COSO

美国反虚假财务报告委员会之发起组织委员会

企业风险管理程序领先思维

# 针对云计算的企业风险管理

翻译：张晓泉　　校对：张翔

2012年12月

## 作者

### 国富浩华会计公司

主要撰稿人

沃伦•陈（Warren Chan）
IT风险服务部主管
国富浩华会计公司—芝加哥

尤金•梁雷格（Eugene Leung）
前任IT风险服务部前任顾问
国富浩华会计公司—芝加哥

海蒂•皮里（Heidi Pili）
前任IT风险服务部前任顾问
国富浩华会计公司—芝加哥

## 审校人

维多利亚•郑陈（Victoria Cheng）
IT风险服务部顾问
国富浩华—芝加哥

拉里•瑞格（Larry Rieger）
首席执行官
国富浩华全球风险咨询—芝加哥




## 序言

本项目受美国反虚假财务报告委员会下属的发起组织委员会（COSO）委托，COSO致力于通过制定全面的企业风险管理、内部控制和反舞弊框架及和指引来提供推广领先思维，以改善组织绩效和治理，减少企业舞弊行为。COSO是一家私营组织，由以下机构发起并提供资金支持及资助：

- 美国会计协会 （AAA）
- 美国注册会计师协会 （AICPA）
- 财务经理人协会 （FEI）
- 美国管理会计师协会 （IMA）
- 内部审计师协会 （IIA）

COSO
Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org

**目录**

# COSO针对云计算的企业风险管理

随着计算机技术的进步，个人电脑和网络服务器已经取代大型中央主机，成为信息处理的主要工具。今天，云计算技术有望成为科技和商业协作领域另一个重要里程牌，许多组织正在认真考虑是否采用这项新技术。通过互联网提供的主机托管强化服务，云计算技术能够极大地提升各类组织的商业模式，企业无需对基础设施、员工培训、专业人员以及软件等进行大量投资就能满足自身计算资源的需求。

2010年秋天，Google的一位高管在接受美国国会下属委员会征询时证实，世界范围内购买Google云服务的企业数量已逾300万家。另据高德纳公司（Gartner Inc）预计，到2014年，整个云计算行业的产值将高达1400亿美元。

系统虚拟化、系统资源管理以及互联网方面的技术改进催生了云计算技术，满足各类企业的技术需求有了切实可行的替代方案。高管们对云计算技术带来的以下好处尤为称道：

- 计算资源可以瞬间获取
- 以更低的技术费用创造更大的价值
- 通过这种通用技术平台能够推动标准化进程
- 可以减少内部技术支持人员的数量

云计算技术能为组织提供不同于以往的协作和人际互动方式、全新的组织依附关系、更快的资源响应以及新的商业模式。与任何新生事物一样，施行云计算技术也会产生相应的风险。

COSO发布了题为《企业风险管理－整体框架》的报告，为企业全方位地评估和监管风险建立了通用语言并奠定了基础。该文表示：“企业风险管理能够使管理层有效应对不确定性因素及与其相关的风险和机会，提升组织的价值创造能力。”[1]云计算技术能够反映企业营运环境的巨大变化，如果采纳《企业风险管理－整体框架》中的建议，企业将能够轻而易举地识别风险，采取针对性的解决措施，并且通过不断演化的云计算模式辨识不确定性因素以及隐藏其中的机会。

本文意在宣传《企业风险管理－整体框架》的中心主旨并提供指导方针，以便企业能够快速地识别云计算技术带来的风险和造成的影响。企业高管对云计算技术的风险和收益认识得越深刻，就能越有效地推动本企业为将来做好准备。下文中的指南将协助高管识别、监管、减轻或承受采用云计算技术所带来的风险。

标注 1: 引自 COSO 于 2004 年 9 月发布的《企业风险管理－整体框架》报告第 3 页。

# 1. 什么是云计算

## 定义

云计算技术是一种计算资源部署和采购模式，使得企业在任何地点可以通过互联网获取其所需的计算资源和应用软件。依托云解决模式，企业仅需采购少量或根本没必要再采购软、硬件，也无需再自行保存数据。所有的资源将存放在和其他企业共享的技术中心里，并由第三方服务提供商进行管理。

## 云计算专用术语

**•云服务提供商（CSP）**——第三方服务提供商，通过云计算技术提供应用软件交付、托管、监管及其他服务。单个组织根据所需的云解决方案，可以与多家云服务提供商签订服务合同。

**•多租户（Multi-tenant）**——在云服务提供商提供的绝大多数技术解决方案中，一个消费者就是一个租户，与其他众多的租户一起分享共用资源和技术。多租户的概念对资源的整合及交付方式产生了影响，例如，某位云服务消费者将数据保存在大型数据存储平台，而这个平台中的数据对采用同种云解决方案的其他用户而言是开放的。

## 云计算部署模式

根据“美国国家标准与技术研究所”（NIST）的定义[2]，最为常见的云计算部署模式有：

**•私有云（Private cloud）**——云架构仅对单一组织开放，由企业自身或第三方进行管理，企业可自行搭建，亦可由第三方提供。

**•社区云（Community cloud）**——出于共同利益需求（如任务、行业协作以及合规性要求等），云架构由数个企业共享，组成一个特别的社区。云架构由社区企业或第三方管理，社区可自行搭建，亦可由第三方提供。

**•公共云（Public cloud）**——云架构仅对公共部门或大型行业集团开放，所有权归云计算服务提供机构所有。

**•混合云（Hybrid cloud）**——是上述两种或三种云计算部署模式的混合体，每种模式仍然保持相对地独立，通过标准化或专利技术组合在一起，便于数据和应用软件的传递。

## 云服务的交付模式

由云服务提供商提供的云解决方案通常被称作“云服务交付模式”，主要有：

**•软件即服务（SaaS）**——各类应用程序，企业使用它们可实现特定功能或进程，如电子邮件、客户管理系统、企业资源规划系统以及电子表格等。SaaS的升级版本——业务流程即服务（BPaaS），一经面世就大获好评。通过BPaaS，在云服务交付解决方案的支持下，企业的业务流程（包括工资支付和供应链管理）可全部外包给第三方服务提供商。

**•平台即服务（PaaS）**——一种开发环境，在此可以搭建和部署应用软件。云服务提供商为客户提供专享工具软件，协助客户创建应用系统和程序，可以在云服务提供商托管架构上实现运行。

**•架构即服务（IaaS）**——由云服务提供商提供一个完整的资源数据中心，如网络、计算资源和存储资源。

标注 2: 彼得 • 梅尔和蒂莫西 • 格兰尼斯编写的《NIST 云计算的定义——特别报告编号 800－145》，内容详见 http://csrc.nist.gov/publications/PubsSPs.html#800-145。

## 2. 机会

应用云计算技术所带来的机会和潜在收益包括：

**•节约成本**——云服务的消费者只需为所使用的计算资源付费，而无需采购或租赁相关设备，通常情况下这些设备都会存在或多或少的闲置现象。如果云计算技术能够满足企业所有的技术需求，那么，企业将不再保留内部专用数据中心，也不用在场地和公用事业方面花费额外费用。如果能从云服务提供商处获得其所需的所有计算资源，企业将节约支出，如获得税款减免。而在企业保有内部专用数据中心情况下，由于已经考虑了资本支出和摊销的因素，企业将无法享受这项税款减免政策。

**•加快部署速度**——云服务提供商不仅能够满足企业的计算资源需求（如服务器进程和数据储存），而且与绝大多数企业内部信息技术部门相比，能够更为快速地响应这些需求。随着计算机技术的进步，计算能力和应用软件需求的实现时间将变得越来越短，由长达数月变为数周，再由数周变为数天，直至数天缩短为数小时。

**•可扩展性以及更好的技术资源协调性**——无需额外的资本支出，企业就能自如地调整计算能力，可由一个服务器扩展至数百个服务器。这种可扩展性使企业可以获得大量的计算资源来执行临时性的、高强度的计算任务。在非常规的、高强度的计算需求期间，企业无需对计算能力进行额外投资就能完成计算任务。

**•减少技术管理工作量**——建立IT部门并维持其正常运转花费巨大，且费时费力。云计算技术可以使企业抽出身来，有更多的时间关注核心目标。绝大多数云服务都是建立在预先构建的、标准化的技术基础之上，能够向企业提供更好的支持。与此同时，该技术基础提升了计算资源供给的便捷性，从而能够更加统一地进行技术升级，更加快速地满足IT资源需求。

**•环境收益**——如果每家企业都采用云计算技术，取代自建数据中心的做法，那么电力消耗量、碳排放量以及土地占用量都将大为减少。

## 3．风险

根据《企业风险管理－整体框架》的定义，“风险指的是某个事件发生后，对目标的实现产生负面影响的可能性”[3]。

在绝大多数情况下，云解决方案一旦被采纳，企业的风险水平和风险状况也将发生变化，这是因为与云服务提供商相关的风险事件（不管是固有的或是遗留下来的）发生的可能性及潜在影响会随之加大或减小，当然这也要取决于企业如何以及出于何种目的实施云解决方案。

与云计算相关的典型风险包括：

•**颠覆性力量**——云计算技术能够加快技术革新速度并节约成本，然而这两方面对某些组织而言就是风险事件。由于能够降低新竞争者的进入门槛，云计算技术将威胁或颠覆某些商业模式，甚至让这些模式将来被淘汰出局。例如，流媒体作为一项技术解决方案充斥于整个互联网，这将极大地削减CD和DVD的销售量以及传统销售所依托的实体零售店数量。如果现有竞争者全面采用云计算技术，那么他们将会有新的商业和创新灵感，成为市场中的领跑者。通过减少资本性支出，云计算解决方案能够节省大量的短期成本，那些采用云技术的组织将比没有采用云技术的同行获得更多的利润。因此，一旦某家企业采用了云解决方案，那么本行业中的其他企业也不得不紧随其后，尽快采用。

•**与云服务提供商和其他云租户共处同一个风险系统中**——当一个组织采用了第三方管理的云解决方案，该组织就与云服务提供商在法律责任、风险环境、事件升级、事件响应以及其他方面产生了新的依存关系。云服务提供商和其他云租户的举动会通过多种方式对组织产生影响，需要考虑的因素有：

（1）从法律意义上来说，第三方云服务提供商与接受服务的组织是完全不同的两个实体。但是，如果云服务提供商忽视或未能履行职责，那么接受服务的组织有可能会被牵连，招致法律责任。相反，如果云服务的消费组织未能履行自身的职责，云服务提供商却不太可能因此惹上法律方面的麻烦。

（2）云服务提供商与接受服务的组织可能有各自的企业风险管理计划以应对各自面对的风险环境。仅在极少数情况下（如签订巨额合同），云服务提供商才会将自己的风险管理计划与客户的计划进行整合。一个组织如果使用第三方提供的云计算服务，那么它所面临的风险环境就由该组织自身面临的风险和云服务提供商所面临的风险共同构成（本文第5部分“在云计算模式下开展企业风险管理（ERM）”将就此进行深入探讨）。

•**缺乏透明度**——云服务提供商不可能向外透露云服务的进程、营运、控制以及方法等方面的详细信息。例如，云服务消费者对于数据储存地点、云服务提供商提供及分配计算资源所使用的运算法则、确保云计算架构组件安全所采取的特别保护措施以及消费者数据在云端的隔离方式等知之甚少。

•**可靠性和性能问题**——系统故障是一种风险事件，可发生于任何计算环境中，但却给云计算带来了独有的挑战。此外，虽然服务协议对特定需求进行了约定，但如果云租户或突发事件对云架构提出预料之外的资源需求，云服务提供商提供的解决方案有时候就可能无法实现协议约定的性能指标。

•**供应商锁定以及应用软件缺乏便捷性和互通性**——许多云服务提供商都随云解决方案一并提供了应用软件开发工具，这些工具往往具有专用性，由它开发出来的软件往往只能在云服务提供商特定的解决方案架构上运行。因此，用专用开发工具编写的软件与云解决方案之外的系统可能无法实现很好的兼容。此外，使用专用开发工具开发的

标注3：引自COSO于2004年9月发布的《企业风险管理－整体框架》报告第16页。

软件越多，在特定云服务提供商处存储的结构性数据越多，云服务消费者对云服务提供商的依赖性就越强，这就加大了消费者更换云服务提供商的难度。

**•安全性和合规性担忧**——根据《2002年萨班斯-奥克斯利法案》（SOX）、《1996年健康保险流动及责任法案》（HIPAA）、《美国爱国者法案》（USA PATRIOT Act）、《欧盟数据保护指令》（EU Data Protection Directive）、马来西亚《2010年个人数据保护法案》（Personal Data Protection Act 2010）以及印度《信息技术修正法案》（IT Amendments Act）等数据隐私和保护法案的明确规定，云计算处理流程可能会引发安全以及保有方面的问题。在云解决方案中，数据存储于不受组织直接控制的外部硬件上，而这些硬件为云服务提供商所有，因此不论云服务消费者采用何种云解决方案（SaaS、PaaS或是IaaS），他们可能无法获取、检查网络运行和安全事件日志。一方面云服务提供商没有义务公布此类信息，另一方面云服务提供商受限于对云架构其他共享租户的保密责任而无法公布。

**•由于所蕴含的高价值易成为黑客攻击目标**——共存于一个云服务提供商架构下的多个组织联合体比单个组织的吸引力更大，从而遭受黑客攻击的可能性更高。因此，在绝大多数情况下，云服务提供商的云解决方案在保密性和数据可信度方面的内在风险水平很高。

**•数据泄露风险**——在多租户的云环境中，使用者及应用软件共享资源会产生数据泄露风险，而拥有专用服务器和专有资源的单一组织不会有此困扰。因此，数据泄露风险是考虑数据隐私和保密合规性时需要重点关注的一个领域。

**•IT部门的人事变动**——如果一个组织大量采用云计算，那么该组织仅需少量的内部IT员工就能完成架构管理、技术部署、软件开发以及日常维护等工作，剩余IT员工的工作态度和奉献精神可能因此而成为风险因素。

**•云服务提供商的生存危机**——许多云服务提供商的成立时间不长，相对年轻，而且对于一个具有良好建制的企业来说，云计算服务业还是一个新生事物。因此，云服务的生命力和获利能力尚不确定。因为无利可图，某些云服务提供商会降低所提供的云服务，而且云计算服务提供商最终可能会经历并购和整合，这些因素可能导致云服务提供商的消费者处于无法获取相应服务的困境，不得不花费时间和金钱重新搜寻和采纳替代方案，比如重新回到自主开发解决方案的老路上。

除了上述风险之外，云计算本身所具有的某些特性会引发其他不甚明显的挑战，具体情况有待评估（本文第7部分“其他事项”将详述这些不太明显的风险点）。

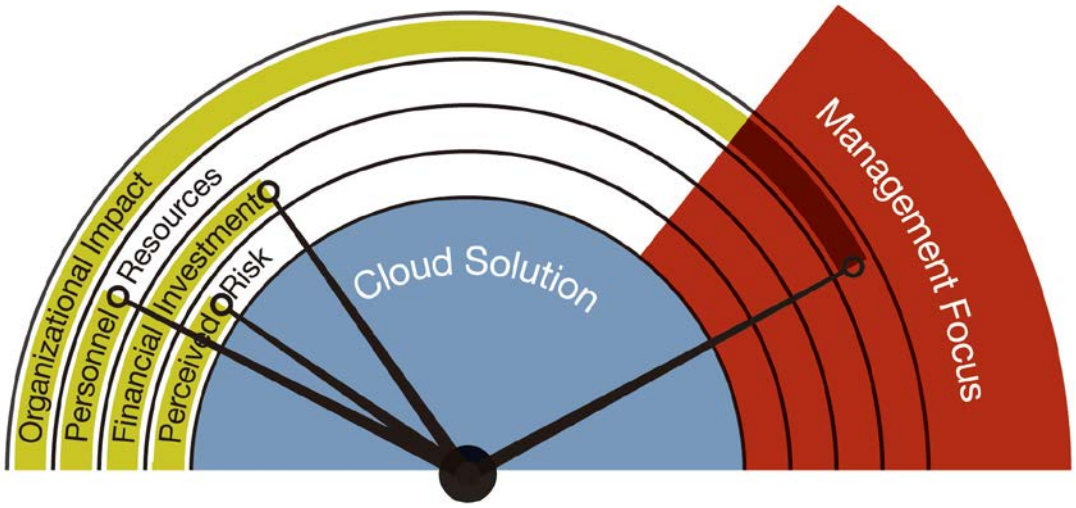
某些管理团队可能因为“公共云”较少的前期资本需求而愿意承受企业整体采用“公共云”而产生的风险。初创企业和风险资本青睐的往往是商业模式，而不是技术架构，这是因为风险投资一旦失败，技术架构能够挽回的投资损失要小很多。与上一代技术选择相比，云解决方案能够帮助初创企业以更快的速度、更经济高效的方式部署他们的商业模式。

本文所讨论的云计算风险都很重要，须予以充分的重视，否则一旦发生将带来相当严重的后果。即便一个组织与云服务提供商签订合同做了相关约定，即使这些合同得以全面履行（然而多数云服务合同并未得到切实履行），上述风险也不太可能因此而得到减缓。因此，在云服务提供商直接提供的云解决方案之外，一个组织还应该考虑风险减缓措施并确保这些措施能够得到执行。

## 4．云计算技术面世后，商业营运环境所发生的改变

一个组织应该辨识云计算技术对其营运环境所带来的风险和其他影响，并将这些风险和影响纳入企业风险管理程序中予以考量。在某些情况下，云计算技术能够绕过常规的管理层监控体系，轻而易举地进入企业。如果一个项目需要投入大量资源，并且要耗费数月甚至数年的时间才能完成，此时企业管理层就需要介入常规程序，实施控制措施并进行审批。毫不意外，企业高层对于此类项目一定非常关注，会进行相应的风险评估、业务审计，乃至组建各类专业指导委员会。某些云解决方案只需少量的经费和人员投入，能在很短的时间内得以采纳。对于云计算技术而言，“大投资等于大影响”已经成为老黄历，相反小投资也能产生大影响。“应花大力气对云计算技术的风险进行分析并开展相关尽职调查”，这一观念似乎与我们的直觉相抵触，因此管理层可能会懈怠，不愿意耗费大量的时间确认相关法律和监管规定是否得到了遵守，或评估云服务提供商对于企业营运以及风险状况的潜在影响。图例4.1说明了在云计算技术采用后，某些典型的控制触发点（如员工资源和必要投入）可能无法触及应有的警戒水平，以至于无法引起高管们的监管重视。

图例4.1 云解决方案可能规避管理层监管

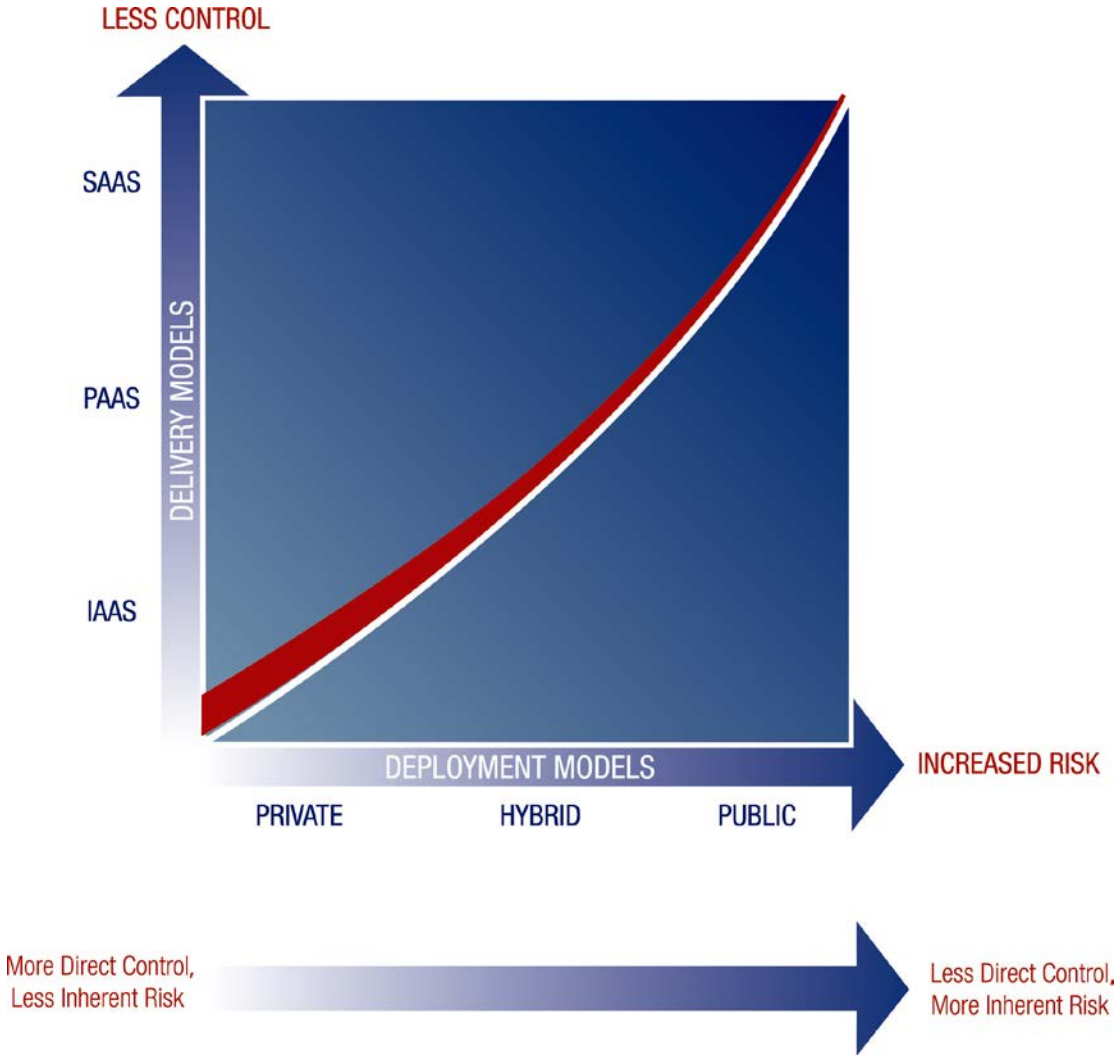



最重要的一点是，企业的管理层明白，除了某些内部私有云外，企业对于绝大多数云解决方案都缺乏直接管控，随之产生的结果就是固有风险水平进一步上升。

例如，某家企业采用了基于“公共云”的SaaS云服务交付模式，相应地，包括控制在内的某些或全部的IT管理职责就从该企业转移至第三方云服务提供商。图例4.2说明了，在不同的云服务交付和部署模式下，企业保有和让渡控制权限的程度。

具体而言，在IaaS模式下（一种基于私有云的解决方案），企业保留的控制程度最高，固有风险最小。与之相反， 在SaaS模式下（一种基于公共云的解决方案），企业的控制程度最低，固有风险最大。不管采用何种云解决方案，管理层都应该依据企业可承受的风险水平，对云服务的部署和交付模式进行评估，以确定最优的云计算环境和相关的必要控制。

图例4.2　与云服务交付及部署模式相关联的固有风险



## 5. 在云计算模式下开展企业风险管理

云计算技术的出现对于企业风险管理程序的运行环境而言是一件大事。

无论做什么事请，如果事先能够明确目标、理清行动步骤，那么成功的机率就会大大增加。因此，一项经过缜密制定的计划必然对组织目标有着清晰的界定，对云计算技术角色定位有深入的认识，能够帮助管理层做出正确的决策。企业在制定高质量的云计算技术规划并最终实施云解决方案时，应该将企业风险管理（ERM）的某些先决条件纳入考虑框架中，比如强有力的监管模式、运行良好的报告框架、对内部IT技能要求的准确理解以及明确的风险偏好。

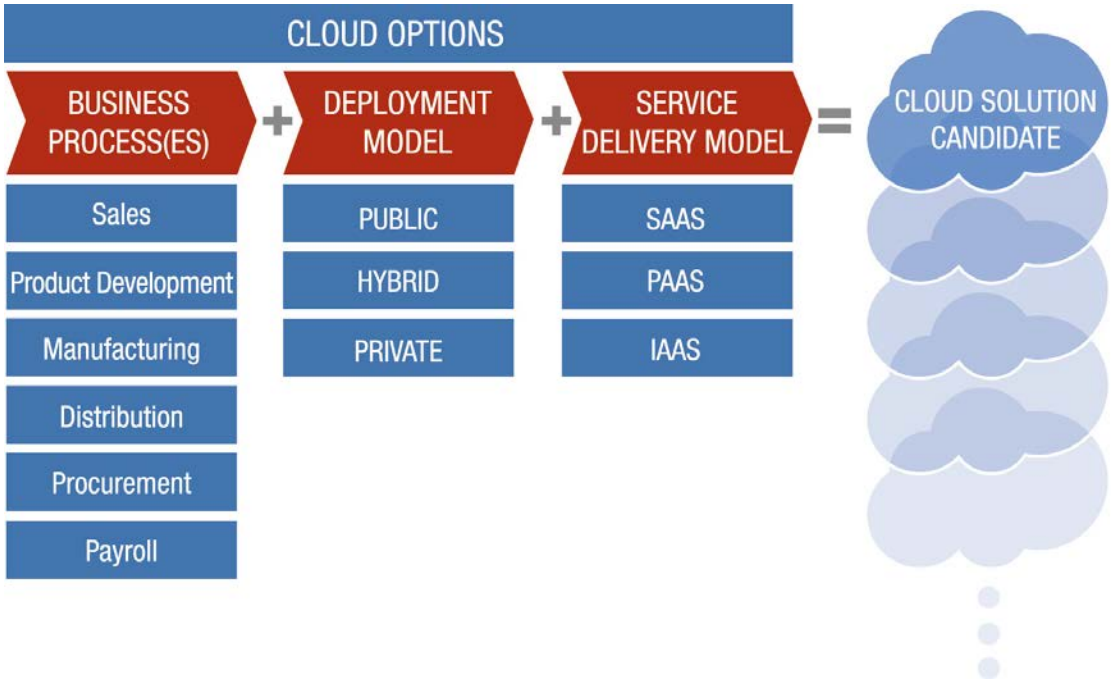
某些管理团队认为风险评估和监管程序可有可无。企业时常在未开展正式的风险评估或未对ERM和监管程序做任何修正的情况下，就采用了云计算解决方案。而最好的做法应该是：在云解决方案采纳之前，企业能在起始阶段，即云计算策略的确立阶段，就开始考虑云计算的监管措施。对那些没有充分实施ERM就采用云计算技术的组织而言，谨慎的做法就是开展风险评估并制定云监管措施。

### 运用COSO框架制定云计算技术监管措施

在云计算模式下，组织对现有ERM程序进行调整的深度很大程度上取决于云计算技术所支持的业务流程、云部署模式、云服务交付模式、签约云服务提供商的风险特性以及控制环境。

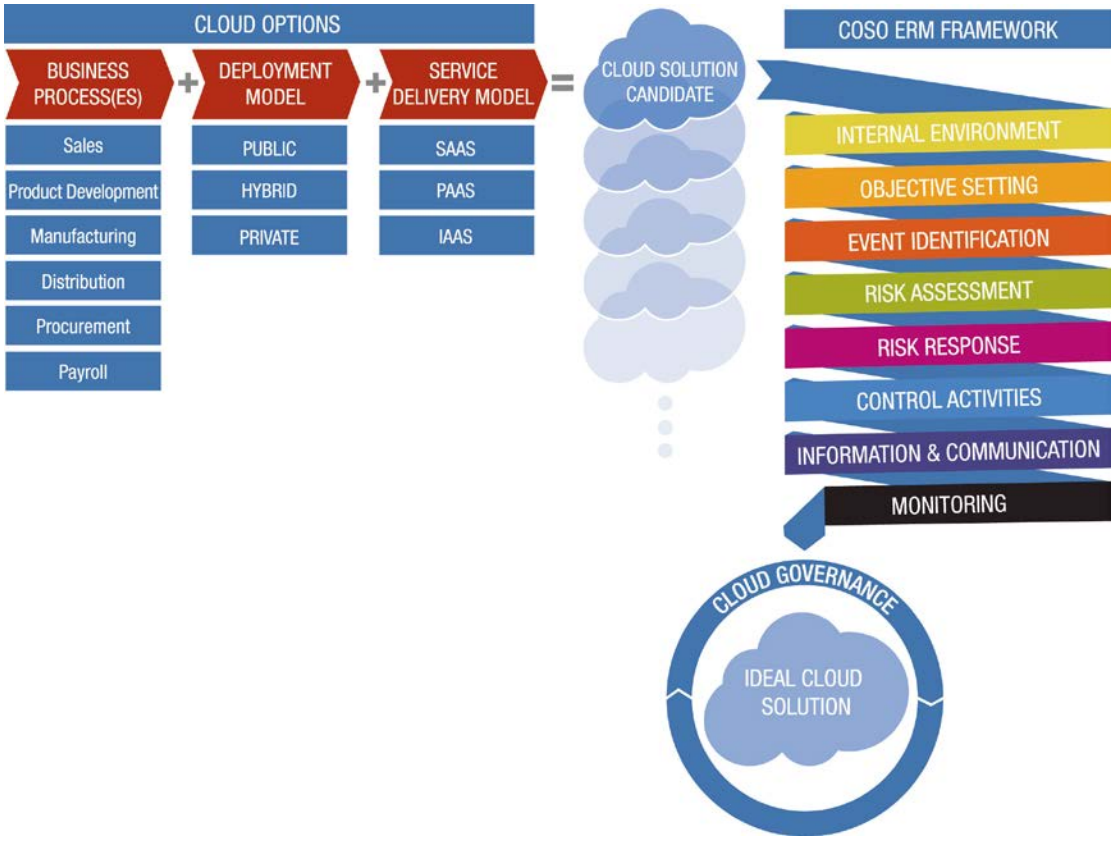
图例5.1描述了组织如何依据云计算技术支持的业务流程、云部署模式以及云服务交付模式，在各种备选云解决方案中进行选择。

图例5.1　云解决方案的制定



对一个组织来说，施行云计算技术是一项重大变革。管理层可以采用经过实践、有效性得以验证的ERM框架来评估和管理有关风险。COSO发布的题为《企业风险管理－整体框架》的报告，为企业风险管理提供了通用语言并奠定了基础，可针对特定的云解决方案构建有效的云监管程序。初始的COSO企业风险管理框架可以通过一个立方体示意图来加以说明。在图例5.2中，整体框架体现为一条管理路径，该路径由ERM各个组成要素（其起始环节为内部环境）共同构成，通过逐一检验组成要素的实现情况，组织就能洞悉备选云解决方案的优劣所在。在对所有备选云解决方案进行分析和比较之后，理想的云解决方案就会自动浮现。

图例5.2　应用COSO企业风险管理框架筛选云计算解决方案




如果云解决方案已经实施，COSO 企业风险管理框架也可以用于建立和完善云监管程序或对其进行质量鉴证检查，确保监管程序的所有重要方面（如目标、风险评估以及风险响应）均已达到管理层的要求。即便云解决方案已经实施，组织还是可以通过施行COSO 企业风险管理框架来实现有效的云监管程序。

最佳的解决方案是管理层应用COSO ERM框架筛选出理想的云解决方案整体架构（如业务流程、部署模式以及服务交付模式），而该架构与管理层的风险偏好应该保持一致。参照COSO ERM框架下的各个组成要素，对云解决备选方案进行评估，管理层能够轻而易举地识别与每个备选方案相关的风险，并设定风险可接受程度以及风险应对策略（因为风险会因选项的不同组合而有所差异）。方案评估能够帮助管理层对风险监控和管理做出审慎决策，甄选出理想的云解决方案，并在云解决方案实施之前创建一个经过周详考虑的云治理方案。

下面我们将重点讨论几个关键的概念。按照COSO ERM框架下的各个组成要素对云解决备选方案进行评估时，我们必定会涉及这些概念。

**内部环境**——内部环境是基石，从根本上界定了企业的风险偏好，进而确定了一个企业的风险和控制理念及氛围。例如，管理层出台政策，禁止外包任何营运业务（这是一种回避风险的氛围），那么，可供选择的云部署和服务交付模式就会大大受到限制，私有云解决方案也许就是企业唯一的选择。

**目标设定**——管理层需要评估云计算与企业组织目标是否一致。对企业而言，施行云计算也许能提升企业能力，实现既定目标，或者能帮助企业获取竞争优势，一旦发生这些变化，企业就要重新设定目标。

**事项识别**——管理层有责任对那些能够影响目标实现的事项（无论是机会还是风险）进行识别。企业一旦与云服务提供商签订协议，事项识别和风险评估程序的复杂程度将会随之增加。

在识别和评估风险事项时，管理层需要同时考虑外部环境因素（如监管力度、经济状况、自然环境、政治局势、社会状况以及科技发展情况）和企业内部因素（如企业文化、员工情况以及财务状况）。此外，在采用公共云或混合云解决方案时，管理层还需要研判受云服务提供商内、外部因素影响的其他事项。由于预期事项会对风险评估程序的性质和质量造成非常大的影响，所以，管理层应该建立预期事项的详细列表。

**风险评估**——管理层应当对与云战略相关的风险事件进行评估，以确定每个云计算备选方案的潜在风险影响。理想的状况是，企业完成风险评估之后，才开始实施云解决方案。

云计算可以影响风险评估的关键要点，这些关键点包括：

- **风险框架**——企业的风险框架应囊括需要管理的全部风险。云解决方案一旦采纳，企业的风险框架就应随之进行调整，因为风险发生的可能性、风险的潜在影响以及云服务提供商风险环境都会发生相应的变化（详细内容请参阅本节最后一部分“云服务提供商和其他云租户对企业风险框架的影响”）。
- **固有风险和剩余风险**——企业必须评估事项的固有风险，以此制定风险响应措施并确定剩余风险。云计算解决方案的固有风险和剩余风险水平可能高于也可能低于非云计算解决方案，不同的企业情况不一样，没有定数。
- **可能性和影响**——随着云解决方案的采纳，在很多情况下，某些事项发生的可能性及其潜在影响也会随之发生变化。做出准确应对策略的前提条件是企业是否全面、准确、及时地掌握这些风险事项。

在某些情况下，管理层无法获取云服务提供商内部控制环境的所有相关信息。因此，为了完成风险评估，企业必须做出某些假设。

**风险响应**——在组织目标的框架下，对云计算相关的风险进行识别和评估之后，管理层需要决定采取何种风险响应措施。以下是四种主要的风险响应类型：

- **风险规避**——杜绝会带来风险的一切活动（例如不采用云计算或只将私有云作为唯一切实可行的云解决方案）。
- **风险降低**——实施控制措施，意在降低风险发生的可能性或削弱风险造成的影响，抑或两者兼而有之。
- **风险分担**——通过转移或其他方式（例如购买保险）来分担部分风险，减少风险发生

的可能性或风险造成的影响。

**•风险承受**——不采取任何措施，无意改变风险发生的可能性或风险造成的影响。例如，如果企业无法对云服务提供商的控制活动进行直接干预，那么，企业就必须承受不断上升的固有风险水平。

在绝大多数情况下，企业一旦采用了混合云或公共云解决方案，那么，管理层就只能依赖于第三方管理的控制措施，管理层直接管控风险的能力就被削弱。这就意味着固有风险水平将会随着上述解决方案的实施而相应上升，而管理层也不得不随之上调自身的风险偏好。

由于风险响应在云计算环境下发挥着重要作用，我们将在本文的第6部分“针对云计算的风险响应建议”中进一步展开论述。

**控制活动**——传统的控制活动类型包括预防、侦察、手动响应、自动响应以及全覆盖等，这些措施同样适用于云计算。不同的是，在云计算解决方案中，某些控制职能仍由企业保留，但另外一些控制职能则转给云服务提供商。

如果企业现有控制措施的效果仅为中等甚至更差，那么，云解决方案的实施可能会加剧内部控制的缺陷。例如，企业将计算环境向公共云或混合云转变后，如果密码保护或数据安全的控制措施不得力，那么它遭受外部侵袭的可能性就会成倍地增加，原因就在于云计算实施后，相关人员通过公共开放的互联网来访问企业的技术平台。

**信息与沟通**——想要高效地开展业务并管理相关风险，管理层必须及时、准确地从各种途径获取与内、外部事项有关的信息并进行沟通。而施行云计算之后，云服务提供商或许不能及时地传递信息，抑或信息的质量无法与企业内部IT部门所提供信息的质量相提并论。因此，管理层需要开拓额外或其他的信息资源和获取流程才能满足自身的信息和沟通需求。

此外，管理层还应该关注与云服务提供商相关的外部信息（如财务报告、公开披露、提交给监管机构的报告、行业期刊以及其他云租户发布的声明等），这是因为某些事项会对云服务提供商或云租户产生影响，同样也会对企业产生影响。

**监控**——“曾经有效的风险响应措施可能会变得无关紧要；控制措施的效力可能会越来越小，甚至不再施行；企业的组织目标可能发生改变。”[4] 。这是2004年版《企业风险管理－整体框架》报告所做的陈述，它仍然适用于云计算时代。管理层必须持续监控ERM的有效性，以确保该程序能充分应对有关风险，并有助于企业目标的实现。从本质上来说，一个有效的ERM应该是不断演进和动态发展的，而且它演化和发展的速度还需要不断加快，以紧跟云计算的革新步伐。

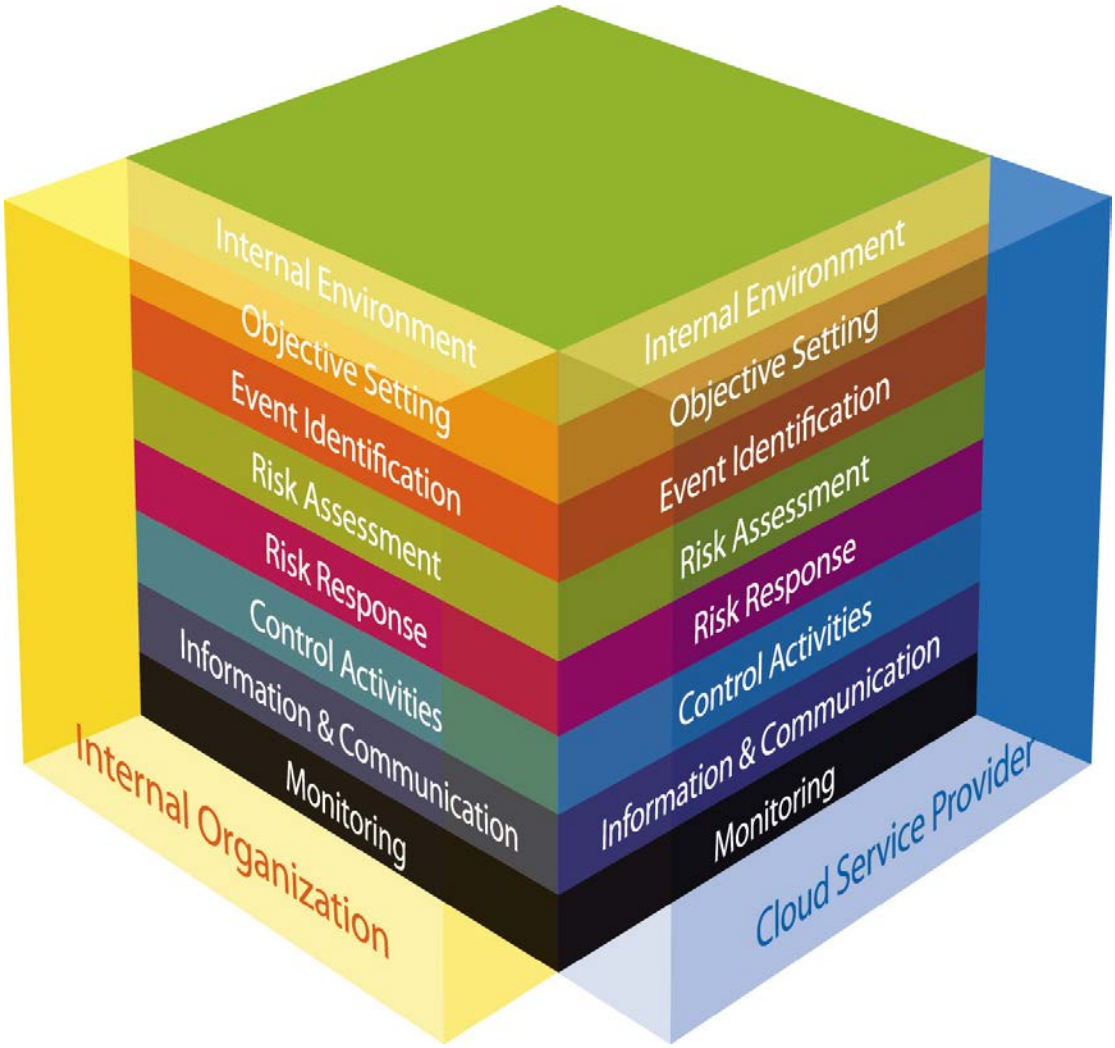
考虑到云计算所带来的潜在和现实影响，企业的全体高管（不仅仅只限于首席信息官）都应该承担相应的云计算治理职责（附录中的“云计算治理——角色与职责”提供了云计算关键职责分工的示例）。

云服务提供商和其他云租户的风险框架对本企业的影响

企业放弃专用的内部计算环境，转而采用公共云或混合云计算解决方案，这必然会导致企业的ERM环境不再独立，它的ERM构件将与云服务提供商的ERM构件相互融合。图例5.3说明了这种融合。

标注4 引自COSO于2004年9月发布的《企业风险管理－整体框架》报告第75页。

图例5.3 企业与云服务提供商融合后的ERM环境




企业与其他云租户共享数据和流程处理所依托的环境，云服务提供商和其他云租户的一举一动都会对企业产生直接的影响。如果与云服务提供商相关的风险会对云服务消费者产生影响，那么，在采用这些服务商所提供的云解决方案时，企业必须将云服务提供商相关的风险纳入企业的风险框架范围。共享的计算环境促使企业对风险框架做出改变，并提出全新的、有别于以往的控制要求。

作为云风险评估进程的一部分，管理层需要考量与其他云租户有关的风险信息，例如他们的身份、他们所部署的应用软件以及他们成为网络攻击目标的可能性。

因此，管理层制定的 ERM 方案需要应对企业自身和云服务提供商的 ERM 组成部件。管理层不仅需要识别能对本企业产生影响的风险和事项，同样还需要识别能对云服务提供商和其他云租户产生影响的风险和事项。

## 6．针对云计算的风险响应建议

随着云计算的出现，无论管理层决定是否采用云计算技术，企业营运所处的环境都在发生快速的变化。而管理层应该主动调整ERM方案和控制程序以应对上述变化。下面我们将针对本文提及的某些重要的云计算风险，详细阐述与之相应的风险响应措施。

### 风险——未经授权的云计算活动

### 风险响应措施——云计算政策和控制

所有企业都应该制定政策，建立防控体系，以此来预防和侦测未经授权的云服务采购和使用行为。相较于传统的技术采购，启用云服务的初始成本要低得多，所以，企业现有的控制措施，如费用限额，也许不再是恰当的控制触发措施，无法引发管理层的关注。

例如，在一个大型企业中，某个小型业务部门为启动一项新产品销售计划，自行决定采用基于云计算技术的客户关系管理系统（CRM）。在企业未制定云计算政策的情况下，该业务部门没有和企业内部IT部门进行沟通，也没有申请资本性支出经费（云解决方案所需要的仅仅是互联网接入和一张信用卡）就开始采用新型的客户关系管理系统。一旦启用，新系统就会存储客户数据和销售前景预测等资料，这样一来，客户的机密信息并不储存在企业内部计算环境中，因此也不受企业的监控措施或营运程序的制约。

如果企业决定采用云计算技术，那么，**对于未经授权的云计算活动我们给出以下4条风险响应建议**：

- 制定云计算使用政策，明确界定管理层认为可适用于云计算解决方案的业务流程和数据。

- 建立或更新授权政策，明确获得授权、能够处理云计算服务相关事宜的责任人。

- 甄别云服务提供商

- 就云服务提供商关系管理制定相应政策，并提供具体指南。

### 风险——缺乏透明度

### 风险响应措施——对云服务提供商的控制环境进行评估

由于所获的信息不完整或者所需要的信息很难得到，所以，企业想要对云服务提供商的环境进行高质量和全面的风险评估是一件非常困难的事。在绝大多数情况下，云服务的消费者是无法完全了解云服务提供商的内部控制环境。

例如，变动管理控制措施（如客户接受度测试、产品生产和开发环境的隔离）通常用来确保应用系统的质量。在公共云或混合云解决方案环境下，云服务的消费企业无法直接控制或深入了解云服务提供商的应用程序变化管控措施。因此， SaaS的云服务消费者需要根据自身的风险偏好以及云服务提供商在《服务型组织控制报告》中披露的信息（假设云服务提供商为编撰《服务型组织控制报告》发生了支出），相应地加强或改变应用程序变化的测试流程。

为了在一定程度上克服无法洞悉云服务提供商营运情况和控制措施的困境，管理层应在征询方案或尽职调查程序中加入控制情况调查。此外，管理层还应该在云服务合同中加入审计权条款。作为评估云服务提供商内部环境的一部分，管理层应该（最好在与云服务提供商签订合约之前）与云服务提供商进行访谈，以确定该服务商是如何看待某些风险事项的。为了进一步获取云服务提供商内部控制环境以及云解决方案的风险和质量信息，管理层应该责成企业的内部审计部门实施评估，抑或要求云服务提供商提交依据美国注册会计师协会（AICPA）制定的《鉴证业务准则第16号——公告》（SSAE 16）和《服务型组织控制报告第2号》（SOC 2）

编制的独立审计报告，内容应涉及安全性、可得性、控制完整性、保密性以及隐私权。

### 风险——安全性、合规性、数据泄露以及数据法律管辖权

### 风险响应措施——数据分类政策和流程

企业转而采用公共云或混合云解决方案将改变现有的数据存储地点、交易流程以及控制结构。企业的营运活动需要遵守现行法律法规，而上述变化对此可能造成影响，需要企业进行细致地分析。云服务合同应该清楚地约定云服务提供商在代表企业时，在合规性和遵从监管规定方面的责任。

如果企业的数据是存放在私有云之外的云端，那么，企业无从知晓数据的现存地点（服务器或存储设备）和曾经存放的地点。这种“地点盲区”是由多租户云环境的本质所决定的，在此类环境中，资源被重复使用并动态地分配给云消费者。无法识别数据存放地点和处理流程也许会成为障碍，让企业无法满足电子化搜寻（e-discovery）或数据沿袭（data lineage）相关要求。这种限制会对数据存储造成重大影响，也会对企业希望通过云计算进行的交易进程造成重大影响，只是影响的程度相对小一些。

在与云服务提供商签订的合同中，凡涉及客户数据存储地点（存放在国内还是国外）的条款都必须依照适用的数据保护法案来拟定并评估。云服务提供商也许并不会告知企业数据的存储地点，但可能会向企业透露司法管辖权方面的特定信息。对管理层而言，谨慎的做法是，在转而采用第三方提供的云解决方案之前，应事先深入了解与企业数据有关的监管要求和法律责任。例如，一家设在美国的云服务提供商对存储在德国的数据进行控制，那么，这家服务商必须同时遵守德国的数据保护法律、欧盟的数据保护及告知法律以及美国的《爱国者法案》。虽然对企业来说，合规性要求以及数据司法管辖并不是新概念，但在云服务环境下，企业为满足这些领域的监管要求，需要对云计算的使用方式方法加强审查。

在公共云或混合云的部署模式下，如果企业无法对数据存储地点进行有效地控制，那么，它就必须对存储于云端的数据类型进行控制。从风险管理的角度来看，任何采用公共云或混合云解决方案的企业都应该制定有效的数据分类政策和恰当的处理流程，这一点至关重要。

数据分类政策应该明确界定敏感数据以及严禁脱离企业直接控制的数据类型。数据分类政策应在企业内部进行传达，确保全体员工充分了解制定分类政策的目的，树立数据所有权意识，并熟知不同类型企业数据的敏感性。

**可用于数据分类的措施包括：**

•针对不同类型的数据，界定法律、监管、知识产权以及信息安全等要求。

•确定各类数据的敏感度，可分为可对外公开、受限以及高度敏感。

•制定数据传输规定，如加密要求。

•明确数据责任人——该责任人（如业务经理和合规专员）应充分了解数据的性质，并有权决定数据访问权限以及访问权限的类型。

### 风险——透明度和放弃直接控制

### 风险响应措施——管理层监管和营运监督控制

在非外包的情况下，管理层能够根据企业的内部控制环境开展直接的控制活动。而在公共云或混合云的模式下，管理层将部分或全部直接控制职能移交给了云服务提供商。在绝大多数情况下，云服务提供商只能从宏观的角度出发，专注于提供稳定和安全的云服

务平台，以满足客户普遍的控制要求，却无法满足每个云服务消费者的特殊需求。因此，管理层有责任对云服务解决方案进行全方位地评估并实施额外控制，以便云服务解决方案能够满足企业所有的控制要求。

管理层应对让渡给云服务提供商的控制职能有着深入细致的理解，这是因为理解程度的不同将直接影响管理层实施具体的监管控制措施。对上市公司而言，如果让渡的控制职能会影响管理层对于财务报表的认定，那么，管理层就必须施行预防性控制措施。采用云计算，让渡部分监管职能并不意味着管理层从此就能高枕无忧了。

采用公共云或混合云模式的企业应该对云服务提供商的控制活动进行验证，并确保服务提供商的控制活动与管理层的风险偏好保持一致。此外，企业还应该定期核查云服务提供商控制活动的有效性。依据所选的云服务交付模式，企业还应明确自己和云服务提供商各自在控制实施、技术运行以及用户访问管理等方面的控制责任。

### 风险——可靠性、执行情况以及高价值的网络攻击目标

### 风险响应措施——事件管理

企业需要对云服务提供商的事件响应能力进行评估，以确保其对系统瘫痪和数据失窃等自身突发事件以及其他突发事件具备快速的响应能力。

如果云服务提供商的系统瘫痪或安全存在漏洞，很可能会对广大的云客户造成影响。上述事件一旦发生，云服务提供商首先会专注于在自身云环境中如何解决这些问题，不太可能向每个云租户阐述所发生的问题，这样造成的后果就是企业因服务商没有发出警示而未能启动事件响应计划。换而言之，除非企业愿意承受负面事件造成的最坏后果，否则企业的突发事件响应机制不能完全依赖云服务提供商。

如果云解决方案发生了系统性故障或遭受网络攻击，**以下内容有助于识别固有风险并采取相应的应对措施**：

**系统性故障**——系统性故障是一种可发生于任何计算环境的风险事件。一旦发生灾难性的系统故障，大量云租户会同时发出技术支持请求，而优先级别较低的企业可能无法从云服务提供商处获得所需的响应服务。

**能够减缓系统性故障风险的控制措施：**

•在主要云服务提供商之外，与提供相同云解决方案的其他服务商签订合同，保留企业数据备份，以便发生意外之后企业能够将数据迅速地部署到后备云服务提供商的服务器上。

•对系统可用状态进行监控。

•应用自动化工具软件，它能够从其他云服务提供商获取云解决方案所需的资源。

•对服务级别协议进行检查，确保在系统发生故障时，云服务提供商能够提供足够的响应。

**网络攻击**——任何企业的系统都存在网络攻击这一固有风险。对黑客来说，多个大型企业共存于一个云服务架构，成为一个更具诱惑力、更为知名的攻击目标。如果一家不出名的小型企业与著名企业共享云架构或接受同一个云服务提供商的服务，那么，该小企业成为网络攻击目标的可能性将逐步上升，最终与知名企业或云服务提供商面临同等的风险水平。

**减缓网络攻击风险的控制措施：**

•在第三方云服务平台上只存放不重要和不敏感的数据。

•对存放在第三方云服务平台上的数据进行加密。

•制定故障切换策略（fail-over strategy），在企业遭受攻击时能够转而采用其他云服务提供商提供的解决方案或依靠内部解决方案。

此外，还存在另外一种突发事件响应办法，虽然这种情形不太常见，即在发生不利突发事件的时候，采用公共云模式的企业将其运营情况对外曝光，引发公众或新闻媒体的关注。例如，某家知名的云服务提供商（如亚马逊或谷歌）因网络攻击而中断服务或产生安全漏洞，该事件将会立刻引起公众的广泛关注。云服务提供商也许无法立刻告知外界具体情况，如受到影响的云服务消费机构、造成问题的原因、系统修复的预计时间以及事件的影响等。而相关企业，即便营运活动没有受到这个不利事件的影响，但因为签约的云服务提供商发生事故，它们的声誉不可避免地会受到损害。

### 风险——未能遵守监管规定

### 风险响应措施——对外部环境进行监控

管理层需要对外部环境进行监控，以辨识那些会对自身以及云服务提供商营运活动造成影响的变化。监管规定的修改或电信营运商的变动会对云计算的使用方式造成重大的影响。

数据隐私权方面的重大监管变化是可以预计到的。许多国家都采取了保护措施，严禁将公民的个人身份信息向境外传递以及存储在其他国家。相应的，云解决方案不能将某些数据任意存放，只能储存在特定的国家。

### 风险——锁定云服务提供商

### 风险响应措施——制定退出机制

一个企业使用某个云服务提供商的云服务越多或者使用云解决方案的时间越长，就会越依赖该服务商。但是，没有什么事情是亘古不变的，管理层需要未雨绸缪，对未来更换云服务提供商或放弃现有云解决方案的可能性进行预判。因此，管理层应将退出机制或应变计划纳入云计算的总体战略中。

### 风险——未能遵守披露规定

### 风险响应措施——在财务报告中增加披露内容

如果上市公司的重要业务流程依托于云服务提供商，那么，该公司就必须对外披露这方面的情况。上市公司应具备披露意识，遵守监管规定，履行信息公开义务，主动对外公布云解决方案对业务营运的潜在影响以及其他风险因素。

# 7. 董事会对云计算的监管、管理决策及其他注意事项

## 董事会对云计算的监管

鉴于云计算所带来的机会以及风险影响的潜在重要性，企业董事会应该对施行云计算的合理性进行讨论和调查，一旦实施将其纳入企业的整体治理活动中。

在履行监管职责时，董事会应认真考虑以下问题：

•在采用云计算的过程中，管理层应进行何种程度的考量？目前，管理层的工作进展到哪个阶段？

•在管理层中，谁对理解并管理与云计算相关的业务风险负有责任？

•竞争对手采取了什么样的云解决方案？

•管理层是否制定了有效的程序以监管云计算的采纳和使用情况？

•云计算会对管理层的内部控制整体结构造成怎样的影响（提升、无影响还是削弱）？

•云计算是否符合企业的风险偏好？

•在初洽以及合同签订阶段，尽职调查程序是否对云计算服务提供商进行了详尽的了解？哪一个阶段应该启动监管程序？

•管理层是否对第三方云服务提供商的服务设置了适当的最低服务水平预期？

•管理层如何减缓因依赖于第三方云服务提供商而产生的组织性风险？

•企业如果采用了云解决方案，是否对云计算风险进行了识别并将情况告知了投资者？

## 云计算的管理决策

在做出是否采用云计算的决策之前，管理层需要对企业的内部环境（包括业务营运情况、流程标准化、IT成本以及未完成的IT项目）和外部环境（包括法律法规、监管规定以及竞争对手的云计算实施情况）进行评估。

管理层在考虑云计算战略时，应重点关注以下问题：

•管理层对外包业务怎么看？

•企业是否预见业务快速增长会对云解决方案产生应用需求？

•企业是否身处成熟市场？是否需要采用云计算解决方案以节约成本、保持竞争力？

•企业的营运功能和业务流程是否已经足够成熟和正规化？是否足以应对基础技术平台的变化？

•企业目前的IT技术能力和成熟度如何？

•采用云计算，企业应做哪些准备工作？

•评估小组应该由哪些人组成？由谁来做出决策？

•处于云计算的商业环境中，企业如何对风险进行有效管理？

在进行云计算解决方案相关决策时，管理层应对各种变量进行充分考量，包括商业流程、特定部署模式、特定服务交付模式以及特定云服务提供商。

需要特别说明的是，因为云服务提供商提供的是商品化的解决方案，双方签订的是格式化合同，所以，对于服务级别协议，企业只能选择接受或者放弃，无法根据自己的意愿

增减条款。

与其他商业决策一样，在实施云解决方案之前，企业需要采取谨慎性措施，如进行投资回报分析、企业全成本分析、对潜在服务商进行尽职调查以及启动试点程序。

## 其他注意事项

在做出云计算决策时，企业需要对下列额外事项以及其他不甚明显方面进行认真考量，因为它们会增加风险或产生新的风险：

**•云解决方案定价的预测性**——许多云服务提供商都采用现买现付（pay-as-you-go）的定价模式，这似乎让云服务的成本计算显得十分简单。但是，由于云计算是新兴事物，缺乏历史价格数据及趋势，企业无法以此为基础预测今后几年的投资回报率。例如，管理层是否能够对云计算解决方案的价格变化做出预测？云服务的现有价格水平能够保持多长时间？价格增长幅度是否能在合同中予以明确？

**•受制于服务商**——如果企业与某一家云服务提供商缔结的合作伙伴关系时间越长，那么，企业在系统处理和数据存储方面（而且这两方面的需求还会不断增长）对该服务商的依赖性就越强。随着时间的推移，更换云服务提供商或重新自行管理的成本将会越来越高。在某些情况下，比如企业解散内部技术部门，云服务提供商就会认为该企业别无他法，只能依靠自己提供的服务来支撑业务处理流程，如此以来，服务提供商每年加价的可能性就会增大。

**•其他员工的参与**——由于云计算对企业的许多方面都会产生潜在影响（如技术、监管遵从、IT员工以及业务营运），所以，在做出是否采用云计算的决策时，来自法律、内部审计、IT以及业务流程等部门的员工均应参与其中。

**•明确界定企业和云服务提供商各自的责任以及必要的互动**——作为ERM计划的一部分，管理层必须对因与服务商签约而产生的潜在控制问题、法律问题、业务营运问题以及IT问题有着清醒的认识。**通过回答下列问题，企业可以明确企业和云服务提供商各自的角色和职责**（相关信息请参阅“附录：云计算的治理——角色与职责”）：

>在企业或云服务提供商中，谁对云解决方案的法律法规遵从事宜负责？

>在企业中，应由谁来负责管理与云服务提供商的关系，并监督云服务提供商对服务级别协议的遵守情况？

>在企业中，由谁负责与云服务提供商签订合同？

>在企业或云服务提供商中，由谁负责设计、管理以及最终审批与云计算解决方案相关的安全、变更管理以及访问权限等控制措施？

>企业是数据的最终所有者，而数据却是存放在云端的，企业中应由谁负责对置于云服务提供商控制之下的用户和数据进行管理？

>云解决方案能为用户提供怎样的服务？

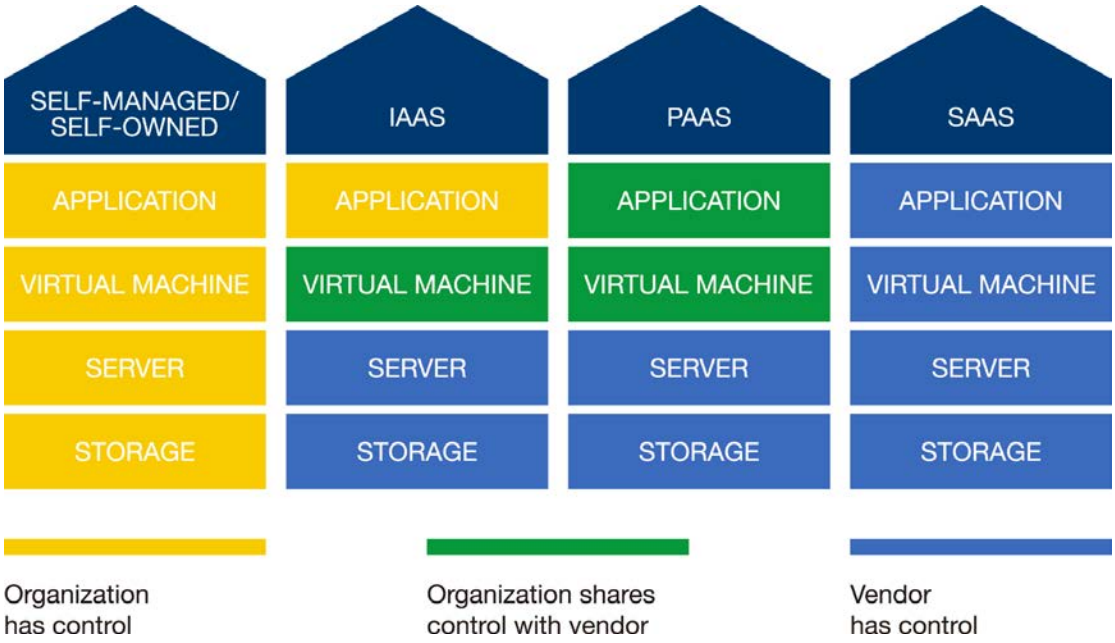
>用户可否通过内部IT部门或是可以直接将问题和要求提交给云服务提供商？

**•对云服务提供商的业务持续能力进行评估**——企业应该对灾难事件发生后，云服务提供商恢复营运的能力进行评估,并在合同中明确约定如果发生此类事件，云服务提供商应承担的义务和经济赔偿责任。

**•特定技术领域直接控制权的让渡**——依据所选用的云服务交付模式的不同，企业对技术架构保有的控制程度也会相应发生变化。图例7.1比较了在设备自有和自我管理情况下以及各种云服务交付模式下，企业对具体

技术组件（如应用系统、虚拟机环境、服务器和存储设施）保留的控制程度。

图例7.1 各类云服务交付模式下，企业保留的控制水平




**•最终法律责任和义务**——如采用公共云或混合云的解决方案，管理层实际上是将部分任务分配给第三方服务商来执行，但并未转移相应的责任和义务，管理层对影响数据和交易进程的风险和控制措施仍负有责任。具体来说，在公共云或混合云的部署模式下，企业只是将架构、软件解决方案以及营运支持部分外包，在绝大多数情况下，让渡给第三方服务商的责任和义务非常有限。

## 关于数据管辖权的司法歧义

由于企业所在地、云架构所在地以及数据存放地可能并不在同一地点，企业也许会受到多重司法管辖。就在本文刊发之际，在“云计算模式该如何遵守国际法并满足监管要求”这一问题上仍未有明确的答案。此外，《1996年版健康保险隐私及责任法案》（HIPAA）、国家性和地区性数据保护法规、法律执行的司法管辖权以及其他监管机构对这一问题有不同的规定和表述，使得公共云和混合云的商业应用变得更加复杂。

作为云计算治理和ERM程序的一部分，企业一旦采用云计算解决方案来处理部分或全部业务流程，管理层应向法律顾问寻求帮助，明确与遵守相关法律有关的风险和挑战。在采用云计算时，**企业应重点考虑下列法律事项：**

>采用云计算解决方案后，企业的数据将存储在哪个国家？

>数据和系统受哪国法律管辖？是否存在多重管辖的情况？

>如果云服务提供商将数据存储在企业和企业客户所在国以外的其他国家，一旦外国法院调阅企业或客户的数据，企业将会涉及怎样的法律事务？将拥有哪些法律权利？

>如果法律机构调阅云服务提供商或其他云租户的数据，企业的数据是否能够独善其身，不受牵连？

>正在进行的商业活动应遵守哪些税收管辖？

>如果某家执法机构在法律权限内扣押了云服务提供商的服务器，而该服务器上存储的企业客户数据受其他司法权管辖，一旦企业将客户的记录存放在公共云或混合云上，它是否会因此而侵犯了客户的法定权利（并违反了相关数据保护法规）？

## 8. 结束语

如互联网在20世纪最后10年的表现一样，云计算为企业变革带来了诸多可能。毫无疑问，云计算将在技术演进史中留下极其重要的印记。

云计算的采用与认同与过去10年间其他趋势（如社交网络站点和虚拟零售）的推广与接纳是相吻合的。在社交网站和虚拟零售中，参与其中的人或物虽无法相见却又备受信赖，沟通交流、店铺信息以及交易流程较以往更为便捷。数十年以前，大型计算机尚未得到大规模的应用。在那个时期，如果企业拥有严密的物理安全措施、规模庞大的数据中心以及大量在用设备，同时企业所有的信息资产都存放在触手可及且防范严密的设备中，那么，该企业的高管就会倍感自豪，并觉得十分放心。而今天，云计算技术的出现使得新一代高管能够获得代价低廉的技术替代方案，无需新添设备（在大多数情况下），也无需知道企业信息资产的确切存放地点。

云计算某些特性成为ERM程序需要应对的新挑战。采纳云计算的便捷性会掩盖风险发生之后管理云计算的复杂性，从而容易让人产生一种误解，认为云计算能够帮助企业避免负面事件（如犯罪活动、人为差错以及意外事件和破坏）的发生，然而事实上任何类型的企业都无法避免这类事件。一个有效的云监管程序在很大程度上取决于企业对风险以及风险削弱或风险接受策略的深入理解。通过利用COSO的ERM框架，管理层能够有效地、连贯一致地识别与云计算机会和决策相关的特定风险，并采取针对性的风险响应措施。

企业没有开展尽职调查，没有部署相应控制就施行云计算解决方案，原因在于企业未对可能存在的问题进行预先研判。通过应用COSO的ERM框架，采取预防性控制措施，企业使用云计算能够获得大量收益，有些收益是截至目前尚未听说或发现的。如果对云计算有关的风险和其它问题有着清晰的认识，管理层就能够在动态和演变的环境中对风险进行管理，就更有可能实现企业目标。

# 附录：云计算的治理——角色与职责

ERM程序要实现对云活动的监管，就需要管理层承担额外的责任。下文阐述了与云计算相关的职责分配：

## 董事会

•关注云计算的发展趋势，了解高管的观点，理清云计算可能对行业及本企业商业模式产生的影响

•了解并洞悉具有变革力的IT项目，如云计算服务

•理解管理层应如何平衡云计算的风险和收益，并将其纳入企业的业务和技术战略

•利用内部审计资源，确保云变革符合企业的风险偏好和控制理念

## 首席执行官

•明确企业对外包业务的观点和政策

•了解云计算对企业所在行业的影响

•知道企业在哪个业务环节以及以何种方式使用云计算

## 首席财务官

•在财务报告中对云计算的使用情况进行披露

•对花费在云计算上的全部成本以及由此产生的投资收益进行评估和监控

•比较云计算和其他替代方案的税收及会计收益

•制定云服务采买政策并进行监控

•对第三方云服务提供商的财务状况进行跟踪

## 首席法务官

•确保企业的云活动遵守相关法律法规

•关注会对企业云解决方案或云服务提供商产生影响的、新颁发的法律法规，并制定应对措施

•复核并审批云服务采买政策

•为数据分类政策和处理流程提供意见

•复核与云服务提供商签订的合同，确保企业的利益和权益得到保护

•当云服务是由别国的服务商提供时，了解与企业营运有关的法律管辖权问题

## 首席信息官

•了解云计算对于现有业务策略以及新商机的潜在影响并进行监控

•为利用以及调整云计算解决方案制定总体策略

•推进云计算解决方案与企业的融合，并嵌入现有的IT架构中

•协助将云治理嵌入到企业的ERM程序中

•与数据所有者一同对数据进行分类

•制定信息资源供应、用户访问管理以及变更管理的云处理流程

•制定企业的云计算突发事件管理程序

•监督并确保云服务提供商执行双方签订的服务级别协议

•监控云服务提供商和其他云租户的活动

## 首席审计官或内审人员

•在混合控制环境中，企业需要与云服务提供商分担控制和流程。因此，有必要开展定期审计，对混合控制环境的设计和有效性进行评估

•对云服务提供商进行审计，或查阅提供商的《服务型组织控制报告》，核实云服务提供商控制措施的有效性

•定期对企业存储在外部云端的数据开展合规性审计，确保其符合企业的数据分类政策

•对云服务提供商的合同执行情况进行审计，核实相关费用

•对云治理情况进行评估