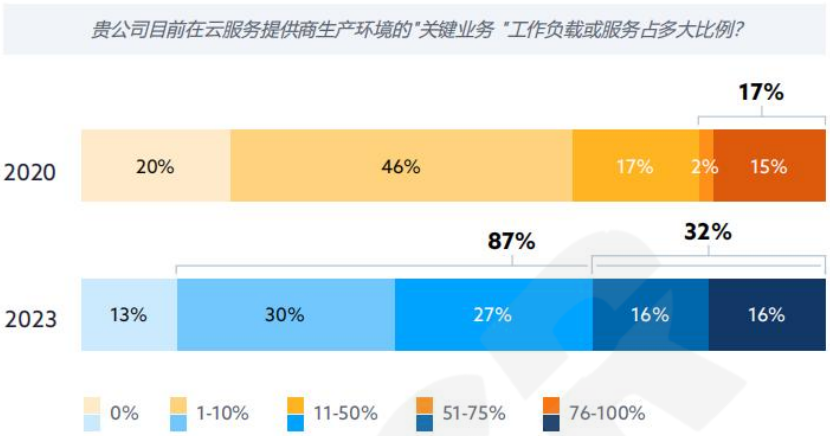


访谈中，受访者认为云服务提供商缺乏透明度、无法向审计人员证明合规性或担心没有足够的

网络安全资源进行从容的管理是不打算进一步在公有云上处理受监管数据的主要原因。

在云中拥有大部分关键业务工作负载（50% 或以上）的企业数量在短短三年内几乎翻了一番。

87%的金融组织已将其关键业务工作负载转移到云中。另有 15%（从 **17%** 增长到 **32%**）的企业正在将一半以上的关键业务工作负载转移到云中。



此外，预计在未来 12 个月内 72% 的企业会将受监管的银行数据转移或存储在云端。（较 2020 年的 63%有所增加），该报告显示未来金融服务业对云的信任和依赖程度有所提高。

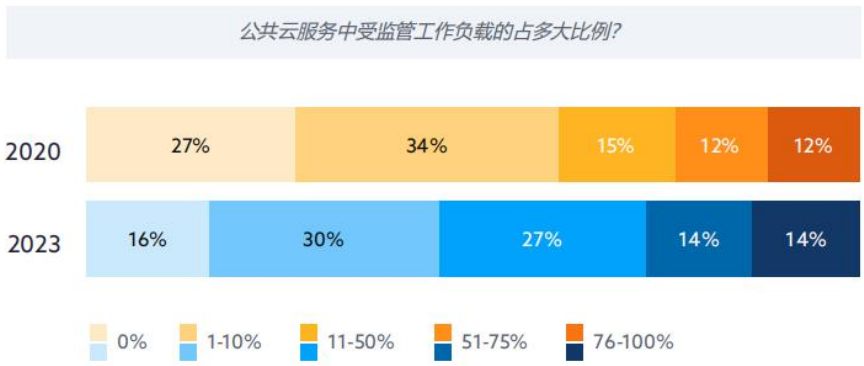
数据隐私、主权和本地化

近年来，世界各国政府已经建立或考虑了有关数据主权和数据本地化的立法，这些立法可能会限制金融服务实体可能拥有的个人金融或其他个人数据的传输。这些法规可能会影响金融服务机构及其客户。此外，这可能会影响在这些国家托管或开展业务的云服务提供商。

某些数据本地化法律要求首先将收集的个人信息存储在国内，然后再进行跨境传输。而其他法规可能更为严格，防止外国系统存储与该国公民相关的任何数据。在访谈中，首席信息安全官们建议内部法律顾问定期监控这些特定的变化，风险专业人员则要制定计划，对可能需要进行的调整保持警惕，以证明遵守了相关规定。

本报告的一些受访者表示，法律复杂程度越来越高，金融服务机构和云服务提供商越来越难搞明白，致使他们对进一步采用云服务犹豫不决。其中一些普遍引用的例子包括欧盟的《欧洲网络安全法案》（EU- CSA）和《通用数据保护条例》（GDPR）。

与 2020 年的调查结果相比，出现了一个明显的趋势，即来自金融服务机构的受监管工作负载在公有云服务中所占的比例总体上有所增加。特别是在报告中受监管工作负载在 11-50%之间的受访者比例从 **15%**增加到 **27%**，而受监管工作负载为 0%的受访者比例从 **27%**下降到 **16%**。



受访者对于识别的隐私和监管阻碍的所有类别没有明显的区分。所有 "阻碍因素 "都被认为在防止部署更敏感的工作负载方面具有中度或高度挑战性，具体包括：

- 数据隐私规则；
- 合规职能部门的要求；
- 技术安全控制差距；
- 满足监管要求；
- 云服务提供商控制实施的保证问题；
- 与云服务提供商 签订的与安全、风险或责任有关的合同问题；
- 员工管理云服务的技能缺口。

监管机构对云服务审计实践的理解

在访谈和调查中提出的一个共同点是，监管机构和审计师需要更广泛地了解云服务的审计方法。

受访者提到的几个主题包括监管机构更好地理解不同云平台之间的差异，例如：

- 每个云服务提供商独特的安全特性和术语；
- 为保证弹性和快速扩展部署多云环境的低效性；
- 管理不同云服务提供商环境所需的额外成本和资源；
- 管理不同云服务提供商环境所需的人员培训和协作；
- 通过一次性评估来满足多个监管要求的验证能力。

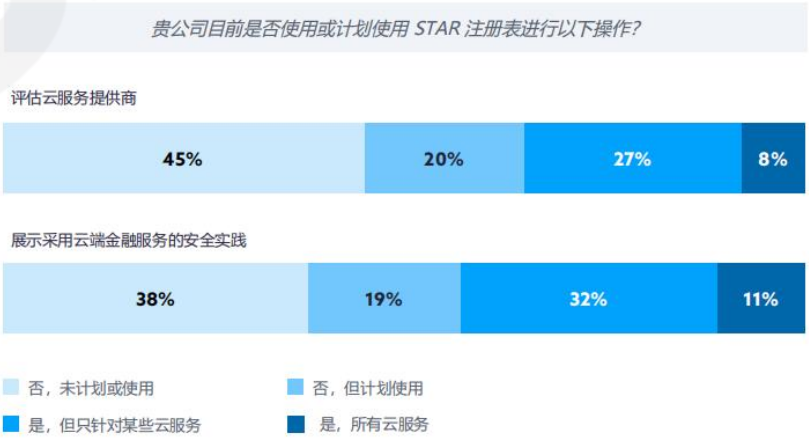
这与大多数受访者提到的需要向多个云服务提供商提交多次审计请求的情况相一致。

CSA云控制矩阵建立统一的云安全方法

调查的另一项发现是，大多数受访者使用 CSA 云控制矩阵（CCM）或共识评估倡议问卷（CAIQ）。鉴于云产品的多样性和各种保障需求，CCM 和 CAIQ 为企业提供了一套供应商中立的控制措施，有助于减轻企业对这些问题的担忧。CCM 的要求涵盖了诸多关注领域，如可用性、密钥管理和第三方管理。在接受调查的企业中，有 65% 的企业使用 CCM 和 CAIQ 来证明对框架的遵守，建立内部云安全控制框架，并制定内部云风险管理方法。然而，只有 33% 的企业将云服务风险评估完全纳入了公司整体风险评估方法。身份与访问管理（IAM）和零信任是新兴的研究领域，可以帮助金融服务业消除对云安全的一些担忧。通过采用这些最佳实践，企业可以在不断演变的威胁抢占先机，并确保其云环境保持安全和合规。

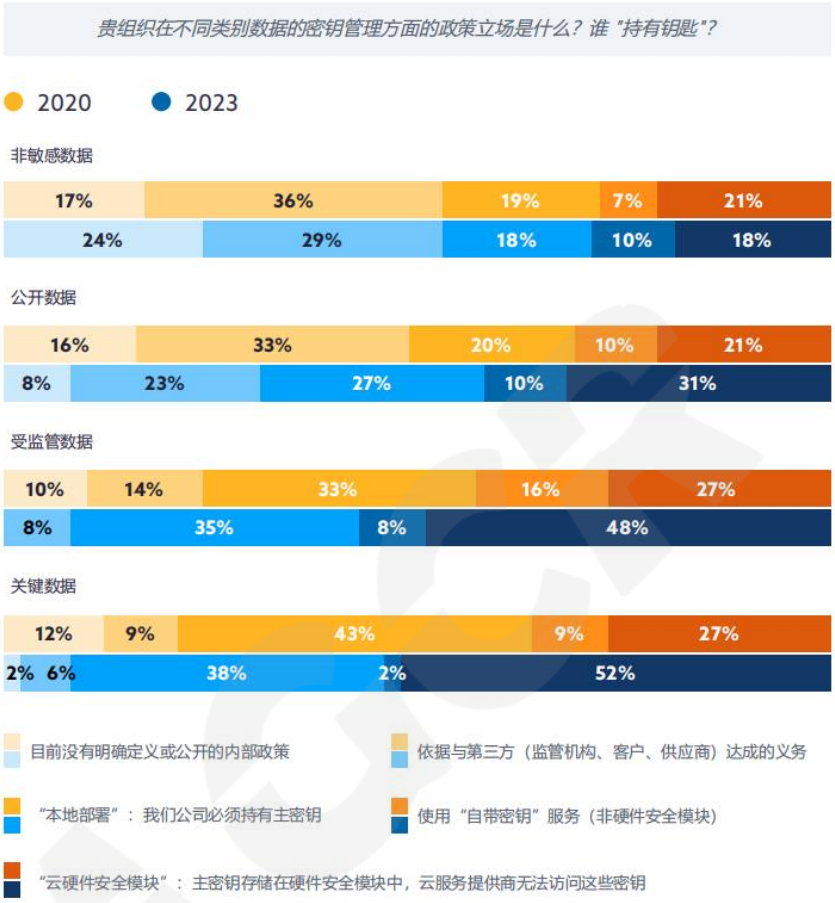
最常引用的框架有 NIST 网络安全框架（NIST CSF）、支付卡行业数据安全标准（PCI DSS）、ISO 27001、通用数据保护（GDPR）、新加坡金融管理局（MAS）、联邦金融机构审查委员会（FFIEC）和 SOC2。而其他回答则表示使用了未具名的框架或要求，以及区域性法律。

CSA STAR 被认为是更透明、更一致地评估云服务提供商的一个机会。有受访者指出，使用 STAR 被视为一种潜在的做法，可以纳入采购活动中，因为它表明第三方供应商进行了适当尽职调查。大多数金融服务机构(80%的受访者)表示，他们在某种程度上使用 CCM 和 STAR 计划。



通过云硬件安全模块和机密计算加强密钥管理

密钥管理是维护数据安全性和完整性的关键环节，尤其是在金融服务行业。受监管的关键数据集有严格的密钥管理政策，以确保金融数据的机密性，并高度保证所使用的加密技术值得信赖。



最新调查显示，仅有 **2%** 的金融服务机构的内部密钥管理政策是未定义或未公开的，低于 2020 年的 **12%**。此外，所有关键数据都制定了密钥管理政策而 这在 2020 年并非如此。针对关键数据、监管数据、公开数据和非敏感数据的密钥管理政策的建立明显增加。

在密钥管理的政策立场方面，**52%**的企业将关键信息置于基于云的硬件安全模块 (HSM)，主密钥存储在 HSM 中，且不允许云服务提供商访问。这一比例比 2020 年增加了 25%。另一方面，**38%** 的企业使用本地解决方案，企业必须持有密钥。这比 2020 年的跟踪数据下降了 5%。

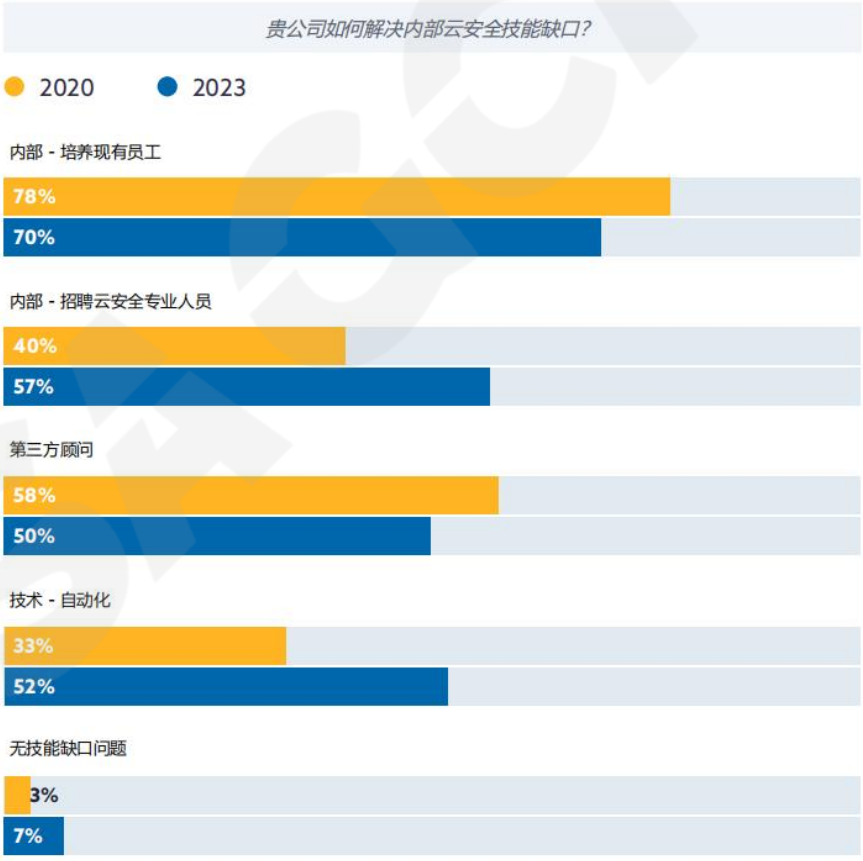
还有其他数据表明，还有其他的密钥管理或加密服务被用来保护受监管和不受监管的工作负载。HSM 即服务、安全隔离和保密计算都被提及用于保护这两种工作负载。

除了数据加密的技术解决方案外，受访者还呼吁监管机构、企业和云服务提供商在云控制矩阵领域（特别是密码学、加密和密钥管理以及数据安全和隐私生命周期管理）和 HSM 即服务方面开展聚焦金融行业的研究、培训和教育。

这些统计数据强调了密钥管理和数据加密解决方案日益重要，以及采用云端服务强化金融服务行业数据安全性和合规性的转变。

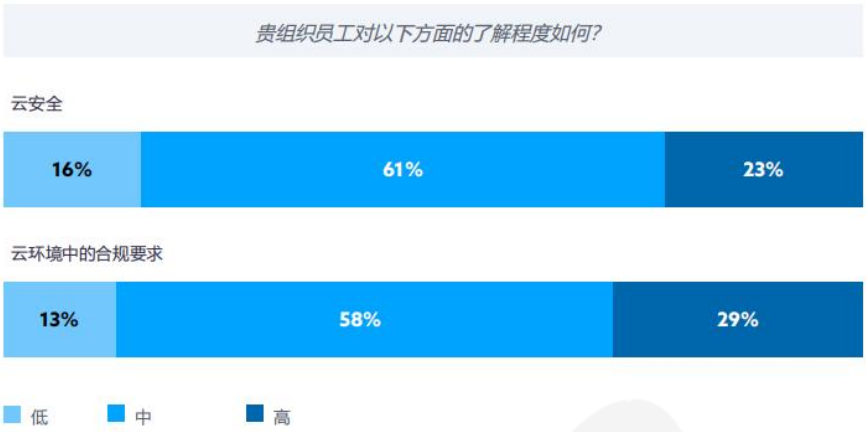
技能缺口在云安全领域仍然存在

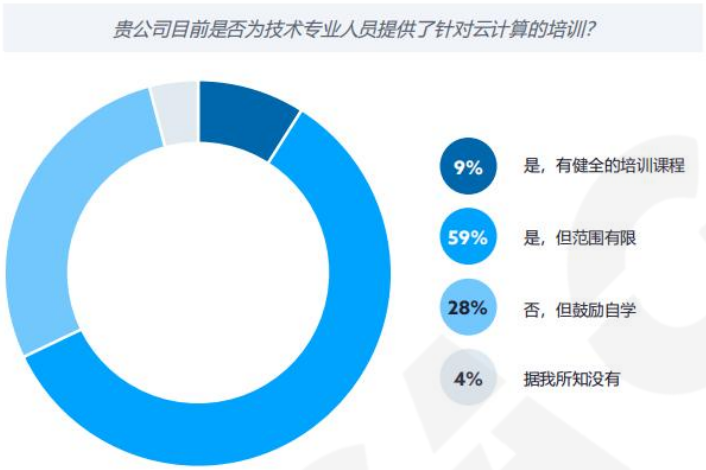
金融服务机构仍然面临的一个普遍挑战是云安全技能缺口，即具备有效管理和保护云环境专业知识的专业人员短缺。为解决这一问题，企业正在竭力培训和聘用云安全专业人员，以弥补这一缺口，改善云安全状况。



50% 的企业选择聘请第三方顾问，**57%** 的企业正在聘用更多的内部云安全专业人员，**52%** 的企业正在依靠自动化来解决这些问题。与 2020 年相比，如今有更多的企业直接引进云安全专业人员（从 **40%** 增长到 **57%**），并保持部分内部现有人员的发展（**78%** 降到 **70%**）。自动化技术的应用有所增加（从 **33%** 增长到 **52%**），这表明部署、整合和实施自动化工具的成熟度和可用性不断提高。

2023 年调查探讨了云环境中的云安全和合规性方面的专业知识水平。少数组织显示其团队的知识水平较低（**16%** 的云安全，**13%** 的云合规）稍多的组织显示出较高的专业知识水平（**23%** 的云安全，**29%** 的云合规）。





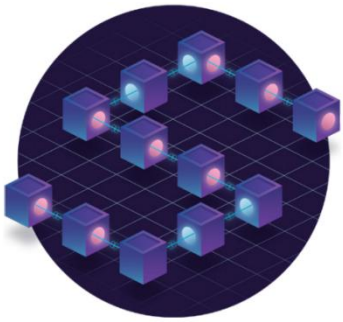
68%的企业提供针对云的专门培训，其中针对云服务提供商的培训最为普遍。调查显示， 尽管 68%的企业为技术专业人员提供了云相关的培训，但只有 **9%** 的企业提供全面的云相关培训，还有 32%的企业没有提供云相关的培训。

在提供的云安全培训中，针对云安全提供商的培训最为常见（54%），其次是 CCSP（**41%**）、CCSK（27%）、其他（**20%**）和 CCAK（**17%**）。

金融服务和云领域的机遇

与新技术和 CSP 功能保持同步

金融服务业在采用新技术创新和增强业务应用时面临着诸多挑战。云技术向物联网（IoT）和边缘计算的扩展为开展商业活动提供了更多的连接性、数据收集和互动，但也增加了安全性和隐私保护的复杂性，需要强有力的保障措施。



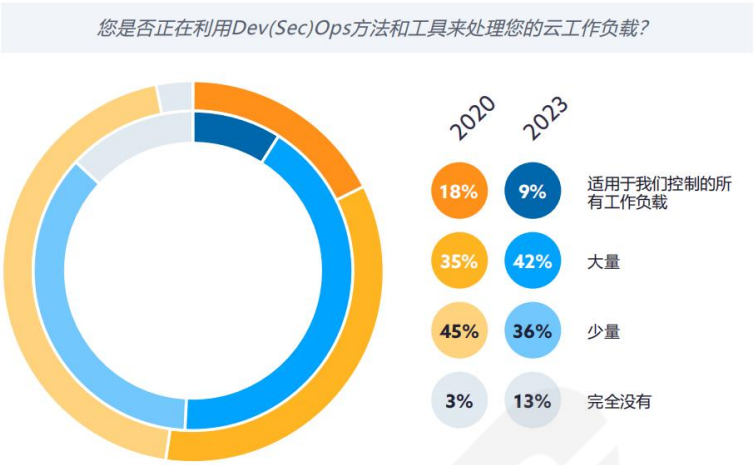
区块链和保密计算技术满足了保护敏感数据、确保交易安全和遵守法规的需求，但在可扩展性和集成性方面存在挑战。

人工智能和大型语言模型（如 ChatGPT/GPT、Bard/LaMDA）的兴起和发展为行业提供了更高的效率、洞察力和能力，但也要求谨慎处理客户数据、提高透明度并考虑道德因素。

量子计算在带来技术优势的同时，也增加了应对未来计算威胁的紧迫性。如前所述，目前依靠加密技术来保密金融信息的做法可能会立即受到挑战，并要求以数字方式提供金融服务的方式发生巨大变化。

金融服务机构必须审慎应对这些挑战，在创新和风险管理之间取得平衡，以充分发挥这些技术的潜力，同时保障客户信任和数据安全。

其他高级安全技术可能涉及在金融服务行业中进一步使用DevSecOps。



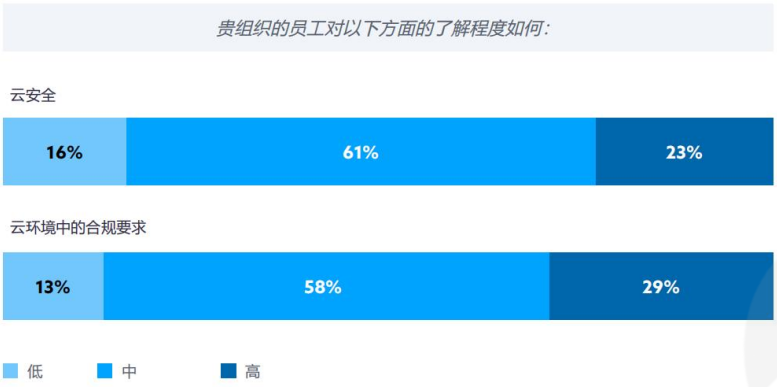
DevSecOps 方法的使用实际上比 2020 年的调查结果略有下降云安全联盟进一步分析认为，将复杂的 DevOps 实践与安全集成和自动化相结合的能力已经影响了一些组织对 DevSecOps 的采用。 在金融服务行业，需要强调培训开发人员和安全团队使用这些方法的重要性。云服务提供商的解决方案还必须专注于为这些团队提供简单且破坏性较小的安全性和 DevOps 集成。

其他传统 IT 服务管理流程（如发布和变更管理）也受到云服务利用中固有的现代技术和第三方方面的重大挑战。特别是云共享安全责任模型的复杂性。CSP 功能和技术的发展速度通常比金融服务客户采用的速度更快。仍然需要改进可能影响 CSP 客户应用程序、环境和操作的更改通知和管理。

为金融服务行业提供充分保障的云安全

人员：保持相关知识（例如特定平台培训、微培训）

培训



人们已经认识到行业认证培训的重要性，特别是 CCSP 或 CSP 特定培训以及使用 FSI 示例的用例。云安全联盟可能需要进一步分析，以确定利益相关者是否对以 FSI 为中心的特定云平台的云安全培训感兴趣。

只有 9%的受访者认为他们拥有高度强健的云安全计划：

流程：映射到FSI框架，验证到STAR

CCM和行业标准

大多数受访者似乎将云控制矩阵用于多种目的，但看到外部评估的衍生物或将 STAR 计划作为当前业务实践的一部分的情况较少。这可能是由于缺乏意识或将其纳入合规实践中的考虑不足。与监管机构和合规官多些云控制矩阵框架和 STAR 注册表使用裨益方面的探讨，并开展 STAR 认证的宣传活动，可能会促进未来更广泛的采用。

技术：云安全提供商借助安全技术的发展实现对金融服务业的有力支持

新功能，人工智能集成

云服务提供商正在与有安全保障需求的云客户密切合作。

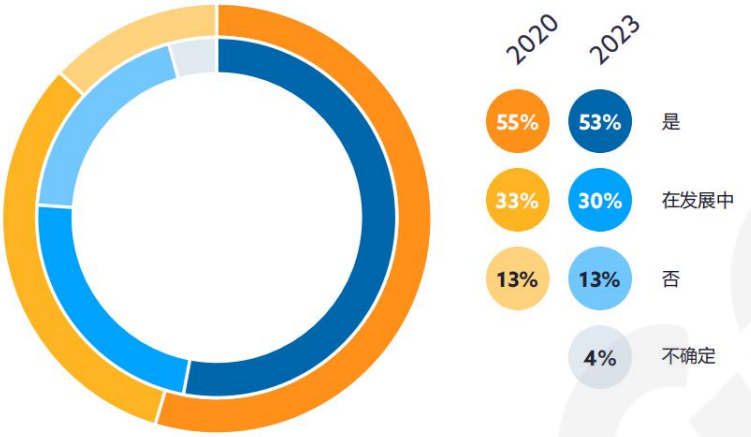
在进行的访谈中，一些金融服务机构提到了云服务提供商有他们自己专门的团队，专门解决如何实现金融服务请求的问题，以满足独特的合规或其他预期需求。

云服务提供商还与业界合作，开发实现机密性和密钥管理的方法，进行权限分离，使云服务提供商无法访问受监管的数据。这方面的示例包括安全隔离和诸如机密计算之类的机制，其防止托管云服务提供商访问可读格式的金融数据。另外，还包括使用 HSM 即服务，其中“信任根”防止云服务提供商访问敏感信息。

企业和云风险管理

许多金融服务企业都有成熟的企业风险管理（ERM）计划，可以解决企业面临的许多不同类型的风险，包括金融市场、监管和信息安全风险。企业风险管理计划通常包括企业风险评估方法和风险接受程序。第三方和供应链风险通常包含在这些计划和程序中。

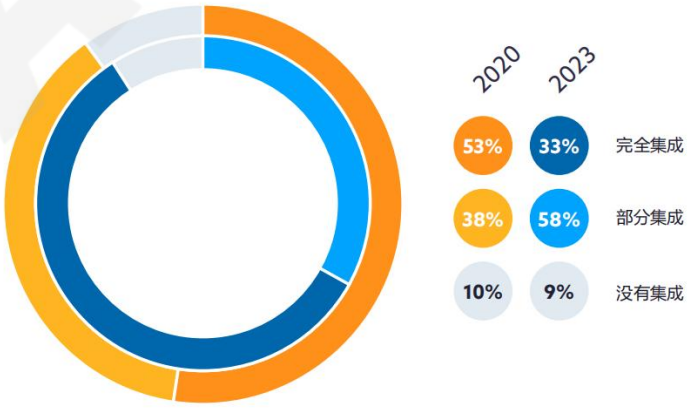
云服务风险评估集成到公司整体风险评估方法中的程度如何?



尽管云服务越来越多地用于关键业务功能和客户参与，但正式的云策略仍在开发中。2020 年的调查结果反映了当前的结果，大约三分之一的企业仍在制定云政策，超过一半的人将其纳入 ERM 计划。

在过去两年中，金融服务的数字化和云的采用已经超过了云策略在 ERM 中实施的速度。 快速采用、更大规模的数字化供应链以及混合云和多云环境增加了传统 IT 系统的复杂性。 随着 90%的金融服务机构将云风险评估整合到整体公司风险评估方法中，部分和完全整合的平衡已经改变。

最令人担忧的是发现新漏洞的速度以及云服务提供商所做的更改可能影响金融实体所需的安全性或所需审计的透明度?



金融服务对云的依赖为传统方法增加了重要的、高度动态的因素，这往往需要专门针对云的风险评估和管理方法。

云环境中仍需要威胁情报和上下文信息

在调查和采访中，信息共享以及了解金融服务行业面临的威胁的中心机制是常见的痛点。 最令人担忧的是新漏洞被发现的速度以及云服务提供商所做的更改可能如何影响金融机构所需的安全性或审计要求的透明度。

正如某银行的一位首席信息官在接受采访时所说：“有过这样的情况，我们在不到 48 小时的时间内收到了（我们的云服务提供商的）重大变化的通知，这些变化将影响我们的环境。虽然一些问题可能是对严重的零日威胁的必要应对，但在这个例子中，本可以与我们更好地协调，以便我们的团队为变化做好准备。”

最令人担忧的是发现新漏洞的速度以及云服务提供商所做的更改可能影响金融实体所需的安全性或所需审计的透明度。

另一个挑战是收集云环境相关的威胁，并进行更广泛的行业共享。 受访者认为，金融服务信息共享与分析中心（FS-ISAC）和 MITRE 等几个组织是受访者获取与其环境相关的漏洞信息所依赖的组织。 一些受访者建议在以云为核心的漏洞方面进行进一步合作，这些漏洞对金融服务可能更重要，并且应更快地被公开讨论，以便于安全专业人员进行应对。

受访者提出的建议包括推进专门针对行业威胁的全球安全数据库，以及云漏洞如何被利用的用例。

此外，在公开评论中提出了一个想法，即如果漏洞被利用，则可能不符合以 FSI 为中心的框架。例如，如果成功安装了禁用日志记录或监控的恶意软件，PCI DSS 要求中的哪些控制将不再符合要求？

然而，人们认识到，如果没有匿名能力，有时很难进一步分享敏感的安全问题。 即使在我们已经匿名的调查结果中，许多受访者表示，由于公司政策或其他原因，像披露金融服务机构必须完成的审计数量等，他们无法共享数据。

提及的其他对策还有某种漏洞标记形式，如果识别到在特定行业（比如金融服务行业）中普遍部署，将会升级其严重等级。

CSA 金融服务计划

通过与行业利益相关者的交流，云安全联盟确定了未来可能考虑的贡献。

为了保持对行业变化的相关观点，云安全联盟将邀请金融服务代表，云服务提供商和其他相关企业参加战略领导委员会，该委员会将召开会议，以确定教育、研究、分析简报、保证框架和计划的优先事项。

教育

教育将包括意识宣传活动，开发和推广与金融服务行业利益相关者相关的培训。

意识宣传活动的例子包括目前正在制定的 HSM 即服务指南的相关性、与金融服务部门内使用的框架的映射以及如何完成共享安全责任模型（SSRM）。

培训从了解可应用于金融资产的云基础知识开始。 但是，但除了金融服务行业的专业人员学习云知识证书或参加入门级云课程外，云安全联盟还将探索与行业合作的机会，开发以金融服务为中心的培训（如果有必要）。 培训的示例可能包括在云环境中对财金融框架或用例进行审计。

研究

金融服务企业指出，在 SaaS 环境中进行开发的能力有助于加速创新，相比传统方法，能更快地将新技术投入生产。 还有大量新的方法论和安全解决方案正在引入，需要指导如何最好地在各种平台上实施。

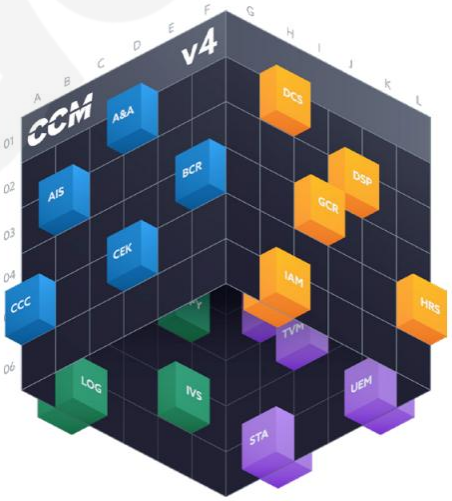
在云安全联盟可以支持的潜在领域中，受访者要求在与云 HSM 相关的完整性和可信性、以及多云环境治理等相关的金融服务实践方面提供更多指导。 云安全联盟可以开发研究调查和论文，确定最感兴趣和最需要的领域，并提供实用的安全建议。

行业简报

云安全联盟成员的一个好处是，与云安全联盟相关的组织能够要求做有关各种云计算或技术（如人工智能、区块链、量子计算等）的分析师简报，这些技术都利用了云服务。

今后，云安全联盟将开始一系列以行业为中心的定期简报会，让金融服务行业的同行们都能听到向专题专家提出的问题，以便他们自己学习，并对贴合他们工作的问题做进一步讨论。参会的主题专家们来自特定的云服务提供商、监管机构或其他相关知识领域，分享在云计算中满足金融服务事务的最新方法。

保障框架和计划



云控制矩阵作为云服务安全最佳实践的参考，在全球范围内被广泛应用。云控制矩阵已应用于许多垂直行业，旨在保护云中的数字资产，金融服务也不例外。像网络安全风险研究所和 IBM 金融服务公司等一些企业已将云控制矩阵纳入其相关框架之中。

云安全联盟已经与几个欧洲联盟和工作组开展了进一步的工作，评估云控制矩阵作为其金融审计实践的一部分。 因此，云安全联盟可以评估为满足常规体系之外的特殊合规或金融数据处置的金融服务机构而设计的其他云控制矩阵需求的相关性。这可能会促使云控制矩阵增加金融服务相关的附录内容或者发布针对这些问题的云控制矩阵适用性白皮书。

云安全联盟会继续将云控制矩阵映射到其他监管框架，最近完成了与新加坡金融管理局数据安全标准的比较和映射，，并正在进行支付卡行业数据安全标准（PCI DSS）最新版本的映射。

云服务提供商和其他拥有云业务的企业可以选择进行云控制矩阵评估，并加入 STAR 认证计划。银行业支持 STAR 计划可作为第三方保障，并可能作为第三方采购中新供应商加入的先决条件。

结论

金融服务行业在许多方面与其他垂直行业一样享受到了云计算的好处。它能高效更快速地将解决方案推向市场，并按照习惯云原生应用的客户所期望的方式进行部署。

企业还可以通告符合公司政策和合规要求的管理员规则加强同质化工作来提高安全性。

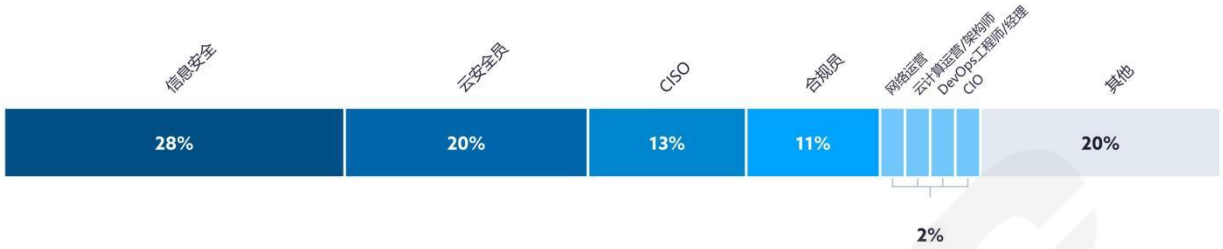
这些调查结果显示，越来越多的企业使用云服务来部署关键业务应用，并在部署的公共云和私有云中处理受监管的财务数据。

最突出的问题主要来自于满足各式各样的合规要求，金融系统完整性、可用性和适当人员访问的弹性需求，第三方合作伙伴的安全控制保障，以及员工正确配置访问控制的能力。

云安全社区可以通过进一步的行业合作来提供帮助，制定易于理解的指导和应用控制的用例，提供专门针对金融服务专业人员的培训，研究保护金融数据的最新方法，并制定良好的安全基线框架，无论使用哪种云服务，都可以满足全球监管的期望。

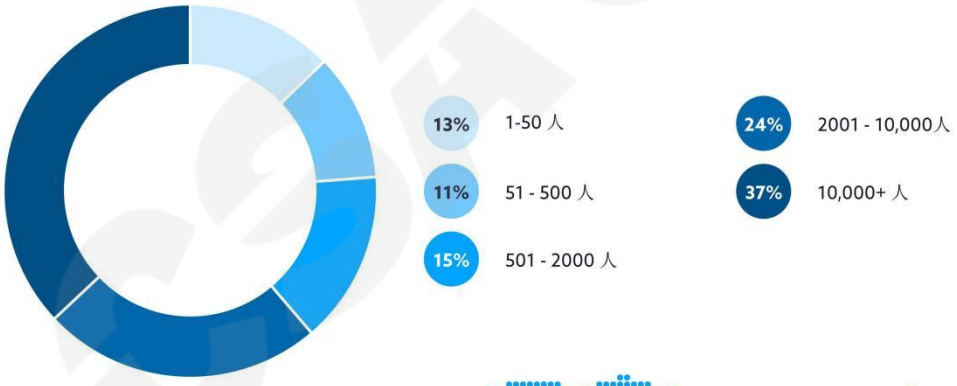
成员资料

您的主要角色是什么？



以下哪项最恰当地描述了贵组织所从事的行业？

您的组织规模如何？



您位于以下哪个地区？

CSA GCR cloud security alliance
GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905