Deloitte.
Insights

FS-ISAC

重塑网络安全格局

数字化和新冠疫情
提升大型金融机构网络安全需求

关于德勤金融服务行业研究中心

德勤金融服务行业研究中心致力于为全球金融服务业提供专业支持，凭借精深洞察和行业研究协助银行、资本市场机构、投资管理公司、保险公司和房地产企业高级决策层做出最优决策。通过研究、圆桌讨论会以及其他方式，提供中肯、及时且可靠的专业洞察，成为可受信赖的专业机构。

与我们联系

敬请访问**http://www.deloitte.com/us/cfs**了解有关本中心更多信息并阅读本中心的最新刊物。

订阅

欢迎您在**www.deloitte.com/us/cfs**中进行注册订阅本中心邮件阅读资料。

关于金融服务信息共享与分析中心（FS-ISAC）

金融服务信息共享与分析中心是一致力于降低全球金融体系中的网络风险的行业联盟，为金融机构及其客户提供服务。中心利用智能平台、丰富的资源和可信赖的专家网络来预测、降低和应对网络安全威胁。FS-ISAC有近7,000家成员机构，用户遍及70多个国家。FS-ISAC总部设在美国，在英国和新加坡设有办事处。敬请访问www.fsisac.com了解更多信息。如欲了解高管对未来金融、数据和网络安全的观点及看发，敬请访问FS-ISAC洞察。

目录

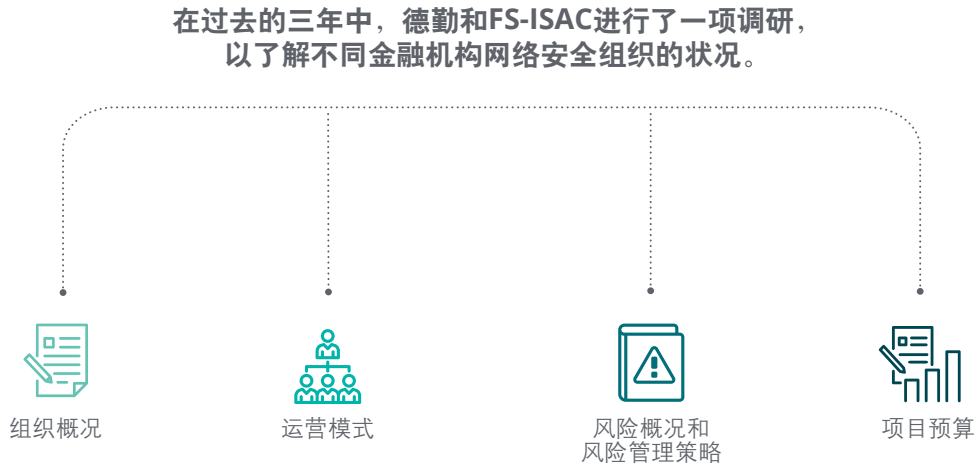
关于调研

本调研基于金融服务信息共享与分析中心（FS-ISAC）与德勤网络与战略风险服务在过去三年中每年对其成员企业及CISO进行的调研。最近一次调研于2019年末启动，于2020年1月27日结束。调研结果根据调研公布的年份确定，最新一份为2020年，之前分别是2019年和2018年。

本调研考察了金融机构网络安全运营的多个环节，包括组织和管理网络安全活动、首席信息安全官（CISO）的汇报路线、预算、董事会对CISO工作的关注程度，以及在财务方面应优先考虑哪些网络安全领域等 (图 A)。

图 A

调研涵盖的网络安全项目内容



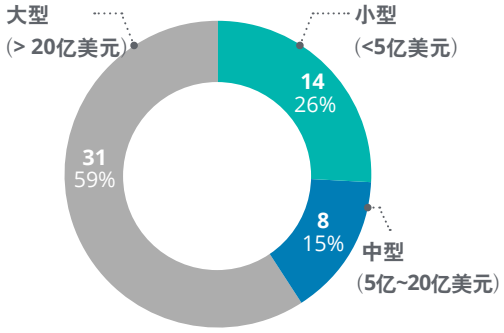
资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

本报告对三年的调查结果进行了分析，旨在发现金融行业网络风险趋势。

共有53家金融机构参与了调研究，代表了不同收入水平(图B)和金融子行业(图C，因受访机构可分属多个子行业，故数量总和超过53）。此外，每项调研的部分或全部受访者可能有所不同。

图B

受访金融机构，按销售收入划分

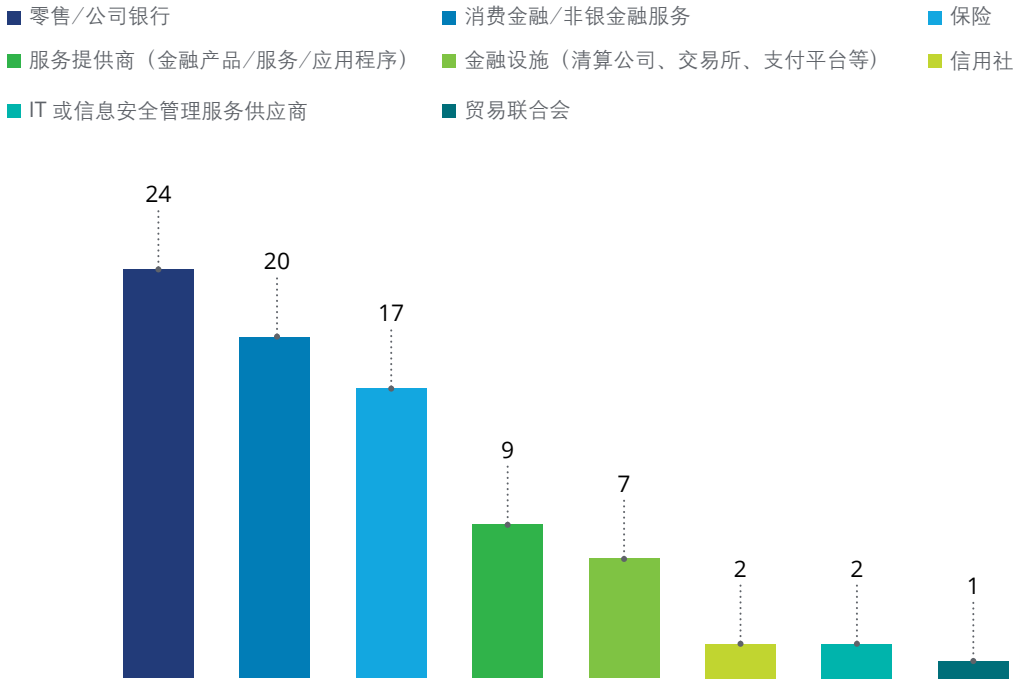


注释：大型机构（销售收入大于20亿小于50亿美元）、巨型机构（销售收入大于50亿小于300亿美元）、超大型机构（大于300亿美元）

资料来源：FS-ISAC/德勤网络与战略风险服务CISO调研报告（2020年）；德勤金融服务行业研究中心分析。

图 C

受访金融机构所处行业



注释：受访机构可多选。

资料来源：FS-ISAC/德勤网络与战略风险服务CISO调研报告（2020年）；德勤金融服务行业研究中心分析。

主要观点

- 受访者表示网络安全支出正在增加，身份和访问管理、网络安全监控和运维、以及终端和通信网络安全支出比重相对更高。
- 受访者表示在过去的三年里，快速且日益复杂的信息科技变化是他们在网络安全方面的最大挑战。为了帮助有效控制不断增加的网络安全风险，公司应考虑在更广泛的IT服务建设过程中以数字化方式启用网络安全功能，而且在技术开发时采用“设计安全”原则也有助于金融机构创设更安全的产品。
- 大多数来自大型金融机构的受访者表示，网络安全通常是IT职能的一部分， 首席信息安全官（CISO）通常向所在公司的首席信息官（CIO）或首席技术官（CTO）汇报。这反映了网络安全与信息技术紧密结合的需求。
- 同时，金融机构可能希望在网络安全方面保持一定程度的独立性，这有助于确保风险管理决策不受信息技术限制的影响。
- 受访者指出云计算、数据分析、机器人流程自动化等新兴技术已经成为网络安全投资最高优先级。而访问控制、安全保护技术和数据安全被强调为基础性的投资。
- 随着数字化与远程办公的加速，员工、客户、承包商及合作伙伴/供应商之间的界限正变得越来越模糊，传统网络的范围和边界也被弱化了。用户、工作负载、数据、网络以及设备已是无处不在。“零信任”概念的出现使得现代企业强制实施“最小权限”原则以应对无处不在的授权访问风险。

网络安全，加速前进

大多数金融机构目前已经在稳步推进数字化转型。出于对效率的追求以及不断提高的客户期望，各种体量的金融机构的运营都已经在走向数字化。在金融服务领域中，转型速度通常会因公司对变化、灵活性和规模以及其他因素的准备程度而有所不同。

在过去的几个月里，新冠疫情迫使许多公司加快了数字化转型的步伐。随着办公室的关闭和行动受限，迫使每个人和所有可能转为线上的工作都转成线上操作。许多机构不得不在运营、交付和客户参与方面更全面的接受数字化转型。

然而，这种突然的转变为许多负责保护公司数字资产的首席信息安全官（CISO）和网络安全团队带来了很多的问题。在大多数员工远程办公的同时，黑客和网络诈骗分子则试图利用不断进化的技术扩大攻击面。今年4月，纽约金融服务部强调，与新冠疫情爆发相关的网络犯罪量显著增加。[1]

当务之急：金融机构应以数字化方式使其网络安全职能与快速变化的信息技术转型保持同步，并保护关键资产免受日益严重的网络威胁和攻击。德勤网络与战略风险服务团队和金融服务信息共享与分析中心（FS-ISAC）连续第三年调研FS-ISAC成员机构如何应对网络挑战。（最近的一次调研时间为2019年末到2020年1月，调研结果在2020年调研报告中予以发布。我们根据出版年份：2020年，2019年和2018年向大家列示调查结果。）（请查阅“关于调研”章节以了解更多调研详情。）

年度调研探讨了金融机构如何构建和管理其网络安全，以及在组织模式、支出方式、外包和投资重点等方面的不同选择。

在过去的三年里，网络安全一直作为金融机构优先发展事项不断地分配到更多的资源，金融机构提高了董事会对网络安全的参与度，并取得与信息技术和业务优先级相匹配的投资。报告同时指出大型金融机构几种关键网络风险管理趋势，以及未来在新冠疫情之后给不同规模金融机构带来的影响。

增加支出满足需求增长

金融机构网络风险管理中最重要的一个工作是为机构配置充足的网络安全资源。对许多机构来说，网络攻击的年平均成本一直在增加。[2] 因此，参与调研的金融机构在网络安全支出方面比上一年有所增加并不意外。(图 1)。

最近一次调研的受访机构平均将其IT预算约10.9%用于网络安全，高于前一年的10.1%。这一比例平均约为金融机构年收入的0.48%，高于此前的0.34%。受访机构平均为每位全职员工在网络安全方面的支出约为2,700美元，高于去年的2,300美元。

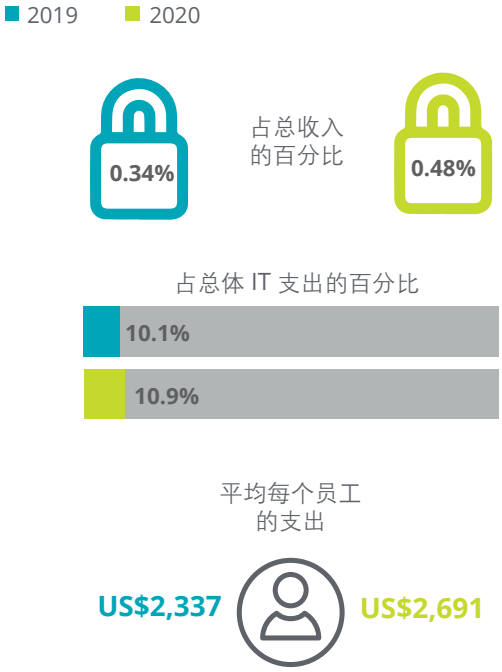
与此同时，不同类型金融机构网络安全支出在不同基准上发生了显著变化。(图 2)。

尽管支出有所增加，但在三年的调研中可以看到，金融机构的预算分配在很大程度上保持了一致。在最新调研中，网络安全监控和运维、终端和通信网络安全以及身份和访问管理总共占据了超过50%的支出比重。(图3)。

图 1

金融机构在网络安全方面持续加大投入

网络安全总体支出对比



资料来源：FS-ISAC/德勤网络与战略风险服务CISO调研报告（2019年及2020年）；德勤金融服务行业研究中心分析。

图 2

不同类型金融机构网络安全支出

■ 占营收比例 ■ 占 IT 支出比例 ■ 平均为每位员工支出

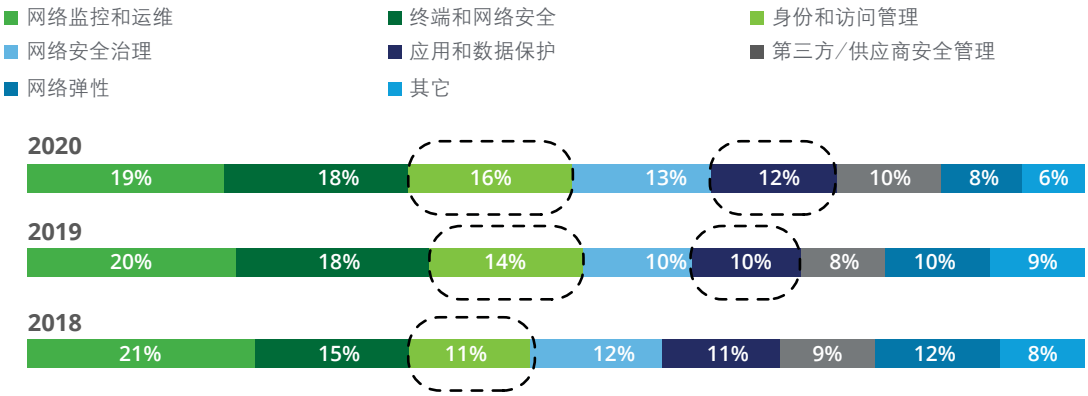
	2019	2020
零售/公司银行	0.3% 10.1% US$2,074	0.6% 9.4% US$2,688
消费金融/非银金融服务	0.3% 9.7% US$2,817	0.4% 10.5% US$2,348
保险	0.3% 9.3% US$2,245	0.4% 11.9% US$1,984
服务提供商	0.6% 8.9% US$1,956	0.6% 7.2% US$3,226
金融设施	0.8% 15.2% US$3,630	0.8% 8.2% US$4,375
总计	0.3% 10.1% US$2,337	0.5% 10.9% US$2,691

资料来源：FS-ISAC/德勤网络与战略风险服务CISO调研报告（2019年及2020年）；德勤金融服务行业研究中心分析。

图 3

不同网络安全领域的预算分配在很大程度上与去年保持了一致，但也有一些显著变化

调研机构在不同网络安全领域的预算分配情况



注释：由于数据四舍五入，百分比加总之和可能不等于100%。

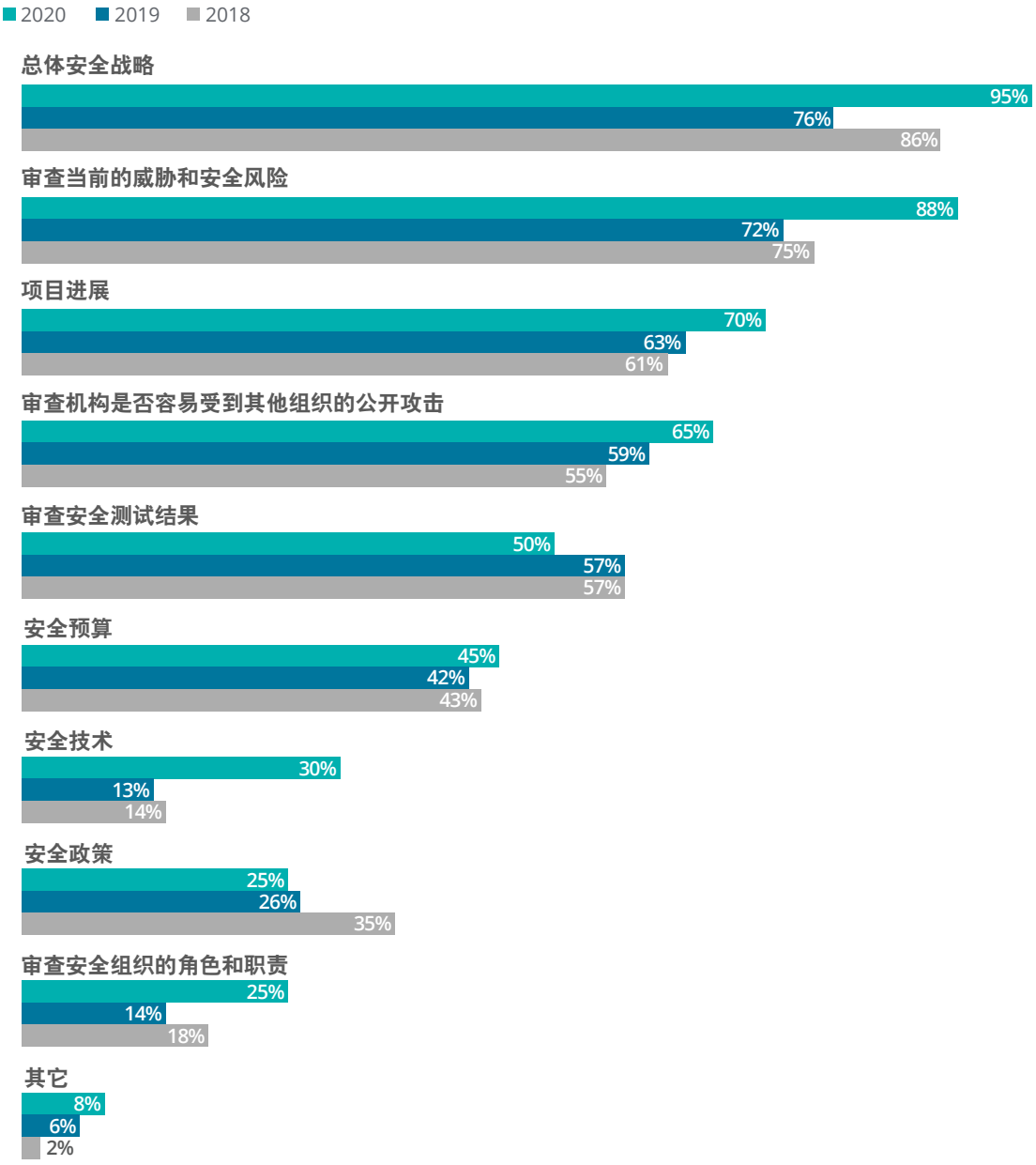
资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

网络安全支出增加的另一个原因是董事会和高管团队承受的压力越来越大，这使得他们对网络安全的关注度持续提高（图 4）。 根据德勤与客户的交流，能够不断完善并向董事会阐明网络安全价值主张的CISO们更有可能确保董事会对网络安全的参与。

图 4

大多数网络安全领域都受到董事会和管理层的极大关注

受调研金融机构中最受董事会/管理层关注的网络安全领域



资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

董事会的参与不再仅限于战略或运营领域。安全技术已从2018年调研的第九名上升到2020年调研的第七名，这表明董事会对了解网络安全的技术方面越来越感兴趣。类似的，与过去相比，董事会对审查安全组织的角色和职责越来越感兴趣。这恰恰证明了一个不断被强调的观点，即网络安全是每个人的职责，而不仅仅是CISO的责任。

与网络风险管理相对不成熟的机构相比，认为其机构网络安全更成熟的受访机构董事会和管理层对网络安全的几乎所有领域都更加感兴趣。这突显了董事会参与的重要性。

展望未来，鉴于新冠疫情所导致的严峻的宏观经济形势，许多金融机构可能会认真考虑是否需要全面削减开支。然而，金融机构在削减网络安全预算之前应尤为慎重。考虑到数字化的不断推进和远程工作环境带来的挑战，以及内部威胁的增加，大多数金融机构所面临的网络安全风险正在加剧。[3]

数字化进程塑造大型金融机构网络安全计划

技术是金融机构所有工作中的一部分，但跨业务采用新技术会增加网络风险。因此，受访机构将IT的快速变化和复杂度的增加列为过去三年网络安全管理的首要挑战（图5）并不意外，而第二大挑战则是在如此快速发展的IT环境中缺乏有经验的网络专业人员来帮助维护系统安全。

图 5

网络安全管理面临的挑战

受访金融机构选出的大型金融机构五大挑战

	2018	2019	2020
1	IT 的快速变化和复杂度的增加	IT 的快速变化和复杂度的增加	IT的快速变化和复杂度的增加
2	缺乏有经验的网络专业人员	缺乏有经验的网络专业人员	缺乏有经验的网络专业人员
3	在安全解决方案功能和互操作性不足的情况下，难以确定保护机构网络安全工作优先级	更关注合规，较少关注网络风险管理	业务增长和扩张
4	更关注合规，较少关注网络风险管理	业务增长和扩张	在安全解决方案功能和互操作性不足的情况下，难以确定保护机构网络安全工作优先级
5	对网络风险和安全的理解不足	难以确定保护机构网络安全优先级	难以确定保护机构网络安全优先级

资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

与此同时，金融机构普遍已将关注重点转向疫情的应对和恢复。因此在2019年报告中受访金融机构提出*业务增长和扩张*这一挑战可能会暂时消退。

首要业务问题及其安全影响

越来越多的金融机构正在使用新兴技术来创新和开发新的产品、服务和数字渠道。但这些关键的驱动因素可能会成为其他网络攻击的目标。因此，在接受调查的大型金融机构中，将网络安全嵌入新产品和服务以及嵌入新渠道仍然是最重要的两个涉及安全影响性的业务问题(图 6)。

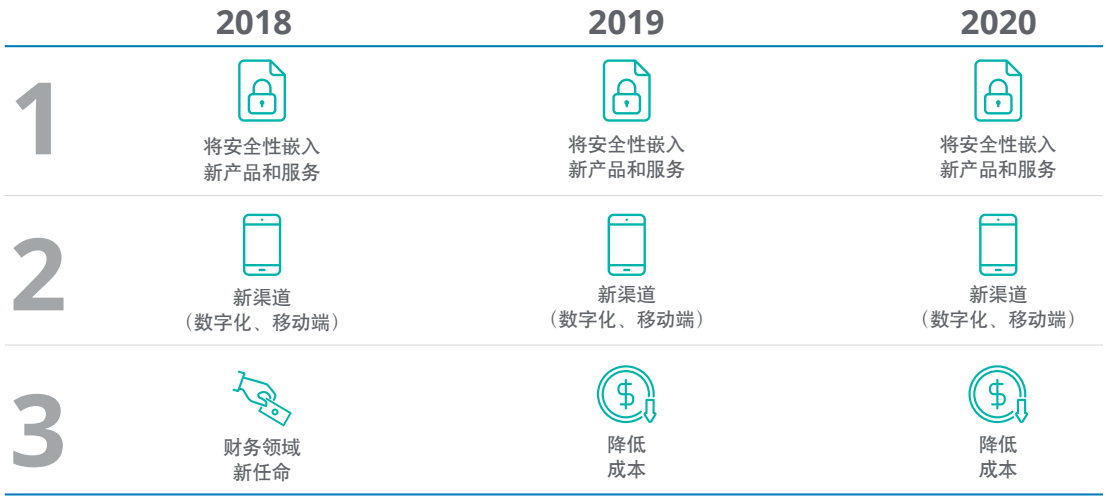
新产品和服务: 目前，金融机构经常在产品和服务创新方面与金融科技公司展开竞争和合作。当公司努力抢占市场先机时，这些创新往往需要足够的敏捷性和灵活性才能取得成功。公司在设计、构建和利用创新时应确保采取足够的预防措施，因为在任何一个阶段都可能出现新的网络安全威胁。一个组织的网络安全职能所面临的挑战是建立与所承担的额外风险相匹配的控制措施，而不是成为创新的障碍。

新渠道：金融机构通常会寻求更新、更简单的方式与客户开展业务，但新渠道可能会伴随其自身的一系列网络安全脆弱性。

图 6

对大型金融机构而言，将安全性嵌入新产品和服务以及新渠道仍是其最为关注的两大业务安全性问题

大型金融机构受访者最为关注的三大业务安全性问题



资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

以增强现实或虚拟现实（AR/VR）为例。即使金融机构尝试使用AR/VR与客户进行交互，黑客也已经设计出复杂的网络攻击来危害AR/VR应用程序和设备安全，这可能会对金融机构造成严重的物理或财务损失。传统的网络安全控制可能不太适合防范这类攻击。

网络安全职能部门应评估数字化需求并加强其控制以适应和保护这些新的数字渠道。公司还应考虑采用“安全设计”原则，即在新渠道设立和运营时，即开发定制各类安全控制措施，并将其嵌入到新渠道的核心结构中。

降低成本 已经成为很多受访机构重要关注点之一，甚至在新冠疫情的影响成为另一个担忧之前，在过去的两次调查中都排名第三。

在未来，降低成本在后疫情时代可能变得更加重要。在经济复苏的前景下，许多公司将面临削减开支的压力，这意味着要采取可能的措施，如调整人员结构、部分员工继续远程工作以减少办公空间，以及增加对自动化或云计算功能的使用等。

机构应考虑采取整改措施，以确保降低成本的举措不会使机构面临额外的网络风险，例如内部安全威胁。

金融机构应仔细评估为降低运营成本而采取的行动对网络安全可能带来的影响。考虑采取整改措施，确保降低成本的举措不会使机构面临额外的网络风险，例如内部安全威胁。

CISO也可能会被要求提出成本管理方面的建议。他们可以考虑使用选择性外包或提高自动化程度以支持机构的降本计划（例如，通过将数据和/或系统安全地迁移到云端）。

新兴技术推动网络安全的投资重点

大型金融机构的受访者表示，在过去的三年里云技术一直是他们希望投资的第一大新兴技术（图7）。许多机构已经在云端拥有相当一部分的IT基础设施，而下一步则要考虑核心业务应用程序的迁移。许多机构还直接在云上开发和部署了新应用程序。

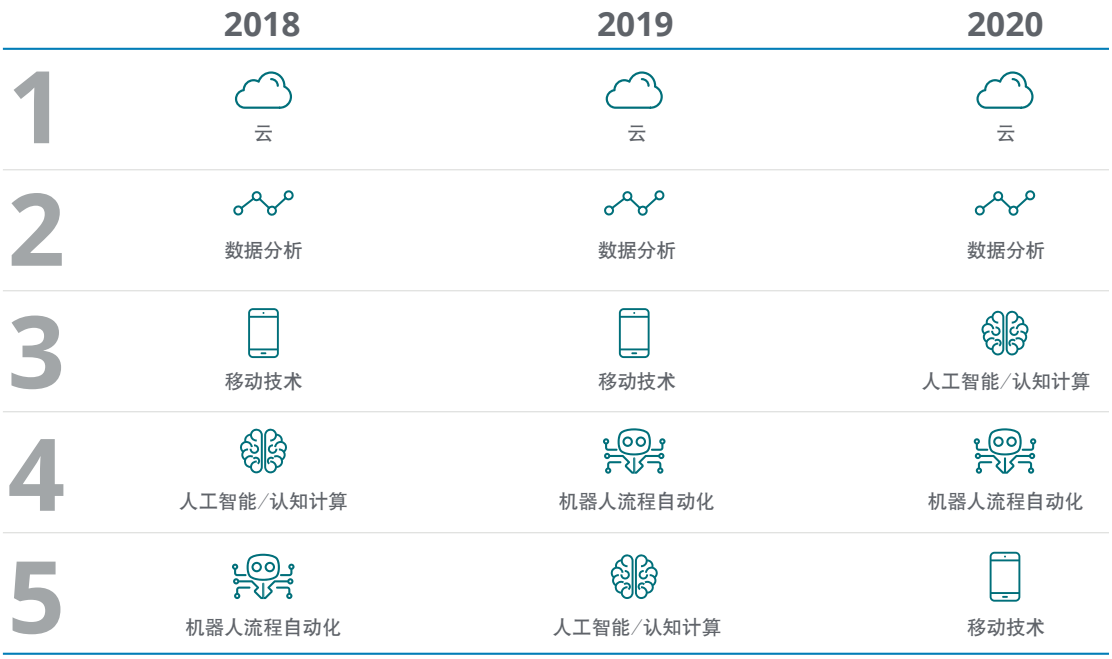
与此同时，云服务提供商正在通过 “分析即服务” 和“自动化即服务”来扩充其产品。调查结果与这一趋势一致：大多数机构有意增加采用“软件即服务”和“平台即服务”的能力。然而，随着越来越多的数据和应用程序转移到传统的安全范围之外，网络攻击的风险也在随之增加。[4]

*数据和分析*是受访机构重点关注的第二大新兴技术。由于金融机构可以访问客户个人敏感信息，数据泄露可能会对金融机构声誉造成重大影响。许多机构依赖于对专有数据的洞察与第三方数据供

图 7

参与调研的大型金融机构数字化投资优先级最高的是云、数据分析和自动化

大型金融机构受访者五大新兴技术优先级



资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

应商的集成。保护数据对于满足客户数据安全和隐私的期望以及满足监管要求都至关重要。

与此同时，监管机构已经注意到企业收集和存储了大量个人数据，这些数据具备可恢复性和数据完整性。监管机构为此建立了数据保护准则，如欧洲通用数据保护条例（GDPR），[5]美国联邦金融机构检查委员会的网络安全概况[6]以及《加利福尼亚州消费者隐私法案》。[7]这些监管举措使数据保护成为网络安全防控的重点领域。

*人工智能/认知技术*排名第三，机器人流程自动化排名第四，可以看出先进的自动化和机器学习技术为企业提供了一套新的解决方案，可以帮助其改变运营方式并降低成本。 虽然金融机构可以在开发和培训过程中采取预防措施，但这些技术仍在不断发展，用户也在逐渐习惯于

使用机器人解决方案进行工作。这些机器人拥有用户权限，可以访问敏感的企业数据和自动化处理系统。这意味着黑客有了一个全新的攻击面，可以用来渗透进入组织的系统。尽管自动化技术拥有巨大的潜力，但在开发、培训和使用过程中，会增加企业的网络安全脆弱性。金融机构应努力解决所有这些潜在的问题。

从大型金融机构的投资优先级中可看出，网络安全团队越来越注重防范与新兴技术相关的安全漏洞(图表 8)。

自从引入共享计算和大型计算机以来，网络安全人员一直在探讨身份和访问管理问题。这仍是一个重点优先事项。在一个越来越依赖云原生和API连接的世界中，访问控制再次成为优先事项，这些技术扩展了身份和设备的类型，从而产生了更多身份类型和新的身份验证要求。[8] 在一个日益自动化的环境中，这种能力对于保护一个组织至关重要，也愈加复杂。

同样，数据安全和保护技术可以在防止数据损坏和拒绝服务攻击方面发挥重要作用。

随着行业发展，数字化步伐只会加快，数字化应继续成为影响和优先考虑网络安全投资和能力的关键驱动力。未来，应将网络安全功能完全整合到公司的数字化进程中，并将网络安全作为转型项目的核心考虑因素。

图 8

新兴技术正在推动受访机构优先考虑网络安全

大型受访金融机构五大国家标准与技术研究院（NIST）投资重点

	2018	2019	2020
1	安全持续监控	防护技术	访问控制
2	访问控制	访问控制	防护技术
3	异常和事件	异常和事件	**数据安全**
4	检测流程	**数据安全**	检测流程
5	**数据安全**	检测流程	异常和事件

资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

将网络安全与信息技术相结合，并保持其战略重要性

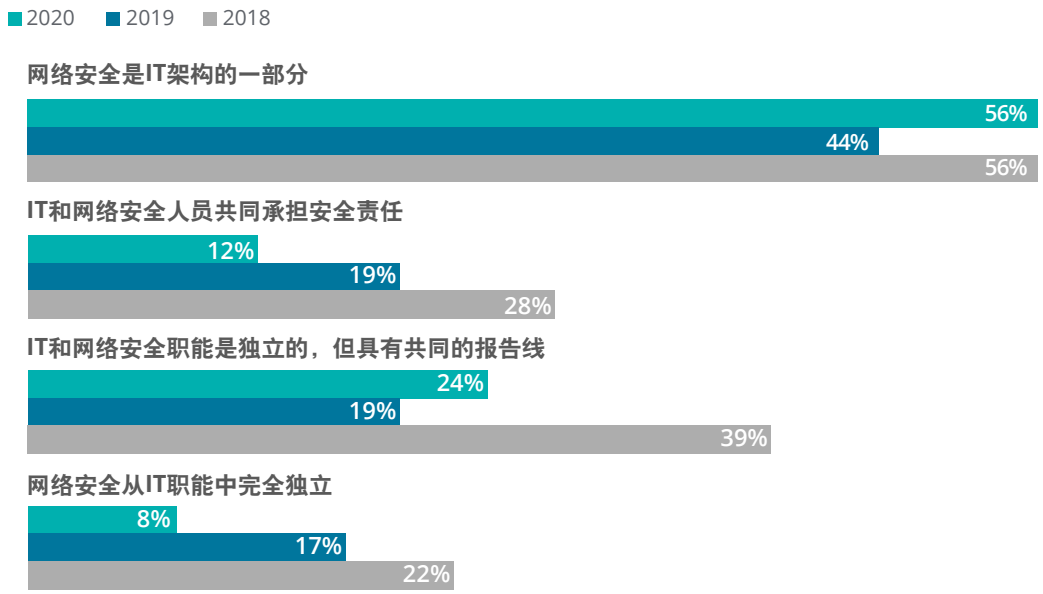
从网络安全架构、汇报机制到建立网络安全支出的重点领域，金融机构在用不同的方式管理和实施网络安全计划，并结合自身目标采取用混搭的方式进行。

从受访的大型金融机构对网络风险管理组织架构的反馈中我们可以看到，在不断变化的环境下，许多金融机构正将网络安全计划与技术变革紧密联系起来，以有效控制不断出现的网络风险。大多数受访机构将网络安全作为其IT架构的一部分(图9)。

图 9

超半数受访大型金融机构表示网络安全是其公司IT架构的一部分

受访大型金融机构网络安全与IT的集成度

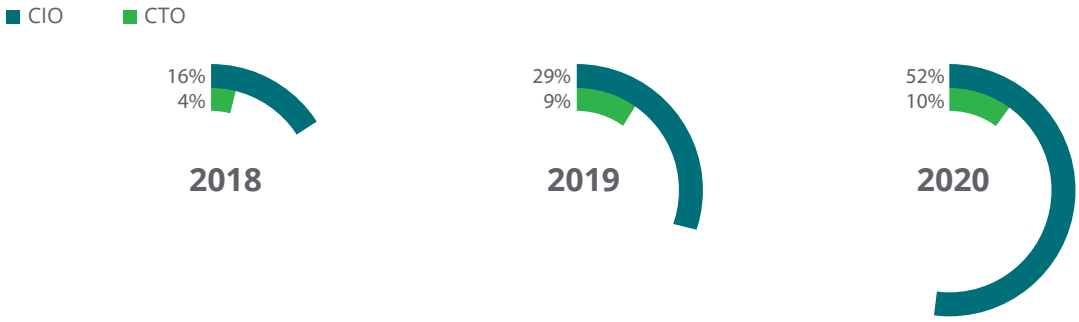


资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

图 10

超半数的CISO向CIO或CTO汇报，反映了网络安全与IT目标之间紧密结合的必要性

参与调研的大型金融机构CISO向CIO或CTO汇报的比例



资料来源：FS-ISAC/德勤网络与战略风险服务CISO调查报告（2018年、2019年及2020年）；德勤金融服务行业研究中心分析。

网络安全和信息技术目标之间的密切配合也反映在调查对象的汇报架构中。在对大型金融机构CISO的调研中，有62%的CISO向首席信息官（CIO）或首席技术官（CTO）汇报，较去年的38%大幅上升，而前年仅为20%(图 10)。

通过将网络安全与IT职能紧密结合，金融机构可以更好、更快、更有效的方式应对新出现的网络风险，帮助其IT合作伙伴变得更加敏捷。

虽然网络安全的第一道防线往往通过共同的汇报路径与技术职能紧密结合，但安全人员通常有明确的角色和职责分工。在第二道防线中，网络安全通常只是技术或风险职能的一部分，没有明确设定的要求、角色或责任。

因此，金融机构应通过明确的角色和职责分工界定第一和第二道防线上网络安全与技术或风险职能间的区别。

保持网络安全的战略重要性

网络威胁和攻击不再仅仅是一种技术风险，也是业务风险。[9]这就是为什么网络安全职能应该拥有足够的独立性和重要性。这有助于确保与风险管理相关决策得到充分的考虑，而不受其他IT考量或约束的影响。

如果网络安全是IT的一部分，它将缺乏可预见性并与实际业务线联系不足。与此同时，CISO

图 11

网络安全如何在IT内部保持独立性?

保持风险管理决策的自主权

风险管理决策已得到适当考虑，不会被IT约束所限制

建立网络安全与业务之间的联系

业务与网络安全建立联系有助于使网络安全计划与业务计划保持一致

在董事会层面提升网络安全优先级

建立由CISO主持的网络风险指导委员会有助于增加董事会的参与度

资料来源：德勤金融服务行业研究中心分析。

向CIO报告，将受到来自其他利益相关者对平衡风险和业务优先级的影响。

因此，金融机构应考虑采取具体措施在业务线、风险合作伙伴和网络安全之间建立联系。通过设立指导委员会、雇用业务信息安全官（BISO）和其他方式来实现。这些措施也有助于使网络安全与未来业务计划保持一致(图 11)。

最后，金融机构应努力确保董事会和管理委员会将网络安全放在其议程的首位。如前所述，拥有一个积极参与的董事会可以帮助整个组织专注于管理网络安全风险的挑战，同时确保分配到足够的资源。董事会的监督应该是持续的，而不仅仅在初期或发生网络安全事件时才予以监督。

前进之道

新冠疫情严重扰乱了金融机构及其在全球范围内的运作方式。远程工作显著增加，视频会议和团队协作应用程序的使用激增。这些变化可能不会随着公司业务恢复正常运转而消失。实际上，德勤最近的一份报告发现，许多金融机构正在评估让至少部分员工永久性远程办公。根据与行业领导人的交流，一些机构正在考虑让其30%或更多的员工永久性远程办公。[10]

网络安全组织需要通过实施增强型控制和终端保护技术对终端用户设备进行更好的控制，从而迅速适应这种新的操作环境。金融机构应该考虑增加培训和提高安全意识的活动，关注居家远程办公的网络安全环境。

随着员工、客户、承包商和合作伙伴/供应商之间界限的模糊，组织的边界已基本消失，金融机构应考虑实施“零信任”原则。这意味着每一个涉及数据流的事务，无论是通过网络、应用程序、用户、设备还是负载，都要受最小权限访问控制。

金融机构还应将其网络安全职能数字化，以提高敏捷性和自动化程度。将“安全设计原则”融入IT服务建设，并将网络安全需求嵌入软件开发生命周期的架构和设计阶段，帮助机构在不断变化的网络安全威胁面前保持领先。

CISO不应将目光从长远目标上移开，这些目标包括与公司的战略重心保持一致、人才管理挑战以及解决监管之类的外部问题。这种广泛的

图 12

维护网络安全的业务价值

资料来源：德勤金融服务行业研究中心分析。

参与可以凸显网络安全为金融机构带来的价值(图 12)。不管使用什么样的运营模式，管理层的参与都将对确保网络安全的良好实施起到至关重要的作用。

证明网络安全的业务价值

有效的网络安全计划可证明其具有业务价值。为了帮助确保网络安全的价值得到最高管理层的充分理解和关注，CISO可以从以下几点着手：

1. 与公司战略保持一致

- CISO应加强和建立网络安全能力，以更广泛地支持企业的业务和技术战略和目标。
- 网络安全团队应通过实施必要的网络安全控制来对公司的降本行动予以支持。
- 安全团队应支持网络安全弹性之外的项目（如业务连续性计划和灾难恢复计划），重点关注实现运营韧性。
- 网络安全职能部门应支持外包战略，帮助选择更具韧性并能满足稳定服务水平的第三方。

2. 外部因素

- 监管要求会更多集中在通过诸如第三方现场评估要求等活动以增强企业韧性。
- 国际社会对疫情的反应可能会增加地缘政治风险，进而影响企业的全球运营以及威胁环境。需要安全团队时刻准备快速适应瞬息万变的情况。
- 在新冠疫情爆发之前，威胁环境的体量和速度都在迅速增加。CISO可增强安全运营中心的自动化水平和协调性以确保不会浪费CISO或管理层的宝贵时间。

3. 注重对人才的支持

- 人才短缺是一个长期的挑战，随着世界从疫情中缓慢恢复，某些因素也会变得重要，例如团队成员的健康、远程办公安排以及包括安全运营中心和会议室在内的办公场所再设计。
- CISO应通过交叉培训团队成员，减少对工具或流程具有丰富知识的特定人员的依赖。
- CISO及其领导团队应努力在其网络安全组织中建立和维护积极、充满活力的工作文化。这对于吸引和留住最优秀的人才至关重要。

虽然给当前的运营环境带来了巨大的的挑战，但CISO应专注于更广泛、更长期的组织目标和计划。这将有助于确保网络安全时刻做好准备，紧跟未来变革。

尾注

1. Peter Baldwin, “New York Department of Financial Services issues new guidance regarding COVID-19 cybersecurity risks,” *National Law Review* 10, no. 176 (2020).
2. Iman Ghosh, “This is the crippling cost of cybercrime on corporations,” World Economic Forum, November 7, 2019.
3. Deloitte, “COVID-19 executive cyber briefing: Read the latest,” May 20, 2020.
4. Aaron Brown and Mark Campbell, *Cloud cyber risk management: Managing cyber risks on the journey to Amazon Web Services (AWS) solutions*, Deloitte, 2017.
5. Andrew Rossow, “The birth of GDPR: What it is and what you need to know,” *Forbes*, May 25, 2018.
6. Dave Kovaleski, “FFIEC backs Cybersecurity Profile tool for financial institutions,” *Financial Regulation News*, August 30, 2019.
7. Devon Coldewey, “The California Consumer Privacy Act officially takes effect today,” TechCrunch, January 1, 2020.
8. Aaron Brown et al., *Cloud and identity and access management: How to do identity and access management in Amazon Web Services*, Deloitte, 2019.
9. Tommy Viljoen, *Cybercrime is not just a tech problem*, Deloitte, accessed June 24, 2020.
10. Francisco J. Acoba, Darin Buelow, and Tina Witney, *COVID-19 return-to-the-workplace strategies: Emerging lessons and key questions for financial services leaders*, Deloitte Insights, May 15, 2020.

本报告原名*《Reshaping the cybersecurity landscape How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions》*，
由德勤中国金融服务业风险咨询团队进行翻译。

致谢

报告联合作者 **Nikhil Gokhale** 在此对 **Meghana Rajiv Kanitkar, Sriram Balakrishnan, Prachi Ashani, Sanjay Vadrevu, Surya Kiran Sharma, Yashvardhan Kabra,** 以及其他对本调研的编制提供有益帮助的人员表示感谢。报告作者特此感谢 **金融服务信息共享与分析中心**（**FS-ISAC**） 对实地调研和分析工作作出的贡献。

关于作者

Julie Bernard | juliebernard@deloitte.com

Julie Bernard 是德勤风险与财务咨询合伙人，同时是德勤美国银行与资本市场网络与战略风险服务主管合伙人。拥有超过25年为全球顶级金融机构业务流程和信息技术相关领域服务经验。Julie在安全策略、隐私、消费者认证、欺诈预防和威胁管理方面有着广泛的经验，助力客户更安全、警觉和有韧性地应对越来越多的网络威胁和越来越复杂的技术问题。Julie是高层女性论坛前董事会成员，目前是FS-ISAC顾问委员会成员。Julie毕业于威斯敏斯特学院(Westminster College)获得音乐和工商管理学士学位，在伦斯勒理工学院(Rensselaer Polytechnic Institute)获得金融MBA学位。

Deborah Golden | debgolden@deloitte.com

Deborah Golden是Deloitte & Touche LLP合伙人，同时是德勤风险与财务咨询美国网络与战略风险服务主管合伙人。在过去六年中，Golden担任政府与公共服务（GPS）网络风险服务主管合伙人，以及GPS咨询市场主管合伙人、GPS福祉领导合伙人以及和一主要联邦政府医疗保健供应商主管合伙人。Golden在多个行业的信息技术领域拥有超过25年服务经验，深入关注政府和公共服务、生命科学和医疗保健以及金融服务领域，给予客户网络安全、技术转型、隐私和监管方面的帮助。

Mark Nicholson | manicholson@deloitte.com

Mark Nicholson是Deloitte & Touche LLP合伙人，是德勤风险与财务咨询网络与战略风险服务金融服务行业主管合伙人。Nicholson致力于帮助组织架构复杂的企业更好的利用先进技术建立网络风险防范项目，使网络风险投资与风险优先级更好地结合起来，增强风险预警并助力客户加强面对网络安全事件的应对能力。

联络我们

Julie Bernard
合伙人| 德勤风险与财务咨询 | 网络与战略风险服务 | Deloitte & Touche LLP
+ 1 704 227 7851 | juliebernard@deloitte.com

Deborah Golden
合伙人| 德勤风险与财务咨询 | 网络与战略风险服务 | Deloitte & Touche LLP
+1 571 882 5106 | debgolden@deloitte.com

Mark Nicholson
合伙人| 德勤风险与财务咨询 | 网络与战略风险服务 | Deloitte & Touche LLP
+1 201 499 0586 | manicholson@deloitte.com

Steven Silberstein
CEO | FS-ISAC
+1 877 612 2622 | ssilberstein@fsisac.com

德勤金融服务行业研究中心

Jim Eckenrode
合伙人 | 德勤金融服务行业研究中心 | Deloitte Services LP
+ 1 617 585 4877 | jeckenrode@deloitte.com

Sam Friedman
高级经理 | 德勤金融服务行业研究中心 | Deloitte Services LP
+ 1 212 436 5521| samfriedman@deloitte.com

FS-ISAC

Ray Irving
常务董事 | 全球商业服务
+41 76 303 50 70 | rirving@fsisac.com

Brian Hansen
执行董事 | 亚太区
+65 9165 5931| bhansen@fsisac.com

德勤中国联系人

吴卫军
德勤中国
副主席
金融服务业领导合伙人
电话：+86 10 8512 5999
电子邮箱：davidwjwu@deloitte.com.cn

方烨
德勤中国金融服务业
风险咨询领导合伙人（中国大陆）
电话：+86 21 6141 1569
电子邮箱：yefang@deloitte.com.cn

Tony Wood
德勤中国金融服务业
风险咨询领导合伙人（中国香港）
电话：+852 2852 6602
电子邮箱：tonywood@deloitte.com.hk

薛梓源
德勤中国
风险咨询网络安全合伙人
电话：+86 10 8520 7315
电子邮箱：tonxue@deloitte.com.cn

何晓明
德勤中国
风险咨询网络安全合伙人
电话：+86 10 8512 5312
电子邮箱：the@deloitte.com.cn

肖腾飞
德勤中国
风险咨询网络安全合伙人
电话：+86 10 8512 5858
电子邮箱：frankxiao@deloitte.com.cn

冯晔
德勤中国
风险咨询网络安全合伙人
电话：+86 21 6141 1575
电子邮箱：stefeng@deloitte.com.cn

张震
德勤中国
风险咨询网络安全合伙人
电话：+86 21 6141 1505
电子邮箱：zhzhang@deloitte.com.cn

江玮
德勤中国
风险咨询网络安全合伙人
电话：+86 21 2312 7088
电子邮箱：davidjiang@deloitte.com.cn

石沛恩
德勤中国
风险咨询网络安全合伙人
电话：+86 21 3313 8366
电子邮箱：nathanshih@deloitte.com.cn

何微
德勤中国
风险咨询网络安全合伙人
电话：+86 755 3353 8697
电子邮箱：vhe@deloitte.com.cn

郭仪雅
德勤中国
风险咨询网络安全合伙人
电话：+852 2852 6304
电子邮箱：evakwok@deloitte.com.hk

Puneet Kukreja
德勤中国
风险咨询网络安全合伙人
电话：+852 2740 8807
电子邮箱：puneetkukreja@deloitte.com.hk

Miro Pihkanen
德勤中国
风险咨询网络安全合伙人
电话：+852 2852 6778
电子邮箱：miropihkanen@deloitte.com.hk

办事处地址

北京
北京市朝阳区针织路23号楼
中国人寿金融中心12层
邮政编码：100026
电话：+86 10 8520 7788
传真：+86 10 6508 8781

长沙
长沙市开福区芙蓉北路一段109号
华创国际广场3号栋20楼
邮政编码：410008
电话：+86 731 8522 8790
传真：+86 731 8522 8230

成都
成都市高新区交子大道365号
中海国际中心F座17层
邮政编码：610041
电话：+86 28 6789 8188
传真：+86 28 6317 3500

重庆
重庆市渝中区民族路188号
环球金融中心43层
邮政编码：400010
电话：+86 23 8823 1888
传真：+86 23 8857 0978

大连
大连市中山路147号
森茂大厦15楼
邮政编码：116011
电话：+86 411 8371 2888
传真：+86 411 8360 3297

广州
广州市珠江东路28号
越秀金融大厦26楼
邮政编码：510623
电话：+86 20 8396 9228
传真：+86 20 3888 0121

杭州
杭州市上城区飞云江路9号
赞成中心东楼1206室
邮政编码：310008
电话：+86 571 8972 7688
传真：+86 571 8779 7915

哈尔滨
哈尔滨市南岗区长江路368号
开发区管理大厦1618室
邮政编码：150090
电话：+86 451 8586 0060
传真：+86 451 8586 0056

合肥
合肥市政务文化新区潜山路190号
华邦ICC写字楼A座1201单元
邮政编码：230601
电话：+86 551 6585 5927
传真：+86 551 6585 5687

香港
香港金钟道88号
太古广场一座35楼
电话：+852 2852 1600
传真：+852 2541 1911

济南
济南市市中区二环南路6636号
中海广场28层2802-2804单元
邮政编码：250000
电话：+86 531 8973 5800
传真：+86 531 8973 5811

澳门
澳门殷皇子大马路43-53A号
澳门广场19楼H-L座
电话：+853 2871 2998
传真：+853 2871 3033

蒙古
15/F, ICC Tower, Jamiyan-Gun Street
1st Khoroo, Sukhbaatar District,
14240-0025 Ulaanbaatar, Mongolia
电话：+976 7010 0450
传真：+976 7013 0450

南京
南京市建邺区江东中路347号
国金中心办公楼一期40层
邮政编码：210019
电话：+86 25 5790 8880
传真：+86 25 8691 8776

宁波
宁波市海曙区和义路168号
万豪中心1702室
邮政编码: 315000
电话：+86 574 8768 3928
传真：+86 574 8707 4131

三亚
海南省三亚市吉阳区新风街279号
蓝海华庭（三亚华夏保险中心）16层
邮政编码：572099
电话：+86 898 8861 5558
传真：+86 898 8861 0723

上海
上海市延安东路222号
外滩中心30楼
邮政编码：200002
电话：+86 21 6141 8888
传真：+86 21 6335 0003

沈阳
沈阳市沈河区青年大街1-1号
沈阳市府恒隆广场办公楼1座
3605-3606单元
邮政编码：110063
电话：+86 24 6785 4068
传真：+86 24 6785 4067

深圳
深圳市深南东路5001号
华润大厦9楼
邮政编码：518010
电话：+86 755 8246 3255
传真：+86 755 8246 3186

苏州
苏州市工业园区苏绣路58号
苏州中心广场58幢A座24层
邮政编码：215021
电话: +86 512 6289 1238
传真: +86 512 6762 3338 / 3318

天津
天津市和平区南京路183号
天津世纪都会商厦45层
邮政编码：300051
电话：+86 22 2320 6688
传真：+86 22 8312 6099

武汉
武汉市江汉区建设大道568号
新世界国贸大厦49层01室
邮政编码：430000
电话：+86 27 8526 6618
传真：+86 27 8526 7032

厦门
厦门市思明区鹭江道8号
国际银行大厦26楼E单元
邮政编码：361001
电话：+86 592 2107 298
传真：+86 592 2107 259

西安
西安市高新区锦业路9号
绿地中心A座51层5104A室
邮政编码：710065
电话：+86 29 8114 0201
传真：+86 29 8114 0205

郑州
郑州市郑东新区金水东路51号
楷林中心8座5A10
邮政编码：450018
电话：+86 371 8897 3700
传真：+86 371 8897 3710

Deloitte.
Insights

敬请登陆www.deloitte.com/insights订阅德勤洞察最新资讯。

敬请关注@DeloitteInsight

关于德勤洞察
德勤洞察发布原创文章、报告和期刊，为企业、公共领域和非政府机构提供专业洞察。我们的目标是通过调查研究，利用整个德勤专业服务机构的专业经验，以及来自学界和商界作者的合作，就企业高管与政府领导人所关注的广泛议题进行更深入的探讨。

德勤洞察是Deloitte Development LLC旗下出版商。

关于本刊物
本刊物中所含内容乃一般性信息，任何德勤有限公司、其成员所或它们的关联机构并不因此构成提供会计、商务、财务、投资、法律、税务或其他专业建议或服务。本刊物并非代表此类专业建议或服务，亦不可作为任何可能影响您的财务或业务的行动或决策依据。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。

任何德勤有限公司、其成员所或他们的关联机构均不对任何方因使用本刊物而导致的任何损失承担责任。

关于德勤
Deloitte（“德勤”）泛指一家或多家德勤有限公司（即根据英国法律组成的私人担保有限公司，以下称“德勤有限公司”），以及其成员所网络和它们的关联机构。德勤有限公司与其每一家成员所均为具有独立法律地位的法律实体。德勤有限公司（又称“ 德勤全球”）并不向客户提供服务。在美国，德勤指德勤有限公司、在美国以“德勤”的名义运营的关联机构及其各自的附属公司所属的一家或多家美国成员所。根据公共会计条例及法规，某些服务并不向鉴证客户提供。请参阅www.deloitte.com/about以了解更多有关德勤全球成员所网络的详情。

Designed by CoRe Creative Services. RITM0574649