protiviti®
Global Business Consulting
甫瀚

内部审计在云风险管控中的角色

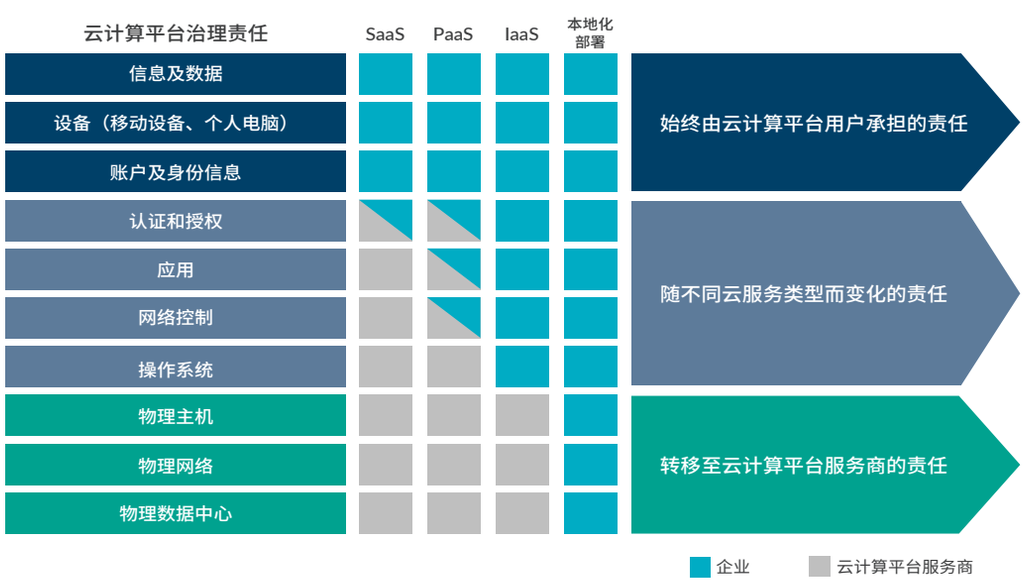
敏于知

自云计算的名词于 2006 年被提出之后，其技术和服务场景逐步成熟，云服务被全球各个国家和地区的企业广泛采用。伴随信息技术的高速发展，云计算正在成为企业的组成部分，并帮助企业快速应对不断发展的消费者行为、频繁变化的商业模式以及新业务带来的机遇和风险。

企业对于云计算的需求不再是以技术为中心，而是越来越多地受到业务转型的推动。尽管云计算平台正在变得更加强大，带来更多的业务价值，但是企业用户却发现单一的云计算平台难以覆盖全部的业务需求。因此，企业用户开始采用多个供应商的云服务，用以满足业务发展需要。多云平台环境存在差异，在对不同的云环境进行管控时存在较大的挑战。

企业采用云服务的潜在风险

企业可以根据自身的技术能力、风险治理能力以及经济成本等因素选择最贴合自身需求的服务类型。在主流的 SaaS、PaaS、IaaS 服务类型中，云计算平台服务商为企业提供从基础设施到软件不同层级的服务。根据服务内容的不同，企业与云计算平台服务商在云治理方面承担的责任不同（参见下图），因此，在各个治理领域，企业所面对的风险及需要关注的问题亦需根据实际情况进行评估。



企业如果能够理解其在采用云计算服务所面临的风险，并提前准备应对计划，那么风险则是可控的。甫瀚咨询结合自身的 IT 审计行业经验及企业客户、监管机构的关注点，梳理了以下启用云服务所面临的首要风险，企业应予以重点关注。

特权用户访问

云服务商将如何控制对企业数据的访问？企业如何才能防止云服务商滥用访问权限？

监管合规

企业自身的业务必须遵守监管要求。企业如何知晓云服务商是否遵守了这些监管要求？

数据的存放地点与所有权

一旦企业的数据上传到云计算平台，数据将会存放在哪里？云服务商的数据中心是否会位于企业未开展业务的管辖区域？

数据分离

如果多个客户的数据被存储到相同的服务器设备中，云服务商如何确保其他客户无法访问到企业的数据？

恢复

云服务是否存在服务中断情况？如果出现了服务中断，谁将负责恢复云服务？服务可以在多长时间内恢复？

调查支持

当企业收到法律保全通知时将如何处理？云服务商是否会帮助企业保护数据？

长期生存能力

如果云服务商倒闭了，企业如何取回自己的数据？如果云服务商是一家初创企业，他们是否有长期的资金和服务模式为企业提供服务？

IT 一般控制

企业所使用的云环境是否拥有基本的 IT 一般控制支持？企业如何知晓云环境是安全的？

未知云服务

企业是否已经知道所有在用的云服务？

企业作为信息和数据的责任方需保障个人信息和数据的安全，在使用云服务的过程中，确保其稳定、安全以及对突发事件快速反应能力的同时，还应关注不断变化的监管合规环境。自 2014 年起，国家监管机构、网络安全行业公司、大学等专业机构共同参与起草了《云计算服务安全指南》《云计算服务安全能力要求》等国家标准；2019 年国家互联网信息办公室、国家发展和改革委员会、工业和信息化部和财政部联合发布了《云计算服务安全评估办法》，进一步加强对党政机关、关键信息基础设施运营者在采购及使用云计算服务时的安全可控水平要求。此外，2016 年起国家陆续发布了《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》三大信息安全相关法律法规，这些法律法规亦适用于云服务的数据、平台、基础设施以及云上应用安全风险的管控。如果出现了个人信息及敏感数据泄露或网络安全事件导致的服务中断等问题，企业除直接经济损失外，还将面临监管机构问询、责令改正、处罚、停业整顿、吊销营业执照等风险，相关人员甚至可能面临刑事处罚。目前已存在企业因用户信息泄漏、可用区服务中断、服务异常、敏感数据传输等问题被监管机构问询、勒令整改或大额处罚的情况。在《中华人民共和国网络安全法》正式实施之前，各行业作为关键基础设施运营者、网络运营者的公司，就已启动了云服务相关的风险评估及应对工作，以降低合规风险。

内部审计支持云服务风险应对

企业上云过程中，内部审计部门应行使保障职能，协助管理层根据企业现状识别其可能面临的风险，以使管理层能够依据企业自身的风险偏好制定贴合企业现状的风险缓释措施。为保证企业对云计算平台的风险进行了全面的评估和管理，内部审计部门应当确保企业管理层对企业上云的全过程进行关注，并向管理层声明内部审计在该过程中的独立保障职能，在云战略的定义和沟通、云服务商评估、云平台实施过程、云服务商持续监控等各环节或阶段，通过参与关键会议或对关键节点出具评估建议的方式，促使云服务风险管控措施设计到位、执行有效。

目前，很多企业内部审计部门的 IT 审计团队，已经越来越关注企业上云之后的安全及日常运营，并将该部分内容纳入到审计计划中。然而，大部分企业的内审职能在云部署完成之前的各阶段参与不足，使得早期阶段潜在风险的影响在云实施后显现。为避免此类情况发生，内部审计部门应在各环节介入，以确保技术风险及相应的问题在初期即被识别并部署应对措施。甫瀚咨询根据对云计算平台实施全生命周期风险的调研，从 IT 审计角度，建议企业内部审计部门应对以下方面进行重点关注。

企业定义云计算平台战略时，内部审计部门应确保企业：

- 已经针对迁移至云计算平台的业务进行论证与价值分析
- 已经评估迁移至云计算平台的决策是否符合业务需要
- 已经了解将要迁移至云计算平台的系统和数据现状

企业在进行供应商评估时，内部审计部门应确保企业：

- 已经确定负责供应商关系管理的人员
- 已经了解如何对云计算平台的公司数字资产进行保护
- 已经可以明确云计算平台数字资产的责任划分
- 已经了解启用云计算平台对系统灾难恢复计划的变化与影响
- 已经了解云计算平台供应商如何对共用平台硬件设施的多租户进行管理
- 已经了解云计算平台对企业科技环境带来的影响
- 已经了解云计算平台中企业数据的物理存储情况
- 已经了解到企业现有的风险与控制措施是否可以覆盖云计算平台的潜在供应商风险

企业在实施云部署时，内部审计部门应确保企业关注：

- 云计算平台的服务水平协议（SLA）、运营水平协议（OLA）的制定情况
- 公司与云计算平台供应商的合规职责方面如何划分
- 如何管理云计算平台的系统问题事件
- 如何分配合理的云计算平台用户的数据访问权限
- 如何制定云计算平台的数据备份策略
- 如何向最终用户 / 使用用户进行推广和操作使用培训

企业在使用云服务的过程中，内部审计部门应确保企业：

- 对供应商关系进行管理
- 确认供应商提供的服务内容与服务金额的合理性
- 确认公司对供应商的服务水平、运营水平进行了合理的评估
- 对供应商合同协议中监管、安全、隐私等方面要求的履约情况进行了监控和评估

达于行

甫瀚咨询可提供的服务

甫瀚咨询为企业提供云计算平台的 IT 审计咨询服务，协助企业提升针对云服务风险治理的内部审计能力，为企业发现并应对云服务风险提供支持。我们可提供的云审计相关服务包括：

云服务实施合规支持

企业迁移至云平台前的跟进审计，评估并确保企业在云平台的战略定义、供应商评估、迁移实施、供应商服务保障监督等环节均进行了适当的风险管控。

云服务安全专项审计

基于企业内审年度或专项审计计划，通过甫瀚咨询成熟的审计方法论，针对企业采用的云服务类别，评估其所承担安全责任的执行情况。

云治理体系评估及优化

理解企业当前的云治理框架，从制度、控制措施、安全标准、企业架构符合性、组织与人员、云服务生命周期管理、监管合规、资源消耗管理等视角对企业的云治理框架进行全面诊断，并协助优化。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2023年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc. (纽约证券交易所代码: RHI) 的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联系我们

徐晨曦
项目总监
Melissa.Xu@protiviti.com

钟楠
经理
Ernie.Zhong@protiviti.com

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话: (86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话: (86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话: (86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话: (852) 2238 0499

protiviti 甫瀚